Galileo Computing

Windows Server 2012 R2

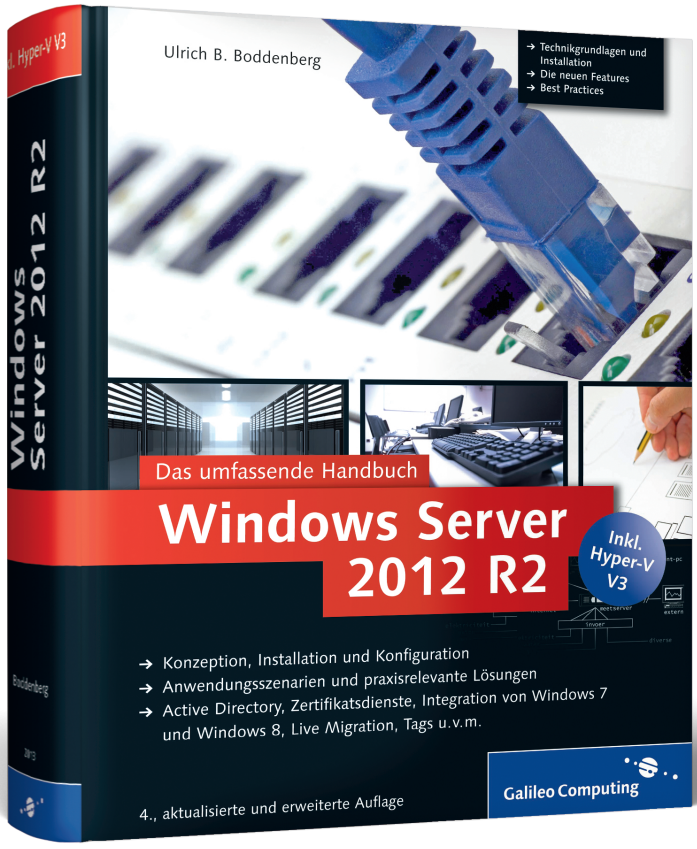
Das umfassende Handbuch. Inkl. Hyper-V

Bearbeitet von
Ulrich B. Boddenberg

überarbeitet 2013. Buch. ca. 1392 S. Hardcover
ISBN 978 3 8362 2013 2
Format (B x L): 19 x 24 cm

Ulrich B. Boddenberg

Windows Server 2012 R2



Galileo Press

Auf einen Blick

1 Warum eine neue Server-Version? 23

2 Editionen und Lizenzen 51

3 Hardware und Dimensionierung 55

4 Protokolle 131

5 Was ist .NET? 185

6 Installation 201

7 Die Core-Installationsoption 209

8 Active Directory-Domänendienste 221

9 Netzwerkdienste im AD-Umfeld 455

10 Active Directory Lightweight Directory Services (AD LDS) 495

11 Active Directory-Verbunddienste (Federation Services) 519

12 Active Directory-Zertifikatdienste 525

13 Active Directory-Rechteverwaltungsdienste (AD RMS) 641

14 »Innere Sicherheit« 675

15 Dateisystem und Dateidienste 787

16 Drucken 885

17 Webserver (IIS) 909

18 SharePoint Foundation und SharePoint Server 1045

19 Remotedesktopdienste (Terminaldienste) 1057

20 Hochverfügbarkeit 1135

21 Datensicherung 1223

22 Servervirtualisierung mit Hyper-V 1237

23 Windows PowerShell 1361

Inhalt

Geleitwort 21

1 Warum eine neue Server-Version? 23

1.1 Rückblick 23
1.1.1 Windows 1, 2 und 3 23
1.1.2 Windows NT 3.1 Advanced Server 25
1.1.3 Windows NT Server 3.5 und 3.51 27
1.1.4 Windows NT 4 Server 29
1.1.5 Windows 2000 Server und Windows Server 2003 31
1.2 Windows Server 2008 und Windows Server 2008 R2 33
1.3 Windows Server 2012 36
1.3.1 Windows Server 2012 R2 40
1.4 Aufgaben und Rollen 43
1.4.1 Rollen 45
1.4.2 Features 46
1.4.3 Zusammenspiel mit anderen Microsoft-Produkten 48

2 Editionen und Lizenzen 51

2.1 Editionen 51
2.2 Lizenzierung 52

3 Hardware und Dimensionierung 55

3.1 Serverhardware 55
3.1.1 Prozessoren 55
3.1.2 Serverarchitektur 58
3.1.3 Hauptspeicher 59
3.1.4 Festplatten 60
3.1.5 Netzwerkkonnektivität 63
3.1.6 Überwachung 64

3.2 Storage-Architekturen ... 65
3.2.1 SAN, NAS, iSCSI ... 65
3.2.2 SAN-Architektur ... 69
3.2.3 Premium Features von Storage-Systemen ... 75
3.2.4 Virtualisierung ... 80

3.3 Netzwerk ... 83
3.3.1 Netzwerkstrukturen und Verfügbarkeit ... 83
3.3.2 Anbindung von entfernten Nutzern ... 87
3.3.3 Netzwerkmanagement ... 90

3.4 Das Rechenzentrum ... 91
3.4.1 Zugangskontrolle ... 91
3.4.2 Feuer, Wasser 92
3.4.3 Räumliche Anforderungen ... 93
3.4.4 Stromversorgung ... 94
3.4.5 Redundante Rechenzentren ... 96

3.5 Mein Freund, der Systemmonitor ... 97
3.5.1 Leistungsindikatoren, Objekte und Instanzen ... 99
3.5.2 Protokoll erstellen ... 104
3.5.3 Protokoll untersuchen ... 108
3.5.4 Leistungsmessung über Computergrenzen hinweg ... 112

3.6 Dimensionierung und Performance ... 113
3.6.1 Festplatte & Co. ... 113
3.6.2 Hauptspeicher ... 128
3.6.3 Prozessor ... 128
3.6.4 Netzwerkkonnektivität ... 129

4 Protokolle 131

4.1 Mein Freund, der Netzwerkmonitor ... 132
4.1.1 Kurzüberblick ... 133
4.1.2 Messen und Auswerten – ein Schnelleinstieg ... 136

4.2 IPv4 vs. IPv6 ... 143
4.2.1 Unterschiede ... 145
4.2.2 IPv6 – die Adressierung ... 146
4.2.3 Vergabe von IPv6-Adressen ... 152
4.2.4 Abschalten von IPv6 ... 154

4.3 Einige grundlegende Netzwerkprotokolle ... 155
4.3.1 DHCP – Dynamic Host Configuration Protocol ... 155
4.3.2 ARP – Address Resolution Protocol ... 159
4.3.3 DNS – Domain Name System ... 162
4.4 Authentifizierung und Kerberos ... 166
4.4.1 Authentifizierung vs. Autorisierung ... 166
4.4.2 Kerberos – Funktionsweise ... 168
4.4.3 Delegierung ... 173
4.4.4 Der Service Principal Name (SPN) ... 173
4.4.5 Kerberos-Delegierung verwenden ... 176
4.4.6 Shoot the Trouble ... 178
4.4.7 Kernelmodus-Authentifizierung im IIS 7 ... 182

5 Was ist .NET? 185

5.1 Der Grundgedanke ... 187
5.2 .NET bei der Arbeit ... 188
5.3 .NET Framework und Compact Framework ... 190
5.4 Code Access Security ... 193
5.5 Von Codegruppen und Berechtigungssätzen ... 195
5.6 WPF, WCF, WWF und CardSpace ... 197
5.7 .NET Framework 3.5 installieren ... 198

6 Installation 201

6.1 Grundinstallation ... 201
6.2 Aktivieren ... 206

7 Die Core-Installationsoption 209

7.1 Verwaltung, Basis ... 211
7.1.1 Verwendung von »sconfig.cmd« ... 211
7.1.2 PowerShell nutzen ... 212

7.1.3 Server-Manager verwenden ... 214
7.1.4 MMC-Snap-Ins verwenden ... 216

7.2 Weitere Rollen hinzufügen ... 217
7.2.1 Server-Manager verwenden ... 218
7.2.2 PowerShell verwenden ... 218

7.3 Umwandeln ... 219

8 Active Directory-Domänendienste 221

8.1 Aufbau und Struktur ... 222
8.1.1 Logische Struktur ... 222
8.1.2 Schema ... 232
8.1.3 Der globale Katalog (Global Catalog, GC) ... 236
8.1.4 Betriebsmasterrollen/FSMO-Rollen ... 239
8.1.5 Verteilung von Betriebsmasterrollen und Global Catalog ... 249
8.1.6 Schreibgeschützte Domänencontroller – Read Only Domain Controller (RODC) ... 252

8.2 Planung und Design des Active Directory ... 256
8.2.1 Abbildung des Unternehmens ... 256
8.2.2 Übersichtlichkeit und Verwaltbarkeit ... 259
8.2.3 Standorte ... 262
8.2.4 Replikation ... 268
8.2.5 Gruppenrichtlinien ... 299

8.3 Ein neues Active Directory einrichten ... 299
8.3.1 Den ersten Domänencontroller einrichten ... 300
8.3.2 Zusätzliche Domänencontroller einrichten ... 308

8.4 Gruppenrichtlinien ... 309
8.4.1 Anwendungsbeispiel ... 310
8.4.2 Richtlinien für Computer und Benutzer ... 313
8.4.3 Verteilung über Domänencontroller ... 315
8.4.4 Vererbung ... 320
8.4.5 Sicherheit und Vorrang ... 323
8.4.6 Filter ... 326
8.4.7 Abarbeitungsreihenfolge, mehr Details ... 326
8.4.8 Lokale GPOs (ab Windows Vista und Windows Server 2008) ... 327
8.4.9 Starter-Gruppenrichtlinienobjekte / Starter-GPOs ... 331
8.4.10 ADM vs. ADMX ... 336
8.4.11 Zuweisen und Bearbeiten von Gruppenrichtlinien ... 349

8.4.12 WMI-Filter ... 365
8.4.13 Softwareverteilung mit Gruppenrichtlinien ... 369
8.4.14 Loopbackverarbeitung ... 372
8.4.15 Gruppenrichtlinien-Voreinstellungen (Preferences) ... 373

8.5 Diverses über Gruppen ... 378

8.6 Delegierung der Verwaltung ... 381

8.7 Das Active Directory aus der Client-Perspektive ... 383
8.7.1 DNS-Einträge oder »Wie findet der Client das Active Directory?« ... 383
8.7.2 Das Active Directory durchsuchen ... 384
8.7.3 Individuelle Erweiterungen ... 386

8.8 Zeitdienst ... 387
8.8.1 Grundkonfiguration der Zeitsynchronisation ... 388
8.8.2 Größere Umgebungen ... 390

8.9 Upgrade der Gesamtstruktur auf Active Directory-Domänendienste (AD DS) 2008/2012/R2 ... 392
8.9.1 Schemaerweiterung und Anpassung der Domänen durchführen ... 392
8.9.2 Windows Server 2012 R2-Domänencontroller installieren ... 398
8.9.3 Kurze Überprüfung ... 404
8.9.4 FSMO-Rollen verschieben ... 407
8.9.5 Alte Domänencontroller deinstallieren und einheitlichen Modus wählen ... 410
8.9.6 Real-World-Troubleshooting – ein Beispiel ... 412

8.10 Umstrukturieren ... 418

8.11 Werkzeugkiste ... 420

8.12 Active Directory Best Practice Analyzer ... 421

8.13 Der Active Directory-Papierkorb ... 424
8.13.1 Voraussetzungen ... 424
8.13.2 Active Directory-Papierkorb aktivieren ... 424
8.13.3 Gelöschte Objekte anzeigen und wiederherstellen ... 426
8.13.4 Wiederherstellen mit der PowerShell ... 431

8.14 Active Directory-Verwaltungscenter ... 432
8.14.1 Kennwort zurücksetzen ... 434
8.14.2 Benutzer suchen und Attribute anzeigen und modifizieren ... 435
8.14.3 Navigieren und filtern ... 437
8.14.4 Neuanlegen von Objekten ... 440
8.14.5 Navigationsknoten und mehrere Domänen ... 441
8.14.6 Technik im Hintergrund und Voraussetzungen ... 443

8.15 Active Directory-Webdienste (Active Directory Web Services, ADWS) ... 443

8.16 Active Directory-Modul für Windows-PowerShell ... 446
8.17 Offline-Domänenbeitritt ... 453

9 Netzwerkdienste im AD-Umfeld 455

9.1 DNS ... 455
9.1.1 Zonen ... 456
9.1.2 Server ... 462
9.1.3 Weiterleitungen und Delegierungen ... 464
9.1.4 Einen DNS-Server für das AD hinzufügen ... 468
9.1.5 Manuell Einträge hinzufügen ... 468
9.1.6 Reverse-Lookupzone einrichten ... 469
9.1.7 Wie findet der Client einen Domänencontroller? ... 471
9.2 DHCP ... 472
9.2.1 Einen neuen DHCP-Server einrichten ... 473
9.2.2 Konfiguration und Betrieb ... 475
9.2.3 Redundanz ... 484
9.3 WINS ... 491
9.4 NetBIOS über TCP/IP ... 492

10 Active Directory Lightweight Directory Services (AD LDS) 495

10.1 Installation ... 498
10.2 Einrichten einer Instanz ... 499
10.3 Administration ... 505
10.4 Replikation einrichten ... 514

11 Active Directory-Verbunddienste (Federation Services) 519

11.1 Ein Anwendungsszenario ... 519
11.2 Installation ... 520
11.3 Die Kernidee ... 522

12 Active Directory-Zertifikatdienste 525

12.1 Einige Anwendungsszenarien ... 525
12.1.1 Internet-Authentifizierung und Verschlüsselung ... 525
12.1.2 Sichere E-Mail ... 528
12.1.3 Codesignatur ... 530
12.1.4 IP-Verschlüsselung ... 532
12.1.5 Anmeldung mit Smartcard ... 532
12.1.6 Wireless Authentification (802.1X) ... 534
12.1.7 Fazit ... 534

12.2 Zertifikatdienste installieren und Migration (einstufige Architektur) ... 534

12.3 Zertifikate aus Sicht des Clients ... 545

12.4 Zertifizierungspfad ... 550

12.5 Zertifikatvorlagen ... 551

12.6 Weboberfläche ... 560

12.7 Mehrstufige Architekturen ... 562
12.7.1 Rollen ... 563
12.7.2 Architekturen ... 565

12.8 Autoenrollment und automatische Zertifikatanforderung ... 567
12.8.1 Automatische Zertifikatanforderung ... 567
12.8.2 Autoenrollment ... 569

12.9 Zertifikate für Websites ... 573

12.10 Zertifikatsperrlisten ... 574
12.10.1 Funktionsweise – ganz grob ... 576
12.10.2 Sperrlisteneinträge ... 579
12.10.3 Gültigkeit einer Sperrliste ... 582
12.10.4 Zertifikatgültigkeit überprüfen ... 582
12.10.5 Der Cache ... 588
12.10.6 ISA Server zum Veröffentlichen des Speicherortes verwenden ... 589

12.11 Das Online Certificate Status Protocol (OCSP) ... 593
12.11.1 Konfiguration des Online-Responders ... 593
12.11.2 Anpassung der Zertifizierungsstelle ... 600
12.11.3 Testen ... 600
12.11.4 ISA Server-Veröffentlichung ... 601

12.12 Zweistufige Architektur implementieren ... 602
12.12.1 Offline-CA installieren und konfigurieren ... 603
12.12.2 Zertifikat und Sperrliste dem Unternehmenszertifikatserver und dem Active Directory hinzufügen ... 618

12.12.3 Unternehmens-CA installieren ... 621
12.12.4 Sperrlisten-Verteilungspunkt mit ISA Server veröffentlichen ... 634

12.13 Zertifikate und Windows Mobile ... 634
12.13.1 Pocket PC und Pocket PC Phone Edition ... 635
12.13.2 Smartphone ... 636

12.14 Zertifikate und das iPhone ... 638

13 Active Directory-Rechteverwaltungsdienste (AD RMS) 641

13.1 Funktionsweise ... 643

13.2 Installation ... 645
13.2.1 Server-Installation ... 645
13.2.2 Feinkonfiguration ... 654
13.2.3 Vorlage für Benutzerrichtlinien erstellen ... 655
13.2.4 Gruppenrichtlinien ... 660
13.2.5 Client-Installation ... 660

13.3 Anwendung ... 662
13.3.1 Word-Dokument schützen ... 662
13.3.2 E-Mail schützen ... 669

13.4 Statistik ... 672

13.5 Abschlussbemerkung ... 674

14 »Innere Sicherheit« 675

14.1 Netzwerkrichtlinien- und Zugriffsdienste ... 676
14.1.1 Wie funktioniert NAP? ... 677
14.1.2 Netzwerkrichtlinienserver ... 681
14.1.3 Client vorbereiten ... 683
14.1.4 Mehrstufiges NAP-Konzept vorbereiten ... 685
14.1.5 NAP für DHCP-Zugriff ... 690
14.1.6 Und die anderen Netzwerkverbindungsmethoden? ... 712

14.2 Windows-Firewall ... 713
14.2.1 Eingehende und ausgehende Regeln ... 715
14.2.2 Basiskonfiguration ... 716
14.2.3 Regeln im Detail ... 718
14.2.4 Verbindungssicherheitsregeln ... 721

14.3 Windows Server Update Services (WSUS) ... 729
14.3.1 Die Funktionsweise ... 729
14.3.2 Erstkonfiguration mit dem Assistenten ... 736
14.3.3 Konfiguration und Betrieb ... 741
14.3.4 Updates genehmigen ... 746
14.3.5 Gruppenrichtlinie konfigurieren ... 750
14.3.6 Kurzer Blick auf den WSUS-Client ... 751
14.3.7 Mit Berichten arbeiten ... 754

14.4 VPNs mit Windows Server 2012 R2 ... 756
14.4.1 Gateway-Architektur ... 757
14.4.2 Grundkonfiguration des VPN-Servers ... 759
14.4.3 VPN einrichten (allgemein) ... 764
14.4.4 Einwahlberechtigung ... 768
14.4.5 PPTP-VPN ... 769
14.4.6 L2TP-VPN ... 771
14.4.7 SSTP ... 774
14.4.8 Automatischer Modus ... 780
14.4.9 Connection Manager Administration Kit (CMAK, Verbindungs-Manager-Verwaltungskit) ... 781

15 Dateisystem und Dateidienste 787

15.1 Allgemeines zum Dateisystem ... 787
15.1.1 Aufbau ... 788
15.1.2 Platten verwalten ... 789
15.1.3 MBR vs. GPT ... 791
15.1.4 Partitionieren ... 793
15.1.5 Basis-Datenträger vs. dynamische Datenträger ... 797
15.1.6 Spiegeln ... 799
15.1.7 Volumes vergrößern und verkleinern ... 802
15.1.8 Weitere Optionen ... 807
15.1.9 Schattenkopien – Volume Shadow Copy Service ... 809
15.1.10 Transactional NTFS und Self-Healing NTFS ... 812

15.2 Installation der Rolle »Dateiserver« ... 813

15.3 Ressourcen-Manager für Dateiserver (RMDS) ... 814
15.3.1 Kontingentverwaltung ... 814
15.3.2 Dateiprüfungsverwaltung (File Screening Management) ... 821
15.3.3 Speicherberichteverwaltung ... 824

15.4 Verteiltes Dateisystem – Distributed File System (DFS) ... 828
15.4.1 Grundfunktion ... 828
15.4.2 DFS und DFS-Replikation ... 830
15.4.3 Ausfallsicherheit ... 831
15.4.4 Verteilen von Daten – standortübergreifendes DFS ... 832
15.4.5 Sicherung von Daten ... 834
15.4.6 DFS installieren ... 835
15.4.7 Basiskonfiguration ... 836
15.4.8 Konfiguration der Replikation ... 845
15.4.9 Redundanz des Namespaceservers ... 850

15.5 Encrypting File System (EFS) ... 851
15.5.1 Konfiguration und Anwendung ... 852
15.5.2 Zugriff für mehrere Benutzer ... 855
15.5.3 Datenwiederherstellungs-Agenten ... 858
15.5.4 EFS per Gruppenrichtlinie steuern ... 863
15.5.5 Cipher ... 864

15.6 ReFS und Speicherpools ... 865

15.7 iSCSI-Zielserver (iSCSI-Taget) ... 870
15.7.1 Einrichten eines iSCSI-Targets ... 870
15.7.2 Ein iSCSI-Target verwenden ... 876

15.8 Datendeduplizierung ... 880

16 Drucken 885

16.1 Einige Begriffe und Definitionen ... 886
16.1.1 Druckerserver, Drucker und Druckerobjekte ... 886
16.1.2 XPS ... 889

16.2 Installation ... 891

16.3 Arbeiten mit der Druckverwaltung ... 893
16.3.1 Drucker installieren ... 894
16.3.2 Zusätzliche Treiber installieren ... 896
16.3.3 Anschlüsse konfigurieren ... 898
16.3.4 Druckerserver konfigurieren ... 899
16.3.5 Eigenschaften und Druckerstandards ... 899
16.3.6 Import und Export der Konfiguration ... 901
16.3.7 Arbeiten mit Filtern (Überwachen) ... 901

16.4 Drucker bereitstellen ... 903

17 Webserver (IIS) 909

17.1 Begriffsdefinitionen ... 911
17.1.1 Webapplikation vs. Webservice ... 911
17.1.2 Website vs. Webseite ... 914

17.2 ASP.NET ... 915
17.2.1 Die Entwicklungsumgebung ... 915
17.2.2 Clientseitig: JavaScript ... 918
17.2.3 Die web.config-Datei ... 919
17.2.4 Kompilierung und Vorkompilierung ... 922
17.2.5 Sicherheit und ASP.NET ... 927

17.3 Installation ... 928

17.4 Kurzer Überblick über die Architektur des Webservers ... 930
17.4.1 Architektur ... 930
17.4.2 Anforderungsverarbeitung ... 931
17.4.3 Anforderungsverarbeitung im Anwendungspool ... 933
17.4.4 Die »Modulbauweise« ... 938

17.5 Webserver, Websites, Anwendungen, virtuelle Verzeichnisse und Anwendungspools ... 943
17.5.1 Die Zusammenhänge ... 943
17.5.2 Webserver ... 946
17.5.3 Anwendungspool ... 947
17.5.4 Website ... 949
17.5.5 Anwendungen ... 954
17.5.6 Virtuelles Verzeichnis ... 957

17.6 Authentifizierung ... 958
17.6.1 Anonyme Authentifizierung ... 959
17.6.2 Standardauthentifizierung ... 962
17.6.3 Digestauthentifizierung ... 969
17.6.4 Windows-Authentifizierung ... 972
17.6.5 Authentifizierungsdelegierung ... 976
17.6.6 Webanwendungen und Kerberos ... 978
17.6.7 Delegierung, eingeschränke Delegierung und Protokollübergang ... 990
17.6.8 Formularauthentifizierung ... 993

17.7 Autorisierung ... 1003
17.7.1 NTFS-Berechtigungen ... 1004
17.7.2 URL-Autorisierung ... 1005

17.8 Sonstiges zum Thema »Sicherheit« 1007
17.8.1 SSL-Verschlüsselung 1007
17.8.2 .NET-Vertrauensebenen 1013
17.8.3 IP- und Domäneneinschränkungen 1019

17.9 Sitzungszustand & Co. 1021

17.10 Load Balancing und Redundanz 1024
17.10.1 Verwendung von Microsoft NLB 1025
17.10.2 Remoteanforderungen 1026
17.10.3 Freigegebene Konfiguration 1027
17.10.4 Sitzungsstatus 1029
17.10.5 Datenbankserver & Co. 1029

17.11 Administration 1029
17.11.1 Remote-Administration 1030
17.11.2 Remote-Administration für Nicht-Server-Administratoren und IIS-Benutzer 1034
17.11.3 Delegierung von Features 1038
17.11.4 Protokollierung 1040

17.12 Der Best Practice Analyzer (BPA) 1042

17.13 IIS-Schlussbemerkung 1043

18 SharePoint Foundation und SharePoint Server 1045

18.1 Warum SharePoint? 1046
18.1.1 Unternehmenswissen 1048
18.1.2 Intranet, Extranet und Internet 1049
18.1.3 Content Manager und andere Rollen 1051
18.1.4 Wie viele Mausklicks? – Oder: Über die Benutzereffizienz 1054

18.2 Projekt und Einführung 1054

19 Remotedesktopdienste (Terminaldienste) 1057

19.1 Die Funktionen aus 10.000 Metern Höhe 1059

19.2 Installation 1063
19.2.1 Basisinstallation 1064
19.2.2 Erster Blick 1070
19.2.3 Lizenzserver konfigurieren 1070

19.2.4 Sitzungssammlung erstellen ... 1074
19.2.5 Desktopdarstellung ... 1079

19.3 Benutzerzugriff ... 1080

19.4 Installation von Anwendungen ... 1084

19.5 Desktop bereitstellen ... 1088

19.6 RemoteApp-Programme ... 1090

19.7 Administration und Verwaltung ... 1098
19.7.1 Bereitstellung konfigurieren ... 1100
19.7.2 Eigenschaften der Sammlung ... 1101
19.7.3 Benutzeradministration ... 1104
19.7.4 Remotesupport für Benutzer ... 1105
19.7.5 Loopbackverarbeitung ... 1107

19.8 Remotedesktopdienstelizenzierung ... 1108

19.9 Drucken, Easy Print ... 1115
19.9.1 Installation von Easy Print ... 1117
19.9.2 Kurze Überprüfung ... 1117
19.9.3 Gruppenrichtlinien ... 1120

19.10 Web Access für Remotedesktop ... 1121

19.11 RemoteApp- und Desktopverbindungen mit Windows 7 und 8 ... 1124

19.12 Remotedesktopdienste-Farmen mit Netzwerklastenausgleich und Remotedesktopdienste-Verbindungsbroker ... 1128

19.13 Schlussbemerkung ... 1133

20 Hochverfügbarkeit 1135

20.1 Vorüberlegungen ... 1136
20.1.1 Allgemeines ... 1136
20.1.2 Hardware und Konfiguration ... 1143

20.2 Failover-Cluster ... 1146
20.2.1 Aktiv vs. Passiv und n+1 ... 1149
20.2.2 Installation ... 1150
20.2.3 Anwendungen hinzufügen ... 1166
20.2.4 Cluster schwenken ... 1172
20.2.5 Feinkonfiguration des Clusters und weitere Vorgehensweise ... 1173
20.2.6 Clusterfähiges Aktualisieren ... 1174
20.2.7 SQL Server 2012 installieren ... 1178

20.3 Network Load Balancing 1188
20.3.1 Funktionsweise des Network Load Balancing 1189
20.3.2 Installation und Konfiguration 1191
20.3.3 Ein paar Hintergründe 1200
20.3.4 Webserver, Kerberos und NLB 1206
20.3.5 NLB-Troubleshooting allgemein 1221

21 Datensicherung 1223

21.1 Sicherung 1225
21.2 Wiederherstellung 1229
21.2.1 Dateien und Ordner 1229
21.2.2 Server wiederherstellen 1233

22 Servervirtualisierung mit Hyper-V 1237

22.1 Allgemeine Überlegungen zur Servervirtualisierung 1241
22.1.1 Scale-out vs. Scale-up 1241
22.1.2 Servervirtualisierung und SAN 1242
22.1.3 Planung und Performance 1244
22.1.4 Was soll virtualisiert werden? 1246
22.2 Editionen und Installationsmöglichkeiten 1247
22.2.1 Windows Server 2012: »normal« und Core 1247
22.2.2 Hyper-V Server 2012 1248
22.3 Der Hyper-V-Manager 1250
22.4 Installation und Grundkonfiguration 1252
22.4.1 Vorbereitung, insbesondere Netzwerkkonfiguration 1252
22.4.2 Installation 1255
22.4.3 Grundeinstellung (Hyper-V-Einstellungen) 1259
22.4.4 Netzwerkeinstellungen 1260
22.5 Administration von virtuellen Maschinen mit dem Hyper-V-Manager 1263
22.5.1 Neue virtuelle Maschine anlegen 1263
22.5.2 Einstellungen bearbeiten 1268
22.5.3 (Dynamische) Speicherverwaltung 1270
22.5.4 Die »laufende« VM 1272

22.6 Verbesserung der Verfügbarkeit 1274
22.6.1 Replikation 1274
22.6.2 Clustering 1287

22.7 Erweiterte Möglichkeiten 1287
22.7.1 Snapshots 1288
22.7.2 VMs verschieben 1292
22.7.3 Exportieren/Importieren 1297
22.7.4 Einfache Sicherung/Wiederherstellung 1297

22.8 System Center Virtual Machine Manager 2012 1303
22.8.1 Aufbau und Architektur 1304
22.8.2 Installation 1305
22.8.3 Schnellüberblick 1323
22.8.4 Virtuelle Maschine anlegen 1326
22.8.5 Virtuelle Maschine aus Vorlage erzeugen 1335
22.8.6 Virtuelle Maschinen verschieben 1346
22.8.7 Konvertieren (P2V und V2V) 1353

23 Windows PowerShell 1361

23.1 Ein paar Grundlagen 1364
23.1.1 Cmdlets 1364
23.1.2 Alias 1367
23.1.3 Skripte 1368
23.1.4 Pipelines 1372

23.2 Die Entwicklungsumgebung 1374

23.3 PowerShell-Fazit 1375

Index 1377

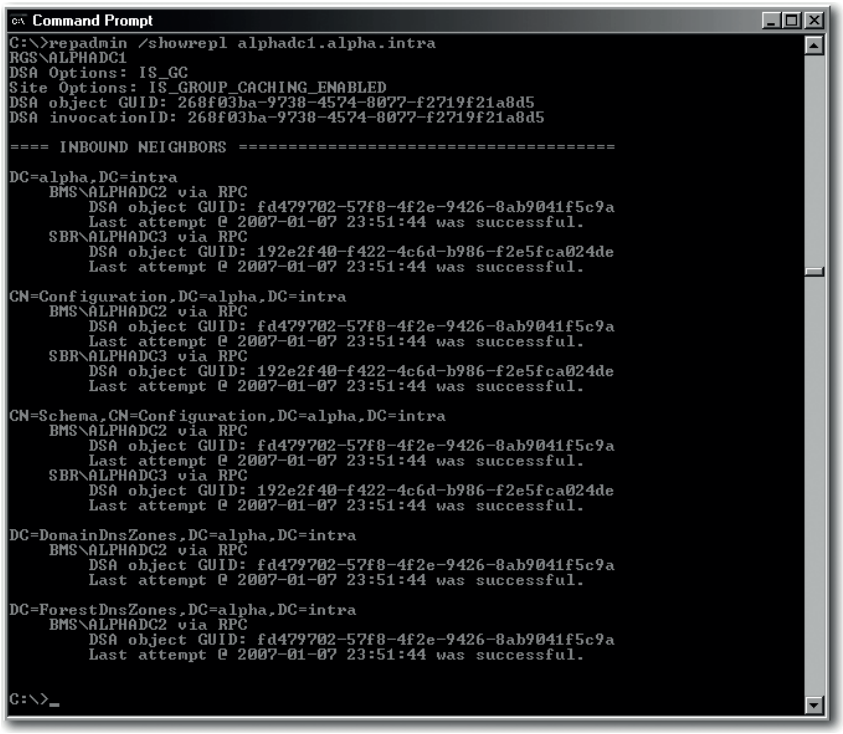


Abbildung 8.80 Mit »repadmin.exe« können Sie überprüfen, ob und wann ein Domänencontroller erfolgreich mit seinen Replikationspartnern repliziert hat.

8.2.5 Gruppenrichtlinien

Das Thema »Gruppenrichtlinien« ist so wichtig, dass es in einem eigenen Abschnitt untergebracht ist, und zwar in Abschnitt 8.4.

8.3 Ein neues Active Directory einrichten

Nachdem ich Sie viele Seiten lang mit Grundlagen (oder dem, was ich dafür halte) gequält habe, wollen wir nun die Installation eines Active Directory betrachten.

Ältere Active Directorys

Falls Sie bereits ein älteres Active Directory verwenden, werden Sie sich vermutlich deutlich mehr für Abschnitt 8.9 interessieren, denn dort geht es um die Migration.

Für diejenigen, die das erste Active Directory installieren, gibt es im nächsten Abschnitt einen Schnelldurchlauf – keine Sorge, die Installation ist wirklich nicht schwierig.

8.3.1 Den ersten Domänencontroller einrichten

Der erste Schritt ist das Hinzufügen der Rolle Active Directory-Domänendienste, was Sie wie üblich mit dem Server-Manager erledigen können (Abbildung 8.81).

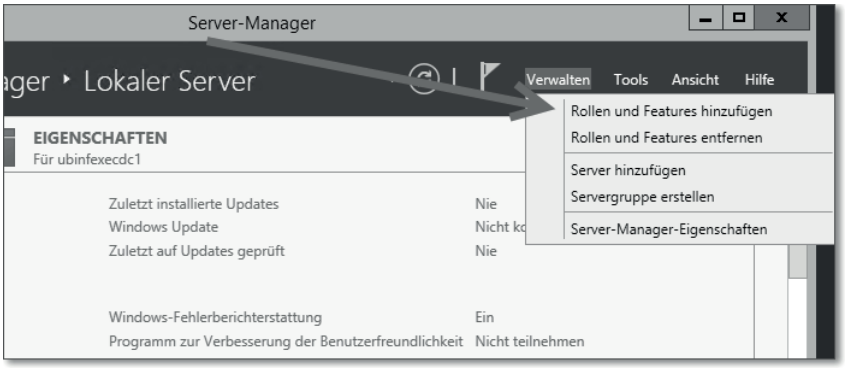


Abbildung 8.81 Hier ist der Startpunkt im 2012er-Server-Manager.

Das Hinzufügen ist im Grunde genommen nur ein Kopieren der benötigten Dateien; die Rolle ist (bzw. die dazugehörigen Dateien sind) zwar vorhanden, der Server ist aber trotzdem (noch) kein Domänencontroller.

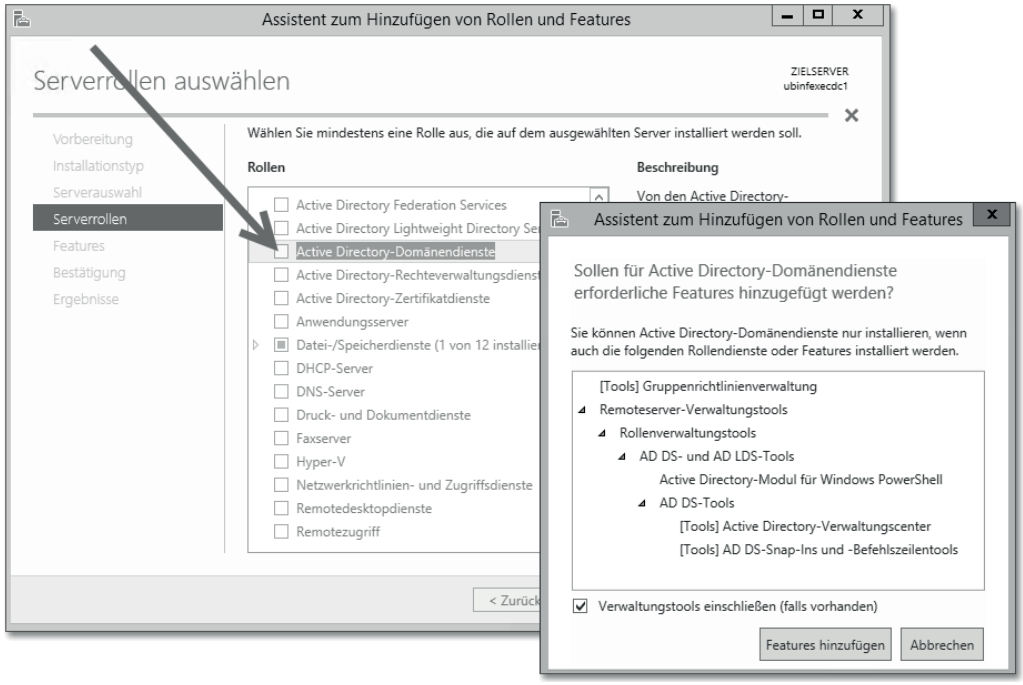


Abbildung 8.82 Der erste Schritt ist die Installation der Serverrolle, benötigte Features werden automatisch hinzugefügt.

Auf der letzten Dialogseite werden Sie den Hinweis finden, dass die eigentliche »Domänencontroller-Werdung« noch durchgeführt werden muss (Abbildung 8.83).

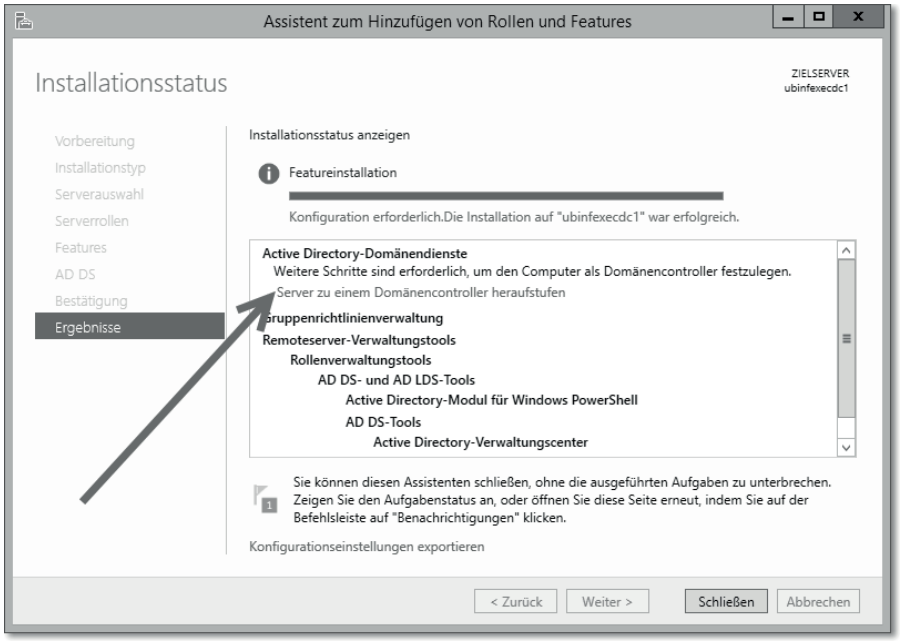


Abbildung 8.83 Nach der Installation der Rolle muss der Assistent aufgerufen werden, der aus dem Server einen DC macht.

Wenn Sie den auf Abbildung 8.83 gezeigten Abschlussdialog schließen, ohne den »DC-Heraufstufungs-Assistenten« gestartet zu haben, schauen Sie im Server-Manager in die Kopfzeile. Dort wird ein Ausrufezeichen darauf hinweisen, dass Meldungen vorhanden sind. Eine davon wird Sie auffordern, den Server zum Domänencontroller heraufzustufen – und schon ist der Assistent gestartet (Abbildung 8.84).

...und dcpromo?

Bisher war an dieser Stelle immer das Eintippen von `dcpromo` angesagt. Das kann man in Server 2012/R2 sogar machen, aber es erscheint lediglich der Hinweis, dass diese Funktionalität jetzt in den Server-Manager integriert ist.

Sie starten nun den Active Directory-Domänendienste-Installationassistenten (Abbildung 8.82):

- Auf der ersten Seite des Assistenten wählen Sie aus, ob der neu einzurichtende Domänencontroller in eine bereits bestehende Gesamtstruktur integriert werden soll oder ob eine völlig neue Gesamtstruktur erstellt werden soll. In unserem Fall wählen Sie die letztgenannte Option und machen so den neuen Domänencontroller zur Keimzelle des neuen Forests.

- Zunächst muss der FQDN der neuen Gesamtstruktur angegeben werden. Es sei darauf hingewiesen, dass es im Allgemeinen keine so glückliche Idee ist, ein Domänen-Suffix (*.de*, *.com*) zu vergeben, das im öffentlichen Internet verwendet wird. Technisch ist das zwar möglich, allerdings machen Sie sich das Leben dadurch unnötig schwer.

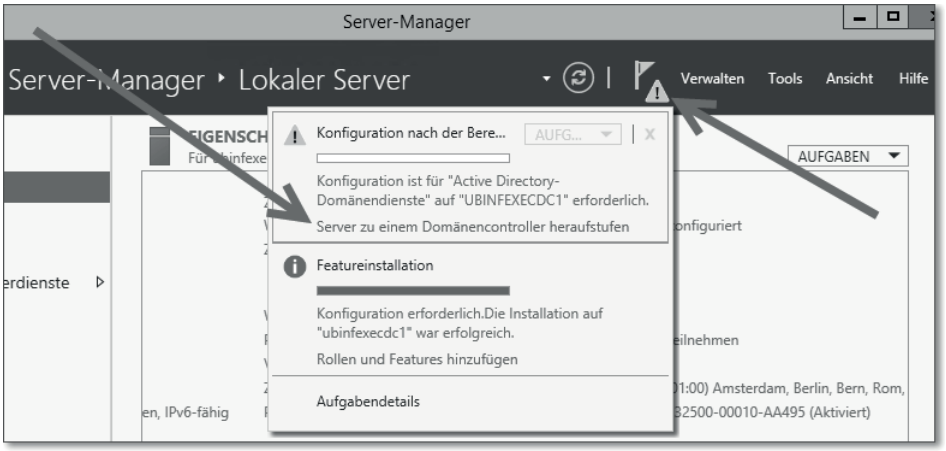


Abbildung 8.84 So kann der Assistent auch gestartet werden.

Benennung

Auf Abbildung 8.85 sehen Sie, dass die Domäne *ubexec.ads.boddenberg.de* genannt worden ist, also ein *.de*-Name, von dem ich einige Zeilen zuvor abgeraten habe. Da aber eine separate DNS-Domäne, nämlich *ads.boddenberg.de*, gewählt worden ist, riskieren Sie nicht die Split-DNS-Probleme, die bei Verwendung von *boddenberg.de* entstanden wären.

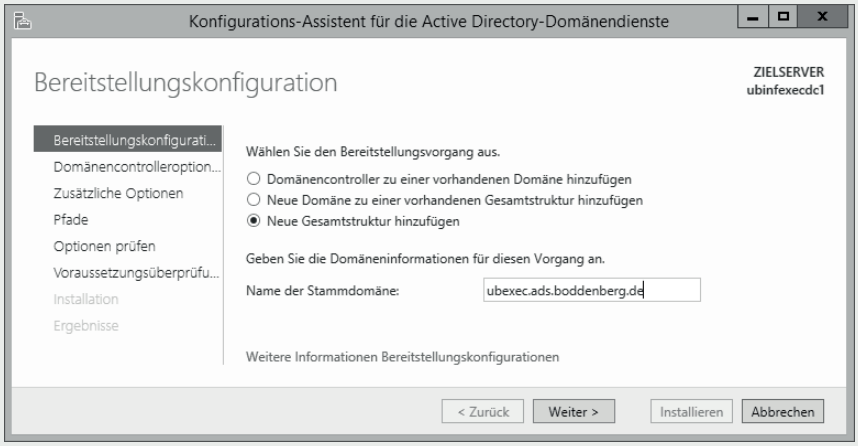


Abbildung 8.85 Der Assistent führt Sie durch das Erstellen einer neuen Domäne in einer neuen Gesamtstruktur.

Achten Sie darauf, dass die Domäne Ihnen »gehört«

Ich habe etliche Kunden, die intern »offizielle« Domänennamen verwenden, obwohl sie nicht im Besitz dieser Domäne sind. Das ist sehr unglücklich. Es gelten also folgende Regeln:

- Geben Sie niemals einer Domäne einen Namen, den Sie nicht besitzen.
- Wenn Sie einen offiziellen Namen verwenden und ihn noch nicht registriert haben, holen Sie das sofort nach – bevor es jemand anders tut.

Abbildung 8.86 zeigt den nächsten Dialog für die Erstellung der neuen Gesamtstruktur:

- Eine wesentliche Entscheidung ist die Festlegung der Funktionsebene für die Gesamtstruktur. Wenn Sie beispielsweise Windows Server 2012 R2 auswählen, bedeutet das, dass es in der kompletten Umgebung nur Domänencontroller mit diesem Betriebssystem geben kann. Es ist kein Problem, Member-Server oder Clients mit älteren Betriebssystemen in der Domäne zu betreiben, aber mit DCs geht das nicht. Die Funktionsebene Windows Server 2008 beispielsweise gestattet DCs mit dem 2008er- und dem 2012er-Betriebssystem. Wenn Sie sicher sind, dass es wirklich nur Windows Server 2012-Domänencontroller geben wird, sollten Sie die Funktionsebene ruhig auf »höchster Stufe« konfigurieren.

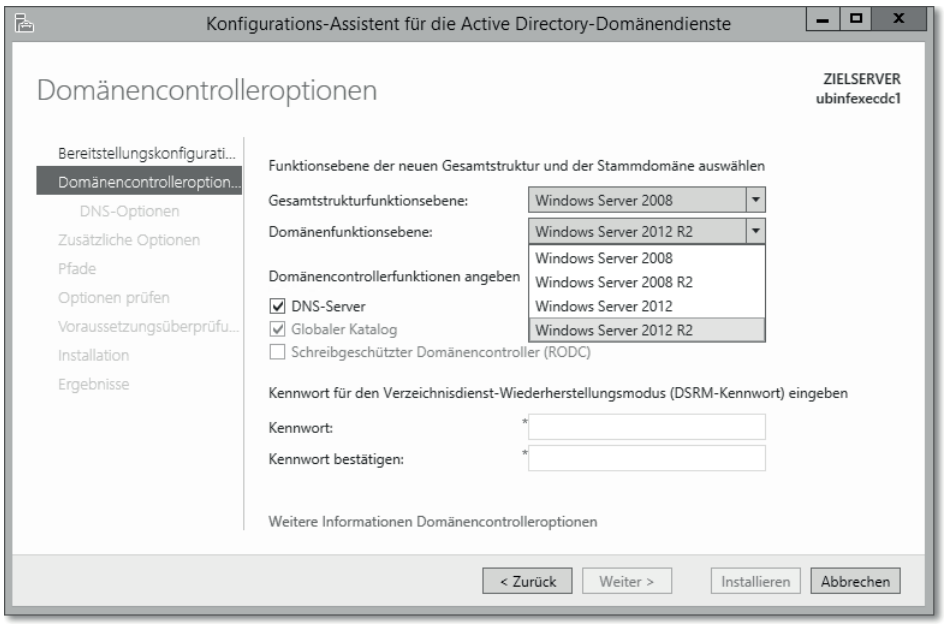


Abbildung 8.86 Hier geben Sie den FQDN der Stammdomäne und der Gesamtstruktur und die Gesamtstrukturfunktionsebene ein.

- Active Directory benötigt zwingenderweise eine funktionierende DNS-Infrastruktur. Bei der Installation eines Domänencontrollers können Sie auf Wunsch den DNS-Server gleich

mit installieren lassen. Beim ersten DC ist das im Allgemeinen eine gute (bzw. die richtige) Wahl.

- Das Kennwort für den Wiederherstellungsmodus sollten Sie gut geschützt aufbewahren. Damit meine ich, dass es zum einen nicht einfach zu erraten sein sollte, zum anderen sollten Sie (oder andere berechtigte Personen) im Fall der Fälle darauf problemlos Zugriff haben.

Der nächste, auf Abbildung 8.87 gezeigte Dialog, ist neu in Server 2012. Sie können wählen, ob eine DNS-Delegierung erstellt werden soll, und können ggf. das zu verwendende Konto hinterlegen. Diese Einstellung macht nur dann Sinn, wenn der übergeordnete Namensserver erreichbar ist und mit Microsoft-Technologie läuft.

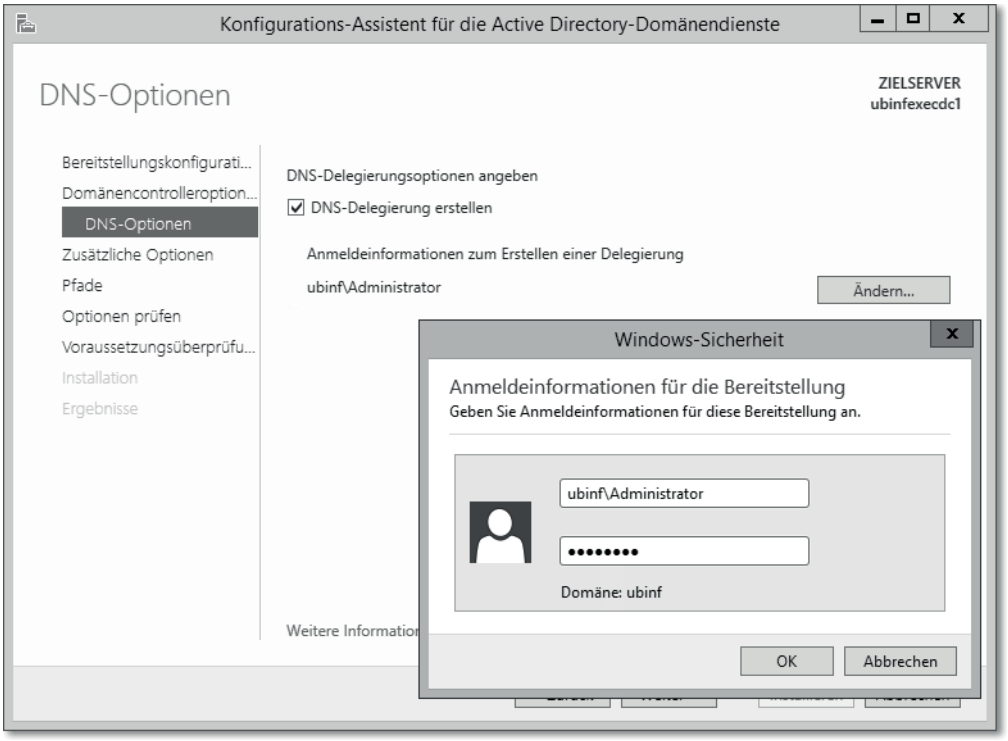


Abbildung 8.87 Entscheiden Sie, ob eine Delegierung erstellt werden soll bzw. erstellt werden kann.

Ein Beispiel für die Delegierung

Was es mit der Erstellung der Delegierung für den neuen DNS-Server auf sich hat, lässt sich anhand eines Beispiels aus dem öffentlichen Internet erklären: Für jede Domäne, beispielsweise *boddenberg.de*, existiert ein autorisierender Namensserver, der die Adressen der Server, wie beispielsweise *www.boddenberg.de* oder *mail.boddenberg.de*, auflösen kann.

Damit dieser Server gefunden wird, wird beim Root-Server der Top-Level-Domain *.de* eine Delegierung dorthin erstellt. Vereinfacht gesagt, sorgt eine Delegierung dafür, dass ein Client, der einen Server im Namensraum *boddenberg.de* sucht, vom Top-Level-Namensserver an den zuständigen Namensserver verwiesen wird.

Auf Abbildung 8.88 sehen Sie die Delegierung, die in dem hier gezeigten Beispiel erstellt wurde:

- Die Domäne *boddenberg.de* wird von Microsoft-DNS-Servern verwaltet.
- *ads* ist als Container erstellt worden.
- In diesem wiederum findet sich die Delegierung auf *ubexec* nebst Nennung des Namensservers.

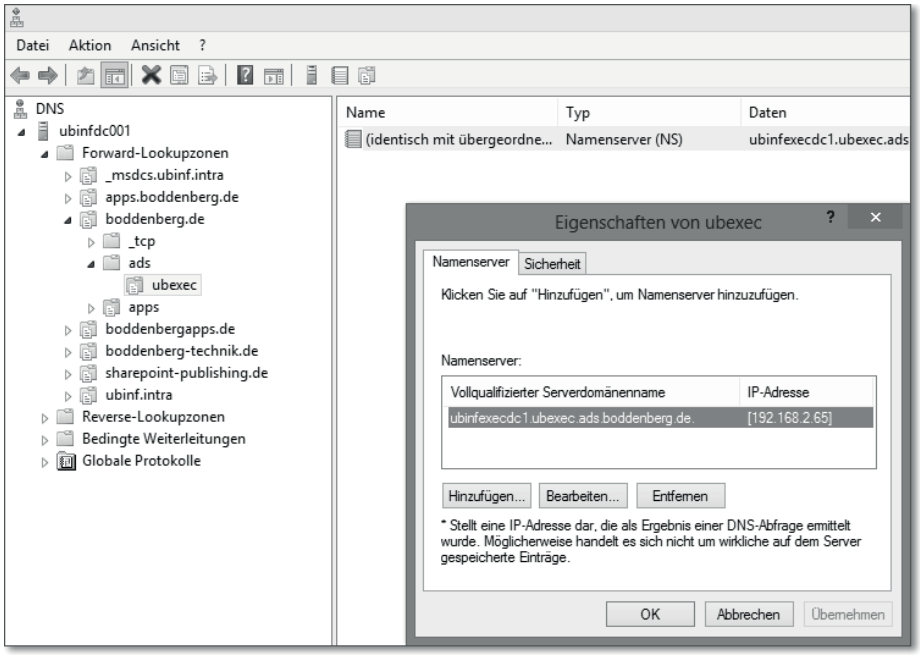


Abbildung 8.88 Diese Delegierung wurde in dem hier gezeigten Beispiel automatisch erstellt.

Abbildung 8.89 zeigt, dass der NetBIOS-Name der Domäne nach wie vor eine Rolle spielt. Dieser Name sollte (muss aber nicht!) dem ersten Teil des FQDNs entsprechen, also *ubexec* bei *ubexec.ads.boddenberg.de*. Wenn Sie von dieser Vorgehensweise abweichen, gibt es zwei mögliche Probleme:

- Es wird unübersichtlich, vor allem, wenn Sie mehrere Domänen haben.
- Es könnte zu erhöhtem Konfigurationsaufwand kommen. Beispielsweise müssen Sie beim SharePoint-Benutzerprofil-Sync-Dienst zusätzliche Schritte ausführen, wenn NetBIOS-Name und FQDN unterschiedlich sind.

Punkte im NetBIOS-Namen

Punkte im NetBIOS-Namen sind absolut tabu! Sie führen zu unlösbaren Problemen.

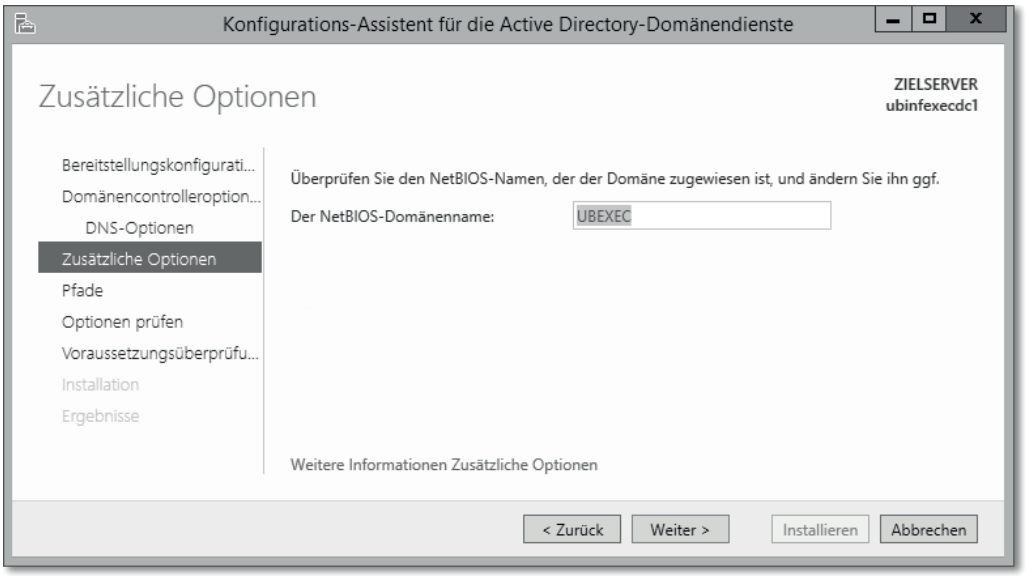


Abbildung 8.89 Der NetBIOS-Name der Domäne ist noch immer gefragt.

Abbildung 8.90 zeigt eine weitere wichtige Dialogseite des Assistenten. Sie müssen entscheiden, wo die Datenbankdateien des Domänencontrollers abgelegt werden sollen. Der »reinen Lehre« entsprechend sagt man zwar, dass keine produktiven Daten auf der C-Platte abgelegt werden sollen. Ich muss allerdings sagen, dass wohl auf 99 % der Domänencontroller dieser Welt die AD-Datenbankdateien genau dort liegen. Aus Gründen der Vereinfachung und Bequemlichkeit tendiere ich auch dazu, diese im Standardpfad zu speichern. Ich habe zudem das unbestimmte Gefühl, dass das eine oder andere Drittherstellerwerkzeug direkt »aus der Kurve fliegt«, wenn die Dateien an einem anderen Ort gespeichert werden. Ebendiese Argumentation gilt für das *SYSVOL*-Verzeichnis, in dem diverse von den Clients bei der Anmeldung benötigte Dateien vorgehalten werden – vornehmlich alles rund um die Gruppenrichtlinien.

Wer Exchange 2007 administriert (hat), kennt die Dialoge, in denen das zum selben Ergebnis führende PowerShell-Skript angezeigt wird. Das Active Directory-Team folgt diesem Beispiel und bietet im Dialog Optionen prüfen (Abbildung 8.91) einen Schalter an, mit dem Sie sich das PowerShell-Skript anzeigen lassen können, das zum Erstellen des neuen Forests dient.

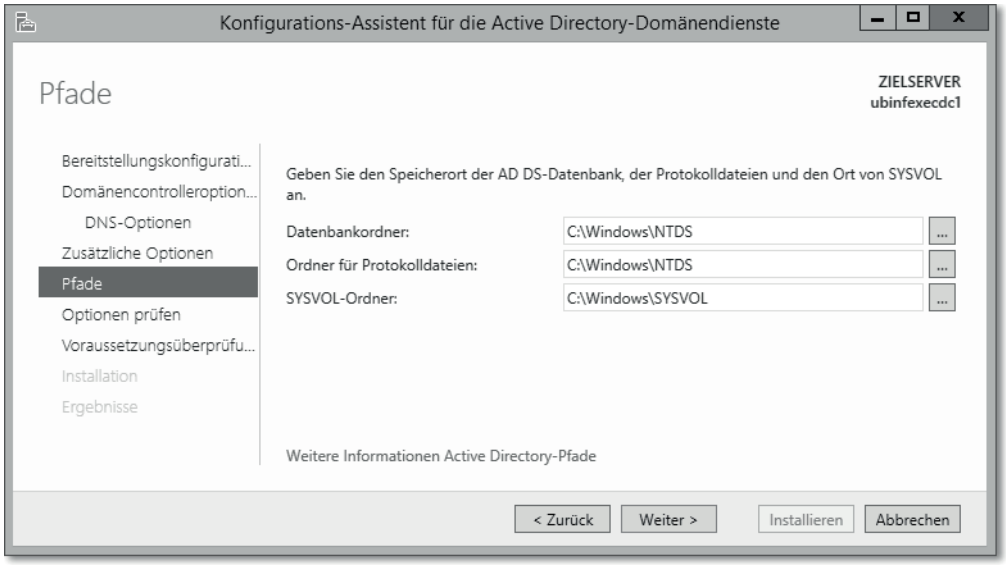


Abbildung 8.90 Der Speicherort für die Systemdateien und die Auswahl des Wiederherstellungskennworts

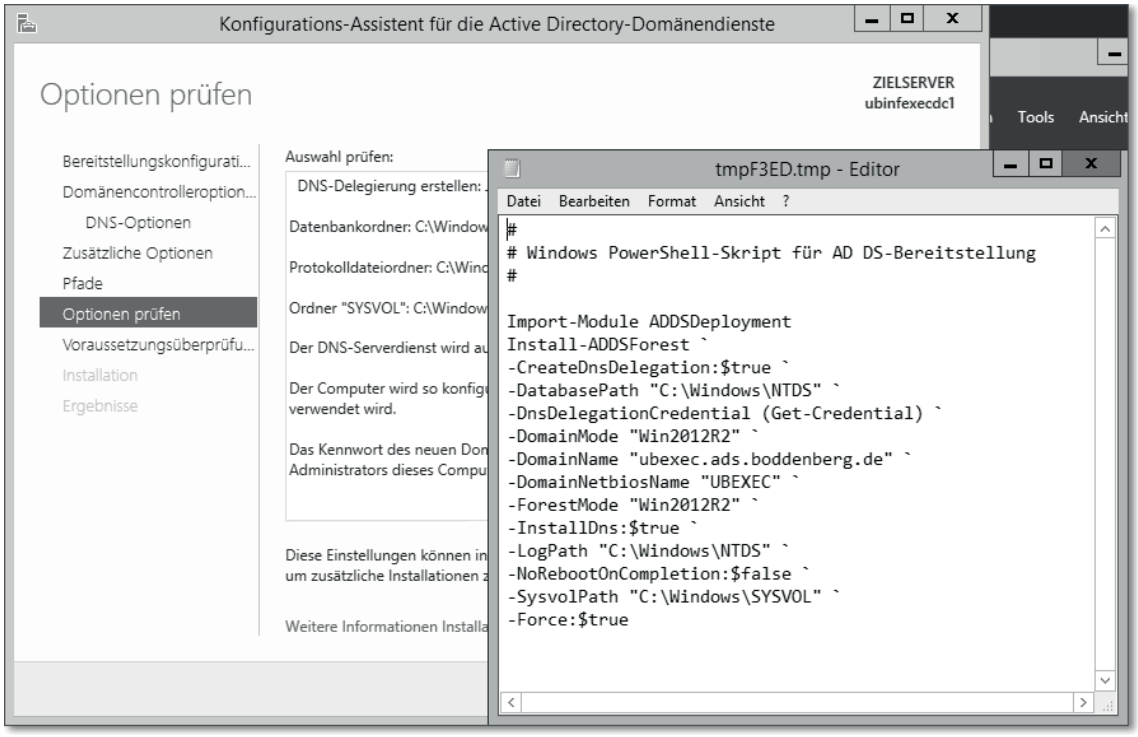


Abbildung 8.91 Das zugehörige PowerShell-Skript kann ausgegeben werden.

Nachdem Sie alle Eingaben im Assistenten getätigt haben, wird die Installation des Domänencontrollers durchgeführt. Sie dauert einige Minuten. Nach dem abschließenden Neustart verfügen Sie über eine funktionsfähige Active Directory-Gesamtstruktur mit einer Domäne.

8.3.2 Zusätzliche Domänencontroller einrichten

Das Einrichten eines zusätzlichen Domänencontrollers funktioniert zunächst wie beim ersten DC. Sie fügen also eine Rolle hinzu und starten den Assistenten. Der wesentliche Unterschied begegnet Ihnen direkt auf der ersten Seite des Assistenten. Dort entscheiden Sie sich jetzt nicht für das Erstellen einer neuen Gesamtstruktur, sondern machen den Server zu einem Domänencontroller in einer bereits existierenden Domäne oder aber zum ersten DC einer neuen Domäne in einer vorhandenen Gesamtstruktur (Abbildung 8.92).

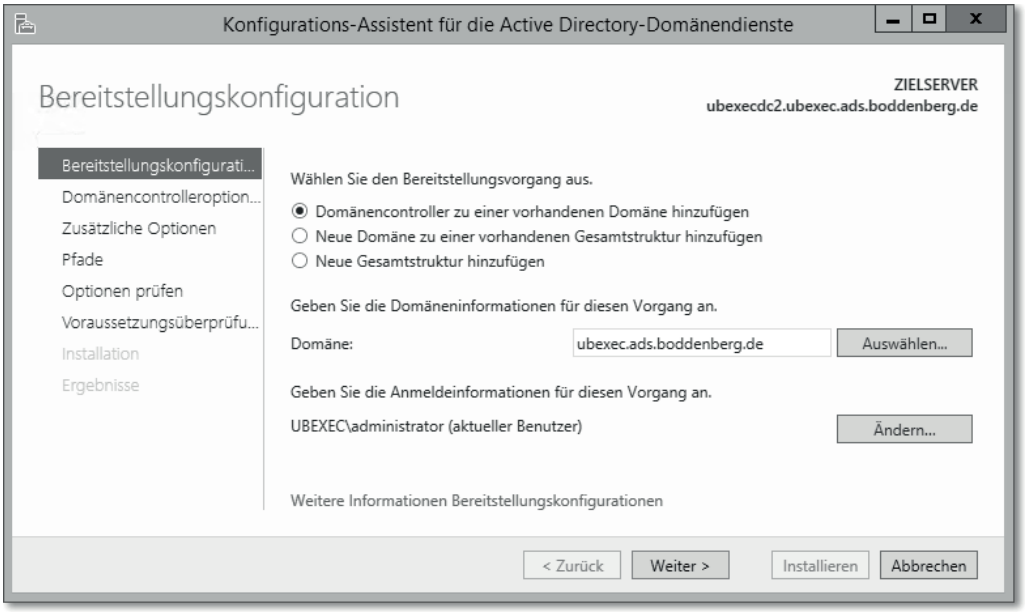


Abbildung 8.92 Wählen Sie eine Option für die Installation des neuen DCs aus.

Der weitere Verlauf des Assistenten wird Sie vor keine größere Herausforderung stellen. Wenn alle Eingaben gesammelt sind, wird der DC eingerichtet und eine erste Replikation durchgeführt. Apropos Replikation: Eine Neuerung ab Server 2012 sehen Sie auf Abbildung 8.93. Sie können die Replikatsquelle auswählen. Sie ist entweder ein – wählbarer – Domänencontroller oder ein Medium.

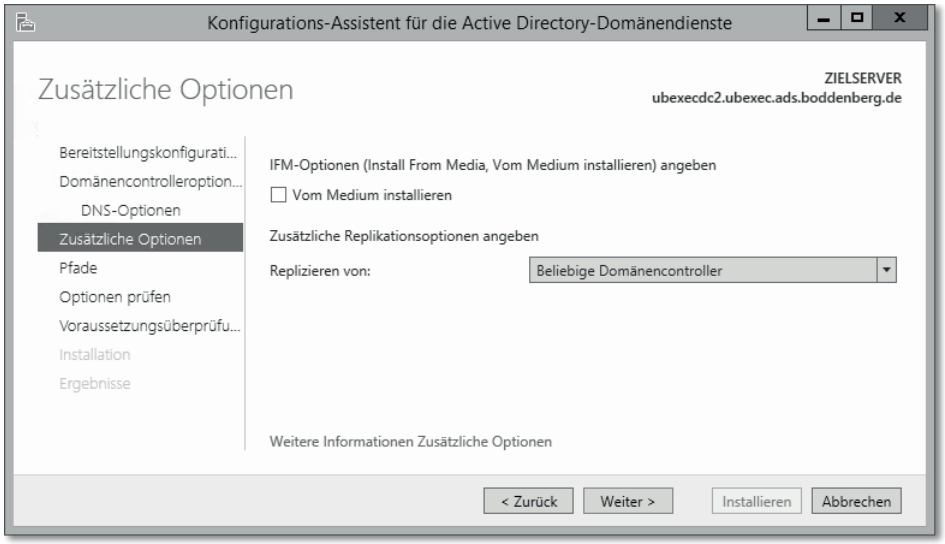


Abbildung 8.93 In diesem Dialog wählen Sie die Replikatsquelle aus.

8.4 Gruppenrichtlinien

Mit Gruppenrichtlinien (GPO, Group Policy Object) können Sie diverse Konfigurationen für Benutzer oder Computer vornehmen – und zwar in Abhängigkeit von dem Standort, der Domäne und der 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. Es können aber auch Einstellungen für Computer vorgenommen werden, z. B. zur Sicherheitskonfiguration für drahtlose Netzwerke.

In den Gruppenrichtlinien konfigurieren Sie übrigens auch die Login-Skripts, die angewendet werden sollen.

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 von *Microsoft SMS* (Systems Management Server), ist aber in vielen Fällen durchaus ausreichend.

Die bereits in Windows Server 2012 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 können Sie beispielsweise das Office-Paket sehr weitgehend anpassen.
- Bei Bedarf können auch eigene Gruppenrichtlinien erstellt werden, sodass man als Administrator die Freiheit hat, alles über Gruppenrichtlinien zu konfigurieren, was über die Registry eingestellt werden kann.

8.4.1 Anwendungsbeispiel

Falls Sie bisher nicht mit Gruppenrichtlinien in Berührung gekommen sind, zeige ich Ihnen zum Einstieg ein Anwendungsbeispiel.

Abbildung 8.94 Das »normale« Startmenü eines Clients

In Abbildung 8.94 ist das Startmenü eines Windows-Clients zu sehen. Viele Unternehmen möchten die Möglichkeiten der Anwender mehr oder weniger stark einschränken. Da das Startmenü der primäre Weg ist (bzw. war), um Applikationen oder Konfigurationsdialoge aufzurufen, läge es also nahe, das Startmenü entsprechend zurechtzustutzen. Auf der Wunschliste stehen weiterhin folgende Punkte:

- Die Einstellungen sollen nicht an jedem PC einzeln 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.

In Abbildung 8.95 sehen Sie, wie ein Gruppenrichtlinienobjekt mit der Organisationseinheit *Vertrieb* verknüpft wird. Es können beliebig viele Gruppenrichtlinienobjekte mit einer OU verknüpft werden. Ein Gruppenrichtlinienobjekt kann mit beliebig vielen OUs verknüpft werden.

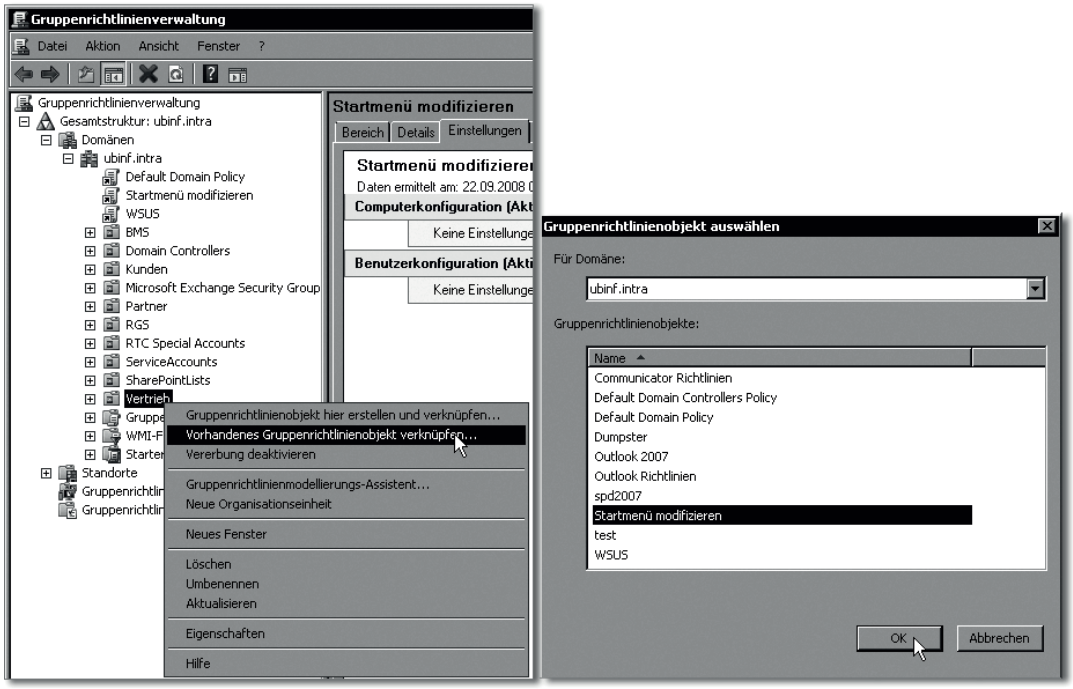


Abbildung 8.95 Ein Gruppenrichtlinienobjekt wird mit der OU »Vertrieb« verknüpft.

Ein Gruppenrichtlinienobjekt enthält jeweils beliebig viele Einstellungen. Man könnte prinzipiell alle anzuwendenden Einstellungen in einem Gruppenrichtlinienobjekt vornehmen. Erfahrungsgemäß ist es zur Administration übersichtlicher, die vorzunehmenden Einstellungen in Gruppen zusammenzufassen und auf mehrere Gruppenrichtlinienobjekte zu verteilen.

Hinweis

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 8.96).

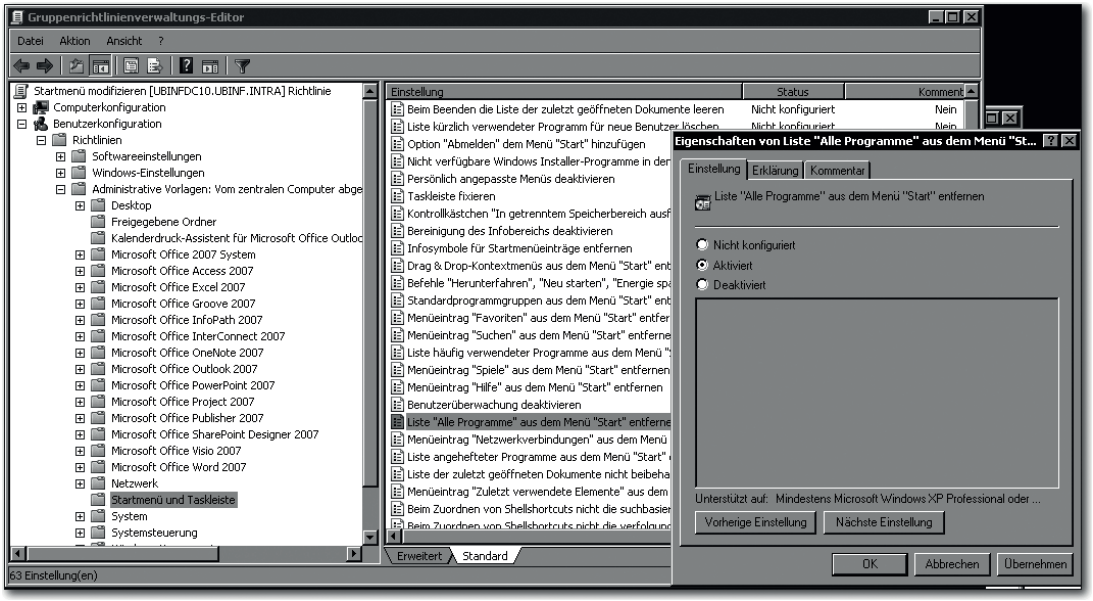


Abbildung 8.96 Bei der Erstellung der Gruppenrichtlinie können Sie aus vielen Hundert Einstellungen auswählen.

Meldet sich der Benutzer das nächste Mal am System an, werden die vorgegebenen Einstellungen angewendet. In Abbildung 8.97 ist zu sehen, dass der Eintrag ALLE PROGRAMME nicht mehr angezeigt wird.

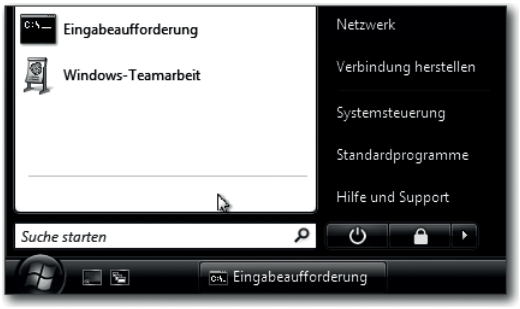


Abbildung 8.97 Die erstellte Richtlinie entfernt »Alle Programme« aus dem Startmenü.

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.

Hinweis

Mir ist klar, dass seit Windows 8 das »traditionelle« Startmenü eigentlich »Geschichte« ist. Daran lässt sich aber erstens gut die Funktionalität erläutern, zweitens gibt es ja noch hinreichend viele Unternehmen, die ältere Betriebssysteme als Windows 8 einsetzen.

8.4.2 Richtlinien für Computer und Benutzer

Ein Gruppenrichtlinienobjekt ist immer zweigeteilt. Es gibt einen Bereich *Computerkonfiguration* und einen weiteren namens *Benutzerkonfiguration*. Abbildung 8.98 zeigt einen Blick in die Computerkonfiguration. 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 folgt im weiteren Verlauf dieses Abschnitts.

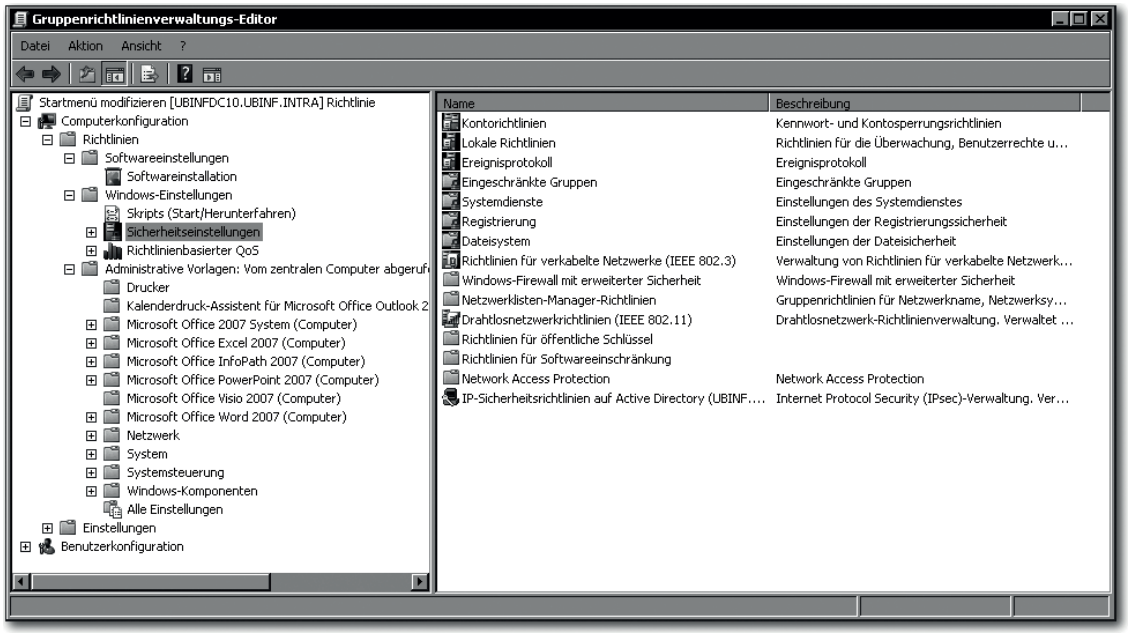


Abbildung 8.98 In Bereich »Computerkonfiguration« des Gruppenrichtlinienobjekts nehmen Sie alle systemseitigen Einstellungen vor. Einige Beispiele sind in der Abbildung zu sehen.

Abbildung 8.99 zeigt einen kleinen Ausschnitt der *Benutzerkonfiguration*. Wenn Sie diese mit der Computerkonfiguration vergleichen, werden Sie erkennen, dass beide grundsätzlich dieselbe Struktur haben, die aus den folgenden drei Gruppen besteht:

- *Softwareinstellungen*: Hier wird die Verteilung von Softwarepaketen (nur Windows Installer-Pakete, also **.msi*-Dateien) konfiguriert.
- *Windows-Einstellungen*: Hier finden Sie die »Windows-nahen« Einstellmöglichkeiten, beispielsweise für die Ausführung von Skripts, die Sicherheitsrichtlinien und einiges andere mehr.
- *Administrative Vorlagen*: Alle anderen Einstellungen finden Sie unter dem Knoten ADMINISTRATIVE VORLAGEN. Die Konfiguration von zusätzlichen Softwarekomponenten oder des Erscheinungsbilds der Oberfläche nehmen Sie mit den Einstellmöglichkeiten vor, 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 Zeit nehmen, in dem Wust von Konfigurationsmöglichkeiten zu stöbern. Man findet häufig Optionen mit dem »Könnte-ich-gut-einsetzen«-Effekt.

In dem Gruppenrichtlinienobjekt-Editor von Windows Server 2012 finden sich bereits die für Windows Vista (und alle Vorgängerversionen) benötigten Einstellmöglichkeiten. Windows Server 2012 R2 enthält bereits auch die für Windows 8.1 benötigten Konfigurationsmöglichkeiten.

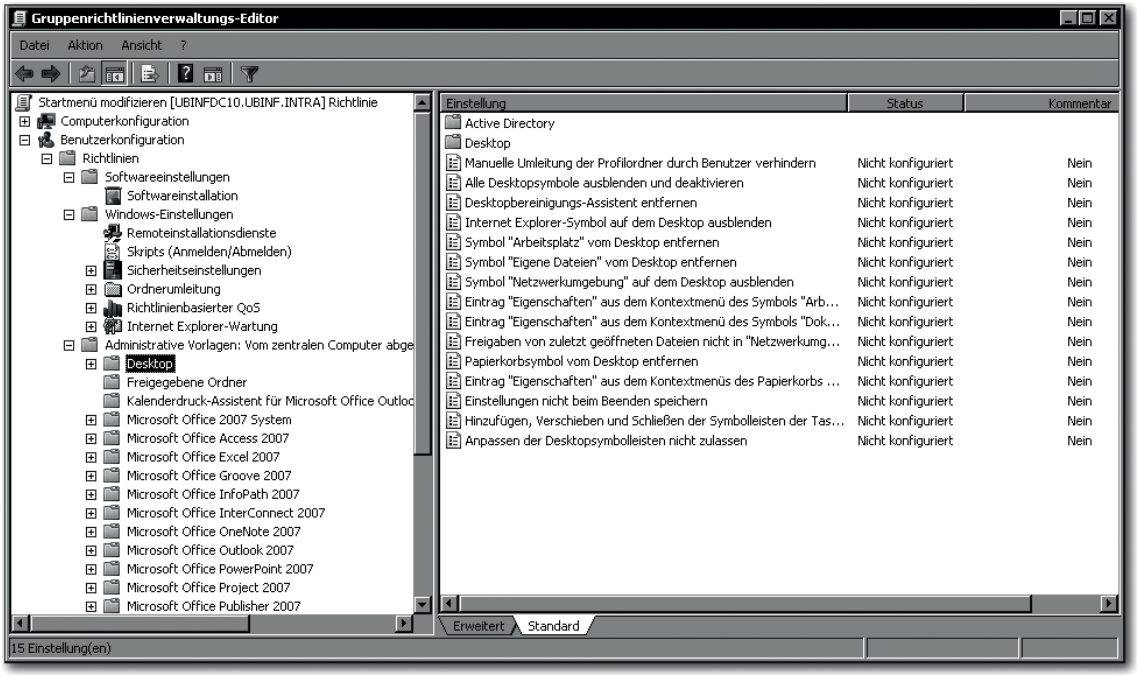


Abbildung 8.99 Der Bereich »Benutzerkonfiguration« des Gruppenrichtlinienobjekts beschäftigt sich primär mit der Fragestellung, auf welche Betriebssystemfunktionen der Benutzer Zugriff hat und wie das optische Erscheinungsbild sein soll.

Vermutlich wird es irgendwann ein Service-Pack zu Windows 8 und später eine neue Version des Client-Betriebssystems geben. Vermutlich wird es bei diesen Nachfolgeversionen weitere Einstellmöglichkeiten geben, die der heute installierten Windows Server 2012 R2-Version einfach noch nicht bekannt sind und die folglich nicht angezeigt werden. Da weitere Einstellmöglichkeiten über die ADMINISTRATIVEN VORLAGEN hinzugefügt werden können, können auch zukünftige Features der Clients mit den heute aktuellen Server-Versionen verwaltet werden.

Falls Sie auf den Clients das Betriebssystem in der Version Windows 8 einsetzen und Ihr Active Directory noch auf dem Stand von Windows 2000 ist, ist die Vorgehensweise identisch: Die administrativen Vorlagen für Windows 8 werden installiert, und demzufolge stehen in dem Gruppenrichtlinienobjekt-Editor des Windows 2000 Servers die Windows-8-Konfigurationsmöglichkeiten zur Verfügung.

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.

8.4.3 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. Abbildung 8.100 zeigt einen Blick mit ADSI-Editor in das Active Directory, genauer gesagt in den Abschnitt `CN=System,CN=Policies` des Domänennamenskontexts. Dort finden Sie mehrere mit einer GUID benannte Einträge: Dies sind die Gruppenrichtlinienobjekte. Wenn Sie sich die Attribute eines solchen Objekts anschauen, finden Sie beispielsweise den Anzeigenamen (`displayName`) der Gruppenrichtlinie und einen Pfad ins Dateisystem (`gPCFileSysPath`).

Der Pfad ins Dateisystem lässt darauf schließen, dass das eigentliche Regelwerk, also die Information über die zu setzenden Registry-Einstellungen, im Dateisystem gespeichert wird. Genau so 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 8.101 zeigt den Blick in das entsprechende Verzeichnis einer Gruppenrichtlinie.

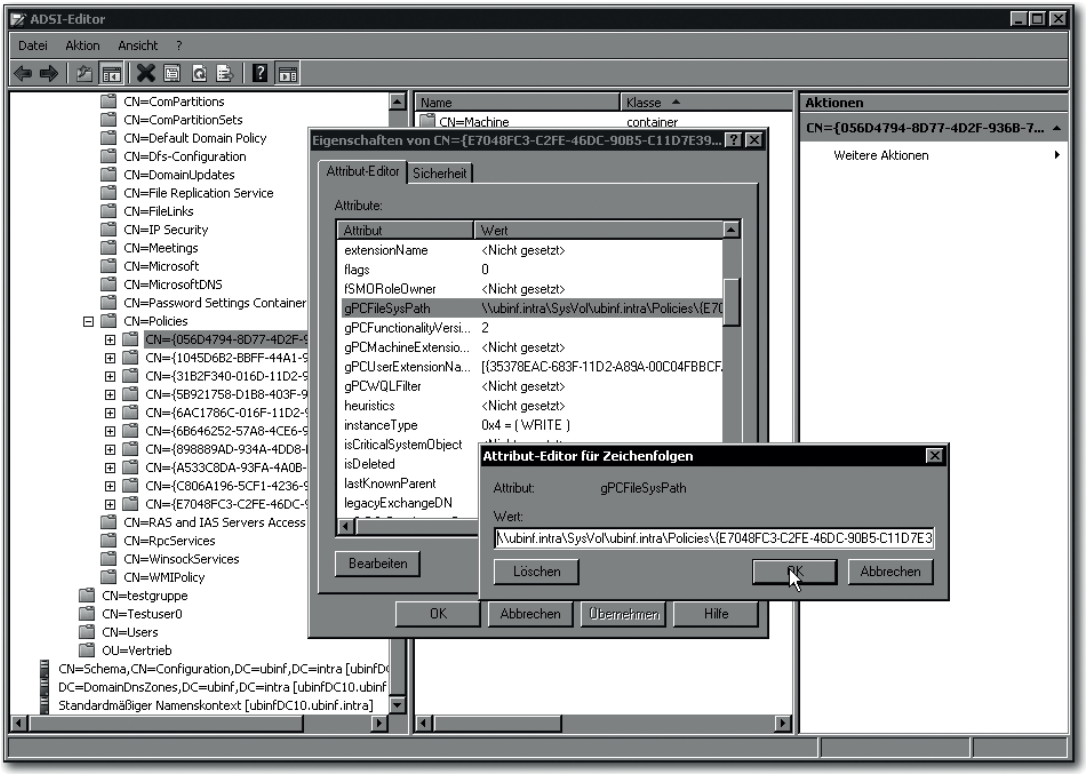


Abbildung 8.100 Die Informationen über die angelegten Gruppenrichtlinen finden Sie im Domänennamenskontext, hier mit ADSI-Editor. Zu sehen ist beispielsweise der Displayname und ein Pfad ins Dateisystem.

In dem Verzeichnis der Gruppenrichtlinie befindet sich ein Ordner *Machine* und ein Ordner *User*. In Letzterem liegt in diesem Fall eine Datei *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 folgt später in diesem Abschnitt).

Damit alle Domänencontroller einer Domäne die Gruppenrichtlinien bereitstellen können, ist es erforderlich, dass die *SYSVOL*-Verzeichnisse repliziert werden. Dies wird vom DFS-Replikationsdienst übernommen. Falls die Replikation der *SYSVOL*-Verzeichnisse nicht funktioniert, ist akut 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 vorfinden – in Abhängigkeit von dem Domänencontroller, an dem die Anmeldung erfolgte.

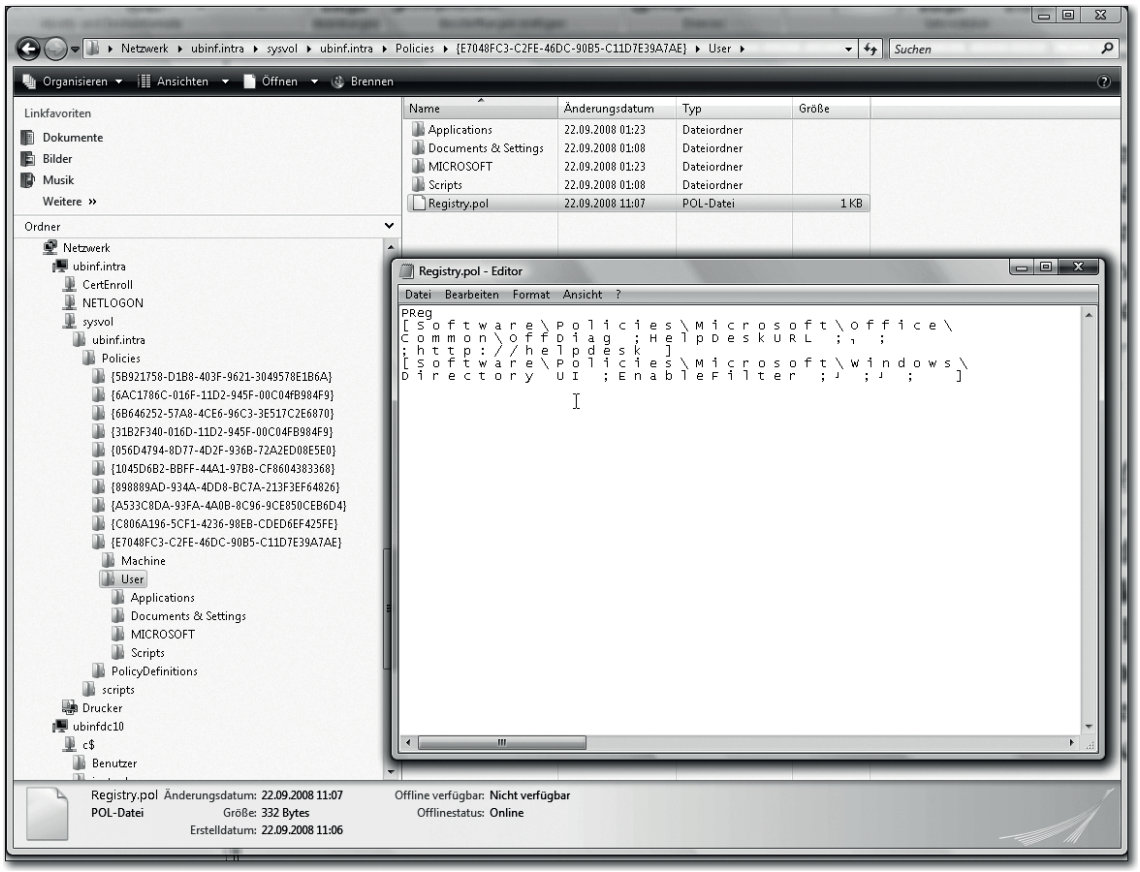


Abbildung 8.101 Die Dateien zu den Gruppenrichtlinienobjekten liegen in der Freigabe SYSVOL, die sich auf jedem Domänencontroller befindet.

Fehler des DFS-Replikationsdiensts werden im Ereignisprotokoll angezeigt. Unterhalb des Knotens Anwendungs- und Dienstprotokolle befindet sich das benötigte Protokoll (Abbildung 8.102). 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).

Nachdem Sie nun wissen, wo die Gruppenrichtlinienobjekte angelegt werden, ergibt sich noch die Frage, wie die Zuordnung zu den Domänen, Organisationseinheiten und Standorten erfolgt. In Abbildung 8.103 sehen Sie in ADSI-Editor die Attribute der Organisationseinheit *Marketing*. Unter anderem ist auch das Attribut gPLink vorhanden, das auf die Gruppenrichtlinienobjekte verweist, die von dieser OU verwendet werden sollen.

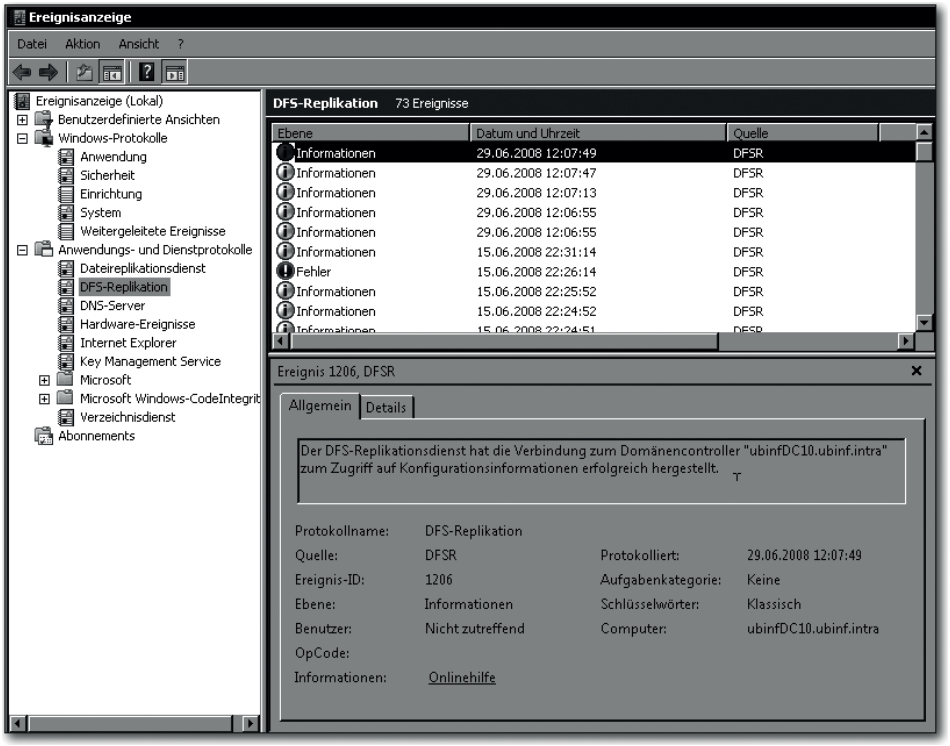


Abbildung 8.102 Meldungen und Fehler betreffs der Replikation werden im Ereignisprotokoll, Abschnitt »DFS-Replikation«, angezeigt.

Nachfolgend ist der Inhalt des GPLINK-Attributs aus Abbildung 8.103 aufgeführt; es sind zwei Verweise auf Gruppenrichtlinienobjekte. Die GUIDs (z.B. ist 056D4794-8D77-4D2F-936B-72A2ED08E5E0 eine GUID) finden Sie in Abbildung 8.100 und Abbildung 8.101.

```
[LDAP://cn={056D4794-8D77-4D2F-936B-72A2ED08E5E0},cn=policies,
cn=system,DC=ubinf,DC=intra;0]
[LDAP://cn={E7048FC3-C2FE-46DC-90B5-C11D7E39A7AE},cn=policies,
cn=system,DC=ubinf,DC=intra;0]
```

Nun wird auch das Gesamtbild klar, das auf der stark vereinfachten Darstellung in Abbildung 8.104 zu sehen ist:

- Organisationseinheiten, Domänen und Standorte speichern Verweise auf Gruppenrichtlinienobjekte.
- Eine Organisationseinheit, eine Domäne oder ein Standorte kann auf ein, mehrere oder kein Gruppenrichtlinienobjekt verweisen.
- Auf ein Gruppenrichtlinienobjekt kann von keiner, einer oder mehreren Organisationseinheiten/Domänen/Standorten verwiesen werden.

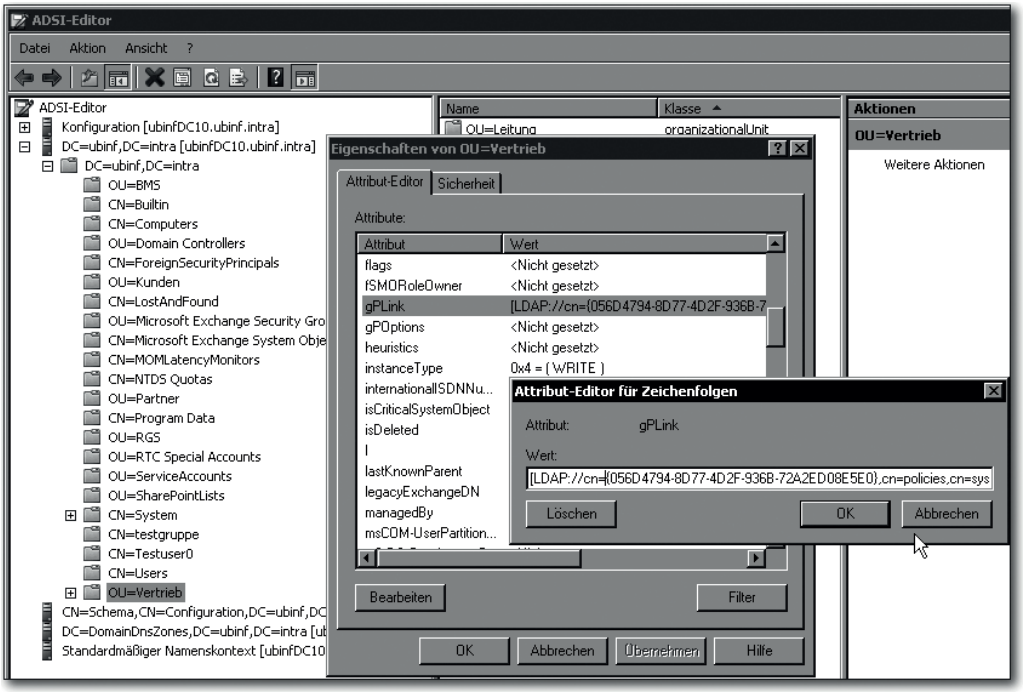


Abbildung 8.103 Die Organisationseinheit verfügt über das Attribut »gPLink«, das Verweise auf Gruppenrichtlinienobjekte enthält.

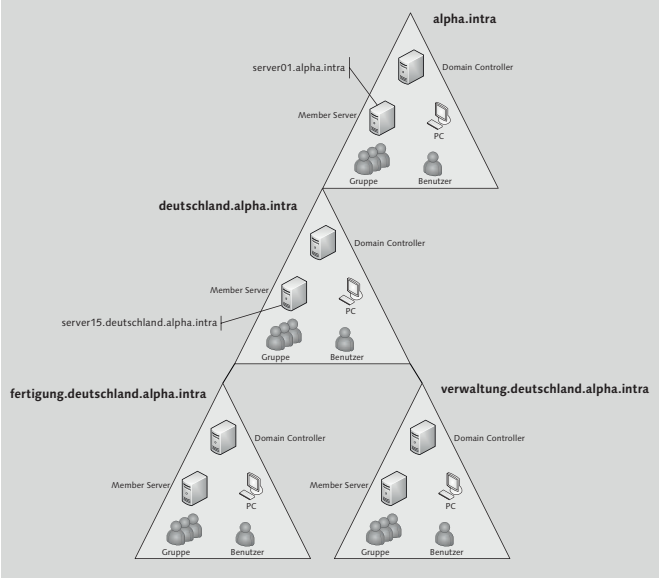


Abbildung 8.104 Standorte und Organisationseinheiten speichern Verweise auf Gruppenrichtlinienobjekte.

Es ist wichtig, diese Zusammenhänge zu verstehen – sonst wird man unter Umständen funktionsgleiche Gruppenrichtlinienobjekte doppelt anlegen und sich eventuell über die Formulierung in einigen Konfigurationsdialogen wundern.

8.4.4 Vererbung

Wie gesagt können Gruppenrichtlinien an drei »Orten« angelegt werden:

- Domäne
- Organisationseinheit
- Standort

Drei lokale Gruppenrichtlinienobjekte

Wichtig zu erwähnen ist, dass Betriebssysteme ab Windows 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 in Abschnitt 8.4.8.

Die Gültigkeitsbereiche der Gruppenrichtlinie sind einfach zu verstehen:

- Eine lokale Gruppenrichtlinie gilt verständlicherweise nur auf dem lokalen Computer. Windows Vista/7/8/8.1 und Windows Server 2008/2012/R2 verfügen über drei lokale GPOs, die eine zusätzliche Einschränkung des Gültigkeitsbereichs ermöglichen. Mehr dazu finden Sie in Abschnitt 8.4.8.
- 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 in der 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 8.105 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« Organizational Unit abgearbeitet.
4. Zuletzt wird die Gruppenrichtlinie der »inneren« OU verarbeitet.

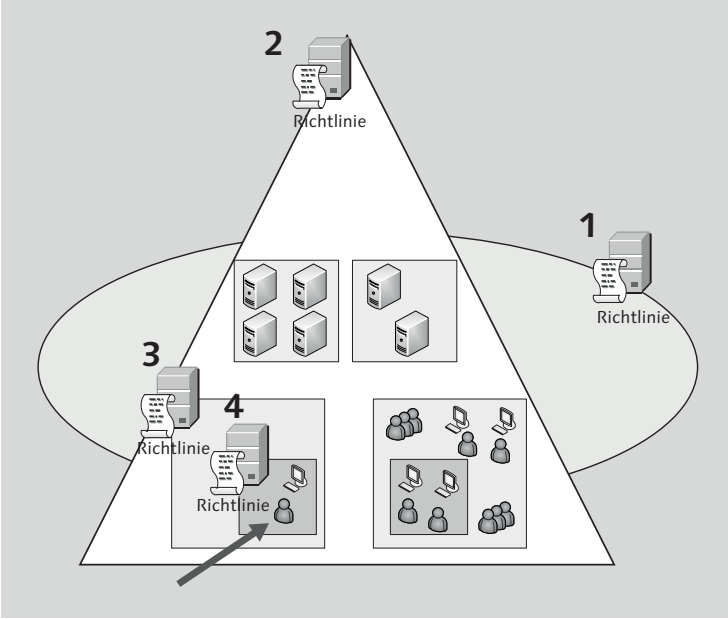


Abbildung 8.105 Die Reihenfolge, in der die Gruppenrichtlinien abgearbeitet werden

Schritt 0

In einem (nicht in der Zeichnung abgebildeten) Schritt 0 werden bei Betriebssystemen ab Windows 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 der folgenden Tabelle, die auch die genaue Abarbeitungsreihenfolge zeigt:

Richtlinie	Konfiguration
Vista/7/8, WS2008/R2/2012/R2: Lokale GPO	Nicht konfiguriert
Vista/7/8, WS2008/R2/2012/R2: Lokale GPO für Admin-Konten oder Nicht-Admin-Konten	Nicht konfiguriert
Vista/7/8, WS2008/R2/2012/R2: Lokale benutzerspezifische GPO	Nicht konfiguriert
Standort	Aktiviert
Domain	Deaktiviert

Tabelle 8.2 Abarbeitungsreihenfolge der Gruppenrichtlinien

Richtlinie	Konfiguration
OU 1 (»äußere«)	Aktiviert
OU2 (»innere«)	Nicht konfiguriert
Resultat	Aktiviert

Tabelle 8.2 Abarbeitungsreihenfolge der Gruppenrichtlinien (Forts.)

Ist das so weit einleuchtend? Gut!

In dem Dialog aus Abbildung 8.106 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 8.106 zeigt, dass bei einer OU mit deaktivierter Vererbung ein kleines blaues Aufrufezeichen angezeigt wird.

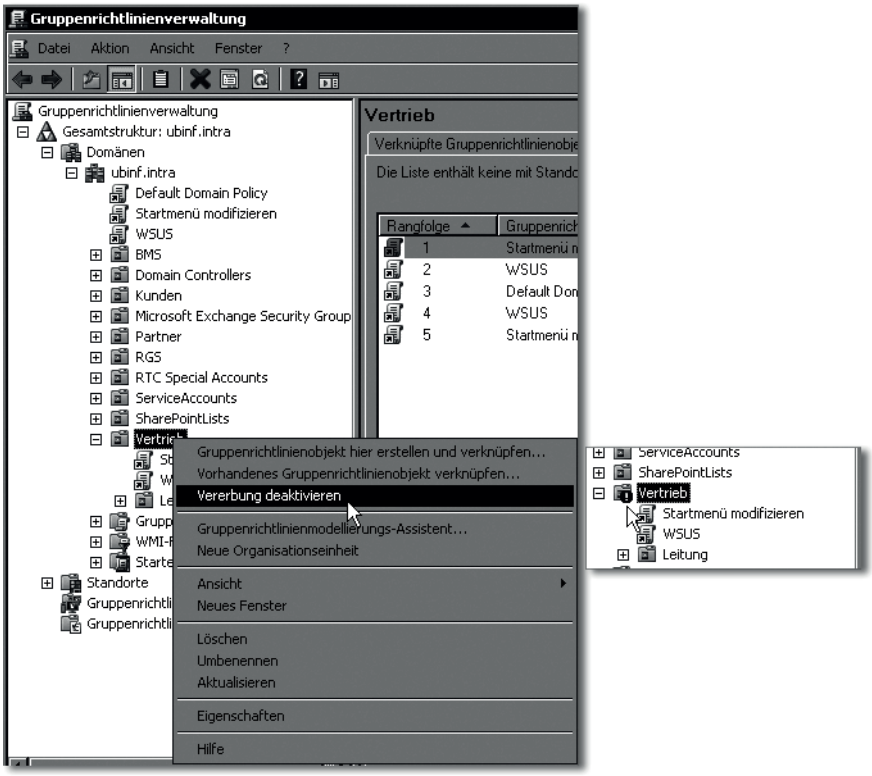


Abbildung 8.106 Die Vererbung der Gruppenrichtlinien kann deaktiviert werden. Ist für eine OU die Vererbung deaktiviert, wird sie mit einem kleinen blauen Ausrufezeichen versehen (rechts).

Gruppenrichtlinienverwaltung

Den Umgang mit dem Konfigurationswerkzeug GRUPPENRICHTLINIENVERWALTUNG zeige ich recht ausführlich in Abschnitt 8.4.11, »Zuweisen und Bearbeiten von Gruppenrichtlinien«. Dort sehen Sie auch, wie man mit dem Werkzeug anzeigt, welche Gruppenrichtlinienobjekte in einer OU tatsächlich angewendet werden.

Abbildung 8.107 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:

- Oberhalb einer OU könnte eine andere OU angesiedelt sein, in jedem Fall ist über einer OU eine Domäne.
- In der physikalischen Struktur des Active Directory gibt es keinen übergeordneten Standort oder »Unterstandort« – Standorte befinden sich sozusagen alle auf derselben Hierarchieebene. Daher kann es auch keine Vererbung geben, was wiederum bedeutet, dass die Einstellung VERERBUNG DEAKTIVIEREN nicht relevant und darum nicht vorhanden ist.

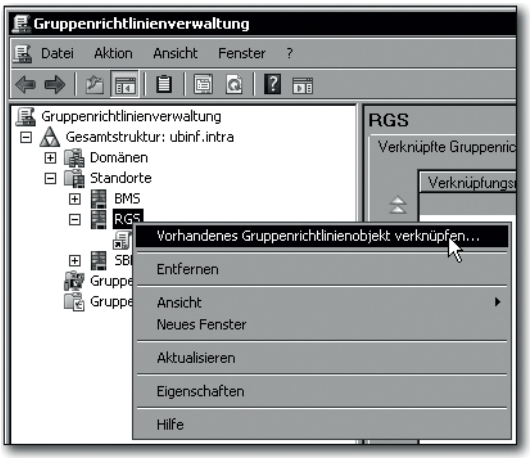


Abbildung 8.107 Bei Standorten gibt es kein »Vererbung deaktivieren«.

Ansonsten gilt auch bei Gruppenrichtlinienobjekt-Verknüpfungen für Standorte, dass bei überlappenden Einstellungen die in der Liste höher angeordnete Einstellung »gewinnt«.

8.4.5 Sicherheit und Vorrang

Wie alle anderen Objekte im Active Directory hat auch ein Gruppenrichtlinienobjekt Sicherheitseinstellungen. Standardmäßig können AUTHENTIFIZIERTE BENUTZER ein Gruppenrichtlinienobjekt lesen (Abbildung 8.108). 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 an dem Standort eine Verknüpfung vorhanden ist. Man könnte sich folgendes Szenario überlegen:

- Für die Organisationseinheit *Vertrieb* wird ein Gruppenrichtlinienobjekt angelegt. Genauer gesagt: 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.

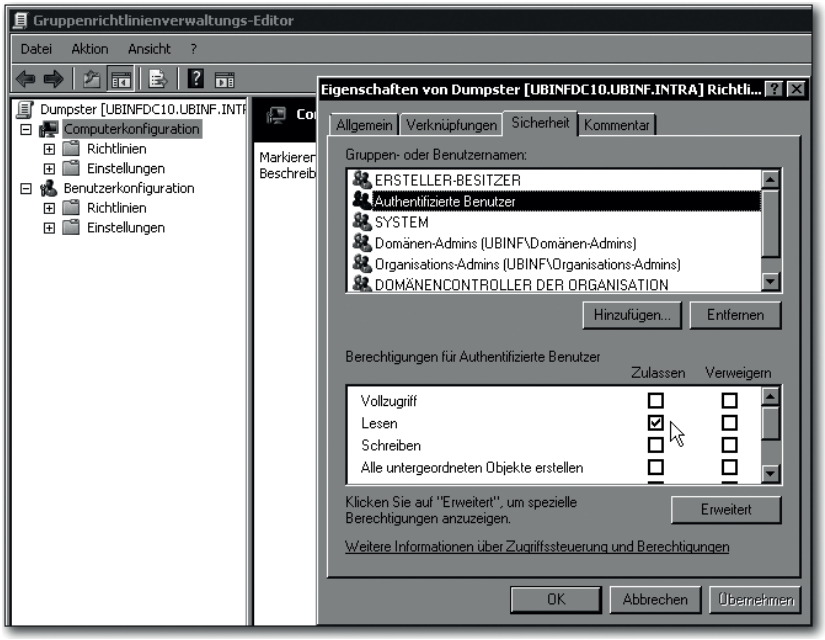


Abbildung 8.108 Auch die Gruppenrichtlinienobjekte sind mit Sicherheitseinstellungen versehen.

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«, können Sie diesen Weg gehen, es sollte aber eine Ausnahme bleiben.

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 8.109).

Hinweis

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 legen Sie mittels einer Verknüpfung auf ein Gruppenrichtlinienobjekt fest, 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 *Verknüpfungs*option (!) 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 8.109 bietet weiterhin die Möglichkeit, eine Verknüpfung zu deaktivieren.

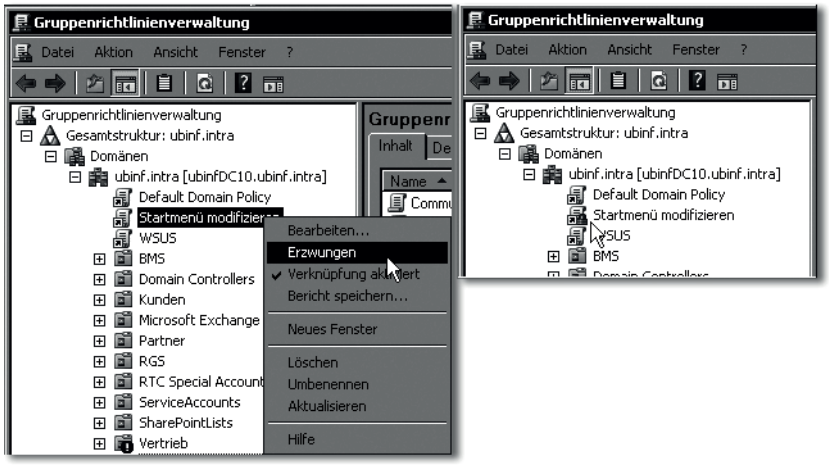


Abbildung 8.109 Ist die Option »Erzwungen« gesetzt, können vererbte Gruppenrichtlinien-Einstellungen nicht mehr überschrieben werden. Eine entsprechend konfigurierte Verknüpfung wird mit einem kleinen Schloss angezeigt.

8.4.6 Filter

Eine weitere Möglichkeit, 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 Betriebssystem-Gegebenheiten. 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.

8.4.7 Abarbeitungsreihenfolge, mehr Details

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 (GPOs) aufzuteilen. Hierdurch wird es einerseits übersichtlicher, andererseits verbessert sich auch die Wiederverwendbarkeit des einzelnen GPOs.

Wenn Sie also, wie in Abbildung 8.110 gezeigt, 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« getroffene Änderungen überschreibt.

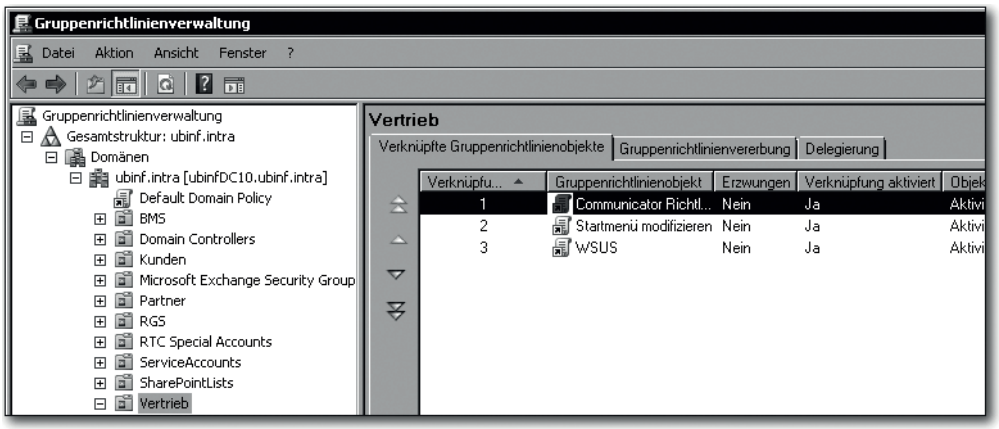


Abbildung 8.110 Wenn Sie mehrere Verknüpfungen zu Gruppenrichtlinienobjekten angelegt haben, ist deren Reihenfolge wichtig.

Nun dürfte der »Überschreiben-Fall« eigentlich nie auftreten – wenn er es doch tut, würde ich empfehlen, zunächst dieses organisatorische Problem zu lösen. Auf der Abbildung habe ich drei Verknüpfungen vorgenommen, nämlich zu einem GPO mit Richtlinien für Office Communicator, einem zur Modifikation des Startmenüs und einem 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 dieses Verfahren 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 8.111): 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, dessen Einstellungen also »gelten«, sofern nicht zuvor für eine bestimmte Einstellung das Attribut *Erzwungen* gesetzt worden ist.

Gruppenrichtlinienmodellierung

Wenn Sie intensiver »forschen« möchten, bietet auch die Ansicht GRUPPENRICHTLINIENVERERBUNG zu wenige Details, sondern nur erste Anhaltspunkte. Genauere Informationen liefert die Funktion GRUPPENRICHTLINIENMODELLIERUNG, die später vorgestellt wird. Alte AD-Hasen kennen diese Funktion als RICHTLINIENERGEBNISSATZ.

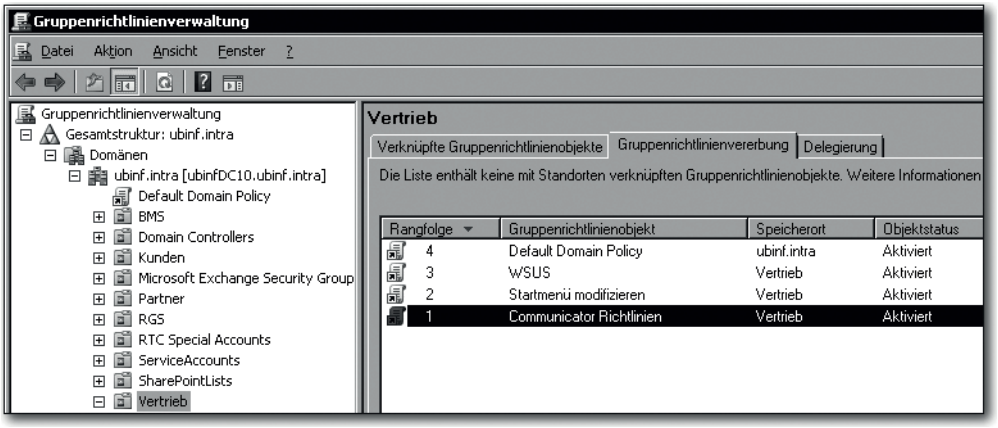


Abbildung 8.111 Auf der Registerkarte »Gruppenrichtlinienvererbung« gibt es einen Schnellüberblick über die Reihenfolge der Abarbeitung.

8.4.8 Lokale GPOs (ab Windows Vista und Windows Server 2008)

Die Betriebssysteme ab Windows Vista und Windows Server 2008 kennen vier lokale Gruppenrichtlinienobjekte (GPOs), mit denen erstaunlicherweise Einstellungen des lokalen Computers konfiguriert werden können:

- das lokale Richtlinienobjekt (Local Policy Object)
- ein GPO für Administratoren und eines für Nicht-Administratoren
- ein benutzerspezifisches lokales 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 Sie zusätzliche Einstellungen vornehmen müssen.

Das Konfigurieren der lokalen Gruppenrichtlinien funktioniert letztendlich nicht anders als bei den »normalen« Active Directory-basierten Richtlinien. Natürlich 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 Server ab Windows Server 2008 sehen die Dialoge aber genauso aus.

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 Gruppenrichtlinenobjekt Lokaler Computer (Abbildung 8.112). Das war's schon.

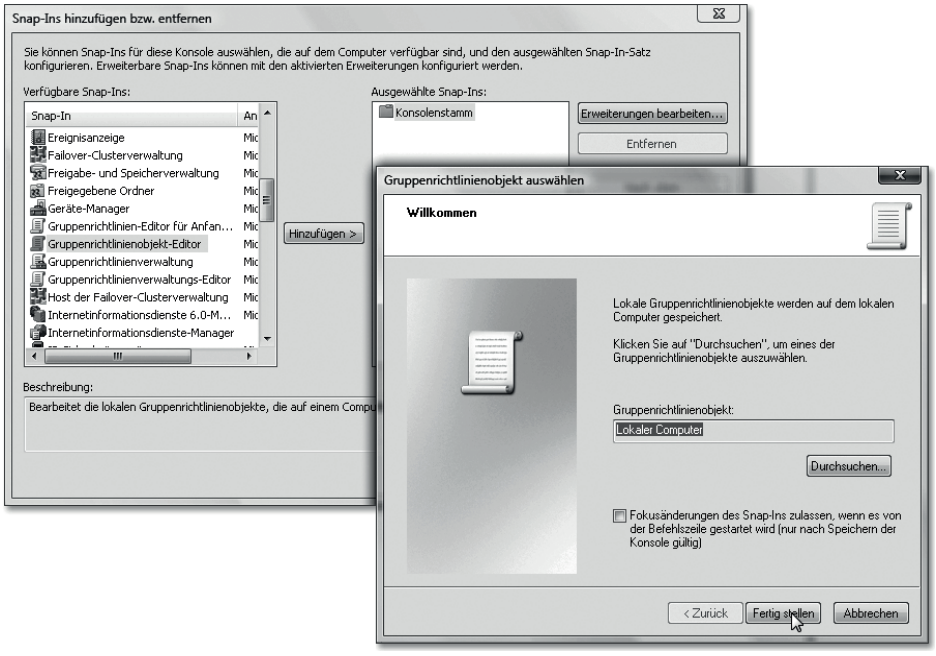


Abbildung 8.112 Um das lokale Richtlinienobjekt zu bearbeiten, öffnen Sie die entsprechende Konsole.

In Abbildung 8.113 sehen Sie die geöffnete lokale Richtlinie. Bezüglich der Konfiguration ist es in der Tat ein »ganz normales« GPO, in dem sowohl Computer- als auch Benutzereinstellungen vorgenommen werden können.

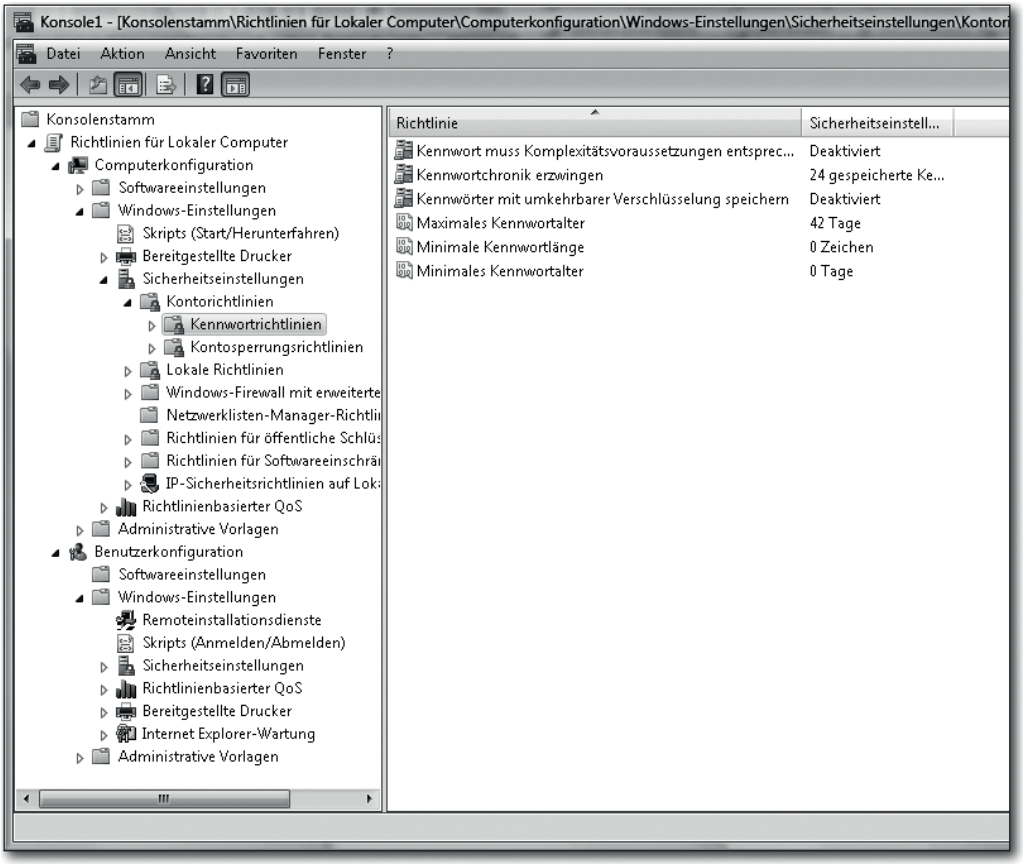


Abbildung 8.113 Das Bearbeiten der »Richtlinien für Lokaler Computer«. Im Grunde genommen ist es ein ganz normales GPO.

GPO für Administratoren und Nicht-Administratoren bearbeiten

Das 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 bzw. NICHT-ADMINISTRATOREN entscheiden (Abbildung 8.114).

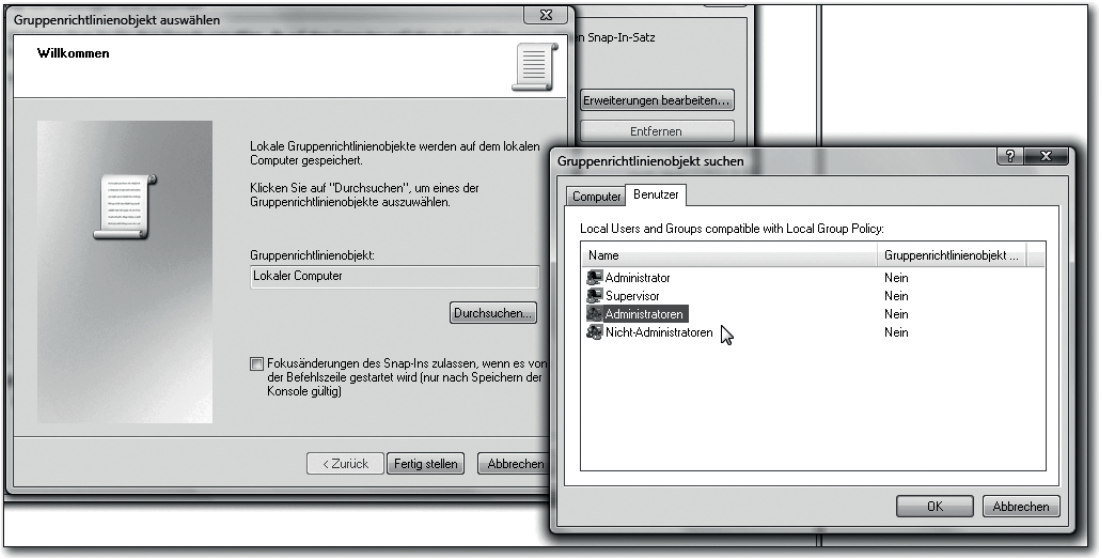


Abbildung 8.114 In diesem Dialog lassen sich die Gruppen »Administratoren« und »Nicht-Administratoren« sowie einzelne Benutzer auswählen.

In Abbildung 8.115 habe ich beide Richtlinien in einer Konsole geöffnet (dazu habe ich einfach zweimal das Snap-In mit unterschiedlichen Einstellungen hinzugefügt). Zu erkennen ist, dass es »nur« Benutzereinstellungen gibt – schließlich handelt es sich hierbei um eine reine Benutzer-GPO.

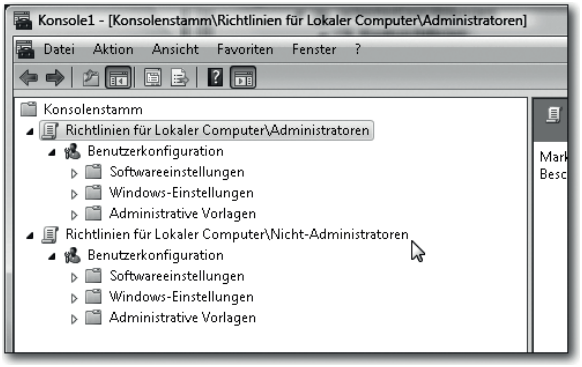


Abbildung 8.115 Hier werden die Einstellungen für lokale Administratoren und lokale Nicht-Administratoren zur Bearbeitung angezeigt.

Benutzerspezifische GPOs

Um ein lokales benutzerspezifisches GPO zu erstellen, beginnen Sie wie in dem zuvor gezeigten Fall. In dem Dialog aus Abbildung 8.114 entscheiden Sie sich für den Benutzer, für den die Richtlinie erstellt werden soll.

Zu beachten ist, dass Sie hier lediglich aus lokalen Benutzern auswählen können. Eine spezielle lokale Richtlinie für einen bestimmten Domänenbenutzer können Sie leider nicht erstellen.

8.4.9 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, muss in jeder Domäne ein Gruppenrichtlinienobjekt angelegt werden.

Mit Windows Server 2008 haben Sie eine Möglichkeit, um das »Immer-Wieder-Abtippen« von bestimmten Einstellungen zu vermeiden – die Lösung lautet Starter-Gruppenrichtlinienobjekte (Starter-GPO). 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.

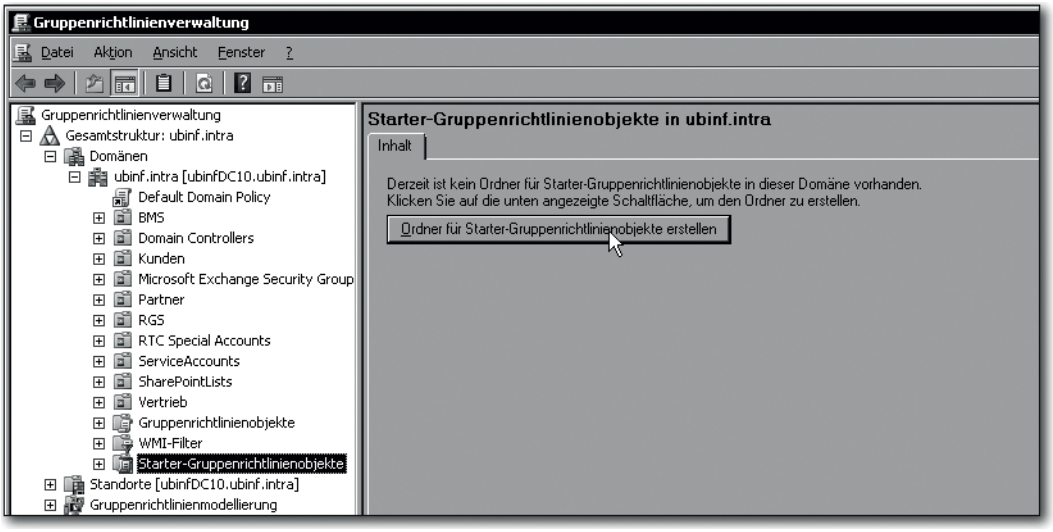


Abbildung 8.116 Beim ersten Anzeigen des Knotens »Starter-Gruppenrichtlinienobjekte« wird das Anlegen eines Ordners angeboten.

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 8.116). Der Erstellungs-

vorgang, den Sie per Mausklick auslösen, läuft ohne weitere Eingaben oder sonstige vom Administrator auszuführende Aktionen ab.

Anlegen

Um ein neues Starter-Gruppenrichtlinienobjekt zu erstellen, wählen Sie zunächst im Kontextmenü des Starter-Gruppenrichtlinienobjekt-Containers den Menüpunkt NEU (welche Überraschung). Der sich daraufhin öffnende Dialog ist maximal unspektakulär, denn Sie können nur einen Namen und einen Kommentar eingeben (Abbildung 8.117).

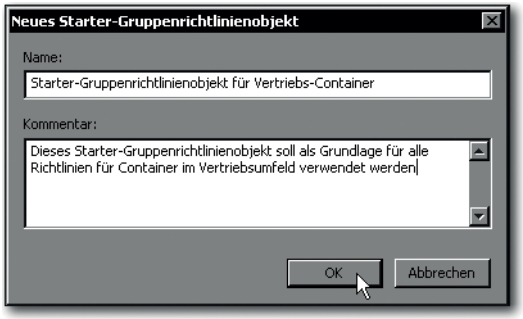


Abbildung 8.117 Das Anlegen eines neuen Starter-GPOs – nicht wirklich spektakulär

Die eigentliche Arbeit beginnt, wenn das neue Objekt angelegt ist. Sie wählen dann in dessen Kontextmenü den Menüpunkt BEARBEITEN (Abbildung 8.118).

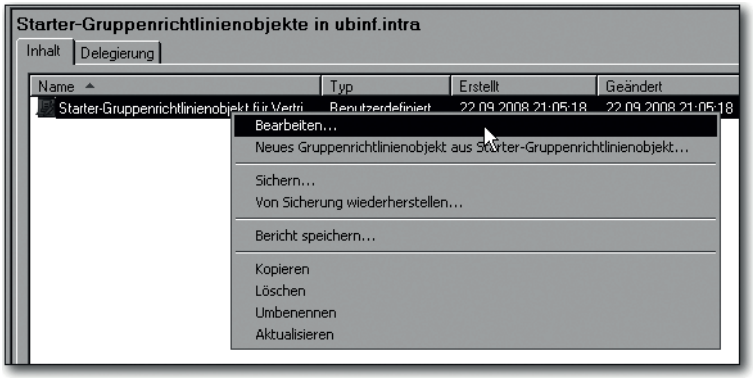


Abbildung 8.118 Das neu angelegte Starter-GPO-Objekt kann nun bearbeitet werden.

Das Bearbeiten der Einstellungen des Starter-Gruppenrichtlinienobjekts geschieht mit einer etwas modifizierten Version des Gruppenrichtlinien-Editors. Sie sehen in Abbildung 8.119 die im Grunde bekannte Applikation, in der sowohl der Knoten COMPUTERKONFIGURATION als auch der Knoten BENUTZERKONFIGURATION vorhanden ist. Sie können aber »nur« ADMINISTRATIVE VORLAGEN bearbeiten.

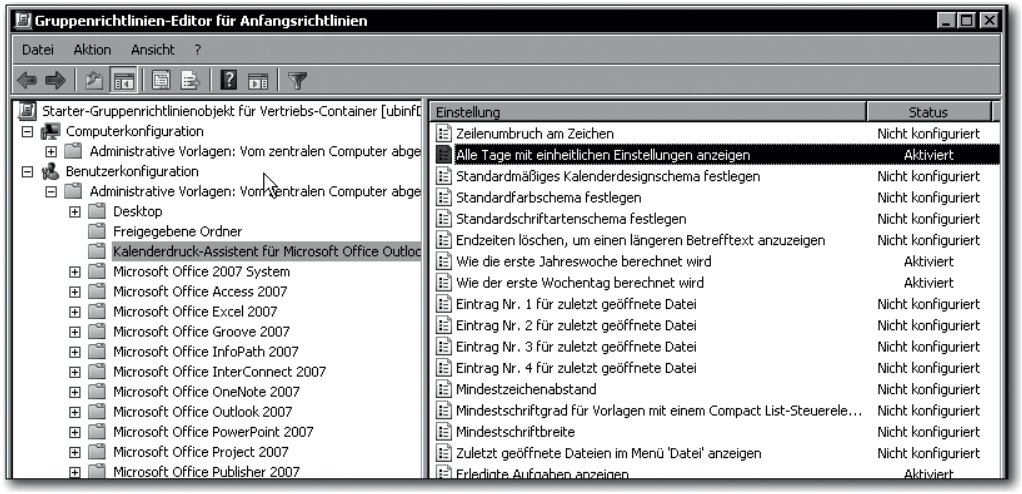


Abbildung 8.119 Das Bearbeiten der Starter-GPOs erfolgt wie gewohnt im Gruppenrichtlinien-Editor. Es gibt allerdings »nur« den Knoten »Administrative Vorlagen«.

Wenn Sie die gewünschten Einstellungen vorgenommen haben, können Sie den Editor verlassen und das Starter-Gruppenrichtlinienobjekt verwenden.

Anwenden

Um ein neues Gruppenrichtlinienobjekt aus einem Starter-Gruppenrichtlinienobjekt zu erstellen, wählen Sie im Kontextmenü des letztgenannten den entsprechenden Menüpunkt (Abbildung 8.120).

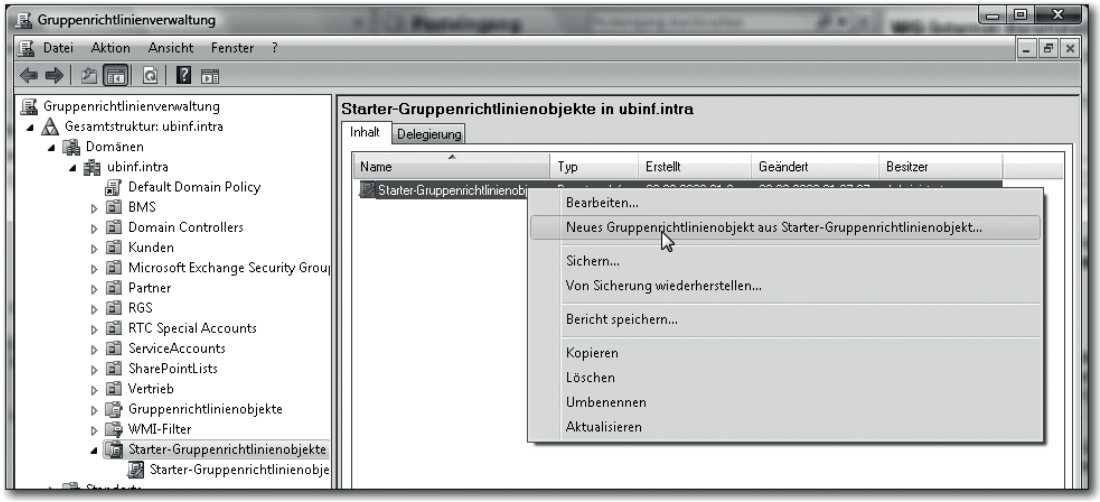


Abbildung 8.120 So wird ein neues Gruppenrichtlinienobjekt aus dem Starter-GPO erstellt.

Die einzige Eingabe, die nun von Ihnen verlangt wird, ist die Festlegung eines Namens für das neue GPO (Abbildung 8.121).

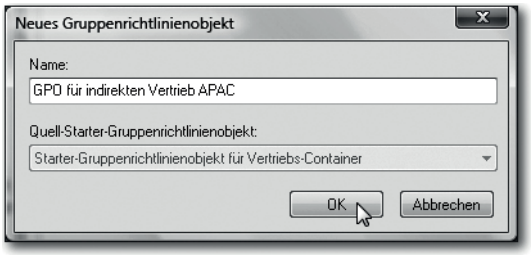


Abbildung 8.121 Bei der Erstellung des neuen Gruppenrichtlinienobjekts muss lediglich der Name angegeben werden.

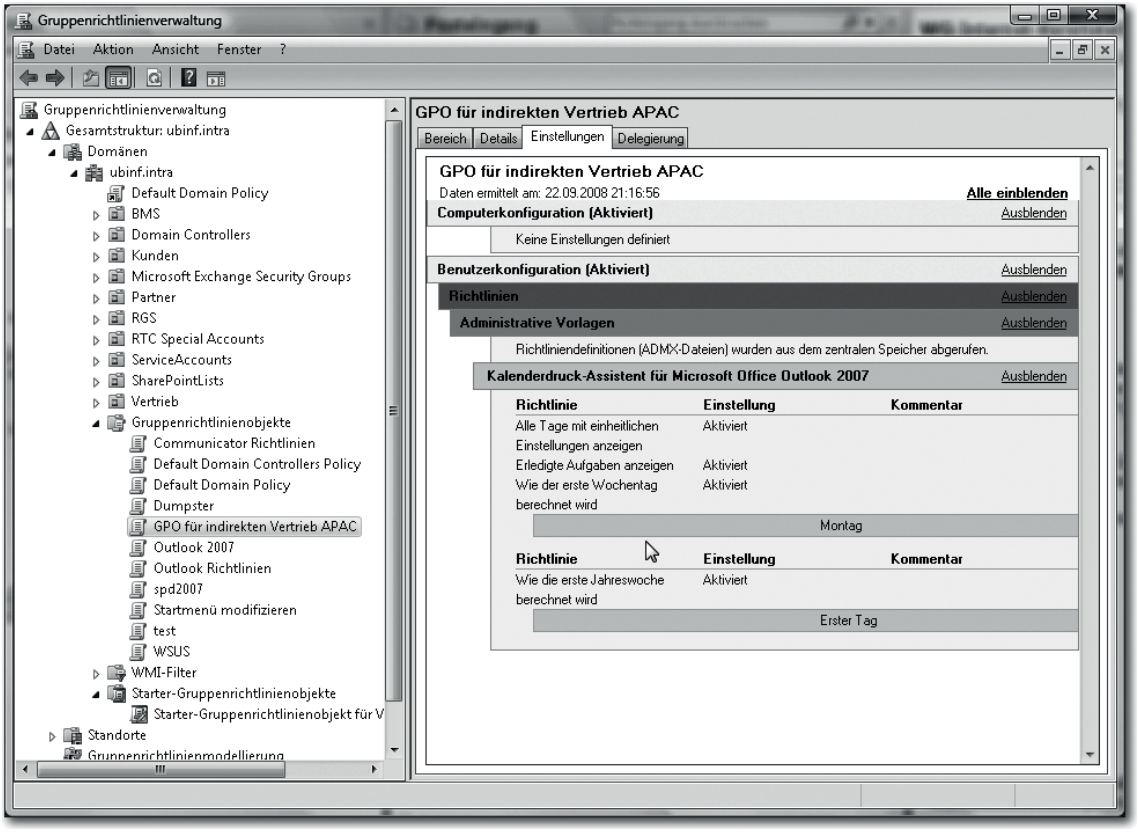


Abbildung 8.122 Et voilà: Alle Einstellungen sind in dem neuen Objekt vorhanden. Es kann nun noch modifiziert und dann einer OU zugewiesen werden.

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 8.122).

Nun können Sie bei Bedarf noch die ein oder andere Ergänzung oder Änderung vornehmen und dann die Verknüpfungen mit den OUs (oder der Domäne oder den Standorten) erstellen. Fertig.

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 angenehmerweise 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 8.123).

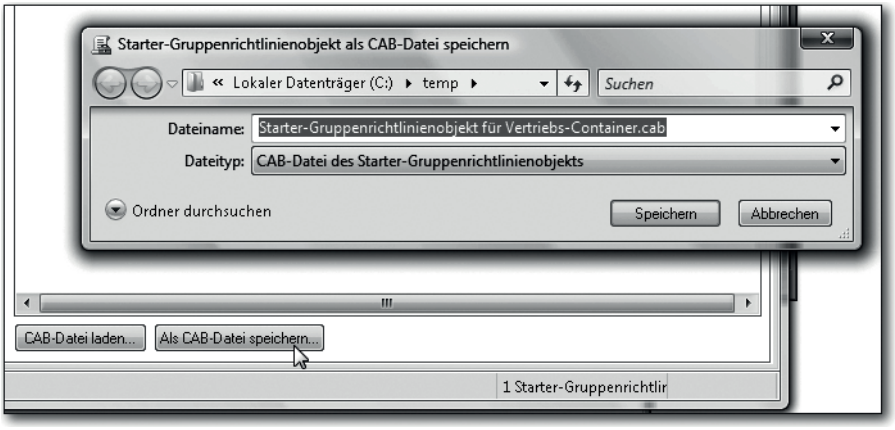


Abbildung 8.123 Das Starter-Gruppenrichtlinienobjekt kann als CAB-Datei gespeichert werden.

- Beim Laden des Starter-Gruppenrichtlinienobjekts wird die gesicherte CAB-Datei herangezogen. Der in Abbildung 8.124 gezeigte Dialog ermittelt einige grundlegende Angaben aus der CAB-Datei und kann über die Schaltfläche EINSTELLUNGEN ANZEIGEN sogar eine Art »Preview« des zu ladenden Objekts ausgeben.

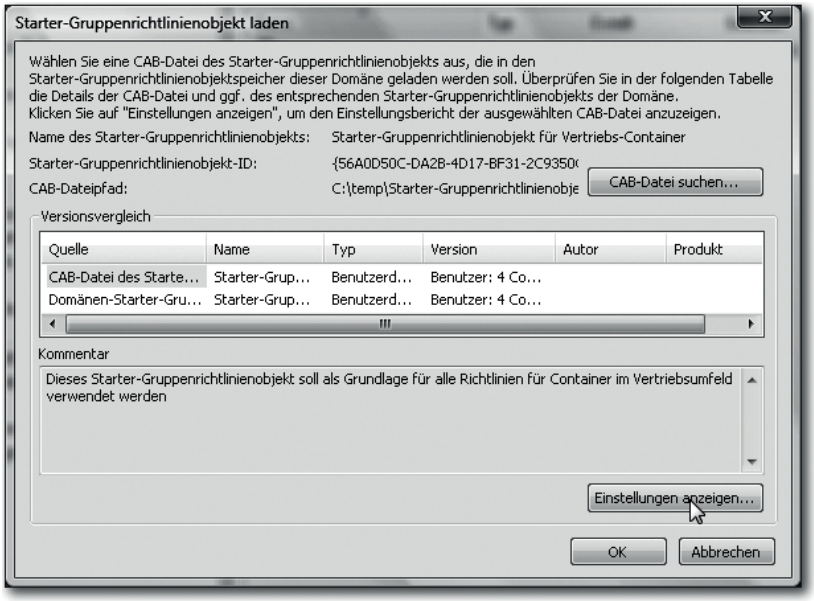


Abbildung 8.124 Eine Wiederherstellung des Starter-Gruppenrichtlinienobjekts ist ebenfalls einfach möglich. Vor der Wiederherstellung kann man sich mittels »Einstellungen anzeigen« einen Überblick darüber verschaffen, was überhaupt »drinsteht«.

8.4.10 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 vom Administrator-PC aus, konfiguriert werden können.

Seit nunmehr knapp 14 Jahren, genauer gesagt seit Februar 2000 mit der Einführung von Windows 2000, werden die administrativen Vorlagen in **.adm*-Dateien gespeichert. Das 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 hat Microsoft die administrativen Templates in ein neues XML-basiertes Format überführt, nämlich in die ADMX-Dateien.

Kapitel 20
Hochverfügbarkeit

Gegen Kalchas zuerst mit drohendem Blicke begann er:
Unglücksseher, der nie auch ein heilsames Wort mir geredet!
Immerdar nur Böses erfreut dein Herz zu verkünden!
Gutes hast du noch nimmer geweissagt, oder vollendet!
Jetzt auch meldest du hier als Götterspruch den Achaiern

In den Anfangszeiten der PC-basierten Server war ein (zeitlich begrenzter) Ausfall letztendlich zu verschmerzen. Die Systeme waren halt gemeinsame Festplatten und konnten den gemeinsamen Drucker bedienen, und darauf konnte man auch schon einmal ein paar Stunden verzichten. Mittlerweile sind die Windows Server in den meisten Unternehmen das Rückgrat der IT-Landschaft, sodass ein Ausfall irgendwo zwischen »sehr ärgerlich« und »katastrophal« rangiert.

Es ist daher sehr verständlich, dass IT-Verantwortliche bestrebt sind, alle Server möglichst ausfallsicher auszulegen. Bei den wichtigsten Servern wird dazu auch gern ein wenig tiefer in die »Trickkiste« gegriffen.

Wenn es darum geht, eine verbesserte Verfügbarkeit eines Servers (oder besser: des darauf laufenden Diensts) zu realisieren, gibt es verschiedene Ansätze:

- Beim Stichwort *Hochverfügbarkeit* denken die meisten Leser vermutlich an den »klassischen Cluster«, bei dem mehrere Knoten einen gemeinsamen Datenbereich (*Shared Storage*) nutzen, auch als *Failover-Cluster* bekannt. Typische Anwendungsfälle sind beispielsweise Dateidienste oder Datenbankserver.
- Die Hochverfügbarkeit kann auch in der Netzwerkschicht realisiert werden: Sind mehrere gleichartige Server vorhanden, werden die Anforderungen der Clients beim Ausfall eines Servers einfach an den oder die verbliebenen Systeme geleitet. Ein typisches Beispiel sind Webserver, die nicht geclustert, sondern über *Network Load Balancing* (NLB) redundant gemacht werden.
- Etliche Funktionen werden allein schon dadurch redundant, dass sie auf mehreren Servern vorhanden sind. Die Paradebeispiele dafür sind das Active Directory oder DNS. Sind mehrere Domänencontroller vorhanden, replizieren diese die Daten. Fällt ein Domänencontroller aus, finden die Clients automatisch einen der anderen DCs.

- Es gibt Applikationsserver, die Hochverfügbarkeit mit ihren Bordmitteln, also ohne Mithilfe des Betriebssystems, realisieren. Ein typisches Beispiel dafür ist die Datenbankspiegelung von SQL Server 2005/2008.

20.1 Vorüberlegungen

Bevor es »so richtig« losgeht, möchte ich Ihnen einige grundlegende Gedanken nahebringen, die mit der technischen Umsetzung eines Hochverfügbarkeitsszenarios zunächst (noch) nichts zu tun haben.

»Hochverfügbarkeit« ist zwar als Begriff in aller Munde, dennoch erscheint es mir wichtig, zu prüfen, was ein Unternehmen oder eine Organisation wirklich benötigt – und wie viel Geld dafür ausgegeben werden kann.

Natürlich können Sie ein System aufbauen, das auch zur Planung und Durchführung der bemannten Mondlandung geeignet wäre. Wenn diese Anforderungen allerdings nicht bestehen, wäre es Geldverschwendung, trotzdem dementsprechend zu investieren. Anders gesagt: Sie könnten das Geld in wesentlich sinnvollere IT-Projekte investieren, als eine Verfügbarkeit aufzubauen, die vom Business nicht benötigt wird.

Ich habe übrigens auch deutlich mehr als einen Fall erlebt, in dem die Geschäftsleitung »Hochverfügbarkeit« bestellt hat – und als dann die ersten Kostenschätzungen über 250.000 € ins Haus flatterten, war doch alles nicht mehr so wichtig. Die Schlussfolgerung ist nicht, dass man, wenn man nicht gerade die Bank von England ist, lieber gleich die Finger von Hochverfügbarkeitsprojekten lässt, sondern dass man sehr genau prüfen sollte, welchen Wert eine bessere Verfügbarkeit der Systeme für das Business hat, und dementsprechende Vorschläge ausarbeitet.

Wenn das Hochverfügbarkeitsprojekt die Geld bringenden Geschäftsprozesse betrifft, ist zumindest in mittleren und größeren Unternehmen auch eine Investition von 500.000 € (und mehr) sicherlich kein Problem. Ist nur ein »Nebensystem« betroffen, dessen Ausfall keine signifikanten Auswirkungen auf das Business hat, werden Sie vermutlich keine 5.000 € dafür bekommen.

20.1.1 Allgemeines

Eine wesentliche Anforderung an eine moderne IT-Umgebung ist die Verfügbarkeit derselben. Zunächst muss man sich allerdings darüber klar werden, was nun genau unter »Verfügbarkeit« zu verstehen ist.

ITIL subsumiert unter »Availability« diese Aspekte:

- Zuverlässigkeit
- Wartbarkeit

- Servicefähigkeit
- IT-Sicherheit

Betrachtet man diese Anforderungen von einem etwas technischeren und serverbezogenen Standpunkt, kann man folgende Punkte nennen:

- Die Systeme müssen stabil laufen.
- Im Fall eines eventuellen Ausfalls muss eine möglichst schnelle Wiederherstellung gewährleistet sein.
- Geplante Ausfälle durch Wartungsarbeiten müssen so kurz wie möglich sein.
- Es dürfen keine Daten verloren gehen.

Die Anforderungen erscheinen zunächst so trivial wie selbstverständlich. An den im Folgenden beschriebenen Szenarien werden Sie allerdings erkennen, dass die Realisierung alles andere als einfach ist.

Der Worst-Case-Fall

Bei den Betrachtungen zur Verfügbarkeit müssen wir stets vom schlimmsten Störfall, also dem Worst Case, ausgehen. Ein Konzept, das nicht diesen ungünstigsten Fall zugrunde legt, hat letztendlich keinen Wert.

Der Worst Case ist nun nicht zwangsläufig die Landung einer Boeing 747 im Serverraum – vermutlich hätte ein Unternehmen dann ohnehin andere Probleme. Der Worst Case ist im Fall eines Servers beispielsweise ein Ausfall des RAID-Controllers, was zu einem Verlust der gespeicherten Daten führt. Das heißt, die Daten liegen zwar noch auf den Platten, können aber nicht gelesen werden.

Wiederherstellungszeit

Zunächst betrachten wir das Szenario der Wiederherstellung eines Servers, dessen lokale Plattensysteme so ausgefallen sind, dass ein Restore der Daten notwendig wird. Dies könnte beispielsweise im Fall eines RAID-Controller-Defekts vorkommen. Wir gehen von einem Fileserver mit einer Nutzkapazität von 300 GByte aus.

In Abbildung 20.1 ist der Vorgang auf einem Zeitstrahl dargestellt:

- Um 10:00 fällt das System aus.
- Kurz danach werden die ersten Störmeldungen eingehen. Bis die Ursache des Problems »Ich kann keine Dokumente mehr speichern« klar ist und die notwendigen Schritte eingeleitet worden sind, vergeht mit Sicherheit eine Stunde. Schließlich ist nicht ständig ein IT-Mitarbeiter in Wartestellung, und wahrscheinlich wird zunächst eine Behebung des Fehlers versucht werden etc.

  Ausfallzeit bis hierhin: 1 Stunde

- Sofern ein Servicevertrag für die Instandsetzung der Hardware vorliegt, wird diese nach sechs Stunden wieder funktionsbereit sein. Eine Wiederherstellungszeit von sechs Stunden ist der schnellste »Standard-Service-Level«, der gemeinhin von Herstellern und Systemhäusern angeboten wird. (Ein Servicevertrag, der eine *Reaktionszeit* von vier Stunden garantiert, ist weniger wert als einer mit sechs Stunden *Wiederherstellungszeit*.)
  Ausfallzeit bis hierhin: 7 Stunden
- Ist die Hardware wieder funktionsbereit, wird ein gewisser Zeitraum, sagen wir eine Stunde, vergehen, bis tatsächlich mit der Rücksicherung begonnen werden kann. Schließlich muss die Backup-Software betriebsbereit gemacht werden, wahrscheinlich müssen Bänder herausgesucht werden – kurzum: Einige Vorbereitungen müssen getroffen werden.

  Ausfallzeit bis hierhin: 8 Stunden

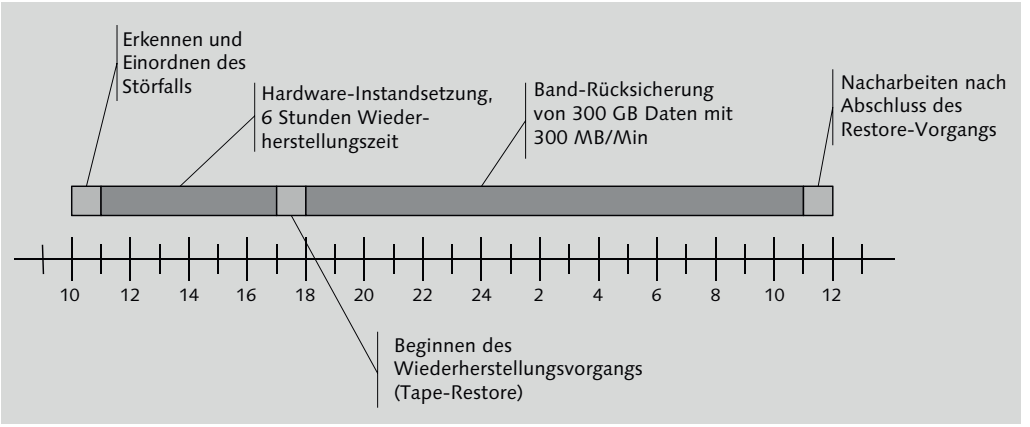


Abbildung 20.1 Wiederherstellung eines Systems

- Nun beginnt die eigentliche Rücksicherung. Eine Restore-Geschwindigkeit von 300 MByte/min ist eine realistische Annahme (wenn Sie nicht gerade die komplette Backup-Hardware erneuert haben), woraus sich ergibt:

  (300 GByte × 1.024) ÷ 300 MByte = 1.024 min = 17,07 Stunden

  Es muss also von einer Restore-Zeit von ungefähr 17 Stunden ausgegangen werden.
  Ausfallzeit bis hierhin: 25 Stunden
- Nach Abschluss des Restore-Vorgangs müssen sicherlich noch einige »Nacharbeiten« vorgenommen werden. Dies wird bei einem Fileserver nicht sehr umfangreich sein, daher ist eine Stunde ein realistischer Schätzwert.

  Ausfallzeit bis hierhin: 26 Stunden

Dieses einfache Beispiel zeigt recht eindrucksvoll, welche enormen Risiken in den IT-Systemen stecken: Ein Ausfall eines kritischen Systems von mehr als 24 Stunden kann für viele

Firmen akut existenzbedrohend sein, zumindest dürfte er als massive Störung angesehen werden.

Letztendlich ist der zuvor geschilderte Ablauf noch recht optimistisch gewesen. Wenn während des Vorgangs – bei welchem Arbeitsschritt auch immer – Probleme auftreten, verlängert das die Restore-Zeiten eventuell deutlich.

Wenn Sie Optimierungspotenzial suchen, finden sich zwei Ansätze:

- die Beschleunigung der Hardwarewiederherstellung
- die Beschleunigung der Rücksicherung

Ersteres lässt sich eventuell mit im Unternehmen gelagerter Ersatzhardware erreichen. Es stellt sich hierbei allerdings die Frage, ob jederzeit ein Mitarbeiter zur Verfügung steht, der Hardwareprobleme eines Servers erkennen und beheben kann.

Die Beschleunigung der Rücksicherung ist natürlich ebenfalls möglich. Schnellere Backup-Hardware und sehr performante Serversysteme ermöglichen zwar höhere Restore-Geschwindigkeiten, dennoch bleibt eine Rücksicherung größerer Datenmengen eine zeitaufwendige Angelegenheit.

Folgende Schlussfolgerung ergibt sich aus dieser Betrachtung für den Worst-Case-Fall:

- Sofern ein Server bzw. dessen Applikationen nicht länger als beispielsweise vier oder sechs Stunden ausfallen dürfen, ist dies mit einem »normalen« Backup/Restore-Szenario nicht zu schaffen.
- Vielleicht wird – entweder aus finanziellen Gründen oder weil die Verfügbarkeit für bestimmte Systeme lediglich eine untergeordnete Rolle spielt – entschieden, keine erweiterten Maßnahmen zu ergreifen. In diesem Fall sollte unbedingt schriftlich festgestellt und kommuniziert werden, dass es im Worst-Case-Fall zu längeren Ausfällen kommen kann.

Um das Szenario eines längeren Ausfalls ein wenig anschaulicher zu gestalten, hier ein Beispiel: Ich habe, sozusagen als externer Beobachter, einen zweitägigen Ausfall eines Exchange-Systems in einem Unternehmen erlebt. Dies führte nicht nur dazu, dass ca. 1.500 Benutzer keine Mails mehr schreiben und empfangen konnten. Viel wesentlicher war, dass die Kalenderinformationen nicht mehr zur Verfügung standen. Zu internen Meetings oder Kundenterminen erschienen nur noch diejenigen Mitarbeiter, die ihre Daten regelmäßig auf ein Smartphone repliziert hatten.

Datenverlustzeit

In vielen mittelständischen Unternehmen wird die Wiederherstellung der Systeme nicht mit so hoher Wichtigkeit belegt. Viel entscheidender ist es häufig, sicherzustellen, dass keine Daten verloren gehen.

Betrachten wir ein Szenario auf dem Zeitstrahl (Abbildung 20.2):

- Die Datensicherung ist um 6 Uhr abgeschlossen.
- Um 8 Uhr nehmen die Benutzer die Arbeit auf und verändern die Daten.

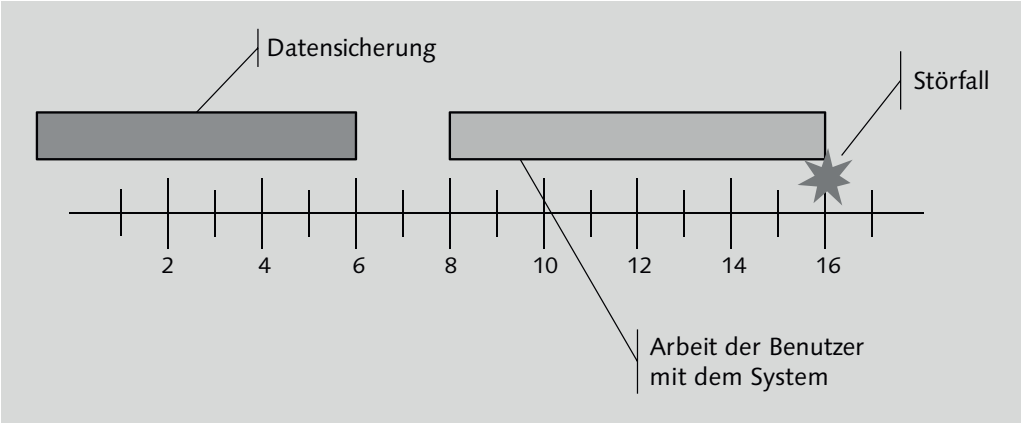


Abbildung 20.2 Die Datenverlustzeit

- Am Nachmittag um 16 Uhr tritt ein Störfall auf. Dieser fällt in die Kategorie »Worst Case«, es werden also beispielsweise die Festplattensysteme »verloren« (d.h., die Daten sind zumindest nicht mehr zu lesen).
- Wenn keine zusätzlichen Sicherungsmaßnahmen getroffen werden, bedeutet dies, dass die in diesen acht Stunden produzierten Daten verloren sind (von 8 bis 16 Uhr).

Bei der Betrachtung des Datenverlusts sind zwei Fälle zu beachten:

- reproduzierbare Daten
- nicht reproduzierbare Daten

Beispiele für reproduzierbare Daten wären Buchungen von Eingangsrechnungen (die Papierrechnungen liegen ja noch vor und werden nochmals eingebucht) oder eine CAD-Zeichnung, die natürlich auch ein zweites Mal angefertigt werden kann.

Nicht reproduzierbar sind beispielsweise empfangene Mails (wenn man nicht zufällig kurz vor dem Ausfall des Systems seinen Posteingang eingesehen hat, weiß man ja nicht, wer geschrieben hat, und kann daher nicht nachfragen) oder die Auftragseingangsdaten eines Webshops.

Wenn die Anforderung an die IT-Abteilung herangetragen wird, dass ein Verlust von Daten auf einigen oder sogar allen Systemen nicht tragbar ist, müssen weitergehende Maßnahmen ergriffen werden; ein normales Backup/Restore-Konzept ist eindeutig nicht ausreichend.

Man sollte sich nicht von der scheinbaren Sicherheit täuschen lassen, die redundant ausgelegte Server oder mit RAID-Leveln konfigurierte Plattensysteme vorspiegeln: Wir sprechen

bei den Überlegungen zur Verfügbarkeit grundsätzlich vom Worst Case, und dieser könnte so aussehen, dass das gesamte Festplattensystem irreparabel beschädigt wird.

Probleme durch logische Fehler

Die zuvor beschriebenen Szenarien basierten jeweils auf einem Hardwareausfall. Natürlich ist auch ein Ausfall wegen eines Problems des Softwaresystems denkbar, beispielsweise eines Konsistenzproblems der Datenbank. Für diesen Fall müssen natürlich ebenfalls planerische Vorkehrungen getroffen werden.

Letztendlich gelten hier die gleichen Fragen, nämlich innerhalb welches Zeitraums die Funktion des Systems wiederhergestellt werden muss und ob ein Verlust von Daten tolerierbar ist.

Bei der Besprechung logischer Fehler denkt man zunächst an Inkonsistenzen in der Datenbank, fehlerbehaftete Software oder versehentlich durch den Benutzer gelöschte Dateien. Zu berücksichtigen ist natürlich auch der Fall eines Vireneinbruchs, bei dem ein komplettes Filesystem innerhalb von wenigen Minuten irreparabel »verseucht« werden kann.

Sie sehen, dass es vielerlei »Gefahren« für die Verfügbarkeit eines IT-Systems gibt, die berücksichtigt werden müssen.

Bewertung der Systeme

Zumeist werden die höchsten Verfügbarkeitsanforderungen nicht an alle Serversysteme gestellt werden. Um die IT-Kosten zumindest einigermaßen im Griff zu behalten, wird man die Systeme unterschiedlichen Kategorien zuordnen, innerhalb deren eine bestimmte Verfügbarkeitsstufe definiert ist:

- Die »beste« Stufe könnte beispielsweise sowohl eine Wiederherstellungs- als auch eine Datenverlustzeit von maximal zwei Stunden definieren. Hier würde man beispielsweise Server für das ERP-System, die Lagerverwaltung und die Kommunikation (Exchange) definieren – Letzteres, weil die Collaboration-Systeme in einem modernen Unternehmen zunehmend in die Prozesse integriert sind und diese darüber hinaus ein wesentliches Werkzeug für die Kommunikation mit Kunden geworden sind.
- Eine mittlere Verfügbarkeitsstufe, beispielsweise eine Wiederherstellungs- und Datenverlustzeit von maximal acht Stunden, käme für ein SharePoint-System, einen Fileserver oder diverse Datenbankanwendungen wie etwa ein Angebotssystem in Betracht. Ein Ausfall dieser Systeme ist zwar für ein Unternehmen unangenehm, aber nicht direkt existenzgefährdend.
- Eine vergleichsweise geringe Verfügbarkeit könnte man für Systeme wie den Zeiterfassungsserver oder ein Softwareverteilungssystem ansetzen. Moderne Zeiterfassungssysteme (Terminals) können für eine gewisse Zeit die erfassten Daten zwischenspeichern. Das Softwareverteilungssystem ist unkritisch, weil im ungünstigen Fall ein oder zwei Tage

keine neuen Softwarepakete verteilt werden können, was zumeist kein Problem darstellen sollte. Die Wiederherstellungs- und Datenverlustzeit könnte man mit 24 bis 48 Stunden beziffern.

Je nach den Anforderungen Ihres Unternehmens werden Sie die Verfügbarkeiten der genannten Dienste vielleicht anders bewerten. Die Beispiele zeigen aber in jedem Fall, wie differenziert unterschiedliche Systeme bewertet werden müssen.

Störfall vs. Notfall

Wenn Sie individuell für Ihr Unternehmen planen, welche Verfügbarkeit für welche von Servern bereitgestellte Funktion benötigt wird, werden Sie auf den Unterschied zwischen *Störfall* und *Notfall* treffen:

- Ein *Störfall* ist ein begrenztes, auf einen Server bezogenes Problem. Der Ausfall eines Netzteils, des gesamten Plattensubsystems oder auch des ganzen Servers mit unbekanntem Grund ist ein Störfall.
- Unter einem *Notfall* verstehen wir ein wesentlich umfangreicheres Problem, wie einen Brand oder Hochwasser am Hauptsitz der Firma, in dem auch die IT-Systeme untergebracht sind. Für ein Unternehmen mit mehreren Niederlassungen wird es von Interesse sein, zusätzlich zu dem »Problem« mit der Zentrale nicht auch noch die eventuell deutschland-, europa- oder gar weltweit verteilten Niederlassungen vollkommen lahmzulegen, weil die EDV nicht mehr arbeitet. Ein Notfallkonzept, das möglichst schnell die wesentlichen Dienste wieder bereitstellt, ist also dringend notwendig. Allerdings wird man hier vermutlich die Wiederherstellungs- und Datenverlustzeit anders definieren als bei einem Störfall, bei dem nur ein einzelnes System betroffen ist.

Wenn Sie bei einem kleinen Unternehmen tätig sind, bei dem alle Mitarbeiter an einem Standort sitzen, werden Sie sicherlich nun denken, dass Sie ganz andere Sorgen als die Verfügbarkeit der Daten haben, wenn Ihr Büro durch ein Feuer eliminiert wird. Auf den ersten Blick mag diese Einschätzung richtig sein, auf den zweiten Blick werden Sie feststellen, dass zumindest einige grundlegende Vorkehrungen für den Notfall getroffen werden müssen: Irgendwann wird die Firma wieder arbeitsfähig sein. Wenn dann überhaupt keine Daten mehr zur Verfügung stehen, weil auch sämtliche Datensicherungen ein Raub der Flammen geworden sind, wird es für die Firma unter Umständen unmöglich sein, den Geschäftsbetrieb wieder aufzunehmen. Auch die Hausbank wird sich beispielsweise bei der Vergabe eines Kredits dafür interessieren, ob Vorkehrungen für den Notfall getroffen worden sind: Wenn die Versicherung zwar die Sachwerte ersetzt, der Geschäftsbetrieb aber mangels Unternehmensdaten nicht mehr aufgenommen werden kann, wird die Firma auch nicht mehr in der Lage sein, die Kredite zu bedienen.

Im mittelständischen Bereich werden die Anforderungen für den Notfall sicherlich niemals die Qualität der Service-Level erreichen, die für den Störfall definiert sind. In einem Szenario

für eine Firma mit mehreren Außenstandorten könnte man definieren, dass grundlegende IT-Funktionen nach drei oder vier Tagen wieder zur Verfügung stehen sollen; der wichtigste Punkt ist, dass eine möglichst aktuelle ausgelagerte Datensicherung existiert. Die Datenverlustzeit wird letztendlich darüber definiert, wie oft diese ausgelagerte Datensicherung aktualisiert wird.

Auch für einen Kleinbetrieb ist es von entscheidender Notwendigkeit, dass die Datenbestände regelmäßig auf extern aufbewahrte Medien geschrieben werden. Das »kleinste Notfallkonzept der Welt« könnte so aussehen, dass der Geschäftsführer täglich das Band mit der Datensicherung mit nach Hause nimmt; auf diese Weise kann zumindest innerhalb weniger Tage auf einem relativ aktuellen Informationsstand weitergearbeitet werden.

20.1.2 Hardware und Konfiguration

Der vorherige Abschnitt vermittelt vielleicht etwas zu sehr den Eindruck, dass die Vorsorgemaßnahmen vor allem auf Katastrophen aller Art abzielen – vom Großbrand bis zum Flugzeugabsturz.

Die meisten Verfügbarkeitsprobleme werden allerdings von wesentlich weniger spektakulären Ereignissen ausgelöst, z. B. durch Probleme mit der Hardware.

Um es einmal ganz drastisch und unfreundlich zu sagen: Wer Billighardware beschafft, braucht sich nicht zu wundern, wenn die Ergebnisse (d. h. die Stabilität der Systeme) unbefriedigend sind. Auch NT4, das von der Codequalität bei Weitem nicht so gut war wie Windows Server 2008, läuft auf stabiler Hardware mehrere Jahre am Stück – mir sind diverse Beispiele bekannt. Mir sind aber ebenfalls Fälle bekannt, in denen der »Server« aus einzelnen Komponenten im Eigenbau zusammengebastelt wurde und sich dann alle wunderten, dass es ständig Bluescreens gab.

Fakt ist: Ein Serverbetriebssystem gehört auf vernünftige Hardware. Wer beim Kauf der Server auf die »großen vier« Hersteller (HP, Dell, IBM, Fujitsu Siemens) setzt, wird deutlich bessere Ergebnisse erzielen als mit B-Marken oder Selbstbausystemen. Ja, ich weiß, der Preis ist auch nicht zu vernachlässigen. Allerdings ist ein instabiler Server auch das vermeintlich »gesparte« Geld nicht wert!

Einige weitere Aspekte zum Thema »Verfügbarkeit und Hardware«:

- *Überwachung der Hardware*: Häufig lassen sich aufkommende Störungen bereits frühzeitig erkennen. Ein Beispiel: Moderne Festplatten können einem Management-System mitteilen, wenn in absehbarer Zeit ein Ausfall zu erwarten ist (Abbildung 20.3). Wer solche Meldungen nicht auswertet, handelt grob fahrlässig!
- *Halten Sie Ersatzhardware vor*: Was passiert, wenn Sie bei einem Hardwareausfall einfach keine Ersatzhardware haben oder kurzfristig bekommen können, brauche ich wohl nicht weiter auszuführen, oder?

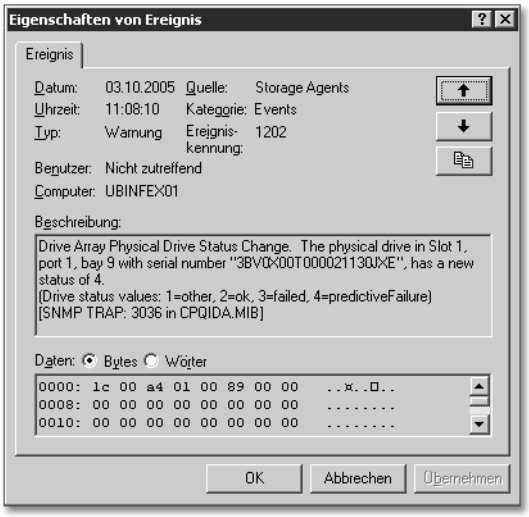


Abbildung 20.3 Eine Serverplatte meldet einen vermutlich bald auftretenden Fehler. Wer solche Meldungen ignoriert, handelt grob fahrlässig und gefährdet die Verfügbarkeit des Systems!

- *Sorgen Sie für ein optimales Sizing der Server*: Systeme, die ständig am Rand des Performanceabgrunds stehen, sind erfahrungsgemäß nicht sonderlich stabil. Da neben der Stabilität auch das Antwortverhalten und generell die Geschwindigkeit (aus Sicht der Benutzer) in die Bewertung eingehen, sollten Sie derlei Aspekte ebenfalls bedenken – und kontrollieren!

Ebenso wichtig wie die Hardware des Servers ist die Konfiguration. Hier gilt nach wie vor die alte Weisheit: *Trennen Sie die Dienste*.

Es ist wirklich keine neue Erkenntnis, aber man kann es nicht oft genug wiederholen: Die Systeme werden nicht stabiler, wenn Sie täglich einen Praxistest durchführen, um festzustellen, wie viele unterschiedliche Applikationsserver auf einer Betriebssysteminstallation ausgeführt werden können. Neben dem Aspekt der »Stabilität« sind bei solchen Systemen auch Administration, Pflege und Wiederherstellung vergleichsweise kompliziert!

Das Designziel »ein Dienst – ein Server« muss heute nicht mehr in einer gnadenlosen Materialschlacht enden. Durch Virtualisierung ist es möglich, mehrere Instanzen des Betriebssystems auf einer Hardware auszuführen – und dabei noch Verbesserungen bei der Wiederherstellungszeit zu erreichen (siehe den nächsten Abschnitt).

Einige weitere Hinweise:

- *Überwachung der Betriebssysteme und Applikationsserver*: Sie überwachen die Hardware. Gut! Sie sollten allerdings auch die darauf laufenden Betriebssysteme und Applikationsserver überwachen. Wenn diese unbemerkt in einen »unglücklichen Betriebszustand« laufen, steuern Sie recht zielsicher den nächsten Ausfall an – und der ist sicherlich nicht nur für das gute Aussehen Ihrer Serververfügbarkeitsstatistik ungünstig.

Systeme wie der *Microsoft System Center Operations Manager* können hier wertvolle Hilfe leisten (Abbildung 20.4).

- *Halten Sie Datenträger, Seriennummern und Patchdateien griffbereit*: Wenn Sie trotz aller Vorsorgemaßnahmen einen Ausfall haben und mit der Wiederherstellung beginnen möchten, wäre das ein sehr unpassender Moment, um mit dem Aufräumen des »Gerümpelschranks« zu beginnen – und schließlich stellt sich noch heraus, dass der Open-Datenträger nebst Seriennummern gar nicht im Hause ist, weil der Praktikant vor zwei Monaten zu Hause etwas installieren wollte.

  Auch aus dem Internet bezogene Patches sollten lokal verfügbar sein, um schnell und ohne großartiges Suchen mit der Wiederherstellung beginnen zu können.

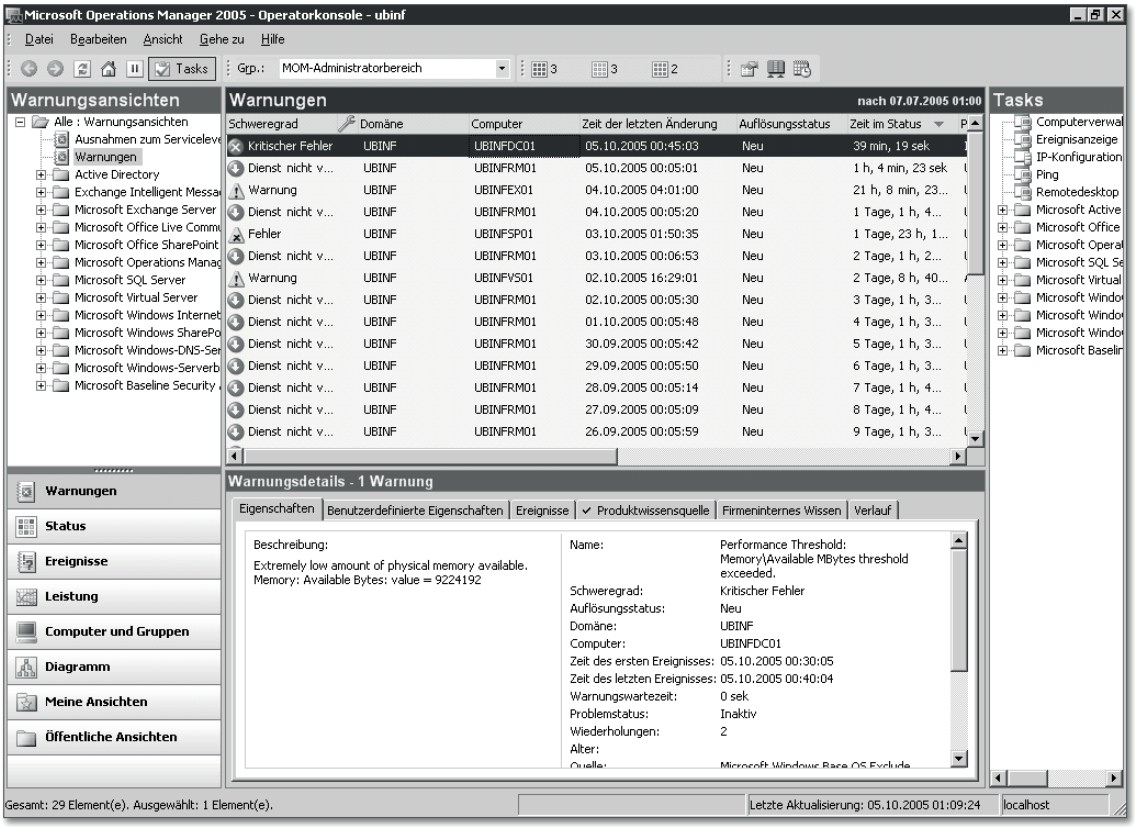


Abbildung 20.4 Ein professionelles Monitoring der Systeme auf Betriebssystem- und Applikationsserver-Level ist ohne ein entsprechendes Werkzeug nicht möglich. Das Bild zeigt die Operatorkonsole des Microsoft Operations Manager.

Zuletzt wären noch einige Sicherheitsaspekte zu nennen: Hierbei sind grundsätzlich Datenklau und Sabotage zu berücksichtigen. Sabotage hat natürlich unmittelbare Auswirkungen

auf die Verfügbarkeit der Systeme. Eine mangelhafte Verfügbarkeit resultiert eben nicht nur aus dem Ausfall von Hardware, sondern ebenso aus Sicherheitsproblemen. Hier wären unter anderem Viren und Trojaner zu nennen. Denken Sie beispielsweise an den SQL-Slammer, der massenhaft SQL Server lahmgelegt hat.

20.2 Failover-Cluster

Der »klassische« Cluster ist der Failover-Cluster, der natürlich auch in Windows Server 2012 vorhanden ist. Die Failover-Clusterunterstützung ist ein nachzuinstallierendes Feature (Abbildung 20.5).

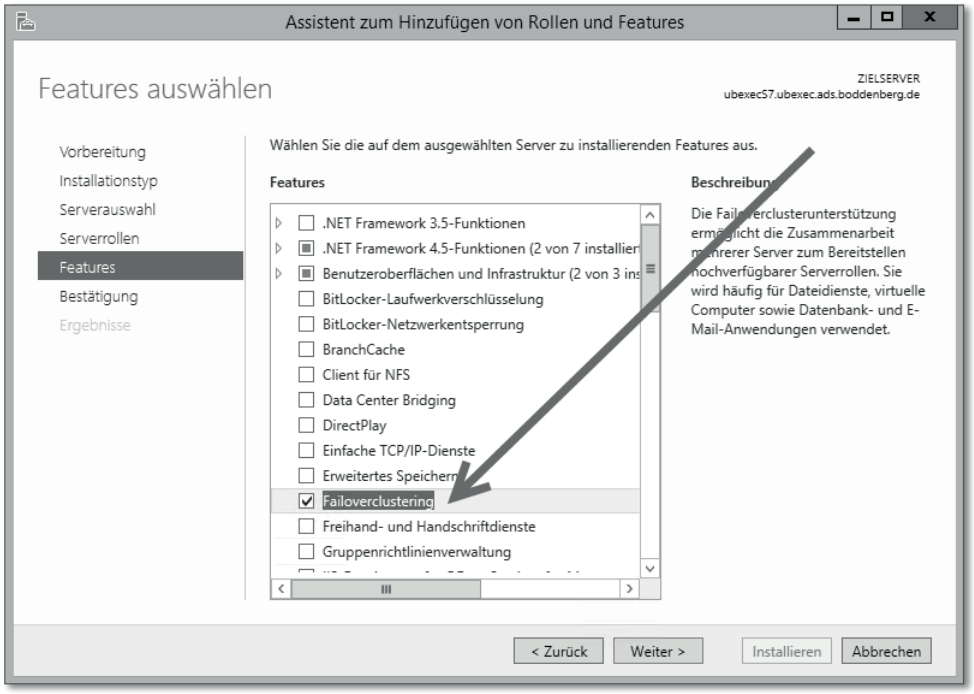


Abbildung 20.5 Das »Failoverclustering« ist ein Feature und wird dementsprechend installiert.

Zwei Hinweise

Der erste wichtige Hinweis dieses Abschnitts ist, dass ein Failover-Clustering auf den Clusterknoten die Enterprise Edition des Betriebssystems voraussetzt.

Der zweite Hinweis dieses Abschnitts ist, dass Sie prüfen sollten, ob ein Failover-Cluster mit gemeinsamem Speicher (Shared Storage) in Ihrem Anwendungsfall wirklich das Optimum ist. Alternative Ansätze sind beispielsweise:

- Der SQL Server 2005/2008/2012 bietet mit der *Datenbankspiegelung* eine sehr interessante Möglichkeit, um Datenbankserver nebst Festplattenspeicher redundant auszulegen, ohne dass Sie sündhaft teure Hardware beschaffen müssen.
- Exchange 2007/2010/2013 bietet mit der *Data Access Group* (*DAG* – vormals Clustered Continuos Replication, CCR) einen Hochverfügbarkeitsansatz, der zwar auf dem Failover-Cluster aufsetzt, aber ohne einen gemeinsamen Speicherbereich aufgebaut werden kann.

Ich möchte mit dieser Anmerkung nicht ausdrücken, dass Failover-Cluster mit gemeinsamem Speicherbereich »irgendwie schlecht« wären. Ich möchte aber sehr wohl darauf hinweisen, dass es durchaus andere Varianten gibt.

Ende 1997, also zur besten NT4-Zeit, veröffentlichte Microsoft einen Clusterdienst, der zur Entwicklungszeit *Wolfpack* genannt wurde – ein Rudel von Wölfen sorgt also für eine bessere Verfügbarkeit.

Der Microsoft-Cluster ist recht einfach zu verstehen (Abbildung 20.6):

- Der Cluster besteht aus mindestens zwei Knoten, die über einen gemeinsamen Festplattenbereich (Shared Storage) verfügen. Dieses Shared-Storage-System kann über Fibre Channel oder iSCSI angeschlossen sein. Paralleles SCSI wird unter Windows Server 2008 *nicht* mehr unterstützt.

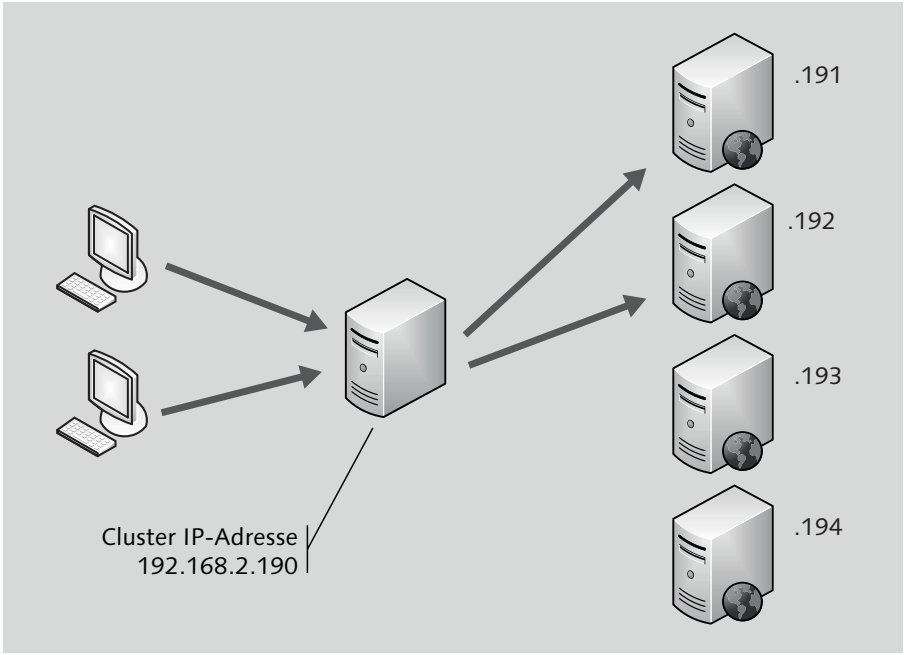


Abbildung 20.6 Das Prinzip des Clusters

- Die Benutzer greifen, zumindest gedanklich, nicht direkt auf einen der Clusterknoten zu, sondern kommunizieren mit einem »virtuellen Server«, der gewissermaßen vor dem physikalischen Clusterknoten angesiedelt ist. In Abbildung 20.6 ist dies zu sehen: Der Benutzer glaubt, dass er mit *alphaClust01. alpha.intra* kommuniziert. Da dieses System aber momentan auf *alphaCN1* ausgeführt wird, greift der Benutzer in Wahrheit auf diese Maschine zu. Der physikalische Server greift auf den Datenbereich auf dem Shared-Storage-System zu. Wenn *alphaCN1* ausfällt oder die Dienste gezielt auf *alphaCN2* geschwenkt werden, wird der Client auf diesen physikalischen Server zugreifen, der aber dieselbe Speicherressource und dort dieselben Daten nutzt.

Vorsicht

Ein Szenario, wie es in Abbildung 20.6 gezeigt wird, ist durchaus mit Vorsicht zu genießen: Einerseits wird natürlich der Ausfall eines Serverknotens abgefangen – der eigentlich viel schwerer wiegende Verlust des Speichersystems wird aber andererseits nicht abgedeckt. Nun argumentieren die Hersteller von Speichersystemen zwar, dass die Systeme unglaublich stabil und ausfallsicher arbeiten – es könnte aber trotzdem etwas passieren! Denken Sie an einen Kabelbrand, einen Wasserrohrbruch und dergleichen. Regel Nummer eins beim Entwurf von Hochverfügbarkeitslösungen lautet: »Traue keiner Komponente!«

Abschnitt 3.4 beschäftigt sich recht ausgiebig mit diesem Thema, sodass ich Sie auf diesen Teil des Buchs verweisen möchte.

Wie bereits weiter oben angesprochen wurde, könnten in Ihrem konkreten Fall vielleicht auch Ansätze interessant sein, die nicht auf einem gespiegelten Shared Storage beruhen, sondern die Daten auf Applikationsebene replizieren, also beispielsweise Exchange 2010/2013 DAG oder die Datenbankspiegelung von SQL Server 2005/2008/2012.

Einige weiterführende Anmerkungen:

- Der »virtuelle« Server, auf den die Clients zugreifen, besteht aus mehreren Clusterressourcen, die zu einer Gruppe zusammengefasst werden. Die Gruppe enthält mehrere Ressourcen, wie eine IP-Adresse, einen Rechnernamen, einen Festplattenbereich oder Ressourcen von Applikationsservern wie Exchange oder SQL Server.
- Clusterressourcen können nicht beliebige Dienste oder Programme sein, sondern müssen vom Softwarehersteller speziell auf den Betrieb im Cluster vorbereitet sein. Es ist insbesondere beim Einsatz von Zusatzprodukten zu prüfen, ob diese im Cluster laufen können oder zumindest »Cluster aware« sind. Ersteres bedeutet, dass das Produkt als Clusterressource ausgeführt werden kann. »Cluster aware« heißt, dass die Software zwar keine Clusterressource zur Verfügung stellt, aber stabil auf einem Clusterknoten läuft.
- Im Fehlerfall werden die Clusterressourcen des ausgefallenen Knotens auf dem anderen System gestartet. Dies kann durchaus einige Minuten dauern! Der Cluster sorgt also nicht für »Zero-Downtime«, sondern für eine »Only-a-few-minutes-Downtime«.

20.2.1 Aktiv vs. Passiv und n+1

Grundsätzlich können alle Clusterknoten aktiv sein, also eine Clusterressource ausführen. Es stellt sich allerdings immer die Frage, ob das wirklich die optimale Lösung ist. Abbildung 20.7 zeigt einen Zwei-Knoten-Cluster, bei dem beide Knoten aktiv sind: Fällt ein Clusterknoten aus, wird dessen Ressource auf den anderen Knoten geschwenkt und dort ausgeführt. Das Problem ist, dass dieser Knoten nun die ganze Last allein trägt, bei linearer Verteilung also doppelt so viel leisten muss. Da mehr als 100 % bekanntlich nicht geht, dürfen beide Knoten also jeweils nur zu 50 % ausgelastet sein. Und damit ist der Aktiv/Aktiv-Cluster schon gar nicht mehr so attraktiv.

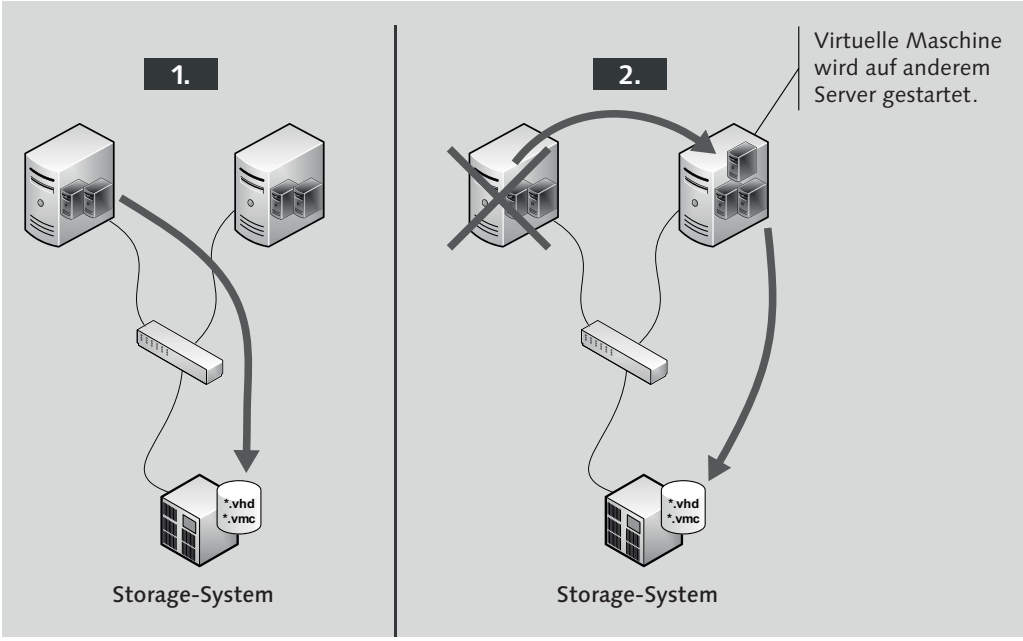


Abbildung 20.7 Bei einem Ausfall in einem Zwei-Knoten-Cluster trägt der verbliebene Knoten die volle Last.

Teilweise wird explizit empfohlen, Zwei-Knoten-Cluster nicht Aktiv/Aktiv, sondern Aktiv/Passiv auszulegen – ein Beispiel dafür ist Exchange Server 2003. Bei Exchange Server 2007 wurden Aktiv/Aktiv-Cluster gar nicht mehr unterstützt, sondern »nur« noch Aktiv/Passiv-Cluster. Die Aktiv/Aktiv-Konfigurationen haben sich in der Praxis schlicht und ergreifend nicht bewährt.

Falls Sie einen Cluster mit noch mehr Knoten benötigen, können Sie bis zu 16 Clusterknoten in einen Cluster einbinden. Bei Clustern, die aus mehr als zwei Knoten bestehen, fährt man grundsätzlich eine n+1-Konfiguration (Abbildung 20.8). Dabei führt einer der Knoten im normalen Betrieb keine Clusterressource aus. Erst im Fehlerfall übernimmt er die Ressource des ausgefallenen Knotens.

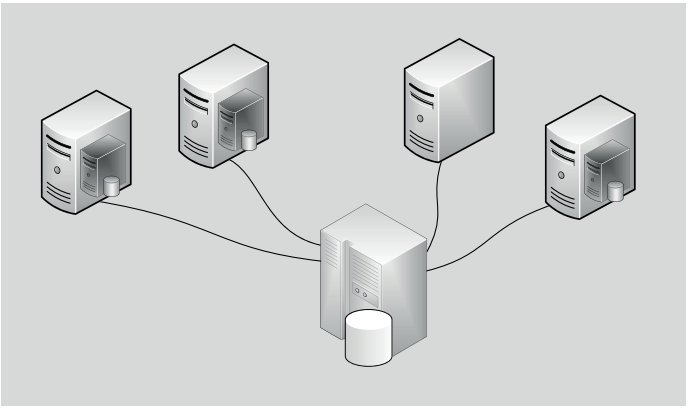


Abbildung 20.8 Bei einem Mehr-Knoten-Cluster bleibt ein Clusterknoten »frei«, um als Ziel für Failover-Vorgänge zu dienen. Man spricht von einer n+1-Konfiguration, in diesem Fall »3+1«.

20.2.2 Installation

Im Gegensatz zum Clusterdienst unter Windows Server 2003 ist als von den Clusterknoten gemeinsam genutzter Speicher kein paralleles SCSI mehr möglich, sondern nur noch Fibre Channel, iSCSI oder SAS (serielles SCSI, Serial Attached SCSI). Für eine Produktionsumgebung hat ohnehin niemand mehr Storage-Systeme über paralleles SCSI angebunden, aber für mit Virtualisierungsprodukten betriebene Testszenarien hat man diese Technologie häufig verwendet.

Wenn Sie zunächst das Clustering mit Windows Server 2012 in einer virtuellen Umgebung testen möchten, empfiehlt sich die Nutzung der iSCSI-Technologie (weil sie preiswerter ist).

iSCSI eignet sich übrigens nicht nur für das Testlabor, auch in der Produktionsumgebung hat sich iSCSI mittlerweile bewährt. Benötigt man höchste Verfügbarkeit und höchste Performance, wird man allerdings nach wie vor zu einem Fibre Channel-SAN tendieren.

Der erste Schritt der Installation besteht darin, dass Sie alle Clusterknoten mit ausreichend Konnektivität ausstatten. Je nachdem, wie Sie den Shared-Storage-Bereich anbinden, benötigen Sie folgende Konfiguration:

- Shared Storage via Fibre Channel:
  - 1 × LAN in Richtung Clients (besser redundant auslegen)
  - 1 × LAN für Heartbeat
  - 1 × FC-HBA für die Anbindung des Storage-Systems (besser redundant auslegen)
- Shared Storage via iSCSI:
  - 1 × LAN in Richtung Clients (besser redundant auslegen)
  - 1 × LAN für Heartbeat
  - 1 × iSCSI-LAN für die Anbindung des Storage-Systems (besser redundant auslegen)

Für iSCSI benötigen Sie also mindestens drei Netzwerkkarten. Das Schaubild aus Abbildung 20.9 verdeutlicht dies.

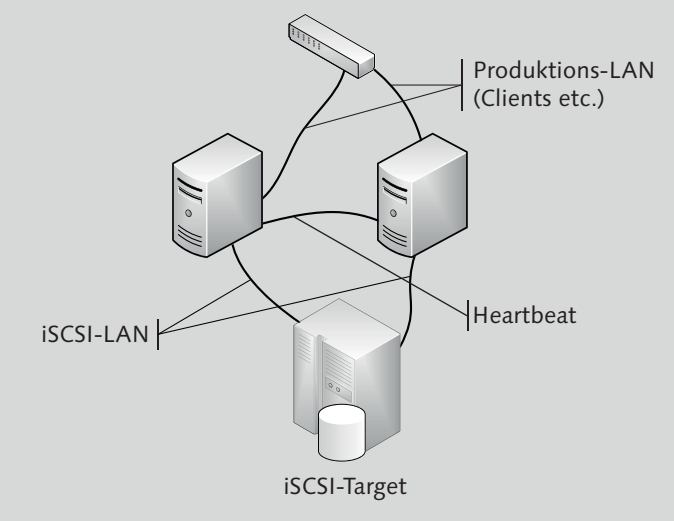


Abbildung 20.9 Ein Clusterknoten in einem iSCSI-Szenario benötigt mindestens drei Netzwerkkarten.

Die Knoten eines Clusters sollten nach Möglichkeit identisch, zumindest aber ähnlich dimensioniert sein.

Ich gehe davon aus, dass viele Leser bisher noch kein iSCSI installiert haben. Daher folgt hier ein kurzer Überblick. Bei iSCSI gibt es zwei Kernkomponenten:

- *iSCSI-Target*: Ein Target stellt Plattenressourcen zur Verfügung. Windows Server 2012 R2 enthält standardmäßig ein iSCSI-Target, das in diesem Buch auch vorgestellt wird. Diverse Hersteller bieten iSCSI-Targets als Hardwarelösung an. Zu nennen wären hier beispielsweise die Systeme von *Network Appliance*.
- *iSCSI-Initiator*: Der Initiator greift auf die vom Target bereitgestellten Ressourcen zu. Ein Initiator kann entweder ein Stück Software oder eine spezielle Netzwerkkarte sein.

Einrichtung des iSCSI-Targets

Erster Schritt ist das Einrichten des iSCSI-Datenträgers. Das Einrichten des eigentlichen Targets habe ich bereits im Dateisystem-Kapitel gezeigt, somit kümmern wir uns hier »nur« noch um den Datenträger. Sie werden eventuell mehrere iSCSI-Datenträger anlegen wollen. Zumindest müssen Sie einen kleinen Datenträger für das Cluster-Quorum anlegen – 1 GB genügt.

Hier die Vorgehensweise:

- Öffnen Sie im Server-Manager den Bereich iSCSI und starten Sie das Erstellen eines Neuen virtuellen iSCSI-Datenträgers (Abbildung 20.10).

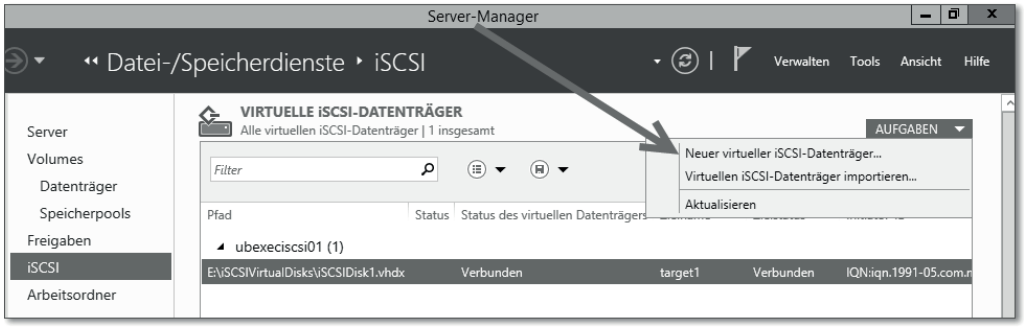


Abbildung 20.10 Anlegen eines neuen iSCSI-Datenträgers

- Auf Abbildung 20.11 sehen Sie das Festlegen der Größe des Datenträgers und die Auswahl des Typs.

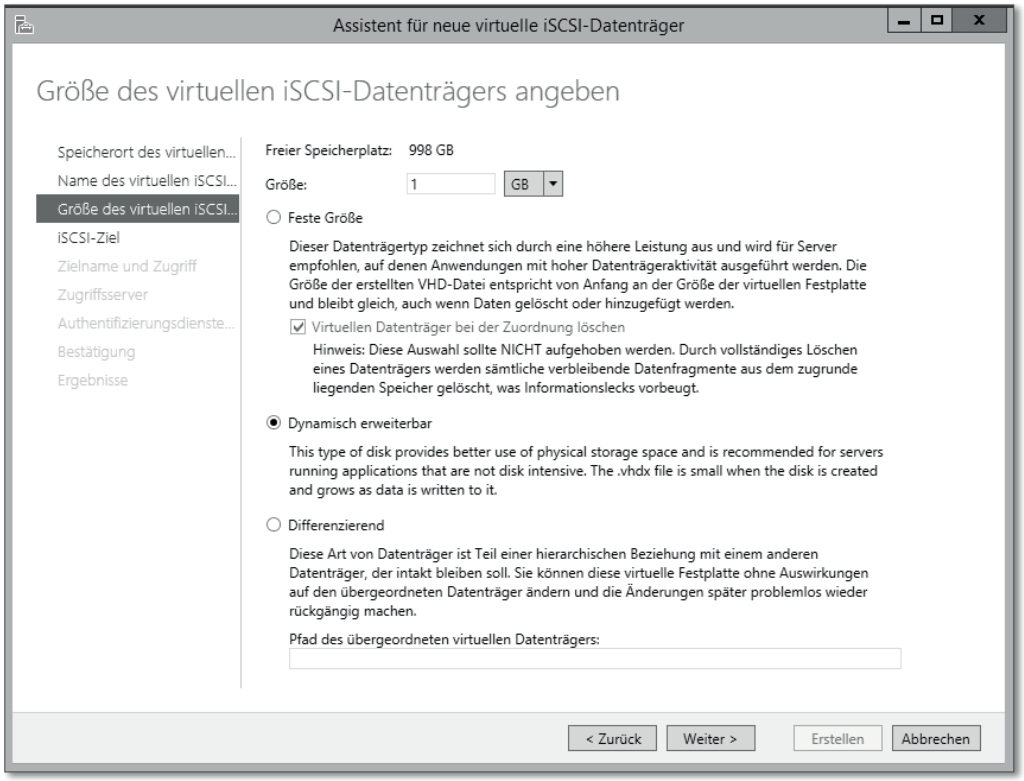


Abbildung 20.11 Für das Quorum reicht ein relativ kleiner Datenträger.

Der iSCSI-Datenträger wird einem Target zugeordnet, das in diesem Beispiel bereits vorhanden ist. Vermutlich werden Sie nochmal die Eigenschaften des iSCSI-Targets kontrollieren

und anpassen wollen. Der auf Abbildung 20.12 gezeigte Dialog befindet sich am unteren Ende des iSCSI-Dialogs im Server-Manager.

Abbildung 20.12 Das iSCSI-Target wird hier konfiguriert.

Ein allgemein notwendiger Konfigurationsschritt ist das Eintragen der iSCSI-Initiatoren, die auf das Taget zugreifen sollen. Hier müssen also die zukünftigen Cluster-Knoten eingetragen werden (Abbildung 20.13).

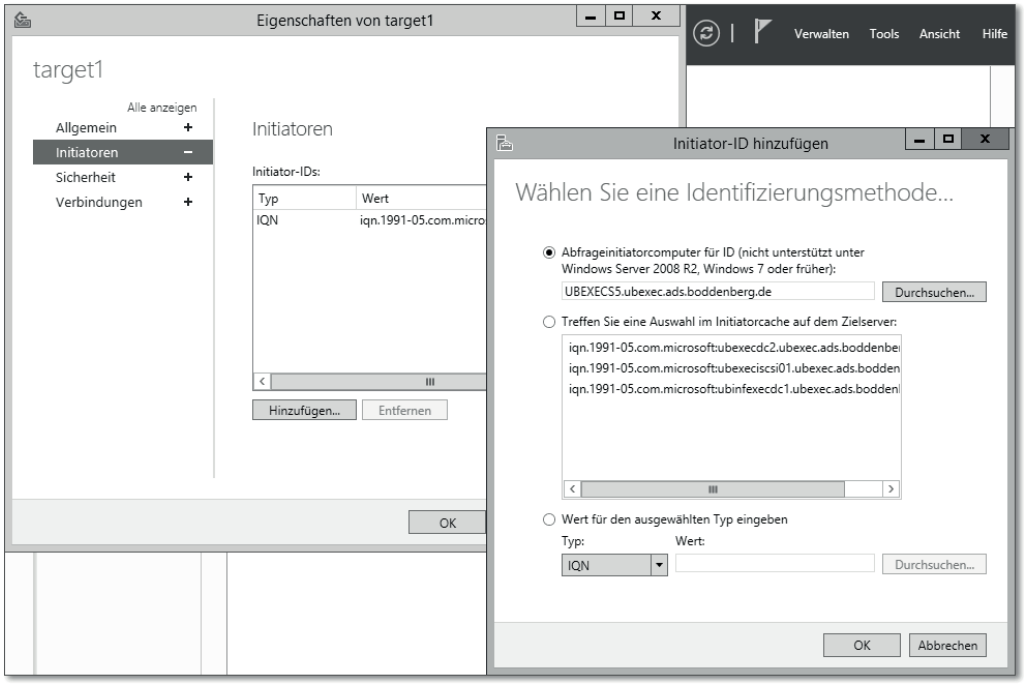


Abbildung 20.13 Die iSCSI-Initiatoren, die zugreifen sollen (die Clusterknoten), müssen eingetragen werden.

Mindestens zwei iSCSI-Bereiche

Erzeugen Sie mindestens zwei iSCSI-Bereiche. Ein Bereich, der nicht größer als 100 MByte zu sein braucht, wird als Quorum verwendet. Vereinfacht gesagt, werden dort »clusterinterne« Daten abgelegt.

Das zweite (dritte, vierte etc.) Device wird für Ihre Daten verwendet.

Konfiguration des iSCSI-Initiators

Nun müssen Sie auf den zukünftigen Clusterknoten noch die Clientkomponente zum Zugriff auf das iSCSI-Target konfigurieren. Eine Installation ist nicht notwendig, da der *iSCSI-Initiator* seit Windows Server 2008 (also auch in Server 2012 R2) bereits installiert ist, aber nicht ausgeführt wird. Rufen Sie daher den Menüpunkt iSCSI-Initiator auf, und starten Sie auf Nachfrage den Dienst (Abbildung 20.14).

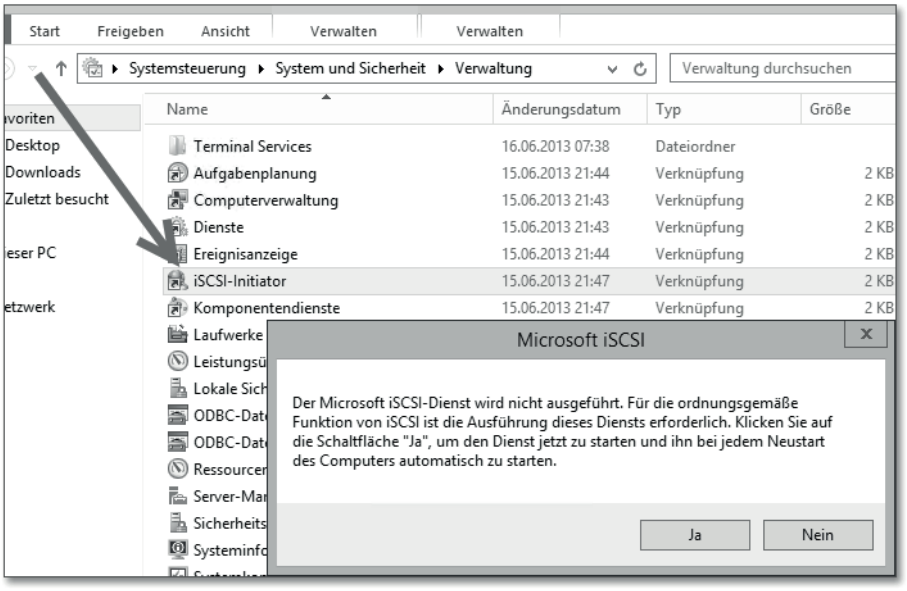


Abbildung 20.14 Der iSCSI-Initiator wird nach dem ersten Start den Dienst beginnen.

Für die Konfiguration des iSCSI-Initiators startet ein Eigenschaften-Dialog mit sechs Registerkarten. Für eine größere iSCSI-Umgebung gibt es recht elegante Konfigurationsmöglichkeiten unter Verwendung eines iSNS-Servers, der in etwa ein DNS-Server für iSCSI ist. Ich möchte an dieser Stelle allerdings nicht in die Tiefen von iSCSI einsteigen, sondern es »nur« zum Laufen bringen:

- Wechseln Sie auf die Registerkarte ZIELE, und nutzen Sie die Option SCHNELL VERBINDEN (Abbildung 20.15). Falls der iSCSI-Server mehrere Netzwerkadressen hat, achten Sie darauf, dass Sie die IP-Adresse des iSCSI-Netzwerksegments eintragen.

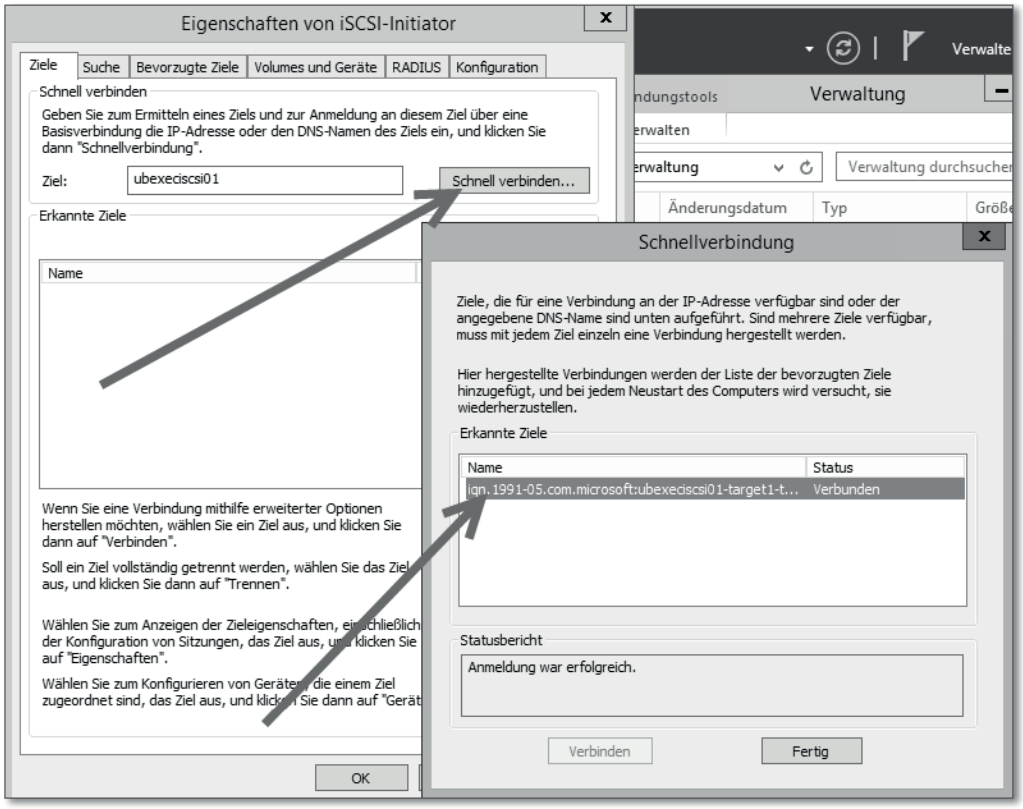


Abbildung 20.15 Das iSCSI-Target wird als Verbindungsziel eingetragen.

Bevor Sie die iSCSI-Konfiguration verlassen, sollten Sie auf die Registerkarte VOLUMES UND GERÄTE wechseln und dafür sorgen, dass die verwendeten Ressourcen in die Liste eingetragen werden. Ist eine Ressource dort vermerkt, sorgt der iSCSI-Initiator dafür, dass die iSCSI-Ressourcen für die darauf zugreifenden Dienste bzw. Applikationen stets vorhanden sind. Das hört sich ein wenig nebulös an, daher erkläre ich es an einem kleinen Beispiel: Wenn der Server beispielsweise Verzeichnisse des über iSCSI gemounteten Festplattensystems per Dateifreigabe zur Verfügung stellt, wird nach einem Neustart die Freigabe nicht mehr vorhanden sein. Das liegt daran, dass zu dem Zeitpunkt, an dem Dienst startet, der die Freigabe bereitstellt, die Verbindung zum iSCSI-Target noch nicht existiert. In der Folge müssen die Freigaben neu angelegt werden. Das Problem tritt nicht auf, wenn Sie die iSCSI-Ressourcen in dieser Liste eintragen (Abbildung 20.16).

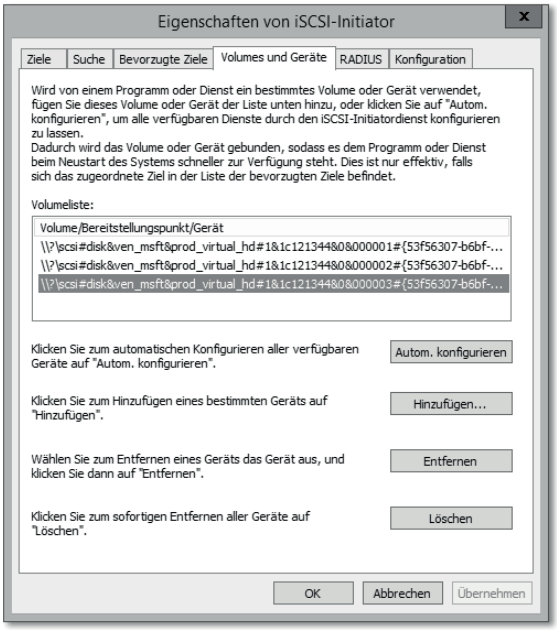


Abbildung 20.16 Wählen Sie »Autom. konfigurieren«, um die Verfügbarkeit der genutzten Geräte sicherzustellen.

Beachten Sie, dass die iSCSI-Ressource auch in der Liste auf der Registerkarte Bevorzugte Ziele vorhanden sein muss. Sie wird dort automatisch eingetragen, aber einmal kontrollieren kann nicht schaden (Abbildung 20.17).

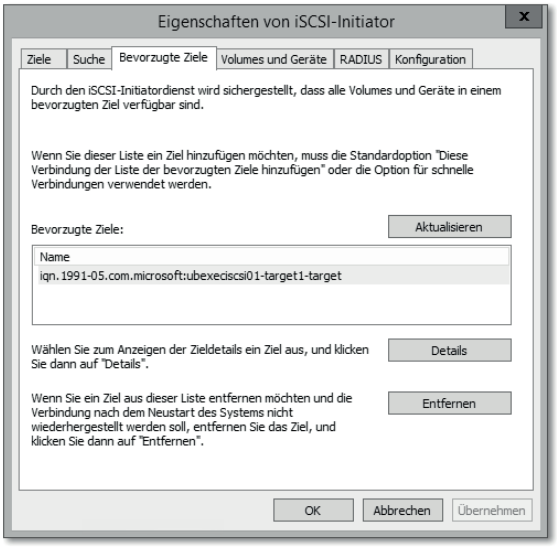


Abbildung 20.17 Das iSCSI-Target muss in den »Bevorzugten Zielen« erscheinen.

In der Datenträgerverwaltung muss sich nun in etwa das Bild aus Abbildung 20.18 ergeben. Die Datenträger müssen noch ONLINE geschaltet werden (im Kontextmenü des Datenträgers), dann können Sie eine Partition anlegen und formatieren. Abbildung 20.19 zeigt, dass die eingebundenen iSCSI-Ressourcen von »normalen« Festplatten nicht zu unterscheiden sind.

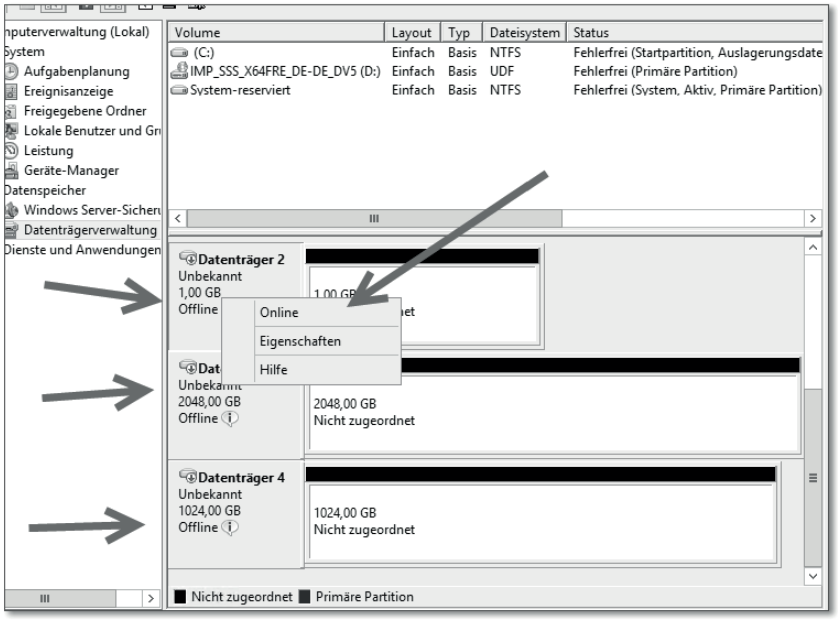


Abbildung 20.18 Die beiden per iSCSI zur Verfügung gestellten Volumes tauchen in der Datenträgerverwaltung auf, müssen aber noch aktiviert, initialisiert und formatiert werden.

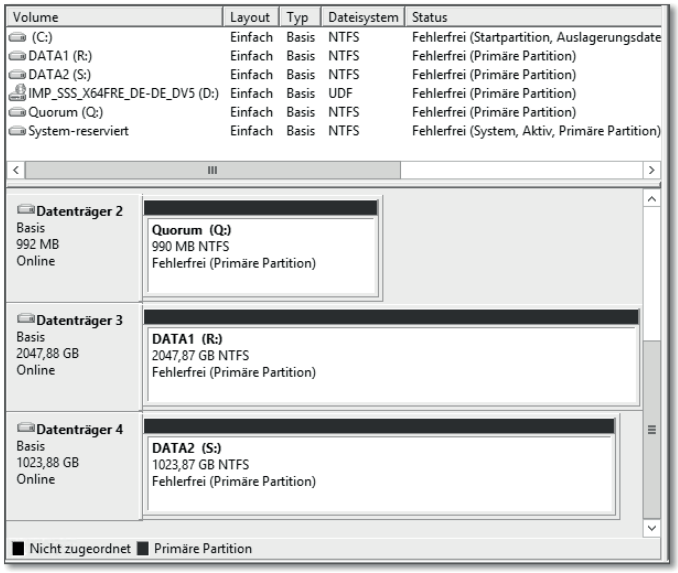


Abbildung 20.19 So muss es aussehen. Und zwar auf beiden Servern!

Keine Laufwerkbuchstaben

Es ist übrigens nicht notwendig, den zukünftigen Clusterfestplatten Laufwerkbuchstaben zuzuweisen. Dies wird ohnehin bei der Clusterinstallation modifiziert.

Hinweis

Die gezeigten Schritte müssen auf allen Clusterknoten durchgeführt werden (natürlich nicht das Partitionieren und Formatieren). Bevor Sie mit der Clusterinstallation fortfahren, müssen alle Clusterknoten auf die Festplattenbereiche zugreifen können.

Sie können übrigens auch im Server-Manager in der Konfiguration des iSCSI-Targets kontrollieren, ob sich alle Server mit dem iSCSI-Target verbunden haben. Es muss sich ein Szenario wie das in Abbildung 20.20 ergeben (s5 und s6 sind die Clusterknoten).

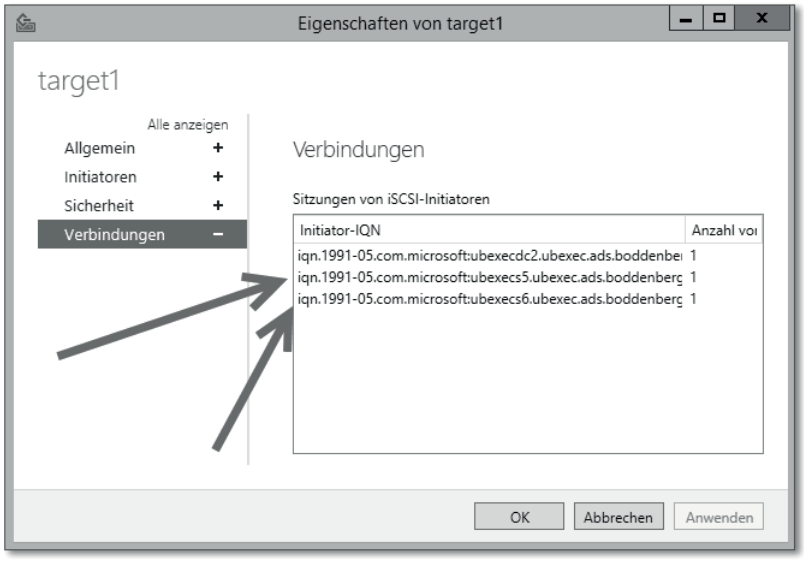


Abbildung 20.20 In der Konfiguration des iSCSI-Targets müssen beide iSCSI-Initiatoren angezeigt werden.

Cluster installieren

Die grundlegenden Arbeiten können Sie mit einem grafischen Werkzeug, dem Failovercluster-Manager, erledigen; das gilt übrigens sowohl für die Einrichtungs- als auch für die Betriebsphase.Die Clusterverwaltung lässt sich übrigens auch auf einem Windows 8-/8.1-PC ausführen; Sie müssen lediglich die Windows Server 2012-Admin-Werkzeuge installieren (RSAT, Download Center). Wie Sie in Abbildung 20.21 sehen können, kann in der Clusterverwaltung

viel erläuternder Text aufgerufen werden. Außerdem sind natürlich die wesentlichen Aktionen (KONFIGURATION ÜBERPRÜFEN, CLUSTER ERSTELLEN etc.) aufrufbar.

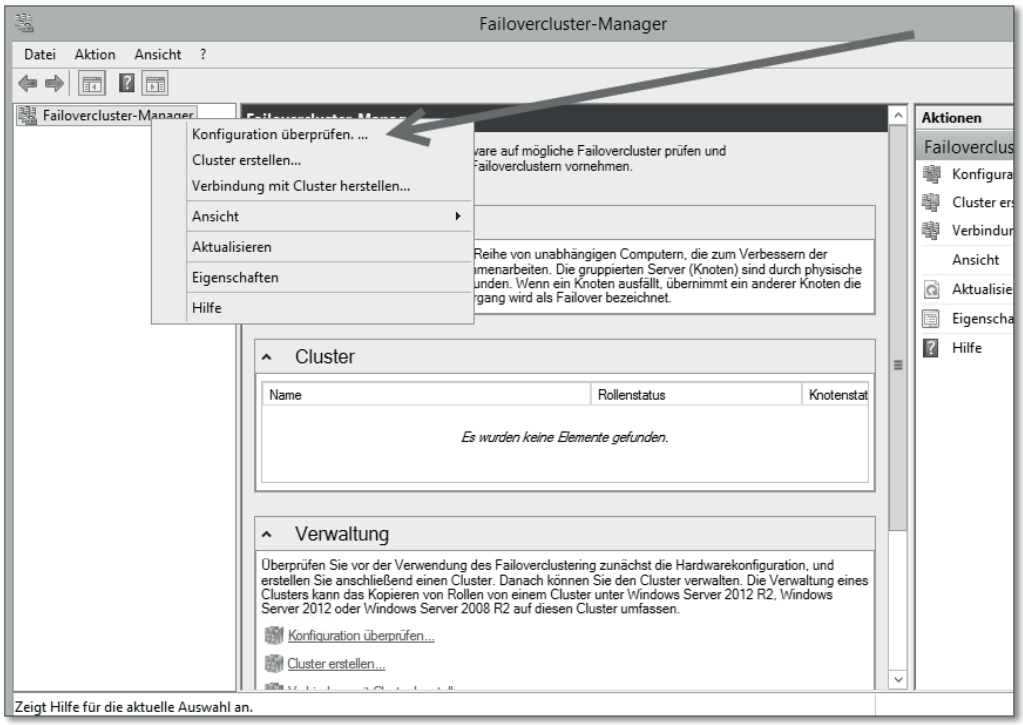


Abbildung 20.21 Die »Failover-Clusterverwaltung« ermöglicht ein komfortables Arbeiten – auch vom Admin-Arbeitsplatz aus.

Konfiguration überprüfen

Eine der Neuerungen beim Failover-Cluster unter Windows Server 2008 waren wesentlich umfangreichere Prüfvorgänge als bei den Vorgängerversionen – in 2012 ist das nochmals erweitert worden. Das ist auch ziemlich gut so, denn meiner Erfahrung nach liegt die Ursache für Clusterprobleme während der Betriebsphase in einer fehlerhaften Grundkonfiguration. Rufen Sie also in der Failover-Clusterverwaltung den Menüpunkt KONFIGURATION ÜBERPRÜFEN auf:

- Zunächst können Sie die zu überprüfenden Server angeben (Abbildung 20.22). Tragen Sie hier alle Server ein, aus denen der Cluster gebildet werden soll.
- Auf der dann folgenden Dialogseite können Sie wählen, ob alle Tests durchgeführt werden sollen oder ob Sie nur einzelne Tests laufen lassen möchten. Der erste Testlauf sollte alle Tests umfassen. Da die Ausführung einige Minuten dauert, kann später, wenn Sie einzelne aufgetretene Probleme korrigiert haben, eine selektivere Vorgehensweise empfehlenswert sein (Abbildung 20.23).

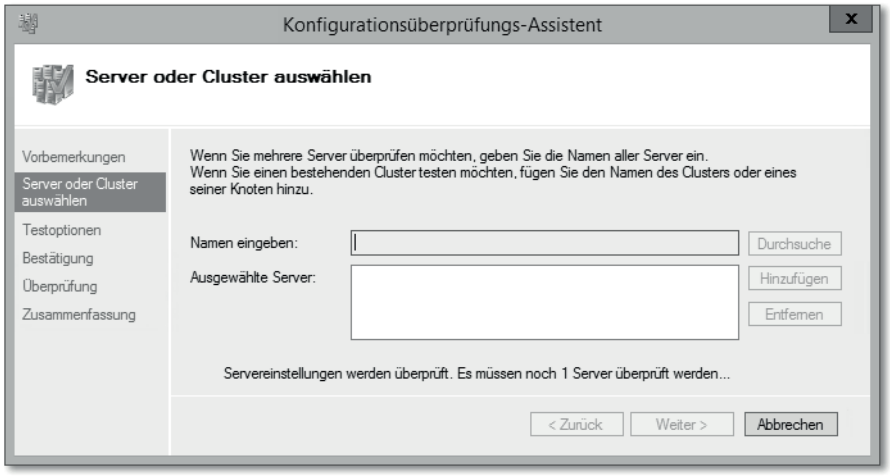


Abbildung 20.22 Wählen Sie zunächst die zukünftigen Clusterknoten zum Test aus.

- Sie können nun den Test starten, der automatisch abläuft. Wie bereits erwähnt, wird er einige Minuten in Anspruch nehmen.

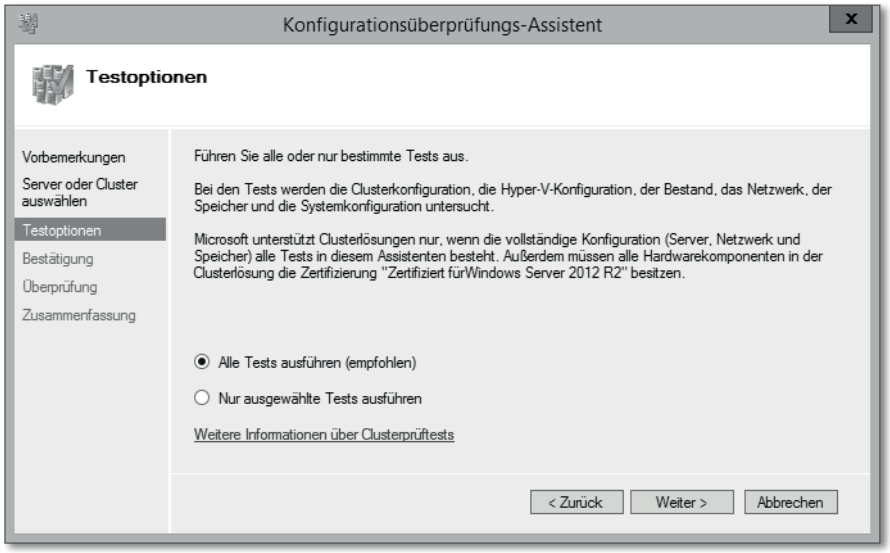


Abbildung 20.23 Sinnvollerweise werden alle Tests ausgeführt.

- Der Dialog aus Abbildung 20.24 bringt zwar keine komplizierten Konfigurationsaufgaben mit, ich finde es aber ganz beeindruckend, zu zeigen, wie viele Tests die Clusterverwaltung bereithält.

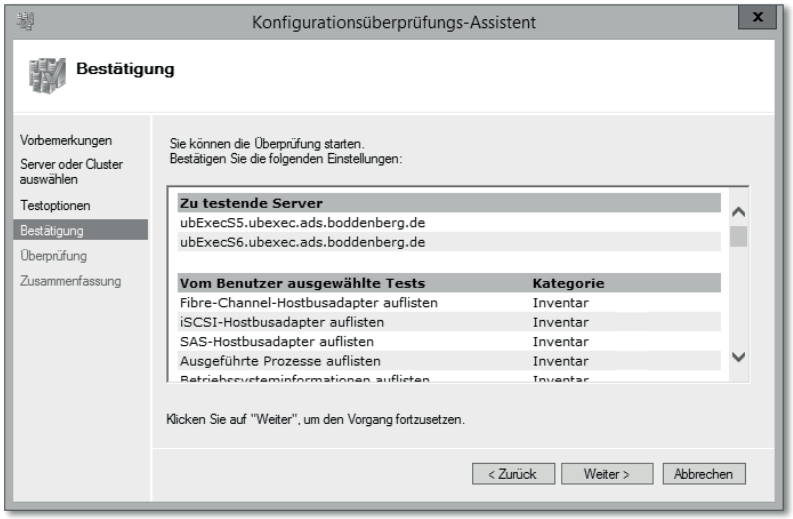


Abbildung 20.24 Es gibt mehrere Dutzend Tests.

Nach Durchführung des Testlaufs können Sie einen Bericht (HTML-Seite) aufrufen, der sehr detailliert die Ergebnisse auflistet. Sofern Probleme aufgetreten sind, erhalten Sie im Allgemeinen recht konkrete Handlungsanweisungen (Abbildung 20.25).

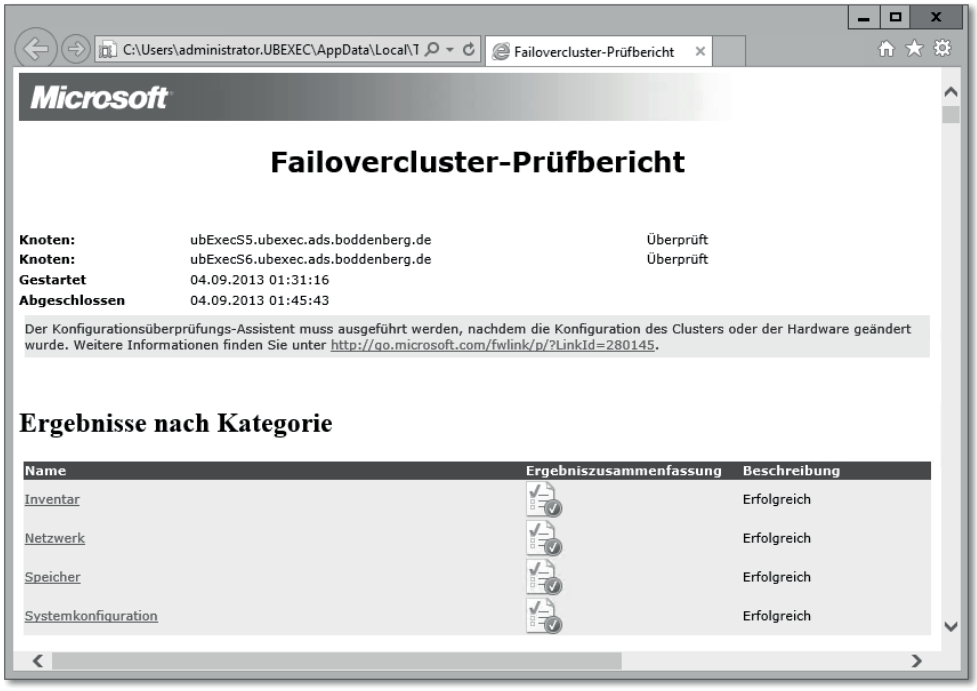


Abbildung 20.25 Der Failovercluster-Prüfbericht

Ich empfehle Ihnen dringend, wirklich so lange zu testen, bis keinerlei Probleme oder Warnungen mehr angezeigt werden. Zwar ist die Clusterinstallation auch möglich, wenn die Konfigurationsprüfung Fehler meldet, allerdings würden daraus zwei Probleme resultieren:

- Eine Konfiguration, die von der Clusterüberprüfung nicht die »grüne Ampel« erhält, wird von Microsoft nicht supportet.
- Wenn die Clusterprüfung Probleme meldet, hat das im Allgemeinen »Hand und Fuß«. Diese Meldungen einfach zu ignorieren, wird mit einer nicht ganz geringen Wahrscheinlichkeit später zu Problemen führen, die dann gegebenenfalls schwer zu diagnostizieren sind.

Cluster erstellen

Nun kommen wir zum eigentlichen Aufsetzen des Clusters. Wählen Sie in der Clusterverwaltung den Menüpunkt Cluster erstellen. Sie werden feststellen, dass Cluster zu erstellen einfacher ist, als Sie es sich vielleicht gedacht haben.

- Zunächst bestimmen Sie, aus welchen Servern der Cluster initial aufgebaut werden soll. Das ist übrigens keine Entscheidung für die Ewigkeit, Sie können auch zu einem späteren Zeitpunkt noch weitere Server hinzufügen (Abbildung 20.26).

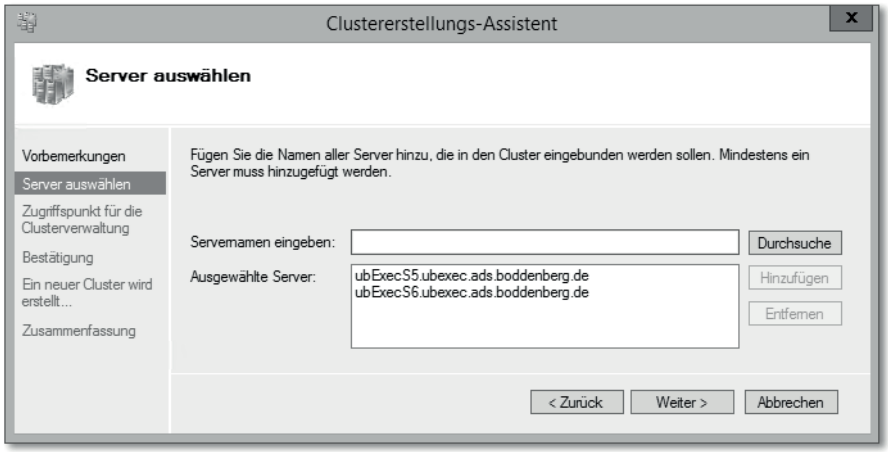


Abbildung 20.26 Wählen Sie die Knoten aus, aus denen der Cluster gebildet werden soll.

- Die eventuell erscheinende nächste Dialogseite ist einigermaßen wichtig. Falls bei dem letzten Validierungstest Warnungen aufgetreten sind, wird der Clustererstellungs-Assistent Sie darauf hinweisen, dass das System nicht von Microsoft supportet werden wird. Sie haben nun die Möglichkeit, den Validierungstest nochmals durchzuführen (vielleicht sind ja die gemeldeten Probleme mittlerweile behoben) oder die Installation trotz der Warnung durchzuführen.

Support

An dieser Stelle sei auf die Bedeutung des Microsoft-Supports hingewiesen. Bekanntermaßen brauchen Sie über wirklich kniffligen Problemen nicht stunden- oder gar tagelang selbst zu brüten, sondern können einen Call bei Microsoft aufmachen. Wenn Sie nicht durch einen wie auch immer gearteten Rahmenvertrag diverse Anrufe frei haben, kosten sie Geld (das staffelt sich u.a. auch nach der Produktfamilie, im Serverumfeld kann man mit ca. 300 € rechnen; Angaben ohne Gewähr!). Für diesen Betrag brauchen Sie nun aber nicht stundenlang selbst nach der Lösung für ein Problem zu suchen.

Ein Call bei Microsoft setzt jedoch voraus, dass die Installation grundsätzlich den »Regeln« entspricht. Wenn Sie wissentlich eine nicht supportete Konfiguration implementieren, verbauen Sie sich die Chance, Ihr konkretes Problem durch Microsoft lösen zu lassen – diesen Weg würde ich mir auf gar keinen Fall verbauen.

Im nächsten Schritt tragen Sie den Clusternamen und eine zugehörige IP-Adresse ein (Abbildung 20.27). Dies ist die IP-Adresse bzw. der Name, über den der Cluster zu Verwaltungsaufgaben angesprochen wird. Benötigt wird hier eine »neue« Adresse, also keine Adresse eines der Clusterknoten!

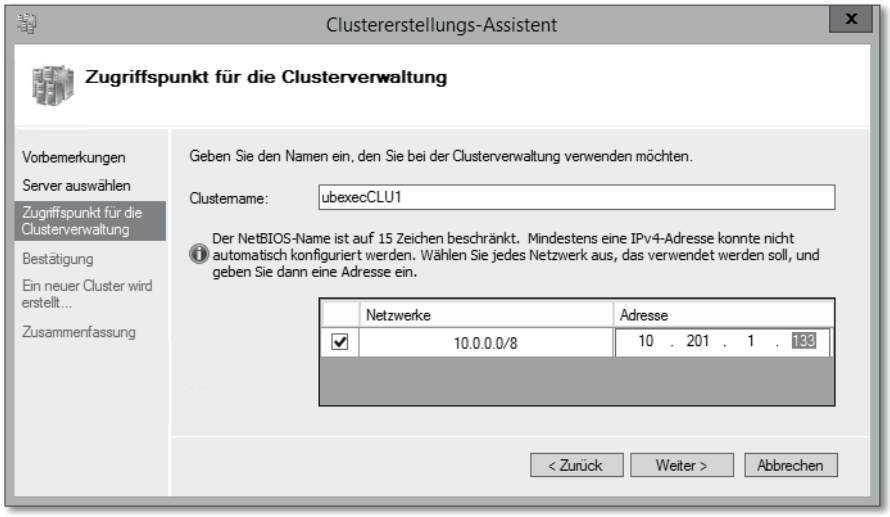


Abbildung 20.27 Für die Clusterverwaltung werden eine IP-Adresse und ein Name benötigt.

Damit haben Sie den Assistenten bereits durchgearbeitet. Nehmen Sie noch eine letzte Überprüfung vor, und dann kann es losgehen (Abbildung 20.28). Die auf dem Screenshot mit dem Pfeil gekennzeichnete Option sollten Sie setzen. Ansonsten müssen Sie beispielsweise auch die Quorum-Disk »per Hand« einbinden. Kann man alles machen, aber wenn der Installations-Assistent das erledigt, ist auch schön.

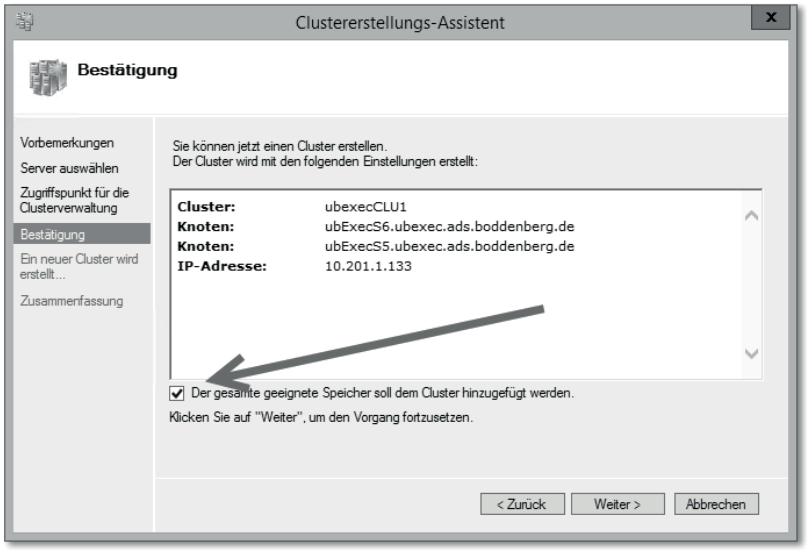


Abbildung 20.28 Ein letzter Check – dann geht es los.

Vielleicht sind Sie erstaunt, dass keine weiteren Parameter abgefragt werden, aber im ersten Schritt geht es »nur« um das Aufsetzen des eigentlichen Clusters. Anwendungen, also Clusterressourcen, werden in einem zweiten Schritt konfiguriert.

Abbildung 20.29 Das war erfolgreich: Es gibt keine Warnungen, und der Cluster läuft.

Der Assistent wird nun ein paar Minuten lang beschäftigt sein. Wenn Sie den Validierungstest erfolgreich absolviert haben, sollte es aber keine Probleme geben. Abbildung 20.29 zeigt

den »Abschlussdialog« einer einwandfrei abgelaufenen Installation. Wenn es Probleme gegeben hat, wird in genau diesem Dialog ein Warnzeichen zu sehen sein. In diesem Fall würde ich übrigens das Problem diagnostizieren (Schaltfläche Bericht anzeigen), den installierten Cluster löschen, das Problem beheben und neu installieren. So können Sie sicher sein, dass Sie wirklich einen »sauberen« Cluster verwenden.

Der Ist-Zustand

Sie werden neugierig sein, wie der Installations-Assistent den Cluster eingerichtet hat. Dies kann in der Failover-Clusterverwaltung problemlos überprüft werden.

Wählen Sie beispielsweise den Knoten Speicher. Dort werden die im Cluster vorhandenen Datenträger angezeigt. Eine besondere Rolle nimmt der Datenträgerzeuge im Quorum ein. Dies ist der Plattenbereich, den der Cluster sozusagen »für sich selbst« benötigt (Abbildung 20.30).

Im Kontextmenü des Knotens Speicher findet sich der Menüpunkt Datenträger hinzufügen, mit dem (Überraschung, Überraschung) dem Cluster weitere Speicherkapazität hinzugefügt werden kann. In Clustern, die auf gemeinsamem Speicherplatz (Shared Storage) basieren, versteht es sich von selbst, dass nur ebendiese gemeinsamen Datenträger hinzugefügt werden können.

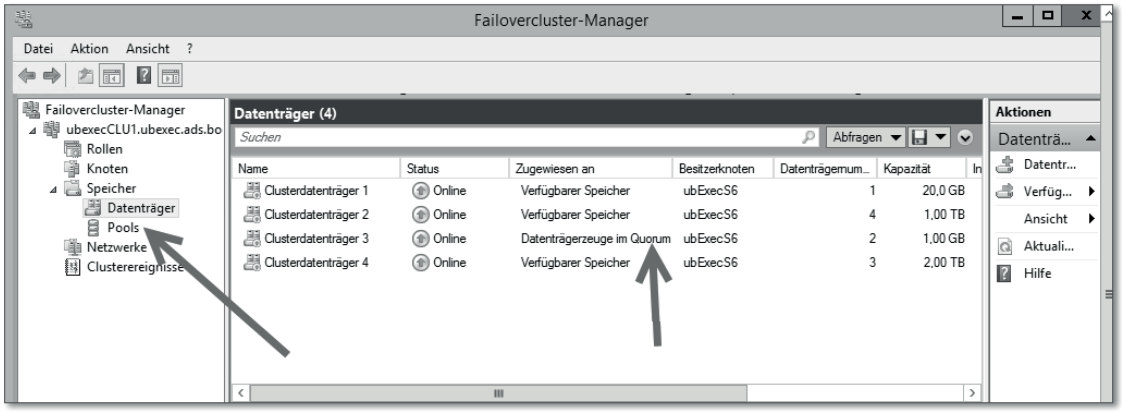


Abbildung 20.30 In der Clusterverwaltung können Sie den im Cluster vorhandenen Speicher einsehen. Beachten Sie besonders den »Datenträgerzeugen«.

Weiterhin interessant ist der Knoten Netzwerke (Abbildung 20.31). Sie können für jedes Netzwerk konfigurieren, ob es vom Cluster verwendet werden darf und ob Clientzugriffe möglich sein sollen. Der Konfigurations-Assistent trifft im Allgemeinen die »richtigen Entscheidungen«, es könnte aber auch sein, dass Sie hier ein wenig nacharbeiten müssen. Rufen Sie dazu den Eigenschaften-Dialog der jeweiligen Netzwerkverbindung auf:

- Die Netzwerkverbindung zum Produktivnetz muss für die Verwendung durch den Cluster zugelassen sein. Weiterhin muss Clientzugriff gestattet sein.
- Für das Heartbeat-Netz muss die Verwendung durch den Cluster aktiviert sein, allerdings muss der Clientzugriff abgeschaltet werden.

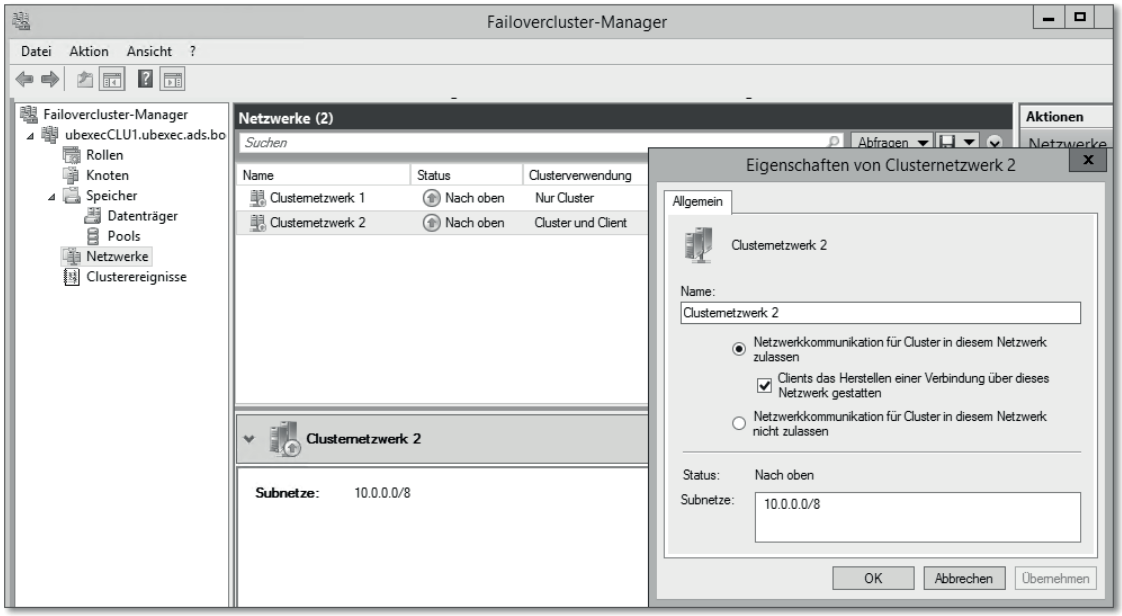


Abbildung 20.31 In der Clusterverwaltung können Sie die im Cluster vorhandenen Netzwerke einsehen und konfigurieren.

20.2.3 Anwendungen hinzufügen

Der Cluster bringt nicht viel, wenn keine Anwendung darauf ausgeführt wird. Die nächste Aufgabe ist also, eine Anwendung oder einen Dienst auf dem Cluster zu konfigurieren. Standardmäßig sind ca. ein Dutzend Anwendungen bzw. Dienste vorhanden, darunter Dateiserver, Druckserver, DHCP-Server und dergleichen mehr. Wenn Sie beispielsweise Exchange Server oder SQL Server auf dieser Maschine installiert haben, werden die entsprechenden Komponenten ebenfalls auf diesem Weg installiert.

Voraussetzung

Die im Cluster auszuführende Rolle muss auf den Clusterknoten, die sie ausführen sollen, installiert sein. Die Fehlermeldungen, die erscheinen, wenn das nicht erledigt wurde, zeige ich Ihnen im weiteren Verlauf.

Als Beispiel in diesem Buch werde ich Ihnen vorführen, wie man einen Dateiserver-Cluster einrichtet. Also:

- In der Failover-Clusterverwaltung rufen Sie im Kontextmenü den Menüpunkt Rolle konfigurieren auf (Abbildung 20.32).

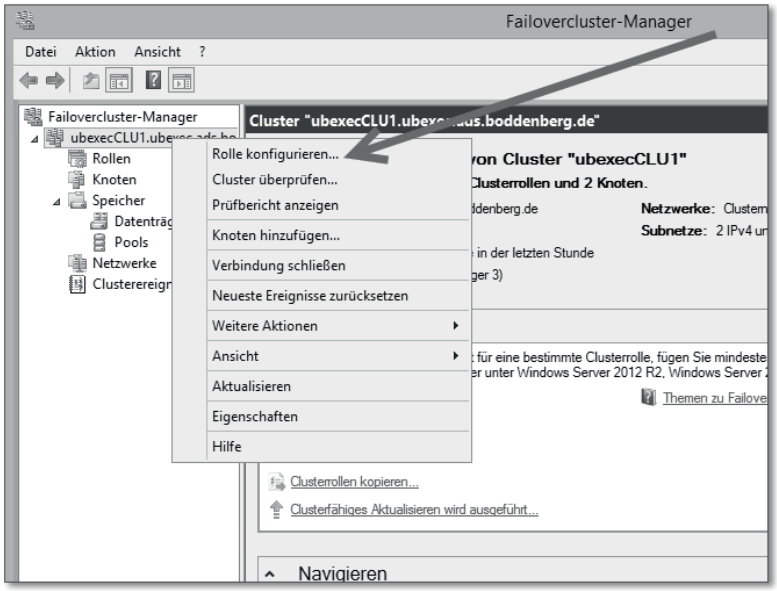


Abbildung 20.32 Hier beginnen Sie mit dem Einrichten eines Diensts oder einer Anwendung.

- Anschließend erscheint der Dialog zur Auswahl der Anwendung, die als Clusterressource installiert werden soll (Abbildung 20.33). Zusätzliche Anwendungen bringen häufig ihre eigenen Installationsroutinen mit, ich zeige Ihnen das später anhand eines SQL-2012-Clusters.

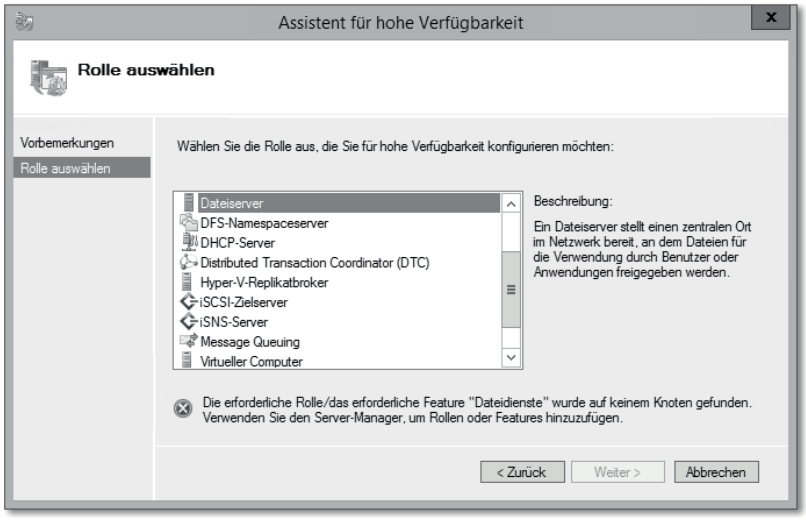


Abbildung 20.33 Eine mögliche Clusteranwendung ist der Dateiserver.

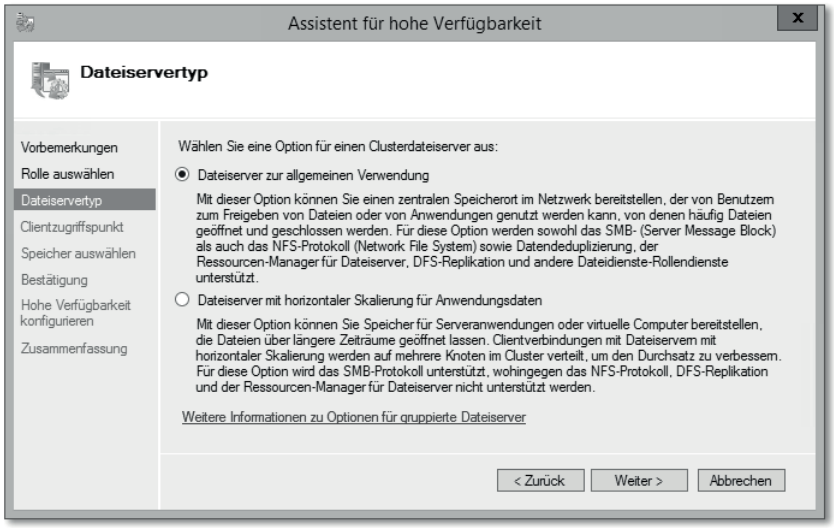


Abbildung 20.34 Ab Server 2012 erscheint diese »Zusatzfrage«. Die Optionen sind ausführlich beschrieben. Für dieses Beispiel wähle ich die erste Option.

Hinweis

In Abbildung 20.33 sehen Sie eine kleine, aber wichtige Fehlermeldung, die besagt, dass die Dateiserverrolle auf keinem Knoten gefunden wurde. Voraussetzung ist, dass die zu clusternden Rollen auf den entsprechenden Knoten vorhanden sind. Die Warnung im Dialog klingt ein wenig so, als müssten sie auf mindestens einem Knoten vorhanden sein – stimmt im Grunde genommen auch. Auf Knoten, auf denen die Rolle nicht installiert ist, kann aber kein Failover stattfinden. Also: Rollen vor Installationsbeginn auf allen Clusterknoten installieren!

Der nächste Punkt ist die Konfiguration des CLIENTZUGRIFFSPUNKTS (Abbildung 20.35). Den hier angegebenen Namen nebst zugehöriger IP-Adresse verwenden die Clients, um auf die Clusterressource, in diesem Fall den Dateiserver-Cluster, zuzugreifen.

Vorsichtshalber möchte ich Sie darauf hinweisen, dass hier ein nicht existierender Name und eine nicht verwendete IP-Adresse gefordert sind, also keinesfalls die Daten eines bestehenden Clusterknotens.

Übrigens, es wird ein Computerkonto angelegt, und der Name wird im DNS eingetragen.

Im nächsten Dialog wählen Sie die zu verwendenden Speicherbereiche. In diesem Beispiel habe ich nur zwei Datenträger angelegt. Einer davon wird für interne Zwecke benötigt (DATENTRÄGERZEUGE IM QUORUM), der andere kann für die Verwendung mit dem Dateiserver-Cluster ausgewählt werden (Abbildung 20.36). Bei Bedarf können Sie natürlich weitere Datenträger hinzufügen.

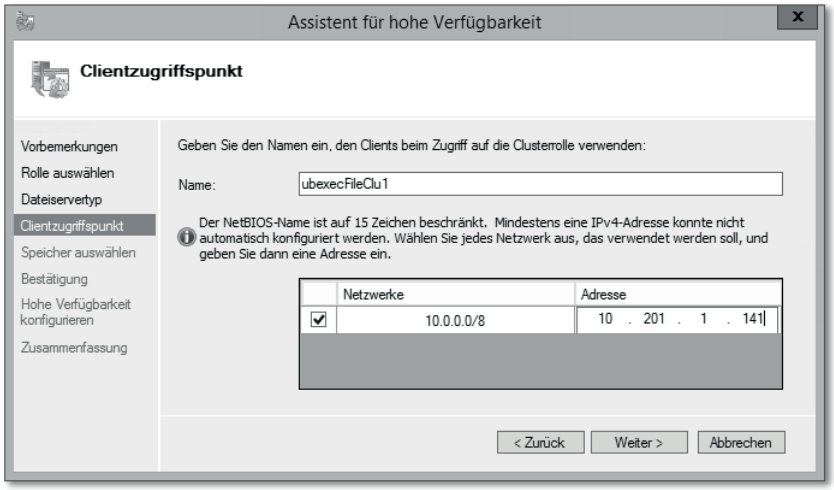


Abbildung 20.35 Wählen Sie einen Namen und eine Netzwerkadresse für den Dateiserver-Cluster.

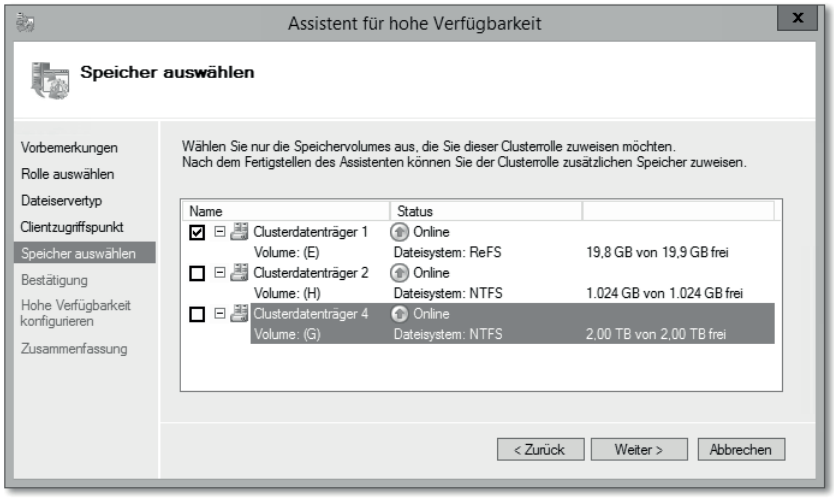


Abbildung 20.36 Legen Sie das Speichervolume fest, das für den Dateiserver-Cluster verwendet werden soll.

Hinweis

Wenn im Cluster Knoten vorhanden sind, auf denen die Rolle nicht installiert ist, erscheint die auf Abbildung 20.37 gezeigte Warnung. Da es sich hier um einen Zwei-Knoten-Cluster handelt, ist die Rolle nicht redundant vorhanden. Das wäre also ein Cluster, der absolut keinerlei Sinn ergibt. Achten Sie darauf, dass das niemals passiert! Wäre sehr peinlich.

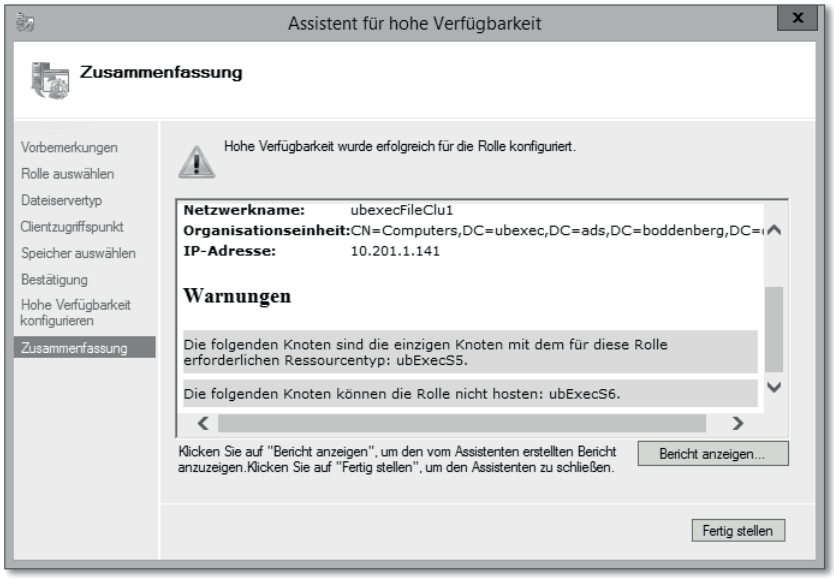


Abbildung 20.37 Warnung, wenn Knoten im Cluster die Rolle nicht installiert haben

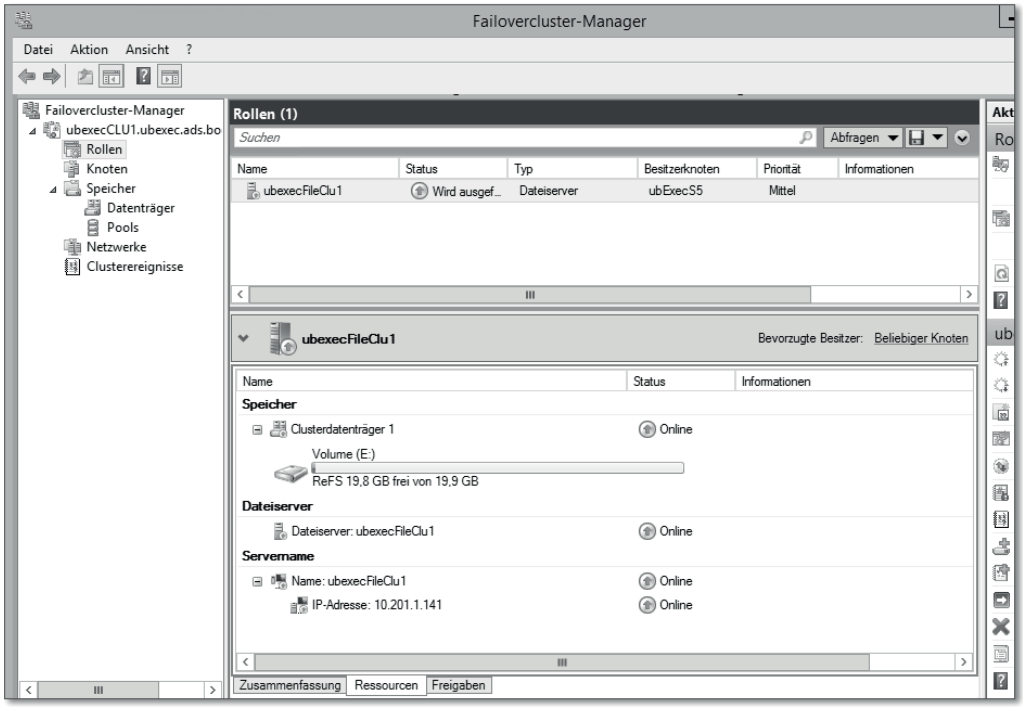


Abbildung 20.38 In diesem Dialog wird der Dateiserver-Cluster konfiguriert. Bisher gibt es nur die administrative Freigabe; immerhin ist alles online geschaltet.

Hat der Assistent seine Arbeit erledigt, können Sie den angelegten Dateiserver-Cluster in Augenschein nehmen (Abbildung 20.38):

- Sie können erkennen, dass der Status des Clusters ONLINE und der aktuelle Besitzer UBEXECS5 ist. Wie unschwer zu erraten ist, ist mit Letzterem der Server gemeint, auf dem der Dienst momentan ausgeführt wird.
- Verschiedene Ressourcen haben den Status ONLINE, und zwar der Name, die IP-Adresse und der Clusterdatenträger.
- Momentan gibt es für den Dateiserver-Cluster nur eine Freigabe, nämlich die administrative Freigabe.

Um nun eine weitere Freigabe einzurichten, wählen Sie im Kontextmenü der Dateiserver-Clusteranwendung den Menüpunkt EINEN FREIGEGEBENEN ORDNER HINZUFÜGEN. Der Assistent, der daraufhin startet, fragt zunächst nach dem freizugebenden Pfad. Dann müssen Sie sich noch durch einige weitere Dialogseiten arbeiten, die aber selbsterklärend sind. Sie sehen, dass die grundlegenden Arbeiten, wie eben das Hinzufügen von Freigaben, in der Clusterverwaltung erledigt werden. Existiert die Freigabe bereits, modifizieren Sie diese in ihrem EIGENSCHAFTEN-Dialog, den Sie über das Kontextmenü aufrufen (Abbildung 20.39, Abbildung 20.40).

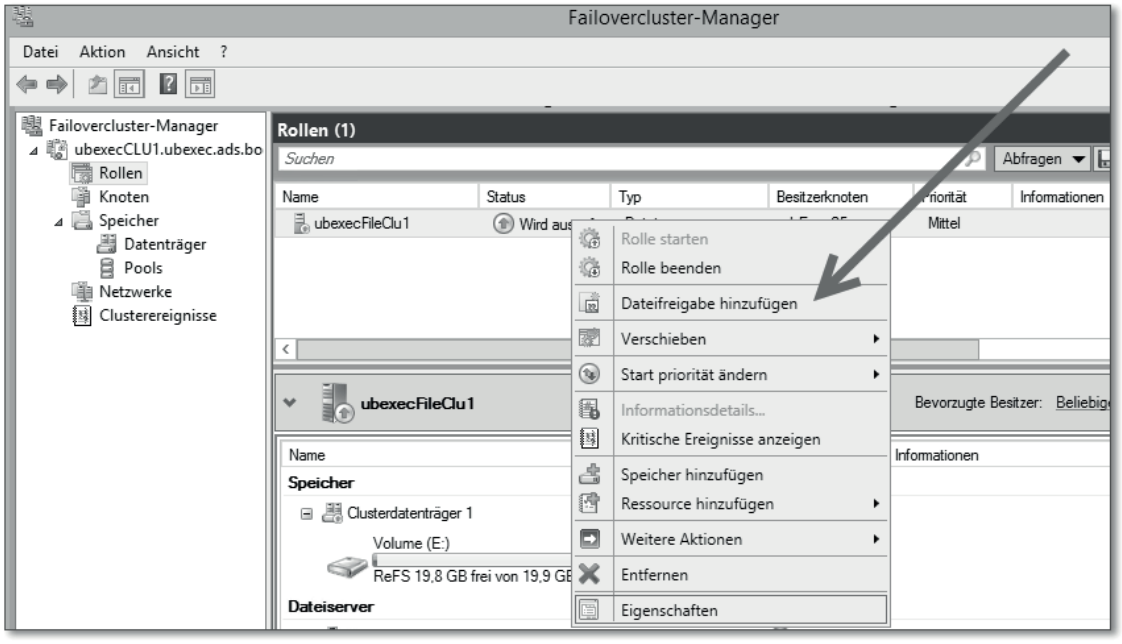


Abbildung 20.39 Jede Menge Menüpunkte: Zum Beispiel könnte man eine »Dateifreigabe hinzufügen«.

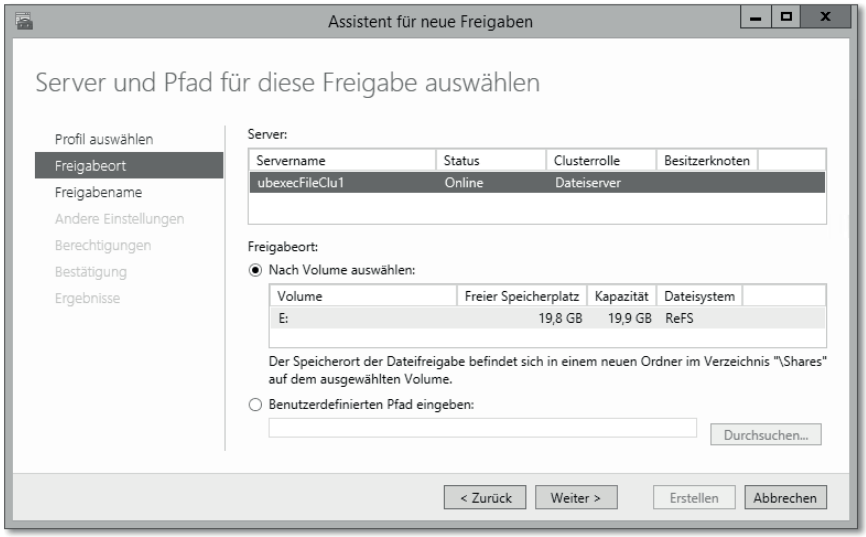


Abbildung 20.40 Geben Sie den Speicherort für den freigegebenen Ordner an.

20.2.4 Cluster schwenken

Die Idee hinter einem Failover-Cluster ist, dass beim Ausfall eines Knotens ein anderer dessen Aufgaben übernimmt. Das Schwenken des Clusters können Sie allerdings auch gezielt initiieren, beispielsweise um einen Knoten zu Wartungszwecken (z. B. zum Einspielen von Patches nebst fälligem Neustart) herunterzufahren, oder einfach, um zu probieren, ob ein anderer Knoten die Funktion übernehmen kann.

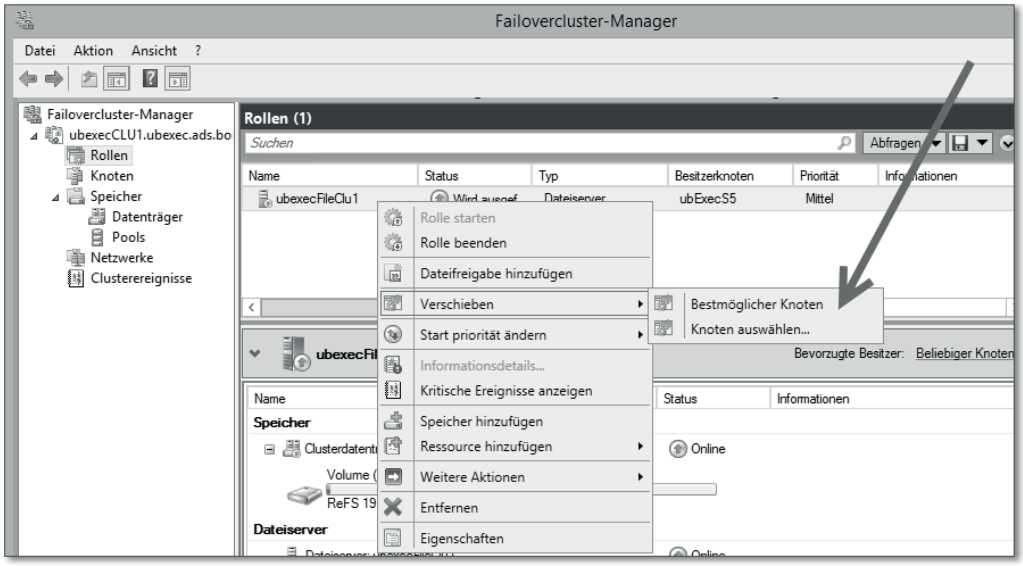


Abbildung 20.41 Der Dateiserver-Cluster kann geschwenkt werden ...

Im Eigenschaften-Dialog der Dienste bzw. Anwendungen findet sich der Menüpunkt Diesen Dienst oder diese Anwendung in einen anderen Knoten verschieben. In diesem Fall (Abbildung 20.41) ist zwar nur ein möglicher Knoten aufgeführt (der Cluster hat nur zwei Knoten), aber so wird's gemacht.

In Abbildung 20.42 sehen Sie einen Zustand, der sich beim Verschiebevorgang ergibt: Die Ressourcen sind während des Verschiebens für kurze Zeit nicht im Zugriff. Die Clients können dann die Verbindung wieder aufbauen, sie ist aber in jedem Fall kurz »weg«.

Dies gilt übrigens auch beim Ausfall eines Knotens: Die Funktionalität wird zwar auf einen anderen Knoten verschoben, die Clients verlieren aber kurzzeitig die Verbindung. In den meisten Fällen ist das zwar kein Problem, Sie sollten sich aber darüber im Klaren sein!

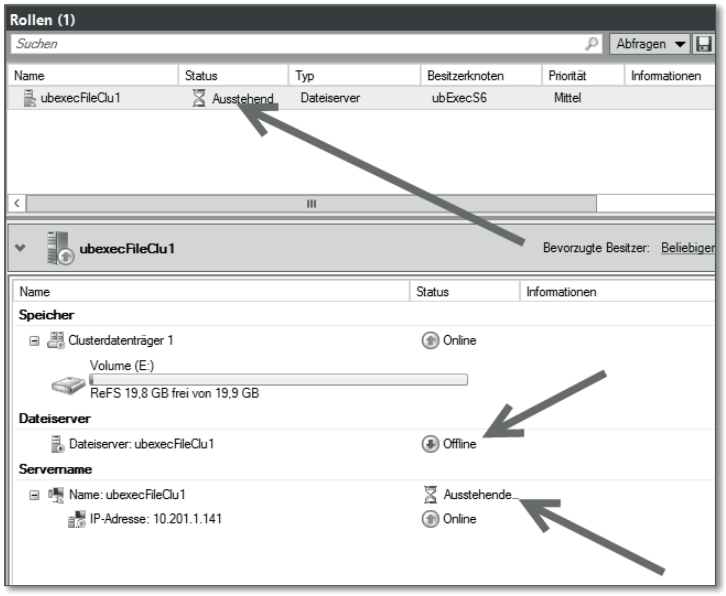


Abbildung 20.42 ... allerdings gibt es dabei eine kurze Funktionsunterbrechung für die Clients.

20.2.5 Feinkonfiguration des Clusters und weitere Vorgehensweise

Das Verwaltungswerkzeug für den Failover-Cluster hält viele, viele Konfigurationsmöglichkeiten bereit. Ich möchte diese hier nicht im Detail besprechen. Wenn Sie einen lauffähigen Cluster haben, sollten Sie in der Failover-Clusterverwaltung die Konfigurationsdialoge durchsehen und sich einen Überblick verschaffen. Die Optionen sind im Großen und Ganzen selbsterklärend, sodass seitenlange Beschreibungen in der Tat nicht notwendig sind.

Weiterhin möchte ich Ihnen dringend empfehlen, das Wiederherstellen des Clusters und einzelner Clusterknoten mit der von Ihnen verwendeten Sicherungssoftware auszuprobieren – und zwar in einer ruhigen Stunde und nicht erst, wenn der Notfall da ist.

20.2.6 Clusterfähiges Aktualisieren

Das Patchen von Systemen ist ein vordringliches Thema – das ist nun wirklich keine neue Erkenntnis. Natürlich ist das auch bei Clustern wichtig, wobei der Arbeitsprozess dabei in etwa dieser ist:

- Alle Ressourcen auf Knoten 2 schwenken.
- Knoten 1 aktualisieren.
- Alle Ressourcen auf den nun aktualisierten Knoten 1 schwenken.
- Knoten 2 aktualisieren.
- Fertig!

Das sind viele Handgriffe mit natürlich einigem Aktualisierungspotenzial. Microsoft hat mit Server 2012 das *Clusterfähige Aktualisieren* entwickelt. Abbildung 20.43 zeigt den Einstieg in diese Funktionalität.

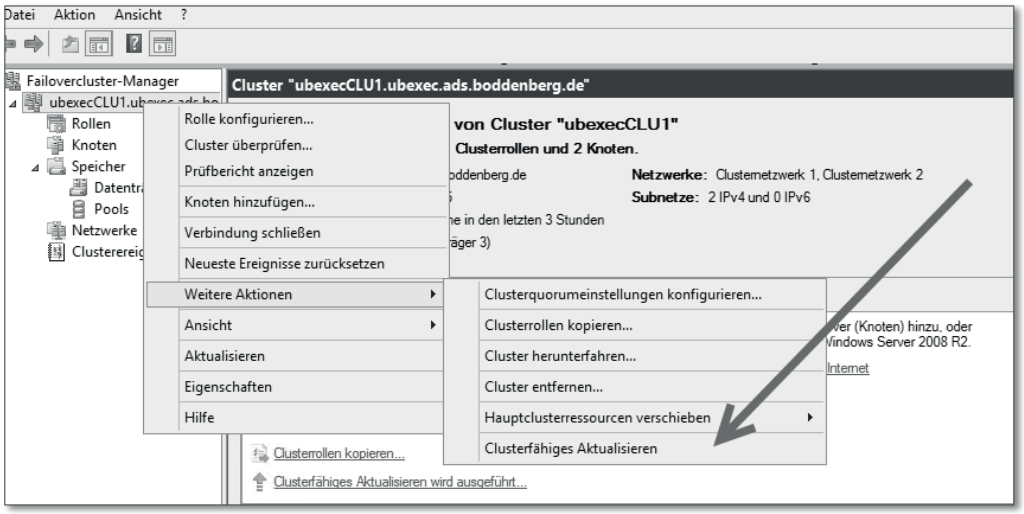


Abbildung 20.43 Eine spannende Option seit Server 2012: »Clusterfähiges Aktualisieren«

Abbildung 20.44 zeigt den Steuerungsdialog für Clusterfähiges Aktualisieren. Dieser Dialog gibt zunächst einen Überblick über den Update-Status des Clusters. Wie Sie sehen, ist das clusterfähige Aktualisieren noch nie gelaufen. Kann ja auch nicht, die Clusterressource ist noch nicht mal installiert.

Sie können sich beispielsweise einen Überblick darüber verschaffen, welche Updates auf den Clusterknoten benötigt werden. Die Updates kommen von dem konfigurierten WSUS-Server. Das Ergebnis zeigt der Dialog Vorschau der Updates anzeigen, der in Abbildung 20.45 zu sehen ist.

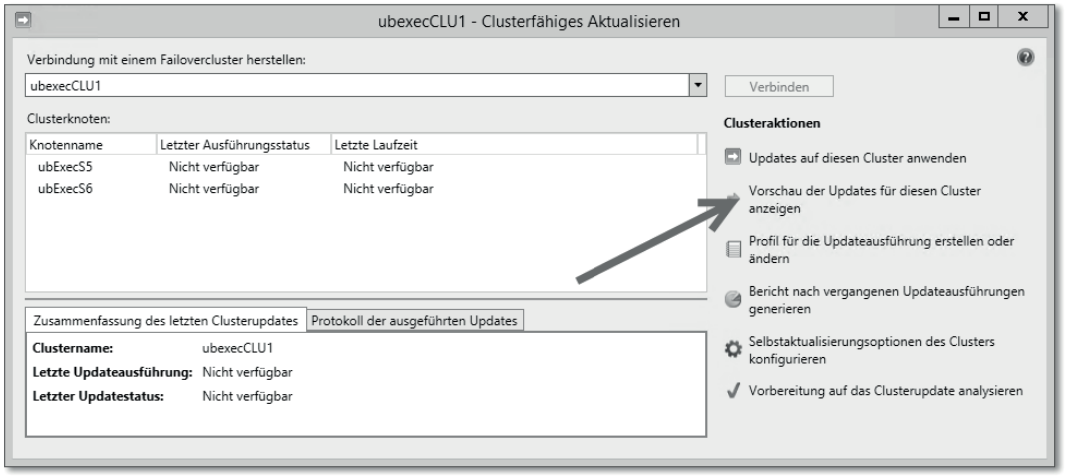


Abbildung 20.44 Der Steuerungsdialog für »Clusterfähiges Aktualisieren«

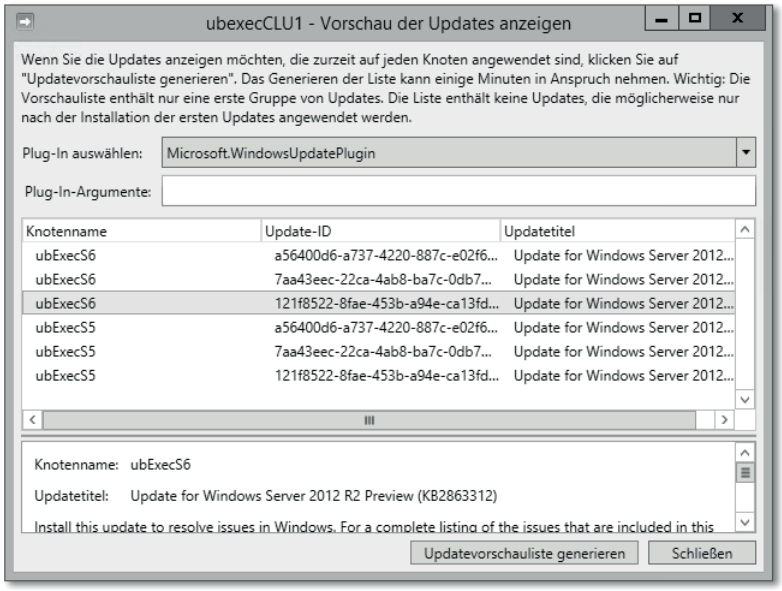


Abbildung 20.45 Die benötigten Updates

Damit das clusterfähige Aktualisieren funktioniert, muss die entsprechende Clusterrolle installiert werden. Das lässt sich per Mausklick im Steuerungsdialog initiieren, es startet der obligatorische Assistent. Abbildung 20.46 zeigt den ersten »wirklichen« Dialog des Assistenten: Ganz klar, wir wollen die Rolle dem Cluster hinzufügen.

Es können diverse Optionen gesetzt werden, die Sie in dem in Abbildung 20.47 gezeigten Dialog konfigurieren können. Die Optionen sind weitgehend selbsterklärend. Die wichtige

Nachricht an dieser Stelle ist, dass Sie keine Optionen setzen müssen. Die Standardeinstellungen sind durchaus in Ordnung. Wichtig ist nur, dass man recht umfangreich in die Konfiguration eingreifen »könnte«.

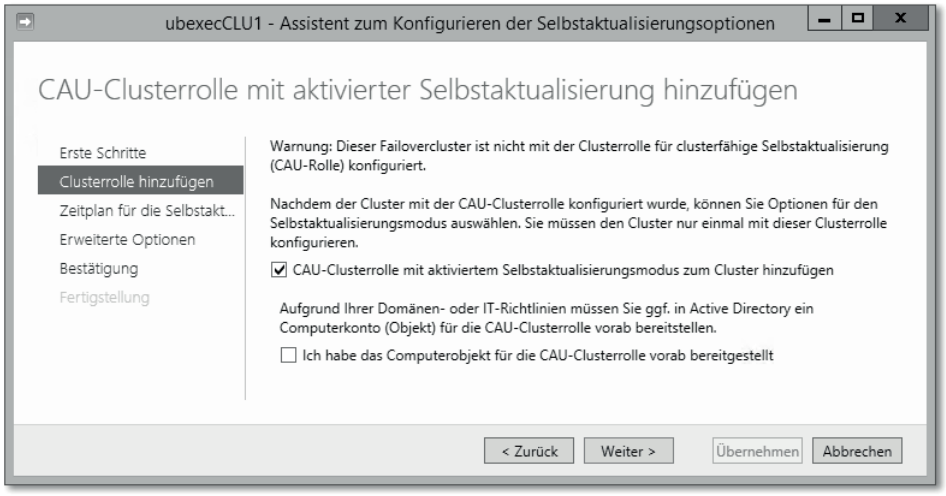


Abbildung 20.46 Installation der zugehörige Clusterrolle per Assistent

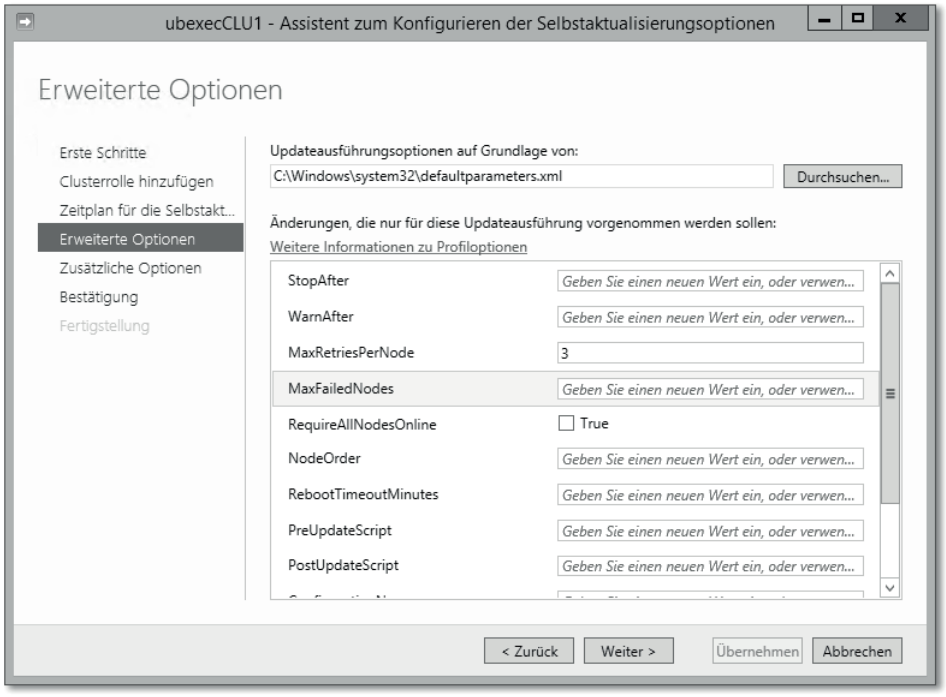


Abbildung 20.47 »Erweiterte Optionen« können, müssen aber nicht unbedingt gesetzt werden.

Abbildung 20.48 zeigt den laufenden Vorgang. Sie können im oberen Bereich des Dialogs erkennen, dass zunächst der eine Clusterknoten aktualisiert wird (auf dem Bild lädt er gerade die Updates herunter), während der andere in »Wartestellung ist«. Die aktiven Rollen sind auf den derzeit wartenden Knoten geschwenkt worden – er wartet also nur im Sinne des Update-Vorgangs, ansonsten ist er sehr aktiv.

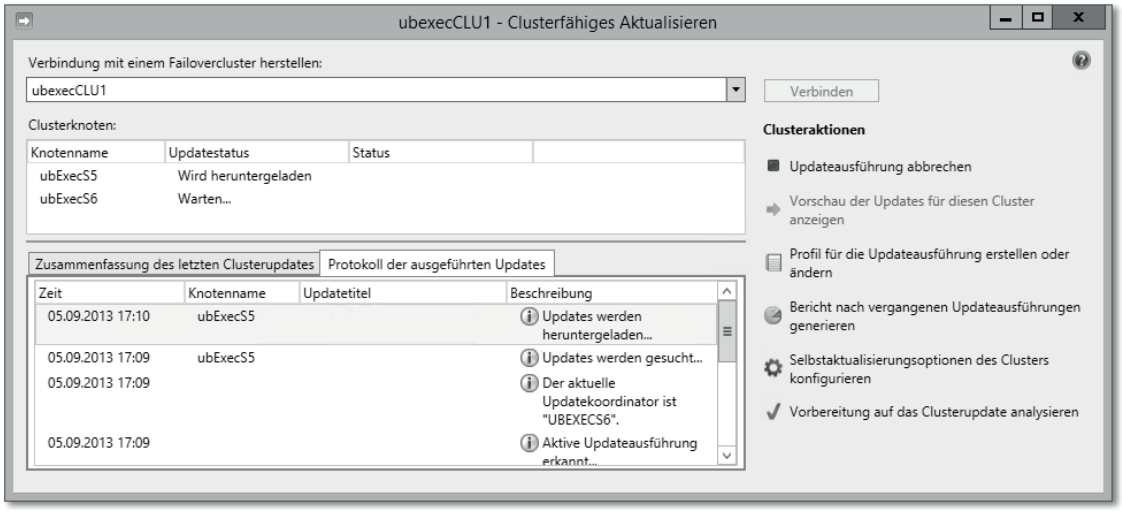


Abbildung 20.48 Hier läuft der Vorgang. Erst wird der eine Server »bearbeitet«, dann der andere.

Wenig überraschend ist, dass nach Abschluss des Updates des ersten Knotens geschwenkt wird, d.h., der frisch aktualisierte Knoten wird bezüglich der anderen Rollen der aktive Knoten, und der andere Clusterknoten wird aktualisiert.

Die beiden Clusterknoten des Demosystems laufen auf virtuellen Maschinen. Auf Abbildung 20.49 kann man erkennen, dass diese mit etwa 13 Minuten Zeitdifferenz neu gestartet worden sind. Das Update des zweiten Knotens hat also genau diese Zeit gedauert.

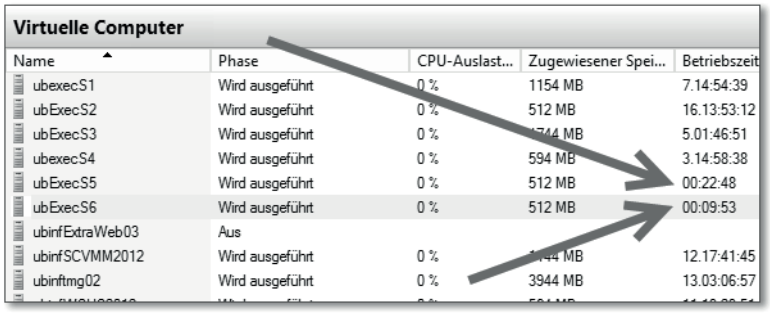


Abbildung 20.49 Da die Clusterknoten in diesem Beispiel virtualisiert laufen, kann man erkennen, dass sie mit 13 Minuten Zeitdifferenz neu gestartet wurden.

20.2.7 SQL Server 2012 installieren

Da der SQL Server ein Dienst ist, der häufig geclustert wird und die Installation etwas abweicht, führe ich diese kurz vor – ohne an dieser Stelle den Anspruch zu haben, eine detaillierte SQL-Anleitung zu liefern.

Sie müssen zunächst einen funktionsfähigen Cluster installieren. Anstatt dann den exemplarisch am Dateiserver-Cluster gezeigten Rollendienst zu installieren, machen Sie wie folgt weiter.

Installation des ersten Knotens

Um den ersten SQL-Clusterknoten zu installieren, führen Sie diese Schritte durch:

- Schnappen Sie sich den SQL Server-Installationsdatenträger, und lassen Sie das SQL Server-Installationscenter starten.
- Dort wählen Sie Option Neue SQL Server-Failoverclusterinstallation (Abbildung 20.50). Um es einmal ganz deutlich auszusprechen: Sie starten nicht die normale SQL-Installation.

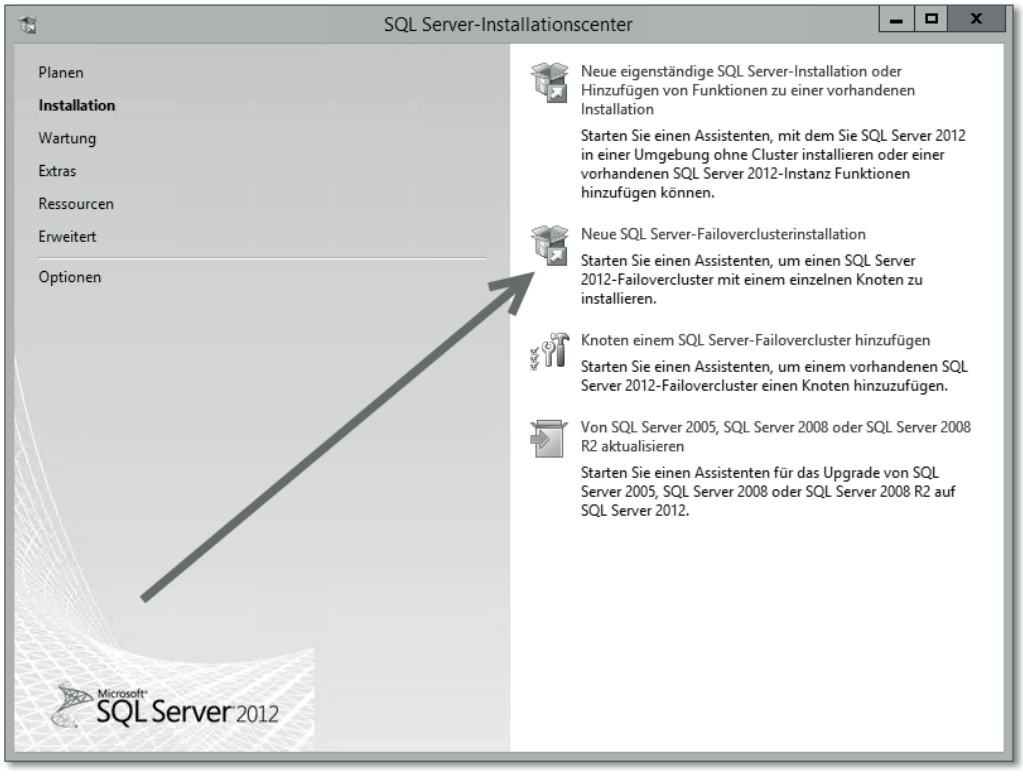


Abbildung 20.50 Im SQL-Setup rufen Sie eine »Neue SQL Server-Failoverclusterinstallation« auf.

Hinweis

Wenn Sie mehrere Instanzen des SQL Server betreiben möchten, gehen Sie auch bei der zweiten und den folgenden Installationen vor, wie hier beschrieben. Sie beginnen dann ebenfalls mit einer NEUEN SQL SERVER-FAILOVERCLUSTERINSTALLATION.

- Die erste Frage des Assistenten bezieht sich darauf, was überhaupt installiert werden soll (Abbildung 20.51). Wählen Sie die SQL SERVER-FUNKTIONSINSTALLATION. Lassen Sie sich nicht davon irritieren, dass hier keine Rede von »Cluster« ist.

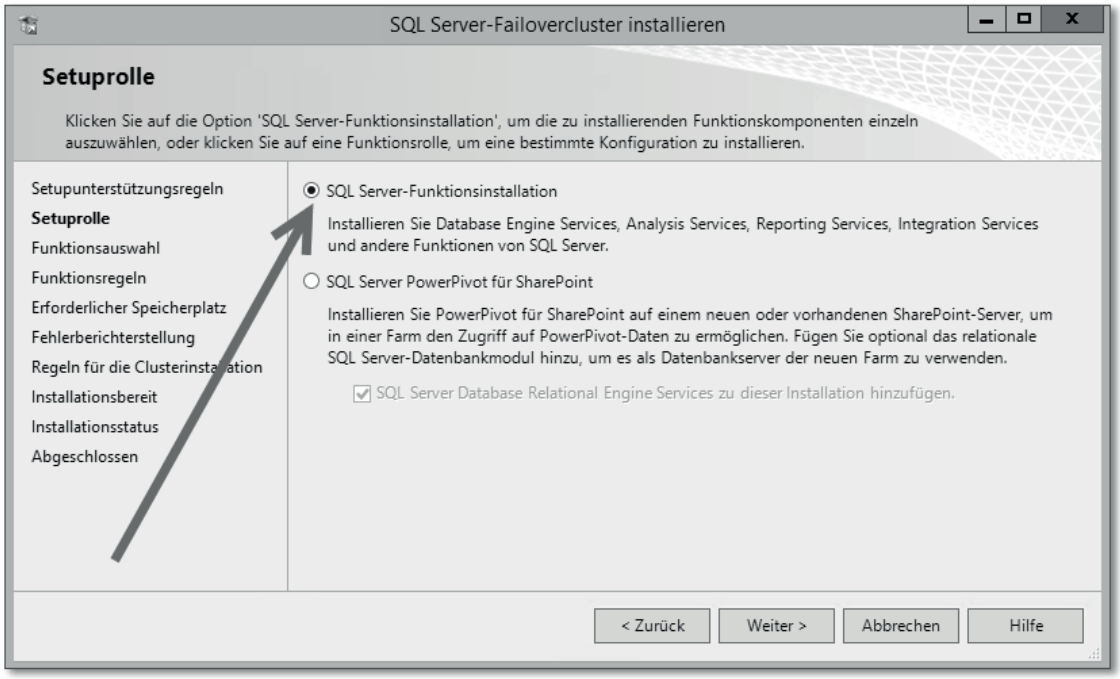


Abbildung 20.51 Wählen Sie diese Option.

- In dem in Abbildung 20.52 gezeigten Dialog wählen Sie aus, was installiert werden soll. Auf jeden Fall wird DATABASE ENGINE SERVICE benötigt, das ist die eigentliche Datenbank. Beachten Sie, dass ANALYSIS SERVICES und REPORTING SERVICES zwar auf Clusterknoten installiert werden können, sie sind aber trotzdem nicht geclustert. Ich würde diese Dienste nach Möglichkeit nicht auf Clustern installieren.

  Zu empfehlen wäre noch, in der Rubrik FREIGEGEBENE FUNKTIONEN die Verwaltungswerkzeuge zur Installation auszuwählen.

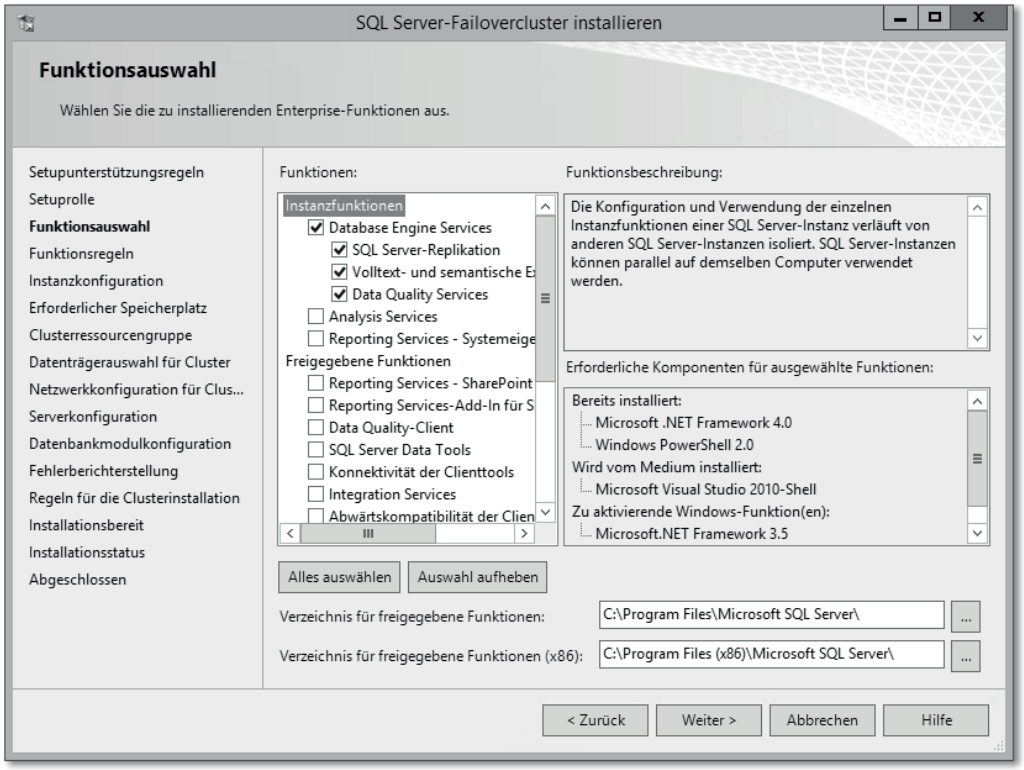


Abbildung 20.52 Für dieses Beispiel wird nur das Datenbankmodul installiert.

- Der in Abbildung 20.53 gezeigte Dialog wird jedem bekannt vorkommen, der bereits einen SQL Server aufgesetzt hat. Es gibt aber einen kleinen Unterschied, nämlich das Feld NAME DES SQL SERVER-NETZWERKS. Dahinter verbirgt sich der Name des SQL-Clusters. Anders gesagt, nach der Installation wird ein Computerkonto dieses Namens vorhanden sein. Noch anders gesagt, diese Instanz des SQL-Clusters wird unter diesem Namen vorhanden sein.

  Sinnvollerweise entscheiden Sie sich für eine STANDARDINSTANZ. Hier eine benannte Instanz zu wählen, bedeutet höchstens Tipparbeit. Das Instanzstammverzeichnis wird nicht auf die Clusterdatenträger gelegt. Da dort keine Daten liegen werden, können Sie auch ruhig das Standardverzeichnis belassen.
- Der in Abbildung 20.54 gezeigte Dialog ist einfach, aber wirkungsvoll. In einer CLUSTERRESSOURCENGRUPPE werden die Ressourcen (wie Platten, IP-Adresse, Name, SQL Server etc.) zusammengefasst. Es ist sinnvoll, diese CLUSTERRESSOURCENGRUPPE wie den Cluster (Netzwerkname, siehe Abbildung 20.53) zu benennen.

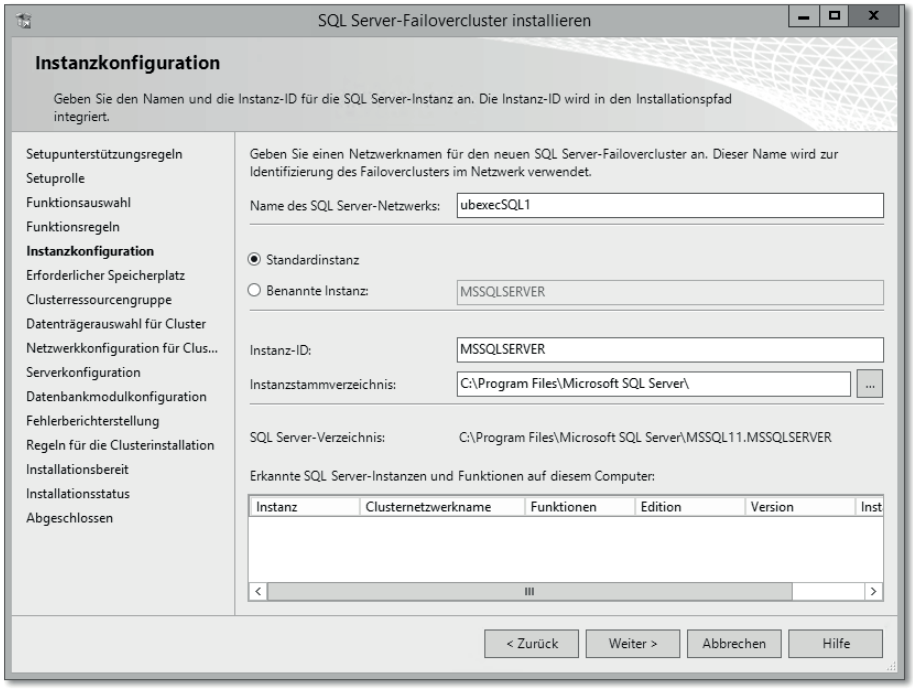


Abbildung 20.53 Interessant ist der Name des SQL-Clusters. Ansonsten empfiehlt sich die Installation einer »Standardinstanz«.

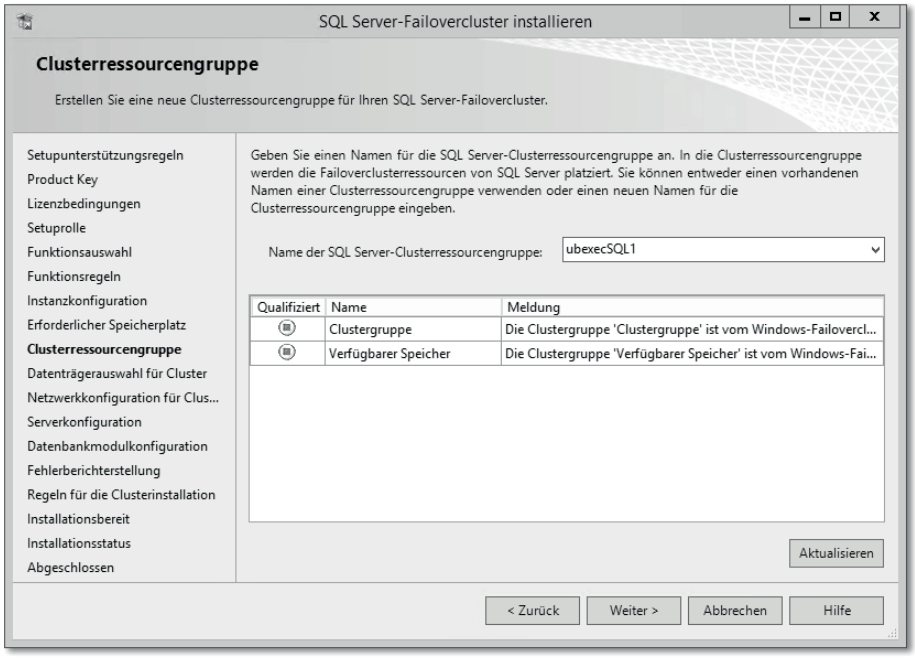


Abbildung 20.54 Erstellen Sie eine neue »Clusterressourcengruppe«.

Nun wird es mit der Zuweisung von Ressourcen ernst:

- In Abbildung 20.55 sehen Sie den Dialog für die Zuweisung von Clusterdatenträgern, die zuvor angelegt worden sein müssen. Sie können einfach die Datenträger anhaken, die für diese Clusterinstanz verwendet werden sollen. Wenn Datenträger nicht zur Auswahl stehen, beispielsweise weil sie schon von anderen Clusterressourcen oder für das Quorum verwendet werden, wird das mit einer kurzen Erläuterung angezeigt.

  Beachten Sie: Wenn Sie mehrere SQL-Cluster (also Instanzen) auf dem Cluster installieren möchten, benötigen diese jeweils eigene Datenträger.

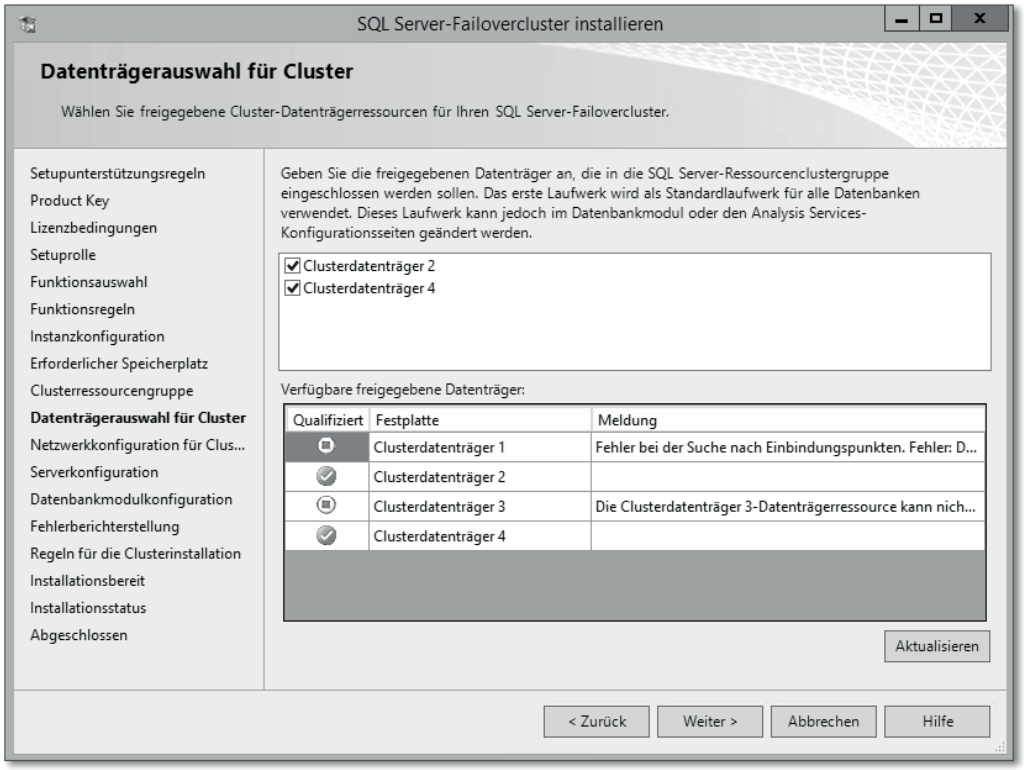


Abbildung 20.55 Wählen Sie die Datenträgerressourcen für den neuen SQL-Cluster.

- Dem neuen SQL-Cluster muss dann noch eine IP-Adresse zugewiesen werden, was Abbildung 20.56 zeigt.
- Als Nächstes werden die Dienstkonten zugewiesen (Abbildung 20.57). Hier müssen Sie Domänenkonten verwenden. Diese Konten brauchen Sie nicht mit »besonderen Rechten« auszustatten – das erledigt das SQL-Setup für Sie.

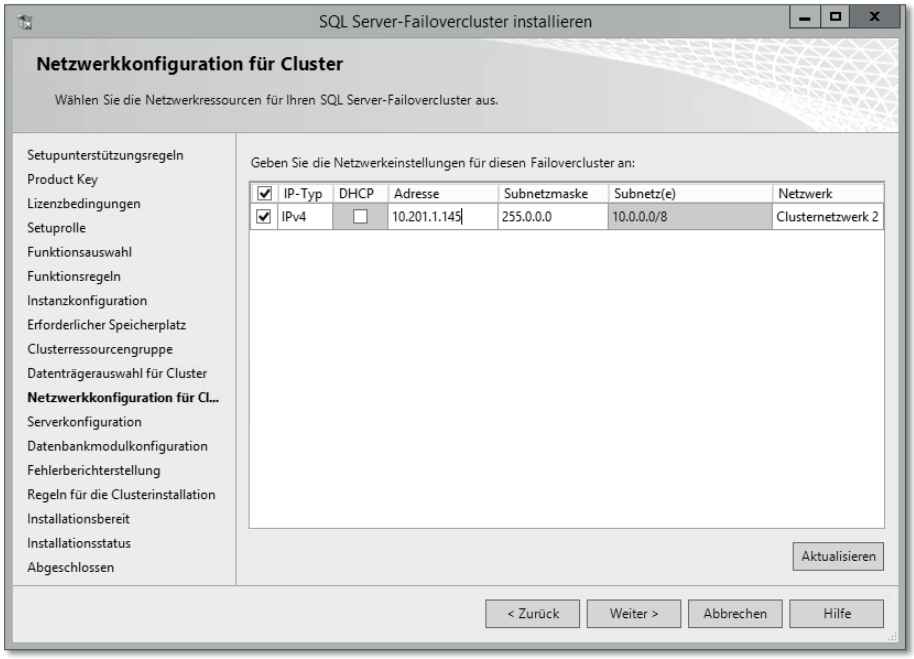


Abbildung 20.56 Zuweisen der IP-Adresse

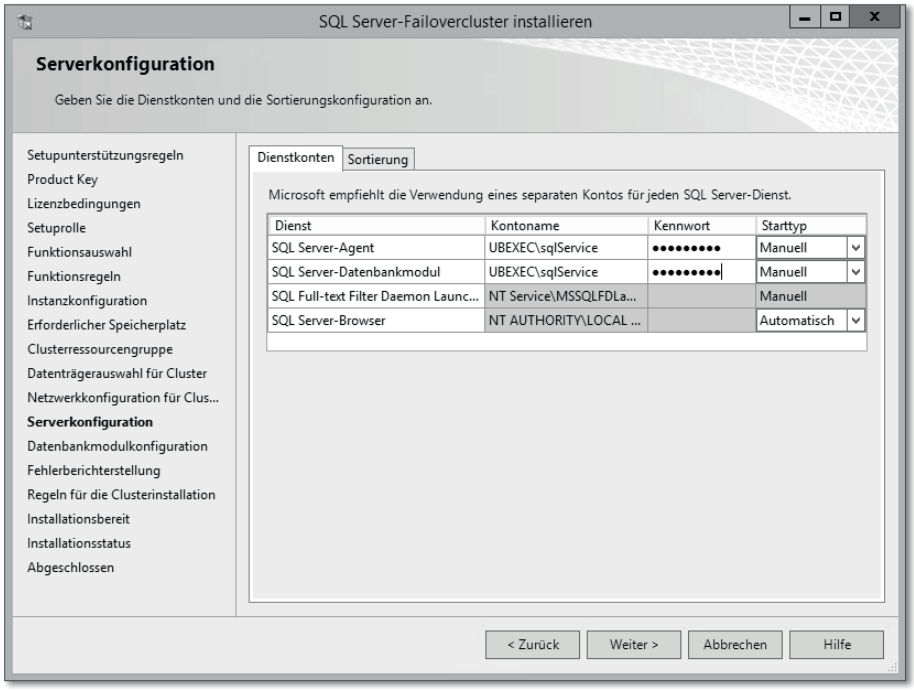


Abbildung 20.57 Angeben der Dienstkonten. Es müssen Domänenkonten verwendet werden.

Hinweis

Beachten Sie, dass SQL Server es bei Domänenkonten aus Berechtigungsgründen nicht schafft, automatisch die SPNs zu registrieren (*SPN = Service Principal Name*). Sie müssen die SPNs entweder manuell anlegen oder eine generelle Berechtigung im AD setzen. Mehr Infos gibt es hier: *http://technet.microsoft.com/de-de/library/ms191153.aspx#Auto*

- Nun müssen im auf Abbildung 20.58 gezeigten nächsten Dialog die Datenverzeichnisse eingerichtet werden. Diese Pfade müssen auf Clusterdatenträger verweisen.

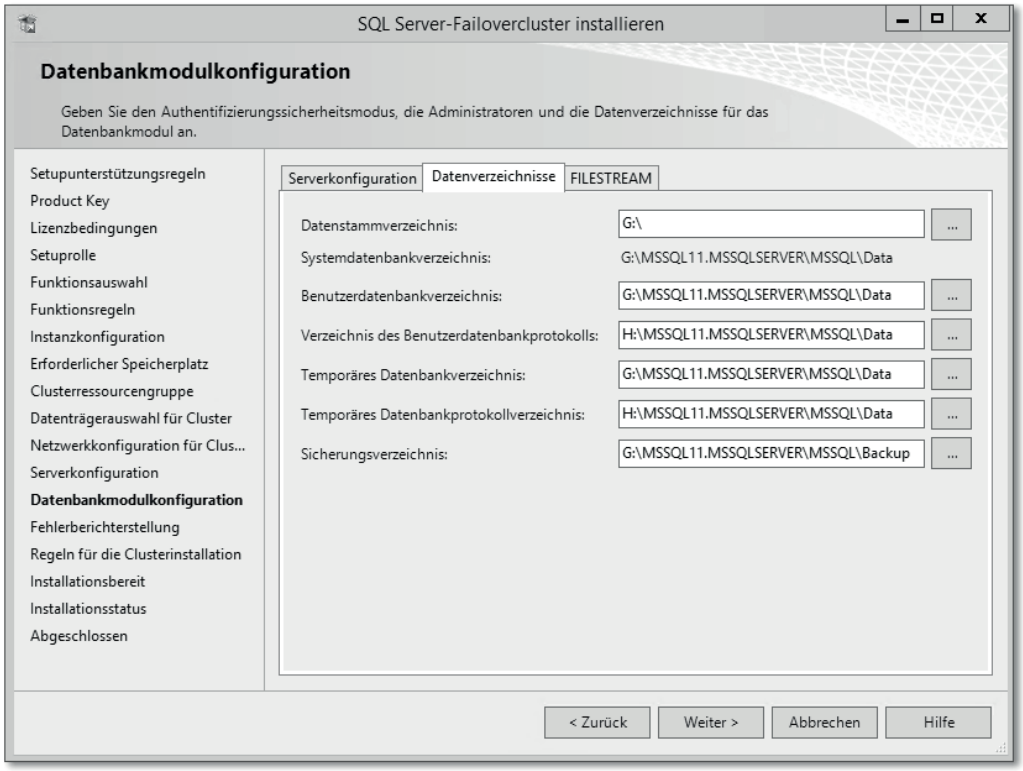


Abbildung 20.58 Hier werden die Datenverzeichnisse eingerichtet.

Hinweis

Auch wenn der SQL Server auf einem Cluster liegt: Er ist nicht automatisch schnell. Der entscheidende Faktor für die SQL Server-Performance sind Platten – und zwar sowohl die Anzahl und der RAID-Level als auch Faktoren wie die Blockgröße oder das Alignment. Sie müssen also auch beim Cluster die »Sizing-Hausaufgaben« sorgfältig erledigen.

Wenn, wie in Abbildung 20.59 gezeigt, alles auf »Grün« steht, ist der erste Schritt getan. Sie haben nun einen funktionsfähigen Ein-Knoten-SQL-Cluster, der übrigens schon funktionsfähig ist – nur eben nicht redundant. Wie man die weiteren Knoten zu SQL-Clusterknoten macht, zeigt der nächste Abschnitt.

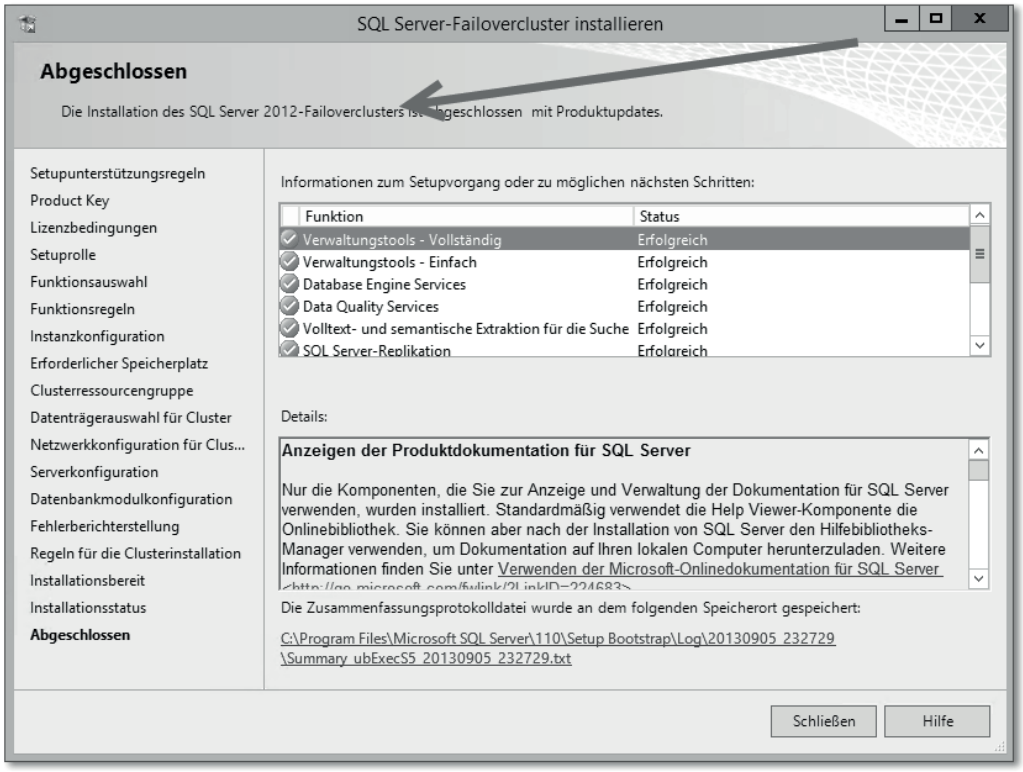


Abbildung 20.59 Der SQL-Failover-Cluster ist erstellt – alles im grünen Bereich!

Zweiter und alle weitere Knoten

Nun müssen noch die weiteren Knoten des zukünftigen SQL-Clusters mit SQL Server ausgerüstet werden.

Der »Trick« ist im Grunde genommen, auf den weiteren Knoten im SQL Server-Installationscenter den Menüpunkt Knoten einem SQL Server-Failovercluster hinzufügen auszuführen (Abbildung 20.60). Die Installation ist nicht aufregend kompliziert, es müssen nur wenige Einstellungen getroffen werden.

- Die erste Entscheidung ist, welchem SQL-Failover-Cluster der Knoten hinzugefügt werden soll. Dies wird in dem auf Abbildung 20.61 gezeigten Dialog erledigt. Beachten Sie, dass es in einem (Windows-)Cluster mehrere SQL-Cluster (Instanzen) geben kann. Der Dialog ergibt also Sinn.

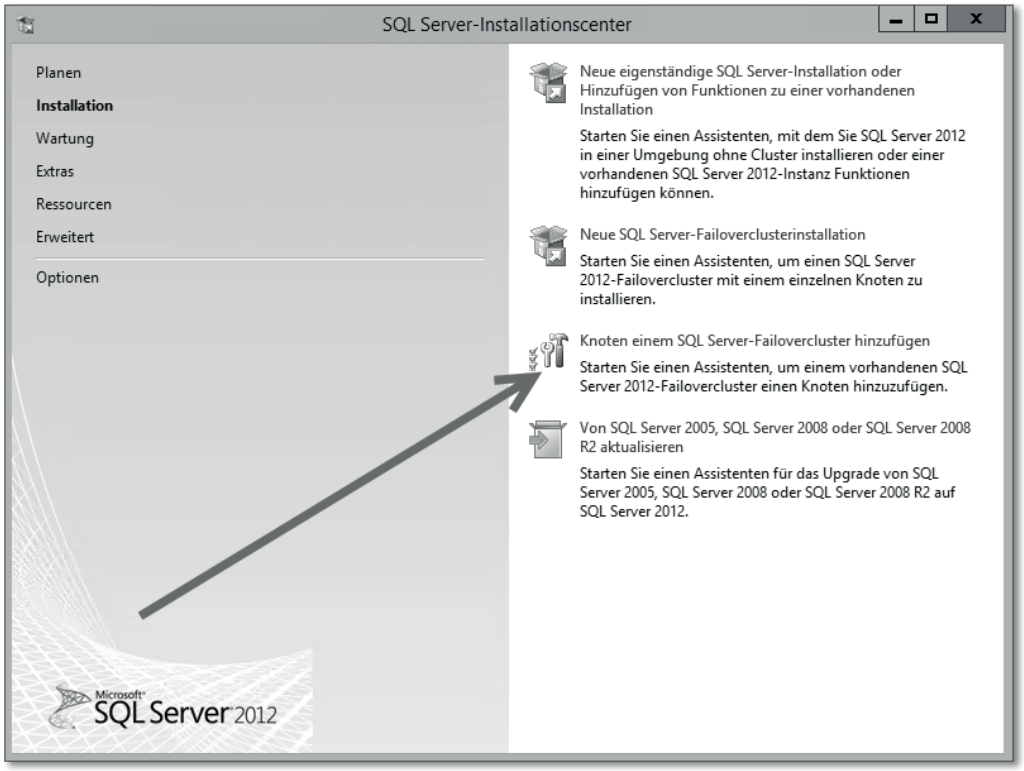


Abbildung 20.60 Diese Option führen Sie auf allen weiteren Knoten aus.

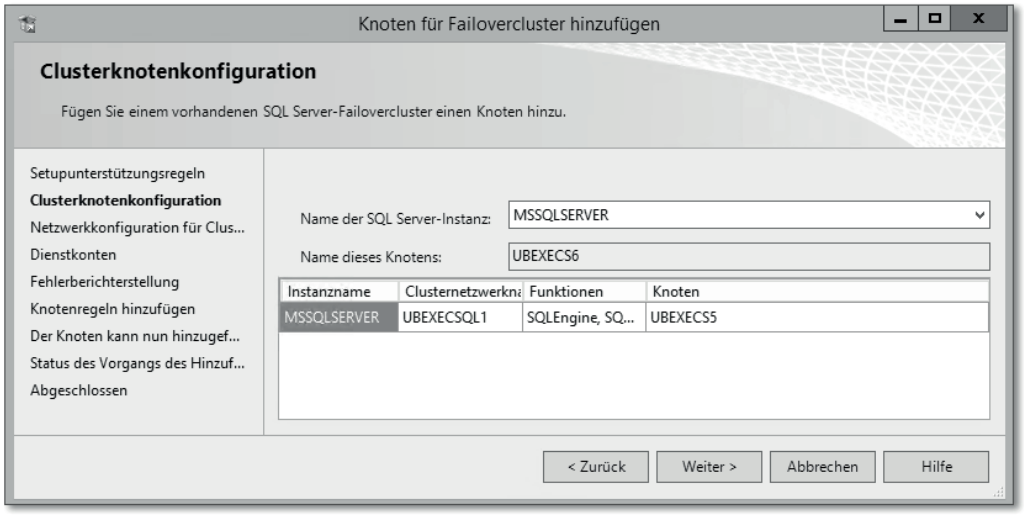


Abbildung 20.61 Auswahl des SQL-Clusters, dem der Knoten hinzugefügt werden soll

- In Abbildung 20.62 sehen Sie die Konfiguration der Netzwerkeinstellungen. Sie selektieren hier das zu verwendende Clusternetzwerk. Vermutlich ist, zumindest in einer kleineren Installation, hier ohnehin nur ein Clusternetzwerk vorhanden.

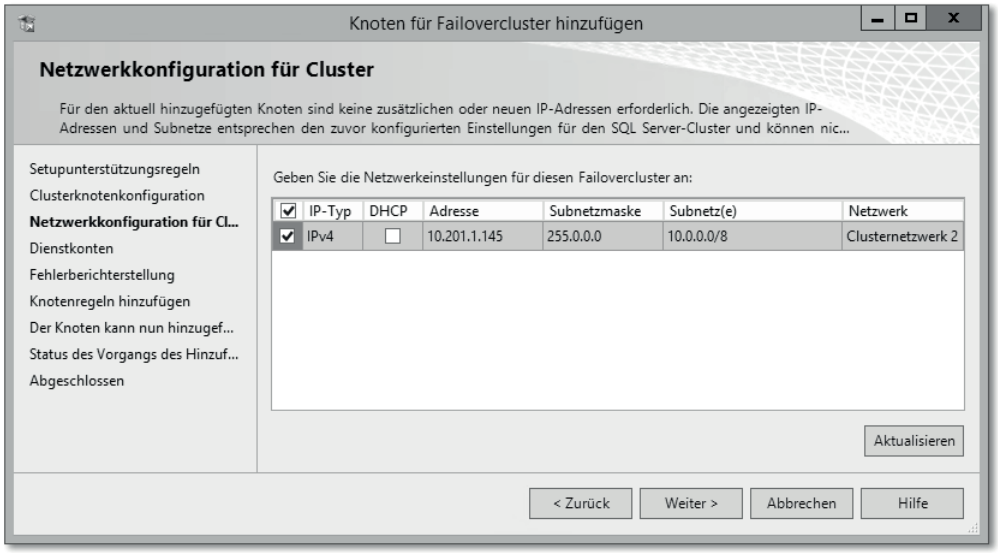


Abbildung 20.62 In der Netzwerkkonfiguration müssen Sie die zu verwendenden Netze selektieren.

- Abbildung 20.63 zeigt den Dialog zur Eingabe der Kennwörter der Dienstkonten. Da der SQL-Cluster ja auf diesem Knoten laufen soll, müssen die Dienstkonten nebst Kennwörtern gespeichert werden.

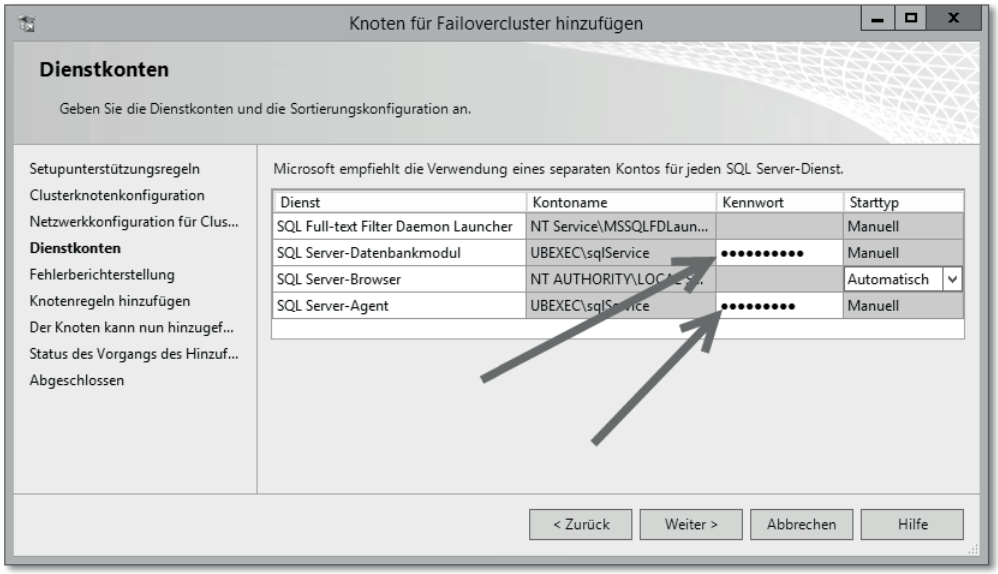


Abbildung 20.63 Die Kennwörter der Dienstkonten müssen eingegeben werden.

An dieser Stelle wird auch klar, warum die Dienstkonten Domänenkonten sein müssen: Damit dasselbe Dienstkonto auf verschiedenen Clusterknoten vorhanden ist, geht das nur mit Domänenkonten – hinter dem Konto NETZWERKDIENST steht letztendlich das Computerkonto, und das wäre auf den verschiedenen Servern bzw. Clusterknoten jeweils ein anderes Konto.

Nach Abschluss des Installations-Assistenten steht der Clusterknoten zur Verfügung.

20.3 Network Load Balancing

Nicht alle Aspekte der Verfügbarkeit lassen sich sinnvoll mit dem Failover-Cluster abdecken. Das Verfahren kommt immer dann zum Einsatz, wenn eine Ressource nicht »dupliziert« werden kann, sondern genau der eine Applikationsserver vorhanden sein muss. Typische Beispiele sind ein Exchange-Postfachserver oder eine SQL Server-Datenbank: Wenn ein Postfach auf dem Server *Exchange01* liegt, hilft es dem Anwender bei einem Ausfall wenig, dass *Exchange02* und *Exchange03* noch funktionieren – auf sein Postfach kann er nicht zugreifen. Es muss also dafür gesorgt werden, dass genau die Ressource *Exchange01* möglichst schnell wieder verfügbar wird. Dies kann, wie beim Failover-Cluster der Fall, durchaus auf anderer Hardware sein, die sich dann aber als *Exchange01* meldet.

Andere Serverdienste werden nicht geclustert, obwohl sie nicht weniger wichtig sind. Einige Beispiele:

- Das *Active Directory* können Sie sehr einfach dadurch redundant auslegen, dass Sie weitere Domänencontroller implementieren. Fällt ein Domänencontroller aus, greifen die Clients automatisch auf die verbliebenen zu. Der Anwender bemerkt den Ausfall nicht einmal. Im AD-Umfeld sind als Ausnahmen die Server zu nennen, die FSMO-Rollen ausführen (siehe ADDS-Kapitel). Steht eine FSMO-Rolle nicht zur Verfügung, leidet der »normale« Betrieb aber nicht darunter.
- *DNS*: Auch in diesem Fall basiert das Redundanzkonzept auf der Fähigkeit der Clients, einfach den nächsten DNS-Server zu kontaktieren.

Die Dienste aus dem zuvor genannten Beispiel sind deshalb relativ einfach redundant auszulegen, weil die »Redundanz-Intelligenz« (d.h. »Wie verhalte ich mich beim Ausfall der Ressource?«) in den jeweiligen Clients implementiert ist.

Nun gibt es aber noch eine dritte Gruppe von Diensten, die durch folgende Kriterien zu beschreiben ist:

- Der einzelne Server ist ersetzbar, d.h., der Dienst ist nicht so »einzigartig«, dass nicht ein anderer Server den Benutzer weiter bedienen könnte.
- Der Client verfügt nicht über integrierte Failover-Mechanismen.

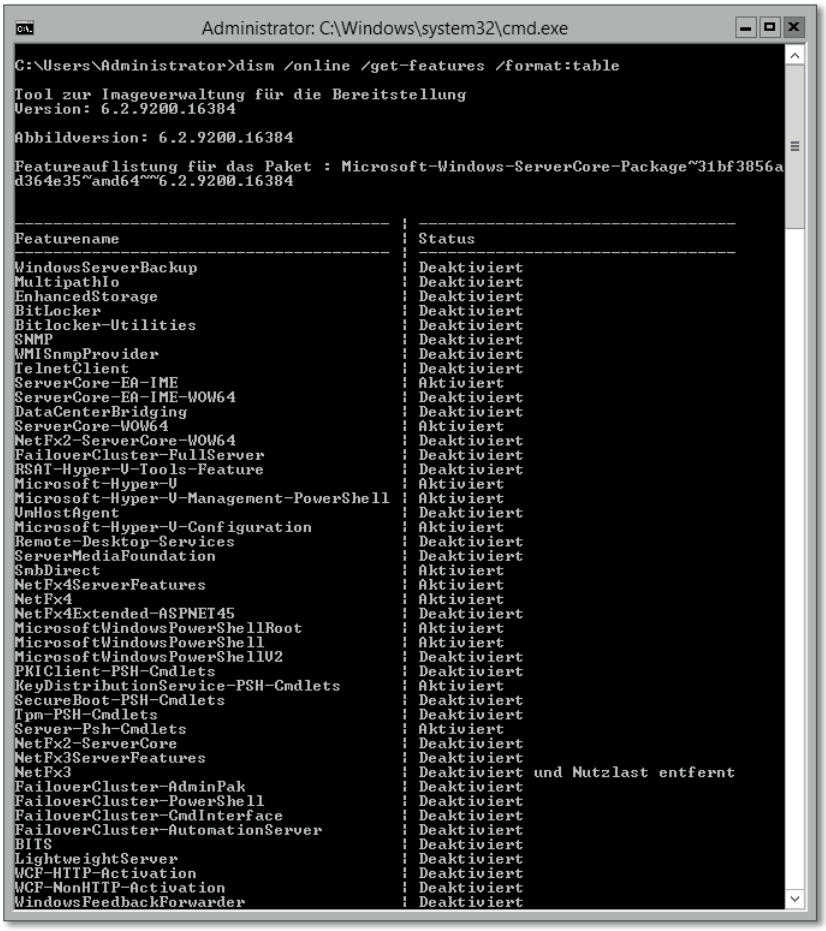


Abbildung 22.11 Das vom Core-Server bekannte Kommando »oclist« zeigt, dass auf einem Hyper-V-Server eher wenige Rollen und Features installierbar sind.

22.3 Der Hyper-V-Manager

Für die Administration von Hyper-V stehen zwei Werkzeuge zur Verfügung:

- der Hyper-V-Manager
- der Systems Center Virtual Machine Manager 2012

Der Hyper-V-Manager ist sozusagen das Standardwerkzeug, das ohne zusätzliche Kosten verwendet werden kann. Wenn Hyper-V auf einem Windows Server 2012 Core-Server installiert ist oder der Hyper-V-Server 2012 verwendet wird, steht der Hyper-V-Manager nicht auf dem Server selbst zur Verfügung. Das Management wird dann von einem anderen Windows Server 2012 aus vorgenommen oder, was ich für noch besser halte, von einem Admin-PC aus.

Zu diesem Zweck stellt Microsoft im Download Center die Remote Server Administration Tools für Windows 8 zur Verfügung, in denen auch der Hyper-V-Manager enthalten ist.

Der Hyper-V-Manager ist einfach und intuitiv zu bedienen; mit ihm kann man neue virtuelle Maschinen anlegen, neue und bestehende VMs konfigurieren und administrieren sowie grundlegende Überwachungsarbeiten durchführen.

Der wesentliche Nachteil des Hyper-V-Managers ist, dass er nur eine sehr serverzentrierte Sicht der Dinge bietet. In einer größeren Umgebung mit mehreren, unter Umständen Dutzenden virtuellen Servern ist es recht lästig, wenn man zunächst suchen muss, auf welchem physikalischen Server die gesuchte virtuelle Maschine läuft, weil es keine »Alle VMs«-Ansicht gibt. Wie Sie in Abbildung 22.12 sehen können, lassen sich zwar mehrere Server registrieren (siehe Serverauswahl auf der linken Seite), um mit einer VM zu arbeiten, muss aber stets der zugehörige Server ausgewählt werden.

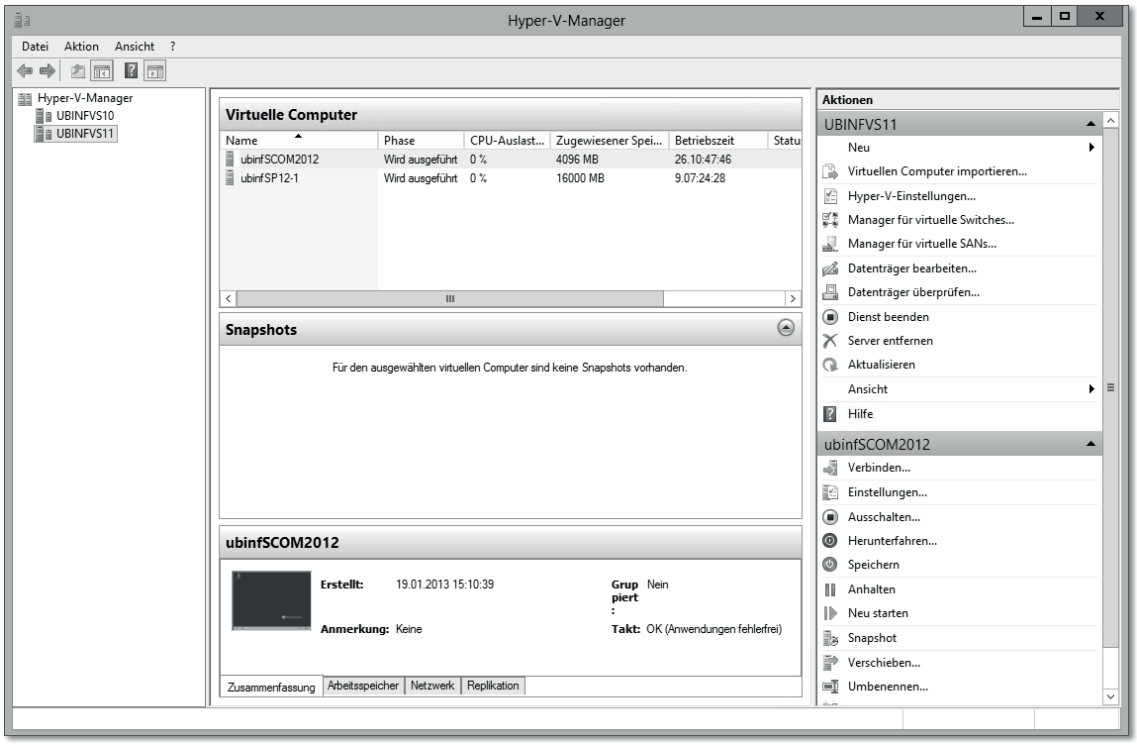


Abbildung 22.12 Der Hyper-V-Manager ist das »Regiezentrum« für die virtuellen Maschinen.

Wie aus Abbildung 22.13 zu entnehmen, gibt es deutlich komfortablere Werkzeuge für das Management von mittleren und großen Umgebungen, die Servervirtualisierung nutzen. Gezeigt ist der System Center Virtual Machine Manager 2012, der viele wesentliche Funktionalitäten bietet, die man sich beim Management einer servervirtualisierten Umgebung wünscht. Zu beachten ist, dass der Virtual Machine Manager kostenpflichtig ist.

SCVMM

Der System Center Virtual Machine Manager wird gegen Ende dieses Kapitels kurz vorgestellt.

Es soll jetzt nicht der Eindruck entstehen, dass man zur sinnvollen Arbeit mit Hyper-V unbedingt den Virtual Machine Manager bräuchte. Die wesentlichen Aufgaben lassen sich durchaus komfortabel mit dem Hyper-V-Manager erledigen. Hat ein Administrator einer Umgebung, die aus mehr als einem Hyper-V-System besteht, einmal die VMM-Möglichkeiten gesehen, wird er diesen erfahrungsgemäß aber sehr gern nutzen wollen.

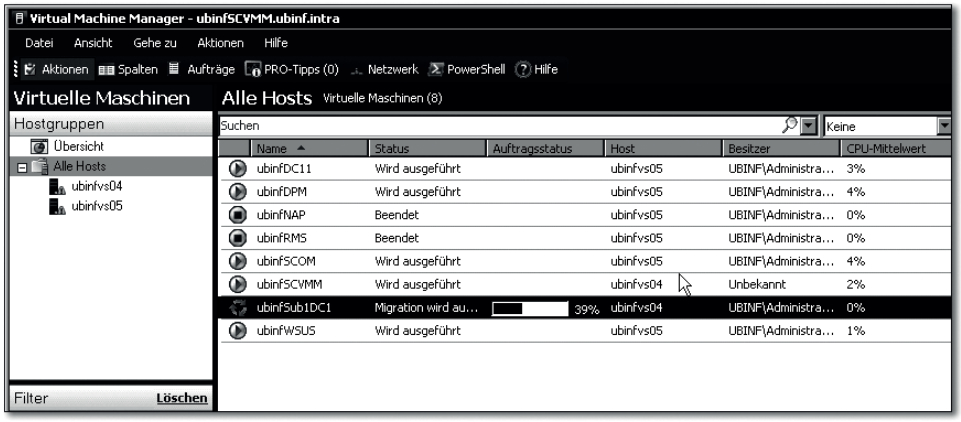


Abbildung 22.13 Der Virtual Machine Manager ist in mittleren und großen Umgebungen ein wesentlich leistungsfähigeres Management-Werkzeug – er ist allerdings kostenpflichtig.

22.4 Installation und Grundkonfiguration

Über die Installation von Hyper-V kann man im Grunde genommen nicht allzu viel schreiben: Server-Manager starten, Rolle hinzufügen, fertig! Ein paar Hinweise möchte ich aber dennoch loswerden.

22.4.1 Vorbereitung, insbesondere Netzwerkkonfiguration

Es empfiehlt sich unbedingt, einen Hyper-V-Server mit zwei Netzwerkkarten auszurüsten (Abbildung 22.14):

- Eine Netzwerkkarte wird für den Zugriff auf den Server selbst verwendet, also für das Management. Auf dieser Karte wird ganz normal das IP-Protokoll gebunden, und die übrigen Elemente, wie Client für Microsoft-Netzwerke, werden aktiviert. Mit anderen Worten: Bei der Management-Netzwerkkarte brauchen Sie außer der Konfiguration der IP-Adressen nichts zu tun.

- Eine zweite Netzwerkkarte wird für die Konfiguration der virtuellen Maschinen verwendet. Bei dieser Karte deaktivieren Sie alle Komponenten, unter anderem auch IPv4 und IPv6. Es braucht hier nichts gebunden zu sein, weil das Serverbetriebssystem selbst über diese Karte nicht kommuniziert.

  Je nach durch die virtuellen Maschinen verursachter Netzwerklast könnte man für die virtuellen Maschinen auch mehrere Netzwerkkarten vorsehen – entweder in einer Teaming-Konfiguration oder individuell einzelnen VMs zugewiesen. Falls Sie virtuelle Maschinen betreiben, die beispielsweise Netzwerkkonnektivität in eine DMZ (*Demilitarized Zone*) benötigen, werden weitere Netzwerkkarten erforderlich.

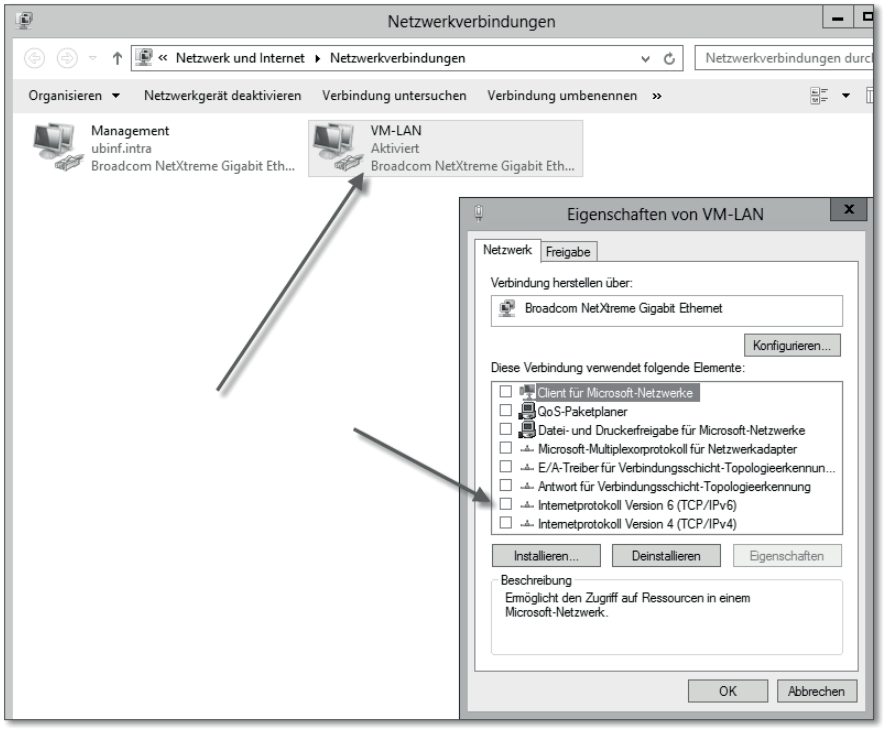


Abbildung 22.14 Ein Hyper-V-Server sollte (mindestens) zwei Netzwerkkarten haben.

Kompatibilität der Netzwerkkarte

Mir sind in der Praxis hin und wieder Probleme mit Netzwerkkarten begegnet. Auf Abbildung 22.15 ist ein unangenehmer Effekt zu sehen. Von einem Client wird eine virtuelle Maschine angepingt, das Antwortverhalten ist zunächst als weitgehend unauffällig anzusehen. Sobald eine RDP-Verbindung aufgebaut wird, bricht die Netzwerkperformance vollständig ein. Zu sehen ist das einerseits an den Ping-Zeiten, die plötzlich dramatisch werden, andererseits benötigt der Verbindungsaufbau ca. eine Minute.

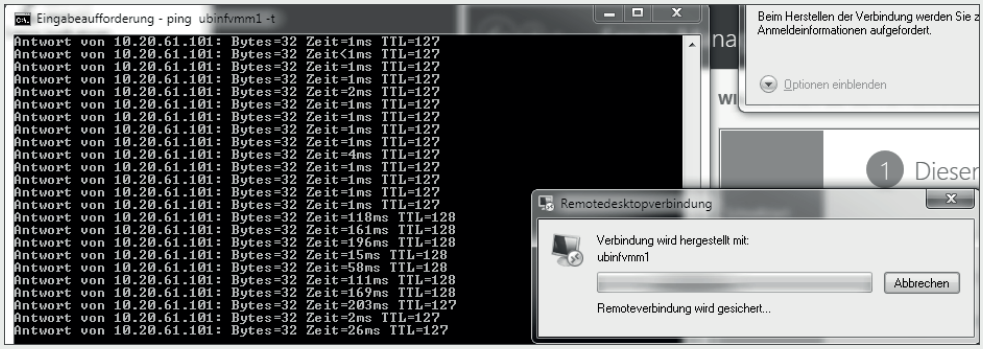


Abbildung 22.15 Problem aus der Praxis: Die Netzwerkleistung bricht ein.

In diesem konkreten Fall lag die Lösung im Deaktivieren der Virtual Machine Queues (Abbildung 22.16). Dies kann in der Konfiguration der Netzwerkkarte erledigt werden – natürlich auf der Netzwerkkarte oder den Netzwerkkarten, die für den Netzwerkverkehr der VMs zuständig ist bzw. sind.

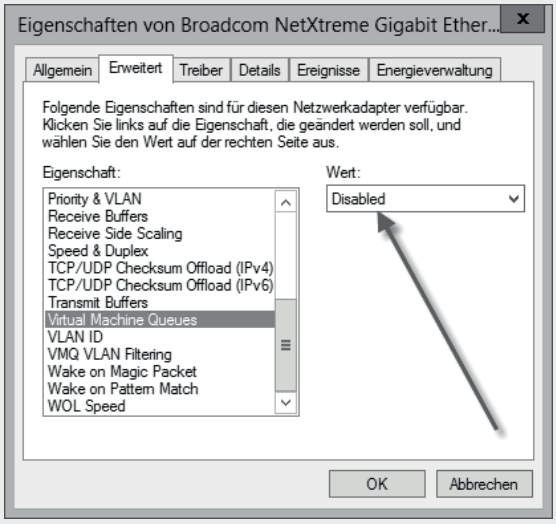


Abbildung 22.16 Lösung in diesem Fall: Deaktivieren der Virtual Machine Queues

Dieser Lösungsansatz ist nicht notwendigerweise die universale Wunderwaffe. Auf aktuellen Dell-Servern mit Broadcom-Gigabit-NICs hat es geholfen, bei anderen Herstellern ist ein weiteres Eingreifen vielleicht gar nicht erforderlich oder kann mit anderen Einstellungen gelöst werden.

22.4.2 Installation

Die Installation der Hyper-V-Rolle startet im Server-Manager mit dem Aufruf des Menüpunkts Rollen und Features hinzufügen. Wer sich in Server 2012 noch nicht so gut zurechtfindet, erhält in Abbildung 22.17 eine kleine Suchen- bzw. Finden-Hilfe.

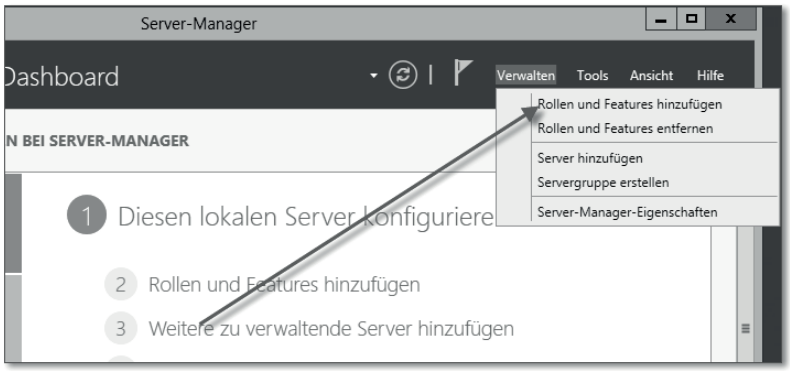


Abbildung 22.17 Das Hinzufügen der Rolle beginnt hier.

Abbildung 22.18 zeigt, dass Hyper-V hier eine zu installierende Rolle ist. Nach dem Setzen des Häkchens werden einige zusätzliche Features angezeigt werden, die ebenfalls installiert werden müssen.

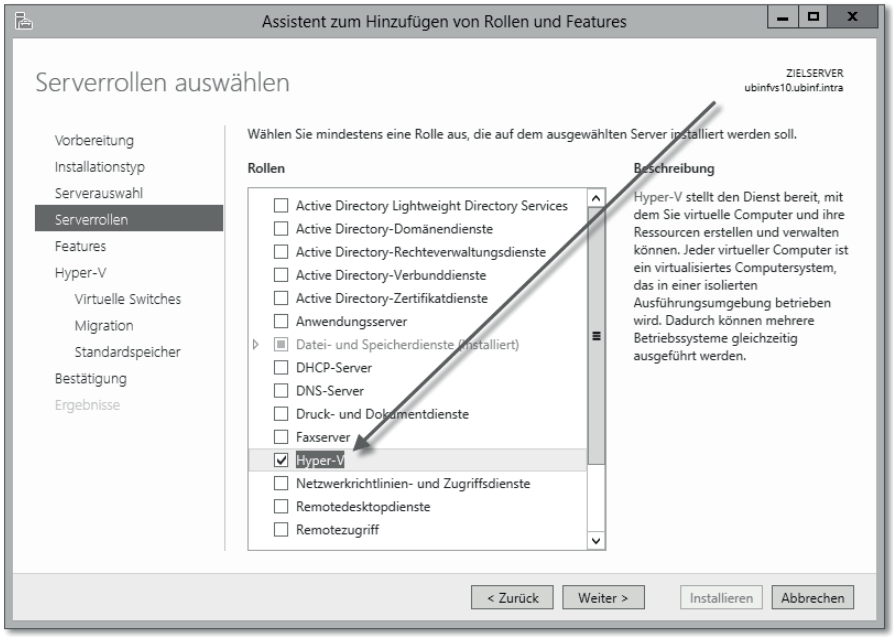


Abbildung 22.18 »Hyper-V« ist eine Rolle. Einige Features werden automatisch hinzugefügt.

Der Assistent zum Hinzufügen der Rolle wird bereits einige Konfigurationsoptionen abfragen: Auf Abbildung 22.19 wird das Einrichten eines ersten virtuellen Switches durchgeführt. Die Netzwerkkarten einer virtuellen Maschine werden mit einem virtuellen Switch verbunden. Dieser wiederum wird mit einer physischen Netzwerkkarte verbunden. Dies ist dann logischerweise die Netzwerkkarte, die für den Netzwerkverkehr der virtuellen Maschinen vorgesehen ist.

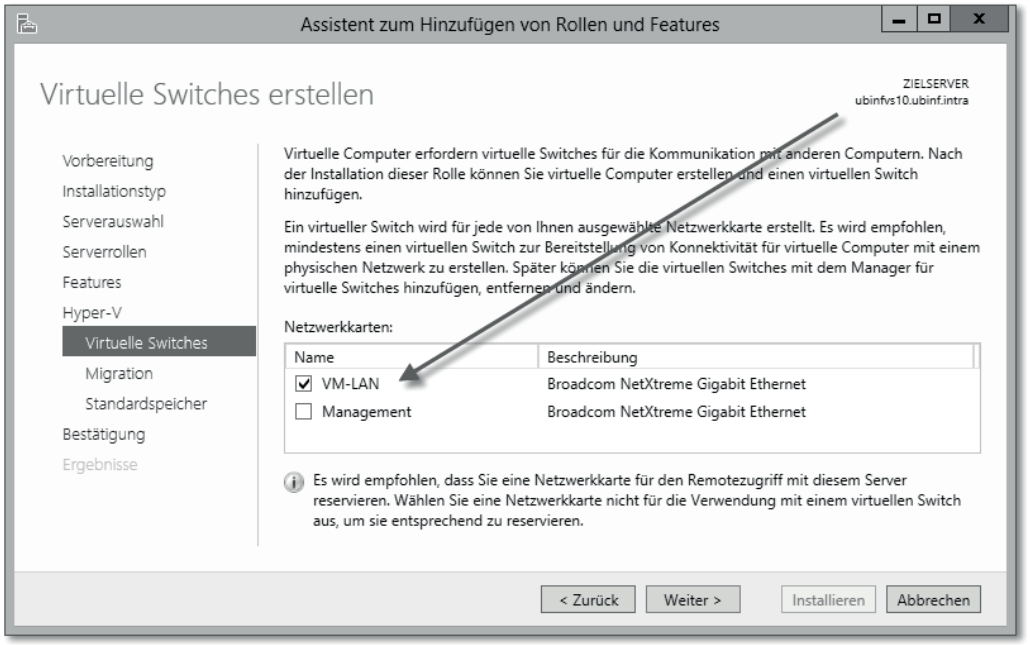


Abbildung 22.19 Wählen Sie die »VM-LAN«-Netzwerkkarte aus.

Abbildung 22.20 zeigt einen Dialog, auf dem festgelegt werden kann, dass dieser Hyper-V-Server Livemigrationen durchführen kann. Unter einer Livemigration versteht man das Verschieben einer laufenden virtuellen Maschine zwischen Hyper-V-Servern. Standardmäßig ist die Checkbox ausgeschaltet und kann natürlich später über den Hyper-V-Manager aktiviert werden. Im Dialog des Hyper-V-Managers lässt sich auch festlegen, über welche Netzwerkkarte die Livemigrationen durchgeführt werden sollen, was in diesem Dialog nicht machbar ist. Die Festlegung der zu verwendenden Netzwerkverbindung ist nicht ganz uninteressant, da dadurch ein erheblicher Netzwerkverkehr entstehen kann.

Weiterhin müssen die Standardspeicherorte festgelegt werden (Abbildung 22.21). Neben dem benötigten Plattenplatz ist die Performance interessant. Der Speicherort für die VHD-Dateien (Festplattenabbilder) muss nicht nur groß, sondern auch hinreichend schnell sein. Wie bereits zuvor erwähnt, ist ein Hauptgrund für die mangelhafte Performance von virtuellen Umgebungen eine unzureichende Festplattenperformance.

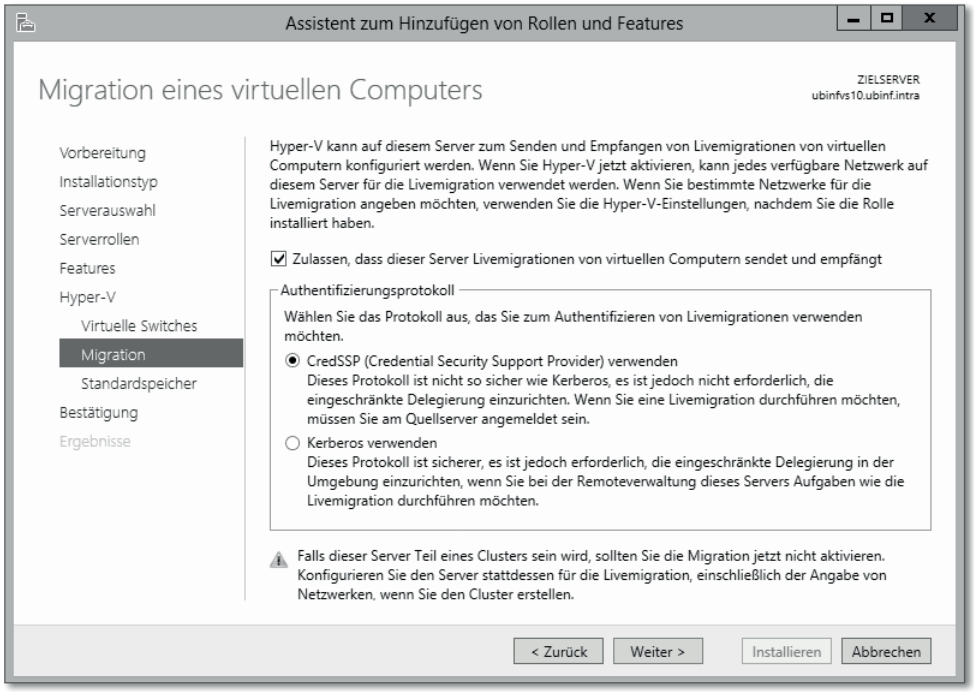


Abbildung 22.20 Wenn Livemigrationen zulässig sein sollen, kann das hier für zugelassen erklärt werden.

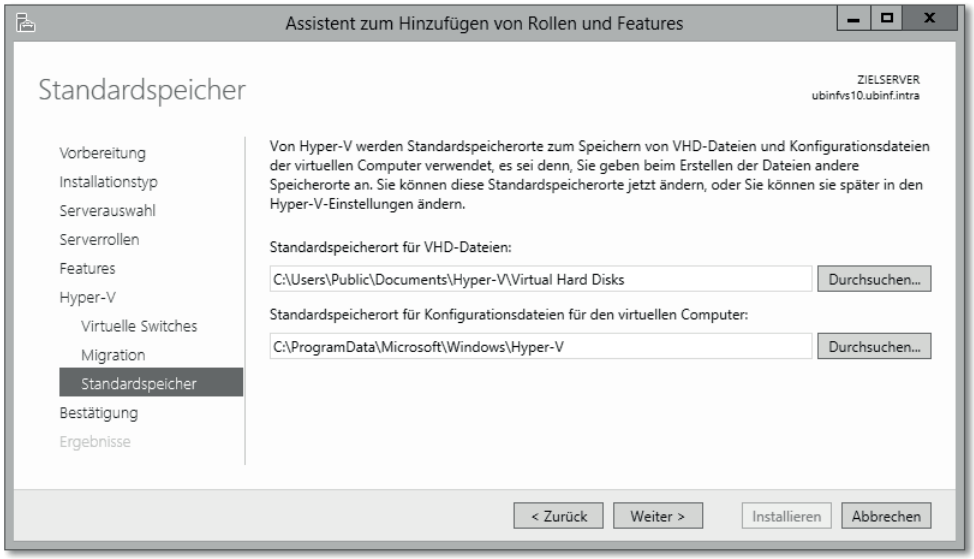


Abbildung 22.21 Die Standardspeicherorte werden gewählt. Vorsicht: Die VHD-Dateien sind performancekritisch!

Die Installation sollte nach kurzer Zeit durchgelaufen sein. Anschließend wird ein Neustart angefordert (Abbildung 22.22). Den Neustart sollten Sie nutzen und die BIOS-Einstellungen überprüfen – siehe folgenden Kasten.

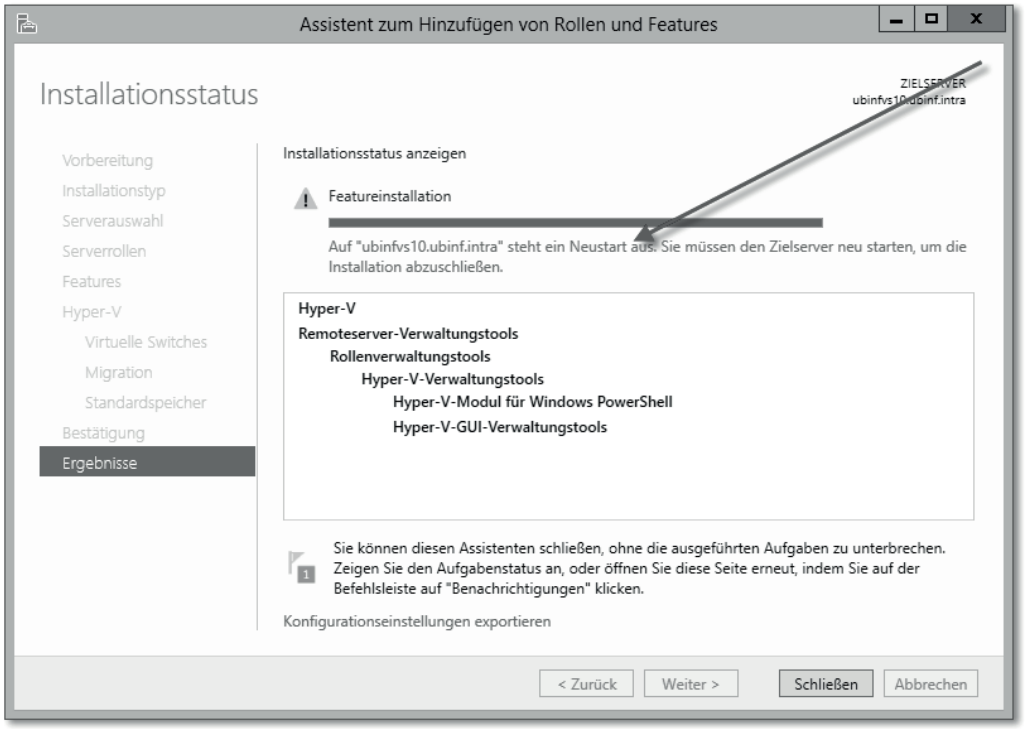


Abbildung 22.22 Nach dem obligatorischen Neustart steht Hyper-V zur Verfügung.

BIOS-Einstellungen

Damit Hyper-V funktioniert, muss die Prozessorvirtualisierung aktiviert sein. Bei der Installation wird das übrigens nicht überprüft, es ist aber trotzdem erforderlich. Diese Einstellung kann im BIOS des Servers vorgenommen werden.

Bei im Jahr 2013 neu erworbenen Servern sollte die Virtualisierungsfunktion des Prozessors im Normalfall aktiv sein, eine kurze Überprüfung schadet aber bestimmt nicht. Vor zwei Jahren hingegen lieferten die meisten Hersteller die Server mit deaktivierter Funktion aus, was man sehr schnell daran merkte, dass die virtuelle Maschine in diesem Fall nicht gestartet werden konnte.

Die weitere Konfiguration geschieht im Hyper-V-Manager. Im dortigen Kontextmenü des Servers können Sie allgemeine Hyper-V-Einstellungen oder den Manager für virtuelle Switches aufrufen (Abbildung 22.23).

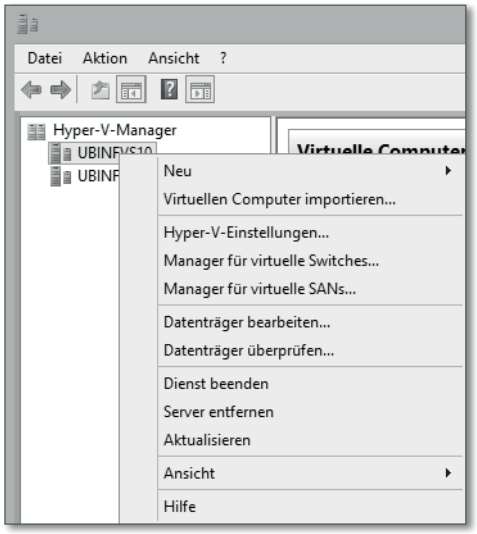


Abbildung 22.23 Die Grundkonfiguration eines Hyper-V-Servers findet hierüber statt.

22.4.3 Grundeinstellung (Hyper-V-Einstellungen)

Den Dialog für die allgemeinen Hyper-V-Einstellungen zeigt Abbildung 22.24. Wer die Hyper-V-Vorgängerversion kennt, wird einige Neuerungen entdecken.

Zunächst werden hier (überschreibbare) Standardpfade definiert, weiterhin gibt es einige Benutzereinstellungen, wie etwa die Behandlung von Tastaturkombinationen oder die Freigabe der Maus. Diese Einstellungen waren schon in den Vorgängerversionen vorhanden. Vermutlich werden Sie dort die Pfade anpassen, an den Einstellungen im Abschnitt Benutzer werden Sie vermutlich nicht unbedingt etwas ändern müssen.

In der 2012er-Version neue Konfigurationsaspekte sind:

- Physische GPUs: Hier geht es um eine reichhaltigere Darstellung für Remotedesktopbenutzer. Dies wird in Kapitel 19, »Remotedesktopdienste (Terminaldienste)«, nochmals genauer angesprochen.
- Aufteilung auf NUMA: NUMA bedeutet *Non-Uniform Memory Access*. Vereinfacht, geht es darum, dass ein Prozessor schneller auf seinen eigenen Speicher zugreifen kann als auf denjenigen, der einem anderen Prozessor zugewiesen ist. Salopp gesagt: Je näher der Speicher, desto schneller! Ist die Option aktiviert, können die VMs mehr Speicher nutzen, eventuell kann es aber zu Performanceverschlechterungen kommen.
  Ist die Option nicht aktiviert, kann es sein, dass eine VM nicht starten kann, weil ein Prozessor nicht über genügend »lokalen« Speicher verfügt.

Die Einstellungen zu Livemigrationen, Speichermigrationen und Replikationskonfiguration werden in den entsprechenden Abschnitten behandelt.

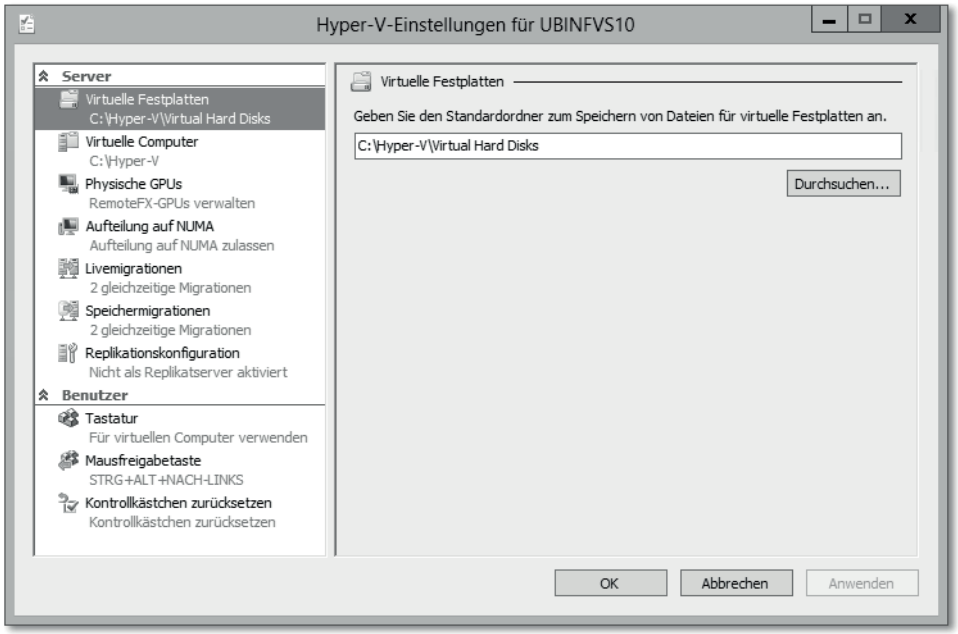


Abbildung 22.24 In den Grundeinstellungen geht es um diverse generelle Einstellungen.

22.4.4 Netzwerkeinstellungen

Eine der wichtigsten Aufgaben bei der Inbetriebnahme von Hyper-V-Servern ist die Anpassung der Netzwerkeinstellungen. Ihre virtuellen Maschinen sollen vermutlich mit der Außenwelt, also den Servern und Clients in Ihrem Netzwerk, kommunizieren. Es gibt drei Typen von virtuellen Netzwerken, die hinzugefügt werden können (Abbildung 22.25):

- EXTERN: Dieses Netzwerk ist mit einer physikalischen Netzwerkkarte verbunden.
- INTERN ermöglicht nicht den Zugriff auf die physikalische Netzwerkkarte, sondern dient der Kommunikation der virtuellen Maschinen auf dem Server untereinander und mit dem Server selbst.
- PRIVAT dient der Verbindung der virtuellen Maschinen auf diesem Server.

Sie werden eventuell keine Netzwerke vom Typ INTERN oder PRIVAT benötigen – ein Netzwerk vom Typ EXTERN brauchen Sie aber ganz bestimmt. Anzumerken wäre noch, dass es auf einem Hyper-V-Server beliebig viele virtuelle Netzwerke geben kann.

Der Dialog zur Konfiguration eines virtuellen Netzwerks ist übrigens bei allen drei Netzwerktypen (Verbindungstypen) gleich. Sie können den Verbindungstyp nach Belieben (und Notwendigkeit) umschalten. Bei Auswahl des Verbindungstyps EXTERN können Sie eine der im physikalischen Server vorhandenen Netzwerkkarten auswählen (Abbildung 22.26).

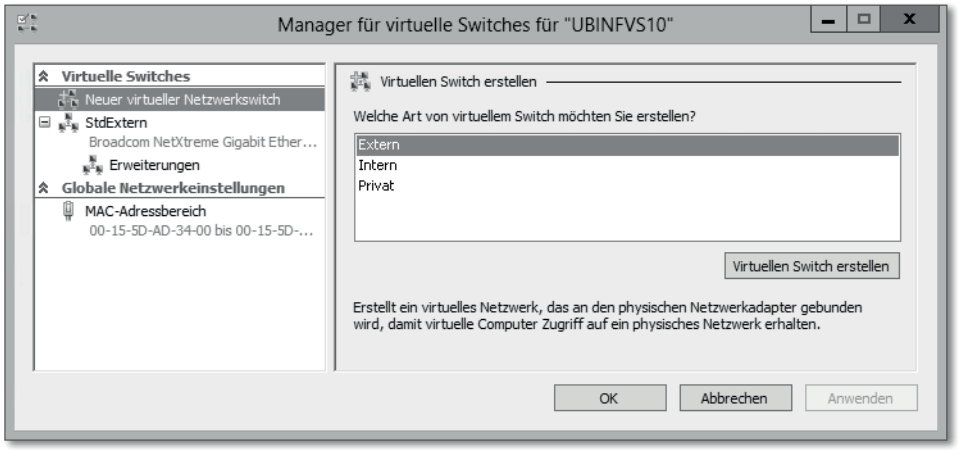


Abbildung 22.25 Sie müssen mindestens ein virtuelles Netzwerk erstellen.

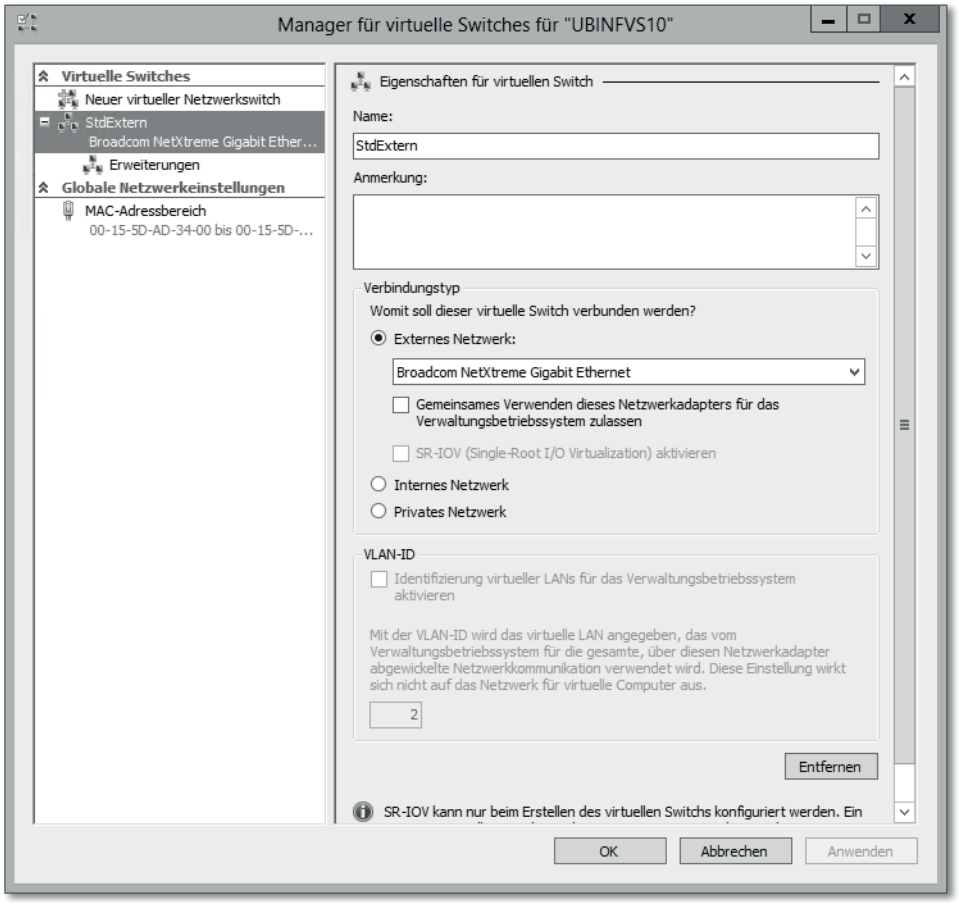


Abbildung 22.26 Die Konfiguration eines virtuellen Netzwerks

Interessant ist, was bei der Konfiguration eines externen Netzwerks geschieht:

- Bei der physikalischen Netzwerkkarte werden sämtliche Elemente mit Ausnahme des Hyper-V – erweiterbarer virtueller Switch entfernt (Abbildung 22.27).
- Falls die Checkbox Gemeinsames Verwenden dieses Netzwerkadapters für das Verwaltungsbetriebssystem zulassen (Abbildung 22.26) aktiviert ist, wird eine weitere Netzwerkkarte eingerichtet, an die die benötigten Elemente gebunden werden, beispielsweise der Client für Microsoft-Netzwerke, die IP-Protokolle und so weiter. Auch wenn das klappt: Es sollte ein separater Netzwerkadapter für VMs und Management-LAN verwendet werden, die Checkbox sollte also besser deaktiviert sein.

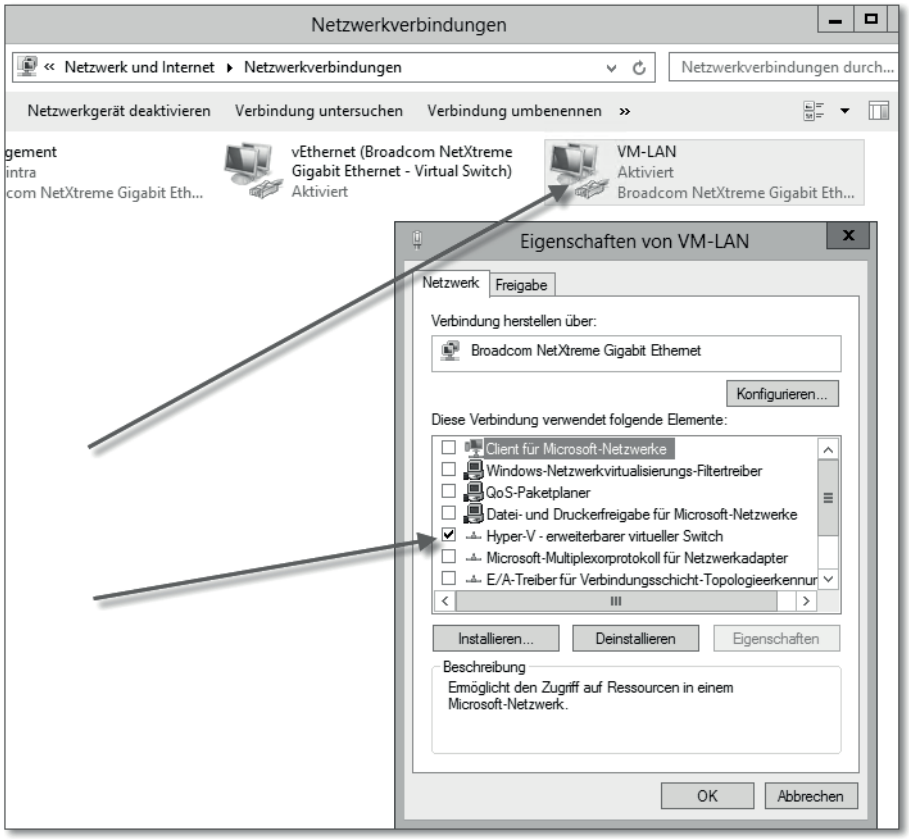


Abbildung 22.27 Bei der physischen Netzwerkkarte für das VM-LAN ist nur der »virtuelle Switch« ausgewählt.

Die in der Netzwerkkonfiguration vorgenommenen Änderungen sind zwar nicht weiter kompliziert, führen aber bei »Hyper-V-Neuadministratoren« immer wieder zu Verwirrungen.

Wie Sie später sehen werden, wird einer virtuellen Netzwerkkarte ein virtuelles Netz zugewiesen. Weitere Grundkonfigurationsarbeiten sind nicht erforderlich, so langsam können virtuelle Maschinen angelegt werden.

Zunächst möchte ich aber noch auf eine Neuerung in Hyper-V 2012 hinweisen: Die virtuellen Switches können erweitert werden. Wie in Abbildung 22.28 zu sehen, können installierte Erweiterungen aktiviert/deaktiviert werden. Diese Erweiterungen können von Microsoft selbst oder von Partnerunternehmen entwickelt werden. Mögliche Anwendungsszenarien könnten beispielsweise im Bereich des Monitorings liegen.

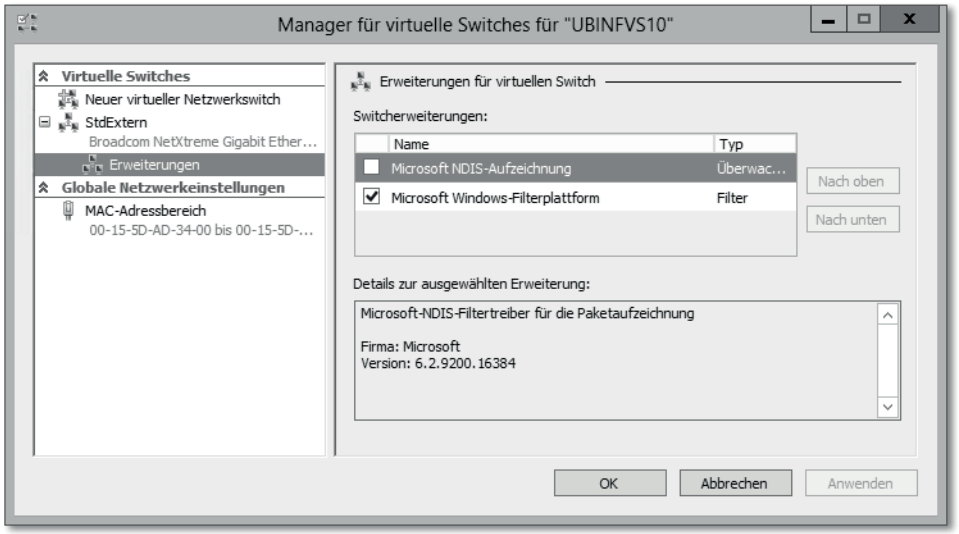


Abbildung 22.28 Neu bei Hyper-V 2012: die Erweiterbarkeit der virtuellen Switches

22.5 Administration von virtuellen Maschinen mit dem Hyper-V-Manager

Damit Sie einen Eindruck von der Arbeit mit dem Hyper-V-Manager bekommen, zeige ich Ihnen exemplarisch einige Handgriffe. Dieser Abschnitt soll und will kein »Admin-Kurs« sein, vielmehr möchte ich Ihnen einen Eindruck davon vermitteln, wie sich die tägliche Arbeit mit Hyper-V »anfühlt«. Festzuhalten ist, dass jeder, der sich in der Vergangenheit mit einem beliebigen Servervirtualisierungsprodukt beschäftigt hat, sofort verstehen wird, wie Hyper-V bedient wird.

22.5.1 Neue virtuelle Maschine anlegen

Die erste Aufgabe ist im Allgemeinen das Erstellen einer neuen virtuellen Maschine, was über das Kontextmenü des Servers im Hyper-V-Manager geschieht (Abbildung 22.29). Im

NEU-Menü sehen Sie unter anderem einen Menüpunkt zum Erstellen einer virtuellen Festplatte. Der Assistent, der eine komplette VM erstellt, legt ebenfalls eine Festplatte an, insofern brauchen Sie eine solche nicht vorab zu erzeugen.

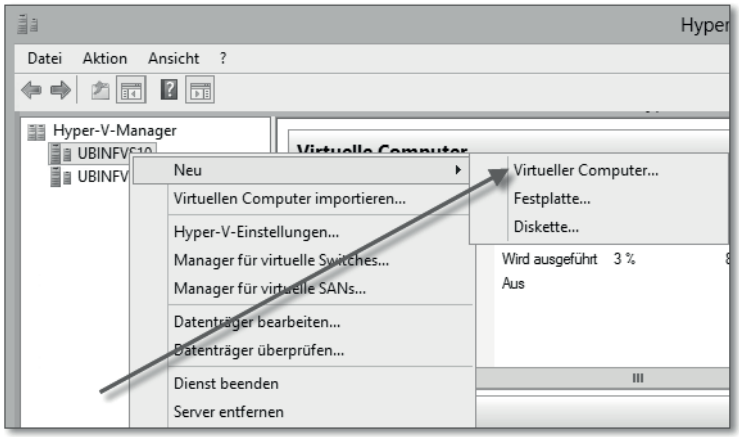


Abbildung 22.29 Das Erstellen einer neuen virtuellen Maschine startet hier.

Das Anlegen der virtuellen Maschine geschieht also mit einem Assistenten, wobei Sie prinzipiell nur die erste Seite sehen, auf der der Name der virtuellen Maschine und bei Bedarf ein vom Standard abweichender Speicherort angegeben werden (Abbildung 22.30). Wenn Sie sich hier für FERTIG STELLEN entscheiden, müssen Sie alle übrigen Ressourcen der VM, beispielsweise Speicher oder Festplatten, manuell konfigurieren. Sie haben dann jedoch deutlich mehr Möglichkeiten, als die nachfolgenden Dialoge des Assistenten zur Verfügung stellen. Selbstverständlich können Sie auch mit den weiteren Dialogseiten des Assistenten eine Basiskonfiguration erstellen, die dann in einem weiteren Schritt optimiert wird.

Zwei weitere wichtige Einstellungen sehen Sie auf Abbildung 22.30 und Abbildung 22.31 – das sieht in beiden Fällen nicht kompliziert aus, aber es gibt dabei einiges zu beachten. Abbildung 22.31 zeigt eine Dialogseite mit nur einer Konfigurationsmöglichkeit, nämlich der Menge des an die VM zuzuweisenden Speichers:

- Dazu muss man wissen, dass der Speicher nicht den des Hosts überschreiten kann, auf dem die virtuelle Maschine läuft. Der auf dem Screenshot genannte obere Wert von 29.674 MByte resultiert daraus, dass die physikalische Maschine, auf der die VM angelegt wird, einen Hauptspeicherausbau von 32 GByte hat.
- Seit Hyper-V 2008 R2 SP1 wird dynamischer Speicher unterstützt. Mehr dazu lesen Sie gleich. An dieser Stelle sei angemerkt, dass ein Startspeicher von 512 MByte mit aktivierter dynamischer Arbeitsspeicherverwendung durchaus sinnvoll ist.
- Es ist ein absolut tödlicher Fehler, mit dem Speicher zu sparsam umzugehen. Hat eine virtuelle Maschine zu wenig Speicher für die auszuführende Anwendung, wird das Betriebssystem das durch mehr oder weniger exzessives »Swappen«, also das Auslagern von

Speicherbereichen auf die Festplatte, ausgleichen. Ist so ein System direkt »auf der Hardware« (also ohne Virtualisierung) installiert, ist das lästig, weil die Performance bescheiden sein wird. In einer virtualisierten Umgebung werden zusätzlich auch die anderen virtuellen Maschinen in Mitleidenschaft gezogen, weil das dauernde Swappen die Plattenperformance des Gesamtsystems negativ beeinflusst. Ich gehe nicht davon aus, dass Sie bei der Planung und Berechnung des Festplattensystems ein »Dauer-Swapping« einkalkuliert haben.

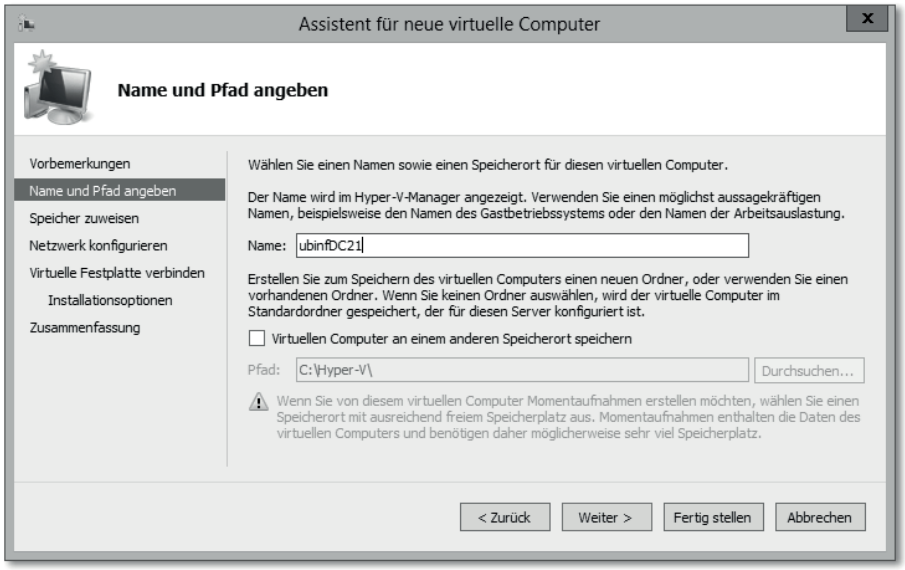


Abbildung 22.30 Beim Anlegen einer neuen virtuellen Maschine muss prinzipiell nur diese Dialogseite ausgefüllt werden.

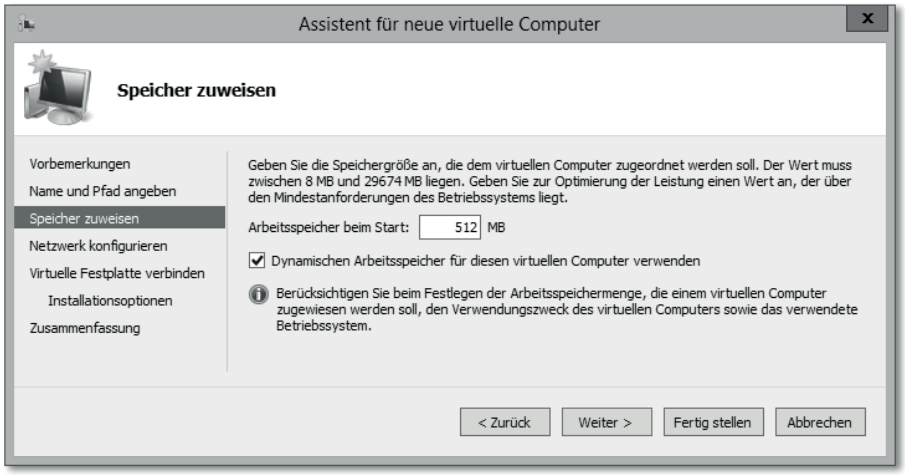


Abbildung 22.31 Eine der wichtigsten Einstellungen überhaupt: der zugeordnete Arbeitsspeicher. Bitte das Aktivieren der Verwendung dynamischen Arbeitsspeichers beachten!

Bevor Sie, wie in Abbildung 22.32 gezeigt, der Netzwerkkarte der virtuellen Maschine eine Verbindung zuweisen können, müssen ein oder mehrere virtuelle Netzwerke eingerichtet werden. Dies wird im Hyper-V-Manager über den Menüpunkt MANAGER FÜR VIRTUELLE NETZWERKE erledigt. Auf der Abbildung ist lediglich ein virtuelles Netzwerk eingerichtet, das mit der physikalischen Netzwerkkarte des Hosts verbunden ist.

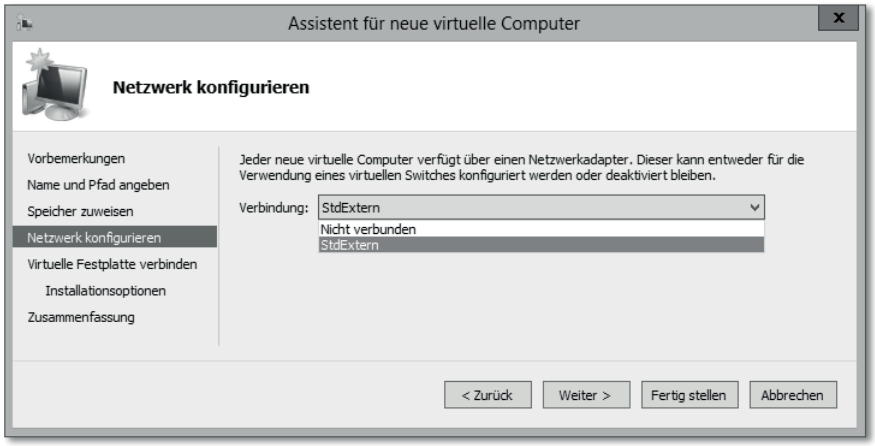


Abbildung 22.32 Zuweisen einer Netzwerkverbindung

Zu dem Thema *Netzwerk* gibt es noch einige Anmerkungen:

- Eine virtuelle Maschine kann mehrere Netzwerkkarten haben. Wenn Sie mehr als eine Netzwerkkarte benötigen, müssen Sie das allerdings später manuell konfigurieren; der Assistent kann nur eine Karte hinzufügen.
- Die Konfiguration virtueller Netzwerke bietet ebenfalls einige Möglichkeiten. Beispielsweise können Netze ohne Anschluss an das LAN eingerichtet und/oder es können VLANs gebildet werden.

Jede virtuelle Maschine benötigt eine oder mehrere Festplatten. Mit dem Assistenten können Sie die erste Festplatte einrichten, wobei Sie entweder eine neue virtuelle Festplatte anlegen oder eine bereits vorhandene verwenden können (Abbildung 22.33). Für das Erstellen einer neuen virtuellen Festplatte bietet der Assistent allerdings nur minimalen Support: Sie können den Namen, den Pfad (vorgegeben ist der definierte Standardpfad) und die maximale Größe angeben. Wenn Sie die virtuelle Festplatte »separat« (also außerhalb dieses Assistenten) anlegen, können Sie beispielsweise eine Platte erstellen, die sofort die endgültige Größe hat. Die hier angelegte virtuelle Festplatte ist zunächst wenige MByte groß und wächst, sobald Daten gespeichert werden – allerdings nur bis zur vorgegebenen maximalen Größe.

Wenn die neue virtuelle Maschine prinzipiell zur Installation des Betriebssystems bereit ist (dazu ist insbesondere eine zugewiesene virtuelle Festplatte erforderlich), können Sie direkt eine CD/DVD in das virtuelle DVD-Laufwerk legen. Dies kann entweder ein physikalisches Medium im Laufwerk des Hosts oder eine ISO-Datei sein.

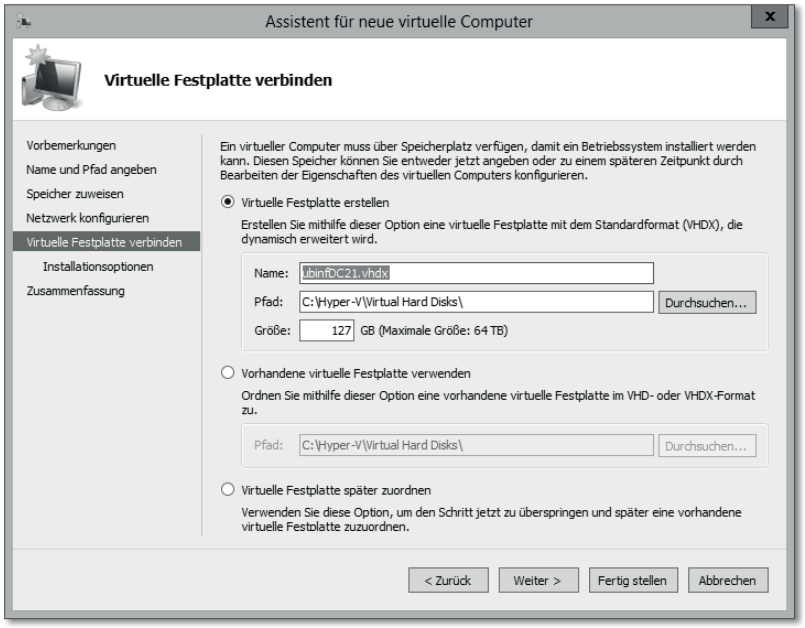


Abbildung 22.33 Hier kann eine neue virtuelle Festplatte erstellt werden. Diese Dialogseite zeigt aber nicht alle möglichen Optionen an.

Alternativ ist eine Installation von einer virtuellen Diskette oder durch einen Netzwerk-Bootvorgang möglich (Abbildung 22.34).

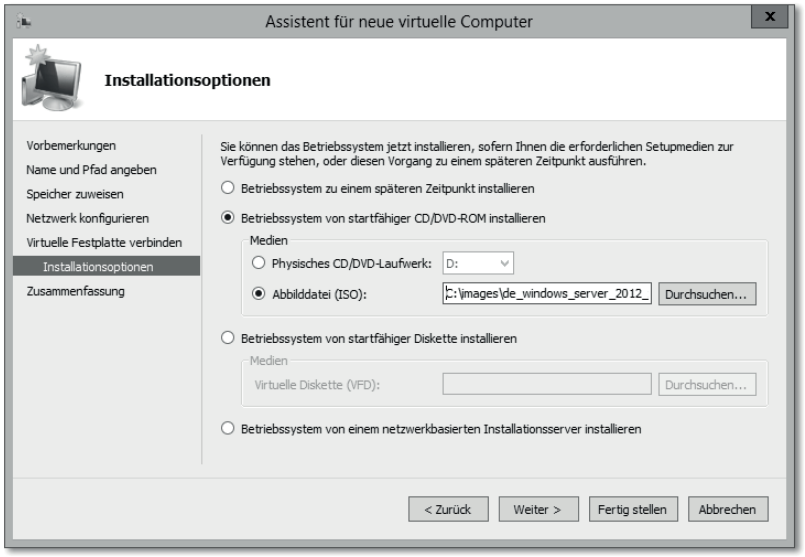


Abbildung 22.34 Sie können der virtuellen Maschine direkt eine ISO-Abbilddatei zur Betriebssysteminstallation zuweisen.

Migration

Das Migrieren von virtuellen Maschinen anderer Virtualisierungslösungen kann beispielsweise mit dem Virtual Machine Manager erledigt werden.

22.5.2 Einstellungen bearbeiten

Die Konfiguration der virtuellen Maschine ist sehr detailliert in deren Eigenschaften vorzunehmen (Abbildung 22.35). Neben der Konfiguration der virtuellen Hardware finden sich im Abschnitt VERWALTUNG diverse »organisatorische« Einstellungen, beispielsweise das automatische Starten der VM beim Hochfahren des Hosts oder der Speicherort der Snapshot-Dateien.

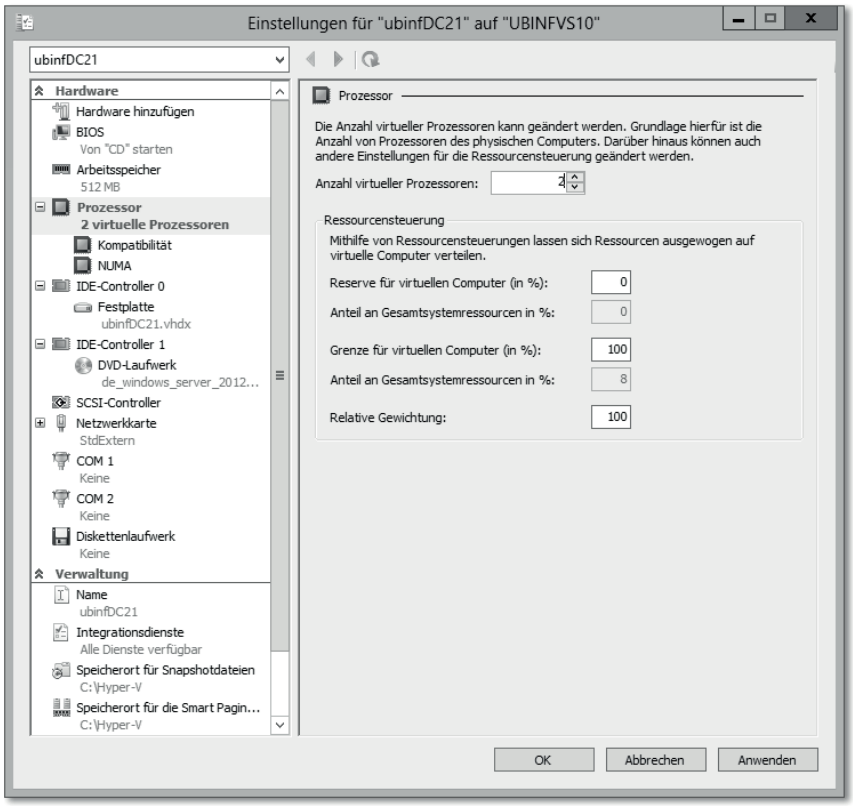


Abbildung 22.35 Eine detaillierte Konfiguration der Parameter der virtuellen Maschine ist in den Einstellungen möglich.

Das automatische Hochfahren einer VM kann übrigens mit einer zeitlichen Verzögerung versehen werden. So wird verhindert, dass das mehr oder weniger gleichzeitige Hochfahren

vieler automatisch zu startender VMs zu Performanceproblemen führt. Diese wirken sich in der Praxis teilweise so aus, dass es in den virtuellen Maschinen Timeouts gibt und deshalb beispielsweise nicht alle Dienste korrekt gestartet werden.

In begrenztem Umfang können Sie »Hardware« hinzufügen. Wie in Abbildung 22.36 gezeigt, gibt es hier drei mögliche Typen, nämlich SCSI-Controller, Netzwerkkarten und ältere Netzwerkkarten. Interessant sind die beiden Netzwerkkartentypen:

- Die Netzwerkkarte, die auch vom Assistenten standardmäßig hinzugefügt wird, basiert auf der *Virtual Machine-Bus-Architektur*. Treiber hierfür stehen nur für Windows Server 2003 ab SP2 und Windows Server 2008 zur Verfügung. Die benötigten Treiber gibt's bei den Integrationsdiensten; das sind die Softwarekomponenten, die in der virtuellen Maschine installiert werden.
- Wenn Sie ältere Betriebssysteme (älter als Windows Server 2003 SP2) installieren, müssen Sie die VM statt mit der Netzwerkkarte mit einer älteren Netzwerkkarte ausstatten.
- Sie benötigen ebenfalls eine ältere Netzwerkkarte, wenn das Betriebssystem über einen Netzwerk-Bootvorgang installiert werden soll.

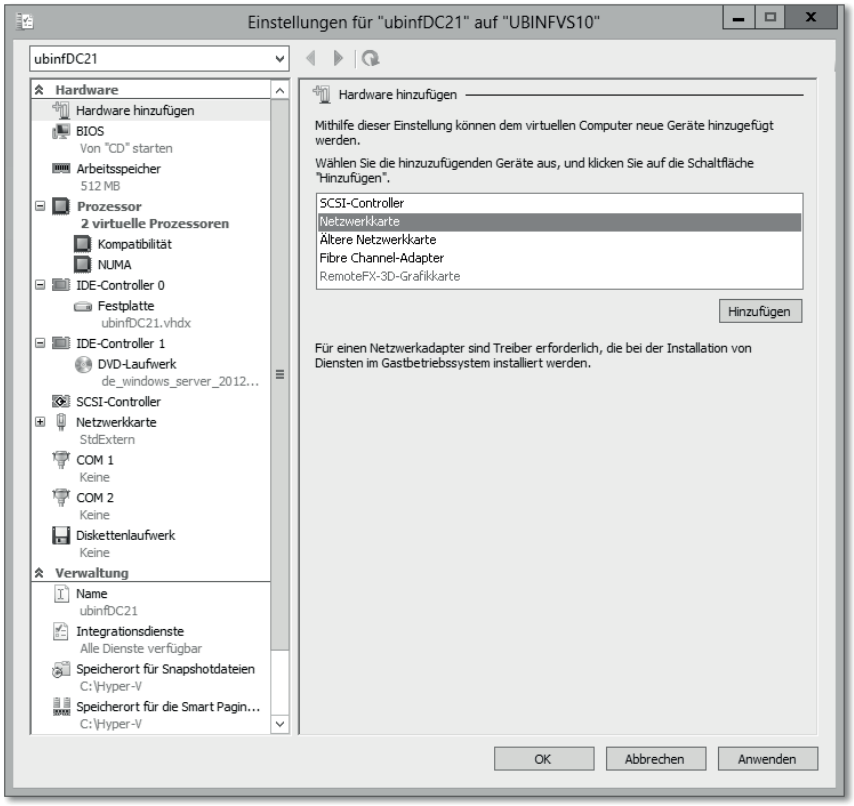


Abbildung 22.36 Es kann in begrenztem Umfang Hardware hinzugefügt werden. Interessant sind die Punkte »Netzwerkkarte« und »Ältere Netzwerkkarte«.

Integrationsdienste

Die Windows Server 2012 enthalten bereits die »passenden« Integrationsdienste.

Bei allen anderen Betriebssystemen müssen die Integrationsdienste implementiert werden.

22.5.3 (Dynamische) Speicherverwaltung

Ein interessantes Feature, das es seit Windows Server 2008 R2 SP1 gibt, ist die dynamische Speicherverwaltung, die natürlich in verbesserter Form auch in Windows Server 2012 enthalten ist.

Die »Idee« dahinter erschließt sich, wenn man den Konfigurationsdialog anschaut (Abbildung 22.37):

- Die virtuelle Maschine startet mit dem bei Minimaler RAM eingetragenen Speicherwert. Für die aktuellen Betriebssysteme (2008 und höher) werden hier 512 MByte empfohlen.
- Der Wert Maximaler RAM beschreibt den Speicher, der der VM maximal zugewiesen wird. Dieser Wert steht auf dem Screenshot auf 1 TByte (TB, Terabyte), was vermutlich nicht sinnvoll ist und tunlichst geändert werden sollte.

Die Überlegung hinter dem dynamischen Speicher ist, dass zumeist der fest zugewiesene Speicher nicht vollumfänglich benötigt wird. Daher startet also die VM mit möglichst wenig Speicher und erhält dann so viel, wie konkret erforderlich.

Die beiden übrigen Optionen auf der Dialogseite (Abbildung 22.37) sind auch nicht uninteressant:

- Der Arbeitsspeicherpuffer beschreibt den zusätzlichen Speicher, der über den momentanen Bedarf hinaus für die VM reserviert wird. Standardmäßig sind das 20 %.
- Der Schieberegler bei Arbeitsspeicherumfang bestimmt die Priorität. Der hier eingestellte Wert wird herangezogen, wenn verschiedene VMs auf dem Server um Speicher »konkurrieren«.

Dynamische Speicherverwaltung und Gastbetriebssystem

Die Nutzung der dynamischen Speicherverwaltung setzt eine gewisse Mitarbeit des Gastbetriebssystems voraus:

- Das Gastbetriebssystem muss Windows Server 2003 SP2 oder höher sein.
- Auf dem Gastbetriebssystem müssen aktuelle Integrationsdienste installiert sein.

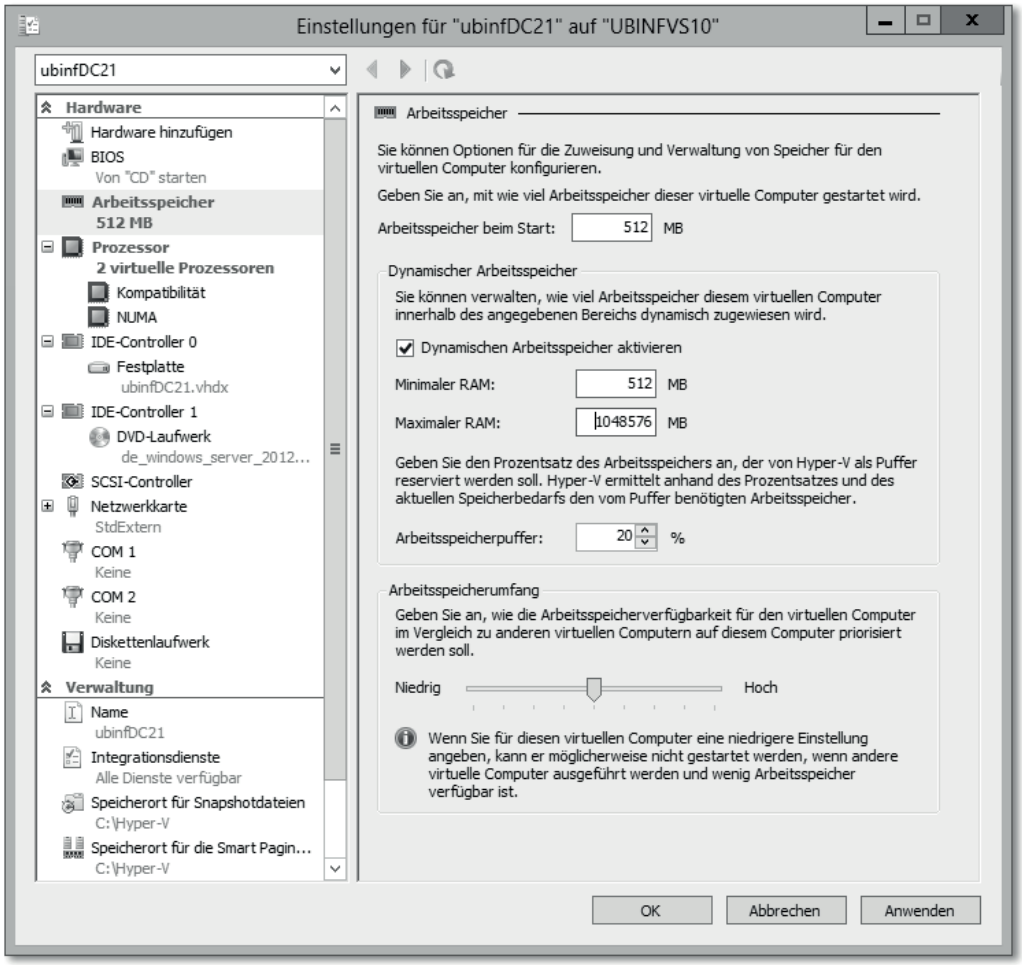


Abbildung 22.37 Die dynamische Speicherverwaltung

Aus Sicht des Gastbetriebssystems sieht es, wenn die VM wie auf Abbildung 22.38 konfiguriert ist, so aus:

- Der maximale Arbeitsspeicher wird mit 1 TByte angezeigt. Das ist so zwar nicht gut konfiguriert, aber möglich. Besser ist es natürlich, eine sinnvolle Maximalspeichermenge einzutragen.
- In diesem Moment werden 957 MByte benötigt.
- Ca. 20 % mehr Speicher steht zur Verfügung.

Der Hyper-V-Manager zeigt standardmäßig die Spalte Zugewiesener Speicher an (Abbildung 22.39). So erhält man schnell einen Überblick darüber, wie viel Speicher in Verwendung ist. Wie Sie sehen, laufen zwei Server in der Tat noch mit dem Minimalwert.

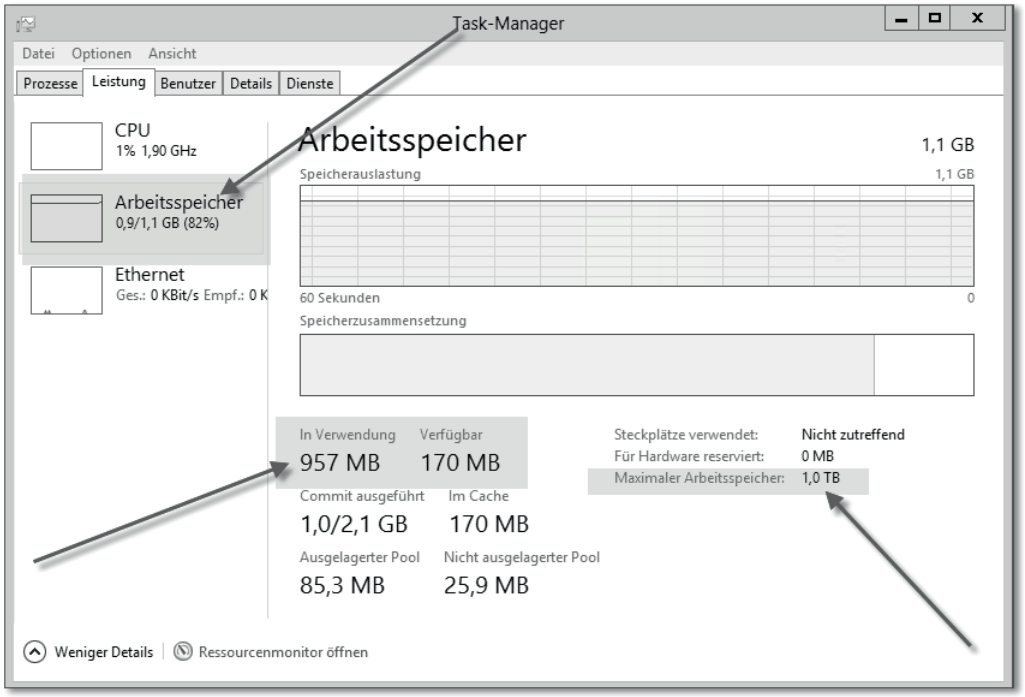


Abbildung 22.38 Im Gastbetriebssystem sieht es so aus.

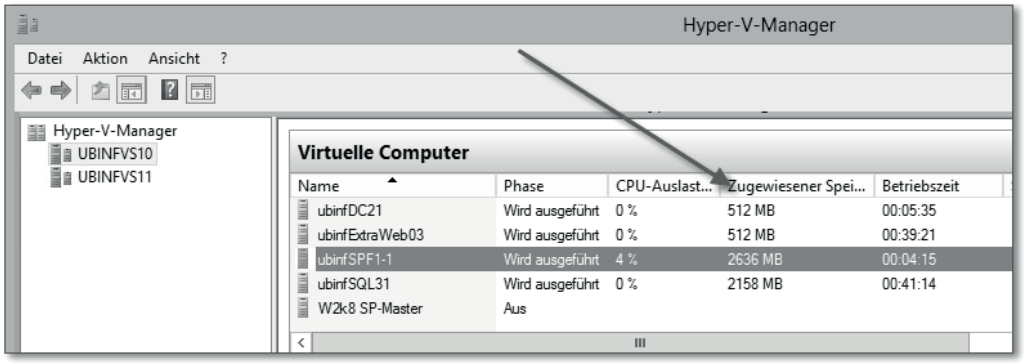


Abbildung 22.39 Der Wert »Zugewiesener Speicher« im Hyper-V-Manager zeigt auf einen Blick, wie viel Speicher in Verwendung ist.

22.5.4 Die »laufende« VM

Wenn eine virtuelle Maschine läuft, stehen die in Abbildung 22.40 gezeigten Menüpunkte zur Verfügung – diese sind so weit selbsterklärend. Interessant ist der Menüpunkt VERBINDEN, der die Steuerungsapplikation aufruft. Einen ersten Blick darauf sehen Sie in Abbil-

dung 22.41. Die wesentlichen Funktionen (*Ein*, *Aus* und *Pause*) finden sich hinter Symbolen, diverse weitere Funktionen gibt's in der Menüleiste. Einige Anmerkungen dazu:

- Sie können auf Ihrem Admin-PC beliebig viele Steuerungsfenster öffnen, also beliebig viele VMs steuern.

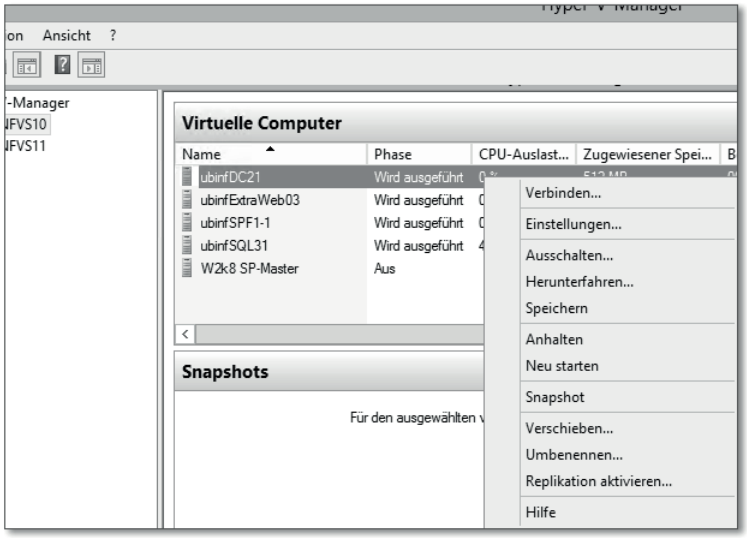


Abbildung 22.40 Diese Menüpunkte stehen für eine laufende VM zur Verfügung. »Verbinden« startet die Steuerung.

- Damit die Anzeige mit einer guten Performance ausgeführt wird, müssen Sie die Integrationsdienste installieren, einen entsprechenden Menüpunkt finden Sie unterhalb des Eintrags Aktion.

  Sofern die Integrationsdienste bei einem älteren Betriebssystem (also älter als Windows Server 2008 R2) nicht installiert sind, müssen Sie den Mauszeiger jeweils »befreien«, wenn Sie mit der Arbeit in der VM fertig sind.

Eine Alternative zu der Steuerungsanwendung ist natürlich weiterhin die bei den Windows-Betriebssystemen standardmäßig vorhandene Remotedesktop-Funktionalität.

Abbildung 22.41 Die virtuelle Maschine in der Steuerungsapplikation

In der Praxis werden auch bei virtuellen Maschinen häufig CDs und DVDs benötigt. Das ist nun grundsätzlich kein Problem, schließlich können die VMs mit virtuellen CD-/DVD- oder

Diskettenlaufwerken ausgestattet werden. Nun geht es aber noch darum, dass in diese virtuelle Hardware auch die benötigten Medien »eingelegt« werden müssen.

Das lässt sich mit wenigen Mausklicks erledigen, wie Abbildung 22.42 zeigt. Sie können entweder ein ISO-Image einbinden, das auf dem Hostsystem vorhanden sein muss, oder aber eine Verbindung mit dem physikalischen Laufwerk des Hyper-V-Servers herstellen (die Übersetzung D: AUFZEICHNEN ist nach meinem Geschmack allerdings nicht allzu glücklich).

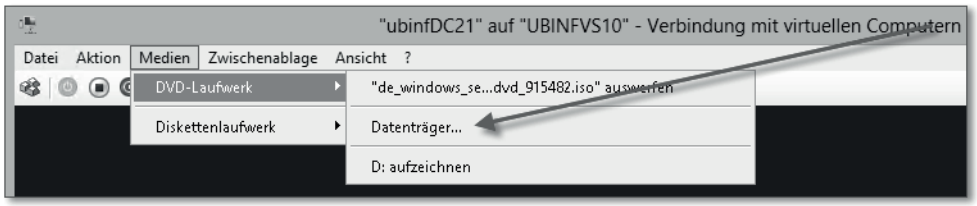


Abbildung 22.42 Über diesen Menüpunkt können Sie in das CD-/DVD-Laufwerk der VM ein ISO-Image »einlegen« oder eine Verbindung zu dem physikalischen Laufwerk des Servers herstellen.

22.6 Verbesserung der Verfügbarkeit

Auch bei virtuellen Maschinen ist die Verfügbarkeit eine entscheidende Herausforderung. Dabei gibt es grob gesagt zwei Ziele, die aber nicht immer zwingend beide erreicht werden müssen – ein bisschen geht es ja auch manchmal um das Budget.

Die zwei Ziele:

- Datenverlustzeit optimieren: Die Datenverlustzeit beschreibt letztendlich die Menge der verlorenen Daten, also die Zeit seit der letzten Sicherung. Durch Hyper-V-Replikation kann die Datenverlustzeit sehr deutlich minimiert werden.
- Wiederherstellzeit optimieren: Hierbei geht es um einen möglichst schnellen Wiederanlauf nach dem Verlust von Ressourcen (= Server, Storage). Durch Failover-Clustering kann die Wiederherstellungszeit beim Ausfall eines Servers optimiert werden.

22.6.1 Replikation

Die Replikation, neues Feature in Server 2012 übrigens, ist eine geniale Sache. Für kleines Geld bekommen Sie eine fabelhafte Lösung zur Minimierung der Datenverlustzeit. Auch die Wiederherstellzeit lässt sich dramatisch verkürzen – wenngleich manuelles Eingreifen erforderlich ist.

Die Funktionsweise ist schnell erklärt:

- Sie brauchen zwei Server mit Hyper-V. Shared Storage (= SAN-Storage auf FibreChannel- oder iSCSI-Basis) ist nicht erforderlich.

Index

.NET
CardSpace 197
WCF 197
Windows Communication Foundation 197
Windows Presentation Foundation 197
Windows Workflow Foundation 197
WPF 197
WWF 197
.NET Framework 190
.NET-Benutzer 1002
.NET-Vertrauensebenen 1013
64-Bit-Welt 57
802.1X 534

A

Active Directory 221
Best Practice Analyzer 421
Drucken 903
Modul für Windows-Powershell 446
Offline-Domänenbeitritt 453
Papierkorb 424
Verwaltungscenter 432
Active Directory Application Mode 495
Active Directory Best Practice Analyzer XE 421
Active Directory Federation Services
Claims-Aware 521
Federation Service 521
Federation Service Proxy 521
Active Directory Lightweight Directory Services 495
AD LDS 495, 497
ADAM 495
Administration 505, 511
ADSI-Editor 507
Ereignisanzeige 512
Featurevergleich 496
Installation 498
Instanz einrichten 499
LDIF 504
Objekt anlegen 510
Portnummern 502
Replikation 514
Update Sequence 517
X.500-Kürzel 502
Active Directory Web Services 443
Active Directory Zertifikatdienste
CAPolicy.inf 604
OCSP 593
Offline-CA installieren 603
Online-Responder 593
zweistufige Architektur implementieren 602
Active Directory-Domänendienste 221
Active Directory 221
ADDS 221
Administrative Vorlagen 314
ADSI-Editor 232, 233
Änderungen erkennen 272
Aufbau 222
Betriebsmasterrollen 239
Betriebsmasterrollen verschieben 244, 407
Betriebsmasterrollen verteilen 249, 250
Bridgeheadserver 293
Client-Perspektive 383
DEFAULTIPSITELINK 286
Delegieren der Verwaltung 381
Design 256
Direct Up-to-dateness Vector 277
DNS-Einträge 383
Domain Naming Master 242
Domäne 223
Domänencontroller 223
durchsuchen 384
Einrichtung 299
ersten Domänencontroller einrichten 300
erweitern 386
Forest 227
FSMO-Rollen 239, 407
GC 236
Gesamtstruktur 227
globale Katalogserver verteilen 251
globaler Katalog 236
globaler Katalog und Infrastruktur 242
Gruppen 230, 378
Gruppenrichtlinien 309
High-watermark 277
Infrastrukturmaster 241
Infrastuktur Master und global 242
Intersite Replikation 282
Intersite Topology Generator 279
Intrasite Replication 281

Active Directory-Domänendienste (Forts.)
ISTG 296
KCC 279, 296
Knowledge Consistency Checker 279
Login-Skripts 229
logische Struktur 222
Namenskontext 233
Namensraum 227
neues AD einrichten 299
Organisationseinheit 228
OUs vs. Gruppen 230
Partition 233
PDC-Emulator 240
Planung 256
Read Only Domain Controller 252
Replikation 268
Replikationsablauf 271
Replikationskonflikte 278
Replikationstopologie 279, 283
RID-Master 241
RODC 252
Schema 232
Schema-Manager 235, 247
Schemamaster 243
schreibgeschützte Domänencontroller 252
Standorte 262
Standorte und Domänen 262
Standortverknüpfungen 286
Standortverknüpfungsbrücken 291
Struktur 222
Transitivität 291
Tree 224
Troubleshooting 412
Übersichtlichkeit 259
Überwachung 298
umstrukturieren 418
Universal Group Membership Caching 237
Update Sequence Number (USN) 272
Upgrade 392
Up-to-dateness-Vector 277
Verbindungen 284
Verfügbarkeit 243
Verschieben der Betriebsmaster 244
Verteilung der Betriebsmasterrollen 249
Verwaltung delegieren 381
Zeitdienst 387
Zeitsynchronisation 388
Zusätzliche Domänencontroller 308
Active Directory-Papierkorb 424
aktivieren 424
gelöschte Objekte anzeigen 426
Ldp.exe 426
Active Directory-Papierkorb (Forts.) 424
PowerShell 431
Voraussetzungen 424
Active Directory-Rechteverwaltungsdienste 641
Abschlussbemerkung 674
AD RMS 641
Anwendung 662
E-Mail schützen 669
Funktionsweise 643
Gruppenrichtlinien 660
Installation 645
IRM 641
Licensor Certificate 643
Lizenzierung 643, 672
Publishing License 643
Rights Management Services 641
RMS 641
Statistik 672
Use License 644
Word-Dokument schützen 662
Active Directory-Verbunddienste 519
ADFS 519
Federation Services 519
Active Directory-Verwaltungscenter 432
Attribute anzeigen 435
Benutzer suchen 435
filtern 437
Kennwort zurücksetzen 434
Navigationsknoten 441
navigieren 437
Neuanlage von Objekten 440
Voraussetzungen 443
Active Directory-Verwaltungscenter → Active Directory
Active Directory-Webdienste 443
Active Directory-Zertifikatdienste 525
AD CS 525
Anwendungsrichtlinien 556
Anwendungsszenarien 525
Architekturen 565
Autoenrollment 567
Autoenrollment, Konfiguration 570
Automatische Zertifikatanforderung 567
Clientsicht 545
eigenständige Zertifizierungsstelle 537
erweiterte Zertifikatanforderung 562
Gültigkeit des Stammzertifikats 542
Installation 534
Intermediate CA 564
Internetinformationsdienste 1008
iPhone 638
Issuing CA 564
mehrstufige Architekturen 562

Active Directory-Zertifikatdienste (Forts.)
Public Key Infrastructure 534
Rollen 563
Root CA 538, 563
Stammzertifizierungsstelle 563
untergeordnete Zertifizierungsstelle 538
Unternehmenszertifizierungsstelle 537
Vorlage duplizieren 553
Weboberfläche 560
Windows Mobile 634
Zertifikat anfordern 547
Zertifikatdatenbank wiederherstellen 543
Zertifikatsperrliste 574
Zertifikatvorlagen 551
Zertifizierungspfad 550
Zertifizierungsstelle 538
AD CS 525
AD LDS 495, 497
AD RMS 641
Address Resolution Protocol 159
ADDS 221
ADFS 519
ADM 336
Administration, IIS 1029
ADMX 336
Adressierung, IPv6 146
Adresssyntax, IPv6 146
Adresstypen, IPv6 147
Adressvergabe, IPv6 152
ADSI-Editor 233
ADWS 443
Affinität, Netzwerklastenausgleich 1195
AJAX 915
Aktivieren 206
Alias 1364, 1367
Allocation Unit Size 795, 796
Anforderungsverarbeitung 931
Animal Farm 239
Anonyme Authentifizierung 959
Anschlüsse, Drucken 898
Anwendung 943, 954
installieren 1084
Anwendungspool 933, 943, 947, 986, 988
Anycast 147
Applikationsvirtualisierung 1087
App-V 1063, 1087
Arbeitsprozess 931
Architektur
IIS 930
System Center Virtual Machine Manager 2012 1304
ARP 159
Address Resolution Protocol 159
Netzwerkmonitor 161
Netzwerkprotokolle 159
ASP.NET 915
anonyme Authentifizierung 959
Entwicklungsumgebung 915
Identitätswechsel 971
IIS 915
JavaScript 918
Kompilierung 922
Sicherheit 927
Vorkompilierung 922, 925
web.config 919
ASP.NET-Runtime 189
Attribute anzeigen, Active Directory-Verwaltungscenter 435
Ausführungsrichtlinie 1369
Authentifizierung 166
IIS 958
Kerberos 166
Netzwerklastenausgleich 1205
Authentifizierungsdelegierung 976
Autoenrollment 569
Active Directory-Zertifikatdienste 567
Automatische Genehmigung, WSUS 746
Automatische Zertifikatanforderung 567
Automatischer Modus (VPN) 780
Autorisierung 166
IIS 1003
Average Seek Time 62
AWE 58

B

BackOffice 28
Baselining 97
Basis-Datenträger 797
Bedingte Weiterleitungen, DNS 464
Begriffsdefinition
Webapplikation vs. Webservice 911
Webseite vs. Website 914
Webservice vs. Webapplikation 911
Benutzer suchen, Active Directory-Verwaltungscenter 435
Benutzereffizienz 1054
Benutzerspezifische GPOs 330
Benutzerzugriff, Remotedesktopdienste 1080
Berechtigungssatz 195
Berichte, WSUS 754

Best Practice Analyzer, Webserver 1042
Betriebsmasterrollen 239
Active Directory-Domänendienste 239
Domain Naming Master 242
FSMO-Rollen 239
Infrastrukturmaster 241
PDC-Emulator 240
RID-Master 241
Schemamaster 243
verschieben 244, 407
verteilen 249
Blockgröße 116, 126, 795, 796
Bottom-up-Ansatz 1053
BPA, Webserver 1042

C

Cache, Zertifikate 588
CAL 53
CAPI2 583
CAPolicy.inf 604
Capture Filter, Netzwerkmonitor 133
CardSpace 197
CASpol 193
change user 1087
Client Access License 52
Clients und ADDS 383
Cluster schwenken 1172
Clusterfähiges Aktualisieren 1174
CMAK 781
Cmdlets 1364
Code Access Security 193
CASpol 193
Codegruppe 195
Codesignatur 530
Common Language Runtime 189
Compact Framework 190
Connection Manager Administration Kit 781
Constained Delegation 990
Constrained Delegation 176, 992
Content Manager 1051, 1053
Core
Hyper-V 1248
sconfig.cmd 211
Core-Installationsoption 209
Rollen 210
Rollen hinzufügen 217
Verwaltung 211
Vorteile 210

D

DAS 65
Dateidienste 787
Dateiprüfungsverwaltung 821
Dateiserver
Ausfallsicherheit 831
Dateiprüfungsverwaltung 821
EFS 851
Encrypting File System 851
Failover-Cluster 1166
File Screening 814
File Screening Management 821
Installation der Rolle 813
Kontingentverwaltung 814
Quota Management 814
Quotas 814
Speicherberichteverwaltung 824
Dateisystem 787
Attribute 808
Aufbau 788
Basis-Datenträger 797
Blockgröße 795
Diskpart 790
dynamische Datenträger 797
EFS 808
GPT 791
MBR 791
Mirrored Volume 797
partitionieren 793
Platten verwalten 789
Schattenkopien 809
Self-Healing NTFS 812
Spanned Volume 797
spiegeln 799
Stripesetvolume 797
Transactional NTFS 812
Volume Manager 788
Volume Shadow Copy Service 809
Volumes vergrößern 802
Volumes verkleinern 802
Datendeduplizierung 880
Datengrab-Effekt 1048
Datenmengen 1047
Datensicherung 1223
Server wiederherstellen 1233
Sicherung 1225
Wiederherstellung 1229
Datenträgerverwaltung 789
Datenverlustzeit 1139

Delegierung ... 990
DNS ... 305, 464, 466
IIS ... 976
Kerberos ... 173, 176, 178
Kernelmodus-Authentifizierung ... 182
Netzwerklastenausgleich ... 1206
Device-CAL ... 53
DFS ... 828
Basiskonfiguration ... 836
DFS im Active Directory ... 841
DFS-Replikation ... 830
DFS-Replikation konfigurieren ... 845
Distributed File System ... 828
domänenbasierter Namespace ... 839
Domänenstamm ... 829
eigenständiger Namespace ... 839
eigenständiger Stamm ... 829
Grundfunktion ... 828
Installation ... 835
Namespace konfigurieren ... 836
Namespaceserver ... 836
Redundanz des Namespaceservers ... 850
Replikationsgruppen ... 845
Replikationstopologie ... 848, 849
Sicherung von Daten ... 834
standortübergreifendes ... 832
verteiltes Dateisystem ... 828
Voraussetzungen ... 829, 831
DFS-Replikation ... 830
konfigurieren ... 845
Replikationstopologie ... 849
DHCP ... 155, 472
80/20-Regel ... 484
Adressbereich, Eigenschaften ... 482
Bereichsoptionen ... 483
Clustering ... 484
DNS ... 479
dynamische DNS-Updates ... 481
Eigenschaften ... 481
Funktionsweise ... 155
NAP ... 690
Netzwerkmonitor ... 157
Netzwerkprotokolle ... 155
Optionen ... 483
Redundanz ... 484
Serveroptionen ... 483
statische Adresszuweisung ... 482
WINS ... 480
DHCP-Server, NAP (Vorbereitung) ... 702
Digestauthentifizierung ... 969
Dimensionierung ... 55, 101, 113
Festplatten ... 113
Hauptspeicher ... 128
IOPS ... 116, 119
Netzwerkkonnektivität ... 129
Prozessor ... 128
RAID-Level ... 120
RAID-Set ... 119
Warteschlange ... 116
DirectAccess ... 759
Zertifikatsperrliste ... 574
DISCOVER-Broadcast, DHCP ... 157
Disk Aligning ... 796
Disk-Layout ... 113
Diskpart ... 790
Diskpart-Utility ... 796
Display Filter, Netzwerkmonitor ... 133
Distinguished Name ... 424
Distributed File System ... 828
DNS ... 162, 455
bedingte Weiterleitungen ... 464
Delegierung ... 305, 464, 466
DHCP ... 479
Domain Name System ... 162
Netzwerkdienste ... 455
Netzwerkmonitor ... 166
Reverse-Lookupzone ... 469
Richtlinien ... 484
Server ... 462
Stammhinweise ... 465
TimeToLive ... 164
Weiterleitungen ... 464
Zonen ... 456
Zonentypen ... 457
DNS-Name nicht vorhanden ... 207
Domain Name System ... 162
Domain Naming Master ... 242
Domäne ... 223
Domänen-lokale Gruppe ... 378
Druckdienste ... 891
Drucken ... 885
Active Directory ... 903
Anschlüsse ... 898
Druckdienste ... 891
Drucker ... 886
Drucker bereitstellen ... 903
Drucker installieren ... 894
Druckerobjekte ... 886
Druckerpool ... 887
Druckerserver ... 886

Drucken (Forts.)
Druckerserver konfigurieren ... 899
Druckerstandards ... 899
Druckverwaltung ... 893
Filter ... 901
Gruppenrichtlinien ... 905
In Verzeichnis auflisten ... 903
Installation ... 891
Internetdrucken ... 892
Konfiguration importieren/exportieren ... 901
LPD-Dienst ... 892
optimieren ... 885
printQueue-Objekt ... 903
PushPrinterConnections.exe ... 906
Remotedesktopdienste ... 1115
Rollendienste ... 891
Treiber ... 896
überwachen ... 901
XPS ... 889
Drucker ... 886
bereitstellen ... 903
installieren ... 894
Druckerobjekte ... 886
Druckerpool ... 887
Druckerserver ... 886
Konfiguration ... 899
Druckerstandards ... 899
Druckertreiber ... 896
Druckverwaltung ... 893
Dünn ... 869
Dynamische Datenträger ... 797

E

EAP ... 770
Easy Print ... 1115
Editionen ... 51
EFI-Boot-Partition ... 792
EFS ... 533, 851
cipher.exe ... 864
Datei verschlüsseln ... 853
Dateien auf Servern ... 854
Dateiserver ... 851
Datenwiederherstellungs-Agent ... 858
Datenwiederherstellungs-Agenten erstellen ... 858
Encrypting File System ... 851
Gruppenrichtlinien ... 863
Konfiguration ... 852
Zertifikate ... 852
Zugriff für mehrere Benutzer ... 855
Eingeschränkte Delegierung ... 176, 990, 992
Einmalsicherung ... 1225
Einwahlberechtigung ... 768
E-Mail schützen ... 669
EMT64 ... 57
Encrypting File System ... 532, 533, 851
Enterprise Virtual Array ... 803
Entwicklungsumgebung ... 1374
EPIC ... 57
Ersten Domänencontroller einrichten ... 300
Erzwingungsclient ... 684
Extensible Authentication Protocol ... 770
Extranet ... 1049

F

Failover-Cluster ... 1146
aktiv vs. passiv ... 1149
Anwendungen hinzufügen ... 1166
Cluster aware ... 1148
Cluster schwenken ... 1172
Clusterressourcen ... 1148
Dateiserver ... 1166
Hochverfügbarkeit ... 1146
Installation ... 1150, 1158
iSCSI ... 1150
Konnektivität ... 1150
n+1 ... 1149
Paralleles SCSI ... 1147
Shared Storage ... 1147, 1150
Support ... 1163
Features ... 46
Federation Services ... 519
Festplatten ... 60
Blockgröße ... 116, 126
Dimensionierung ... 113
Disk-Layout ... 113
IOPS ... 116
Leistungsindikatoren ... 116
RAID-Level ... 120
Systempartition ... 114
Warteschlange ... 116
File Screening ... 814
File Screening Management ... 821
Filter
Gruppenrichtlinien ... 326
Netzwerkmonitor ... 134
Filtermodus
Netzwerklastenausgleich ... 1194
Forest ... 227

Formularauthentifizierung ... 993
Freigegebene Konfiguration ... 1027
fSMORoleOwner ... 418
FSMO-Rollen ... 239, 407
Funktionsweise
Active Directory-Rechteverwaltungsdienste 643
Zertifikatsperrliste ... 576

G

Gateway-Architektur ... 757
GC ... 236
Gelöschte Objekte anzeigen, Active Directory-Papierkorb ... 426
Gemeinsamer geheimer Schlüssel ... 686
Gesamtstruktur ... 227
Global Unicast Addresses ... 148, 151
Globale Gruppe ... 378
Globaler Katalog ... 236, 249
GPT ... 791
Grundlagen, Windows PowerShell ... 1364
Gruppen ... 378
WSUS ... 743
Gruppenrichtlinien ... 309
Abarbeitungsreihenfolge ... 326
Active Directory-Domänendienste ... 309
Active Directory-Rechteverwaltungsdienste . 660
ADM ... 336
ADMX ... 336
Anwendungsbeispiel ... 310
bearbeiten ... 349
Benutzerspezifische GPOs ... 330
Drucken ... 905
EFS ... 863
Filter ... 326
gPLink ... 317
Gruppenrichtlinienergebnisse ... 363
Gruppenrichtlinienmodellierung ... 358
Lokale GPOs ... 327
Lokales Richtlinienobjekt ... 328
Loopbackverarbeitung ... 372, 1107
Preferences ... 373
Sicherheit ... 323
Softwareverteilung ... 369
Starter-Gruppenrichtlinienobjekte ... 331
Vererbung ... 320
Verknüpfungen ... 356
Verteilung ... 315
Voreinstellungen ... 373
Vorrang ... 323
Gruppenrichtlinien (Forts.)
WMI-Filter ... 365
WSUS ... 750
zentraler Speicherort ... 340
zuweisen ... 349
Gruppenrichtlinienergebnisse ... 363
Gruppenrichtlinienmodellierung ... 358
Gruppenrichtlinien-Voreinstellungen ... 373
Gültigkeit eines Zertifikats überprüfen ... 582

H

Hardware ... 55
Festplatten ... 60
Hauptspeicher ... 59
RAID-Controller ... 60
Serverarchitektur ... 58
Hauptspeicher ... 59, 128
Hochverfügbarkeit ... 1135
Failover-Cluster ... 1146
Vorüberlegungen ... 1136
Host für Remotedesktopvirtualisierung ... 1064
Host-basiertes Spiegeln ... 799
Hostheader ... 950
HTTP mit SSL-Verschlüsselung ... 527
Hyper-V ... 1237
Core-Installationsoption ... 1248
Hyper-V Manager ... 1250
Hyper-V Server 2012 ... 1248
Installation ... 1252
Installationsmöglichkeiten ... 1247
Netzwerkeinstellungen ... 1260
neue virtuelle Maschine ... 1263
Vorteile ... 1240
Hyper-V Manager ... 1250
Hyper-V → Servervirtualisierung
Hyper-V Server 2012 ... 1248
Hyper-V-Manager ... 1263

I

IA64 ... 57
IIS ... 909
.NET-Benutzer ... 1002
.NET-Vertrauensebenen ... 1013
Administration ... 1029
Anforderungsverarbeitung ... 931
anonyme Authentifizierung ... 959
Anwendung ... 943, 954
Anwendungspool ... 933, 943, 947, 986, 988

IIS (Forts.)
Arbeitsprozess 931
Architektur 930
ASP.NET 915
Authentifizierung 958
Authentifizierungsdelegierung 976
Autorisierung 1003
Datenbankserver 1029
Delegierung 976, 990
Delegierung von Features 1038
Digestauthentifizierung 969
eingeschränkte Delegierung 990
Features delegieren 1038
Formularauthentifizierung 993
freigegebene Konfiguration 1027
Hostheader 950
Identität des Anwendungspools 986, 988
IIS-Manager-Benutzer 1036
IIS-Manager-Berechtigungen 1034
Installation 928
integrierter Modus 935
Internet Information Server 909
IP- und Domäneneinschränkungen 1019
Kerberos 978
Kernelmodus-Authentifizierung 986, 988
klassischer Modus 934
Load Balancing 1024
modularer Aufbau 938
Negotiate 176
NTFS-Berechtigungen 1004
Protokollierung 1040
Protokollübergang 990
Redundanz 1024
Remote-Administration 1030
Remoteanforderungen 1026
Service Principal Names 980
Sicherheit 1007
Sitzungszustand 1021
SPN 980
SSL-Verschlüsselung 1007
Standardauthentifizierung 962
URL-Autorisierung 1005
Verarbeitungsreihenfolge 937
Verwalteter Pipelinemodus 933
virtuelles Verzeichnis 943, 957
Webserver 946
Website 943, 949
Webverwaltungsdienst 1032
Windows Authentifizierung 972
IIS-Manager-Benutzer 1036
IIS-Manager-Berechtigungen 1034
IKEv2 756
Infrastrukturmaster 241
Initiator 69
Innere Sicherheit 675
Installation 201
Active Directory-Rechteverwaltungsdienste 645
aktivieren 206
DFS 835
Drucken 894
Erstkonfiguration 204
Failover-Cluster 1158
Hyper-V 1252
IIS 928
Netzwerklastenausgleich 1191
Remotedesktopdienste 1063
Installationsoption Core 209
Integrierter Modus, IIS 935
Integritätsrichtlinien 682, 699
Intermediate CA 564
Internet 1049
Internet Information Server 909
Internet-Authentifizierung 525
Internetdrucken 892
Internetinformationsdienste
.NET-Vertrauensebenen 1014
ASP.NET-Zustandsserver 1023
Cookies 1022
Richtliniendateien 1018
Sicherheitskonfiguration 1016
URL-Rewriting 1022
Intranet 1049
IOPS 62, 116, 119, 126
IP- und Domäneneinschränkungen 1019
IPAM 39
iPhone 638
Remotedesktopdienste 1080
IPSec 771
IPv4 143
IPv6 143
abschalten 154
Adressierung 146
Adresssyntax 146
Adresstypen 147
Global Unicast Addresses 151
Link-Local Addresses 148
Protokolle 143
Stateful 153
Stateless 152
Unique Local Addresses 150
Unterschiede zu IPv4 145
Vergabe von Adressen 152

IP-Verschlüsselung ... 532
IQN ... 873
IRM ... 641
ISA Server ... 589
OCSP ... 601
Sperrlisten-Verteilungspunkt ... 634
iSCSI ... 65, 68, 1150
Initiator ... 1151, 1154
Target ... 1151
iSCSI Qualified Name ... 873
iSCSI-Taget ... 870
iSCSI-Zielserver ... 870
ISE ... 1374
Issuing CA ... 564

J

JavaScript ... 918

K

KDC ... 168
Kein Vorrang ... 325
Kennwort zurücksetzen, Active Directory-Verwaltungscenter ... 434
Kerberos ... 166, 168
Authentifizierung ... 166
Constrained Delegation ... 176
Delegierung ... 173, 176, 178
Eingeschränkte Delegierung ... 176
Funktionsweise ... 168
IIS ... 978
Kerbtray.exe ... 172
Kernelmodus-Authentifizierung ... 182
Netzwerklastenausgleich ... 1206
Netzwerkprotokolle ... 166
Service Principal Name ... 173
setspn.exe ... 174
SPN ... 173
Toubleshooting ... 178
Webanwendungen ... 978
Kerberos Two Way Transitive Trusts ... 225
Kerbtray.exe ... 172
Kernelmodus-Authentifizierung ... 986, 988
Delegierung ... 182
Kerberos ... 182
Key Distribution Center ... 168
Klassischer Modus, IIS ... 934
Kommandozeile ... 1361
Kompilierung, ASP.NET ... 922
Kontakt zu Ulrich B. Boddenberg ... 22
Kontingent anwenden ... 818
Kontingentverwaltung ... 814
Kontingentvorlage ... 815

L

L2TP ... 756, 771
LDAP ... 495
Ldp.exe, Active Directory-Papierkorb ... 426
Leistungsindikatoren ... 99
Festplatten ... 116
Leistungsmonitor, Systemmonitor ... 97
Lew Platt ... 1048
Licensor Certificate ... 643
Link-Local Addresses ... 148
Lizenzierung ... 52
Active Directory-Rechteverwaltungs-dienste ... 643, 672
CAL ... 53
Client Access License ... 53
Device-CAL ... 53
User-CAL ... 53
Load Balancing, IIS ... 1024
Lokale GPOs ... 327
Lokale Richtlinienobjekt ... 328
Loopbackverarbeitung ... 372
Loopbackverarbeitungsmodus ... 372, 1107
LPD-Dienst ... 892

M

MAC-Adresse, Netzwerklastenausgleich ... 1202
MAK ... 207
Managed Applications ... 189
Managed Web Applications ... 189
MBR ... 791
Mehrstufiges NAP-Konzept ... 685
Messbarkeit ... 1046
MetaFrame ... 1059
Microsoft Application Virtualization ... 1063
Microsoft Network Monitor ... 132
Migration von VMs ... 1354
Mirrored Volume ... 797
MMC-Snap-Ins, Core-Server ... 216
Multi Activation Key ... 207
Multicast ... 147
Multipathing ... 71
Multipfad-E/A ... 788

N

Namenskontext ... 233
Namensraum ... 227
NAP ... 677
Agent ... 683
Client vorbereiten ... 683
Client-Perspektive ... 707
DHCP ... 690
DHCP-Server vorbereiten ... 702
Funktionsweise ... 678
Gemeinsamer geheimer Schlüssel ... 686
Integritätsrichtlinien ... 699
Kommunikationsvorgänge ... 680
Mehrstufiges Konzept ... 685
Network Access Protection ... 676
Netzwerkmonitor ... 710
Netzwerkrichtlinien ... 696
Netzwerkrichtlinienserver ... 681
RADIUS-Proxy-Server ... 688
RADIUS-Remoteservergruppe ... 690
Systemintegritätsprüfungen ... 700
Verbindungsanforderungsrichtlinien ... 696
NAP Enforcement Points ... 677
NAP-Agent ... 683
NAP-Erzwingungspunkte ... 677
NAS ... 65
Navigationsknoten, Active Directory-Verwaltungscenter ... 441
Navigieren, Active Directory-Verwaltungscenter ... 437
Negotiate ... 176
.NET:CardSpace ... 197
.NET:WCF ... 197
.NET:Windows Communication Foundation ... 197
.NET:Windows Presentation Foundation ... 197
.NET:Windows Workflow Foundation ... 197
.NET:WPF ... 197
.NET:WWF ... 197
NetBIOS über TCP/IP ... 492
Network Access Protection ... 676
Network Load Balancing ... 1188
Remotedesktopdienste ... 1128
Network Policy Server ... 681
Netzwerk
Ausfallsicherheit ... 90
entfernte Benutzer ... 87
Layer-2-Switching ... 85
Layer-3-Switching ... 86
Management ... 90
Metropolitan Area Network ... 86
Netzwerk (Forts.)
Sicherheit ... 89
Strukturen und Verfügbarkeit ... 83
VPN-Verbindungen ... 88
WAN-Verbindungen ... 88
Netzwerkdienste ... 455
DHCP ... 472
DNS ... 455
WINS ... 491
Netzwerkkonnektivität ... 129
Netzwerklastenausgleich ... 1188
Affinität ... 1195
Authentifizierung ... 1205
Clusterknoten hinzufügen ... 1197
Delegierung ... 1206
Filtermodus ... 1194
Funktionsweise ... 1189
Hintergründe ... 1200
Installation ... 1191
Kerberos ... 1206
MAC-Adresse ... 1202
Network Load Balancing ... 1188
Netzwerklastenausgleich ... 1203
NLB ... 1188
Remotedesktopdienste ... 1128
Netzwerkmonitor ... 132
ARP ... 161
Capture Filter ... 133
DHCP ... 157
Display Filter ... 133
DNS ... 166
Filter ... 134
Kurzüberblick ... 133
Microsoft Network Monitor ... 132
NAP ... 710
Netzwerklastenausgleich ... 1203
Parser ... 136
Schnelleinstieg ... 136
Netzwerkprotokolle ... 155
ARP ... 159
DHCP ... 155
DNS ... 162
Kerberos ... 166
Netzwerkrichtlinien ... 682, 696
Netzwerkrichtlinien- und Zugriffsdienste ... 676
Netzwerkrichtlinienserver ... 681
Installation ... 691
NAP ... 681
Network Policy Server ... 681
NPS ... 681
Neuanlage von Objekten, Active Directory-Verwaltungscenter ... 440

NLB 1188
NPS 681
NT 3.1 Advanced Server 25
NT 4 Server 29
NT Server 3.5 27
NTFS-Berechtigungen, IIS 1004

O

OCSP 593
ISA Server 601
Offline-CA installieren 603
Offline-Domänenbeitritt 453
Online Certificate Status Protocol 593
Online-Responder 593
Optimierung der Druckumgebung 885
Organisationseinheit 228
Active Directory-Domänendienste 228
Organizational Unit 228
OU 228
Organizational Unit 228
OU 228
Over-commitment 869

P

Papierkorb, Active Directory 424
Parser, Netzwerkmonitor 136
Partition 233
Partitionieren 793
PDC 224
PDC-Emulator 240
Performance 113
Blockgröße (Festplatten) 116, 126
RAID-Level 120
Richtwerte 97
Servervirtualisierung 1244
Performance-Analyse 100
Performancemonitor, Systemmonitor 97
Pipelines 1372
Planung, Servervirtualisierung 1244
Platt, Lew 1048
PowerShell 1361
Active Directory-Papierkorb 431
Core-Server 212
Modul für Active Directory 446
PPTP 756, 769
Preferences, Gruppenrichtlinien 373
Pre-Shared Key 771
printQueue-Objekt 903
Profile.ps1 1370
Protocol Transition 993
Protokoll erstellen, Systemmonitor 104
Protokolle 131
IPv4 143
IPv6 143
Netzwerkmonitor 132
Protokollierung, IIS 1040
Protokollübergang 990, 993
Prozessoren 55, 128
EMT64 57
Stepping 59
x64 57
PSK 771
Public Key Infrastructure 534
Publishing License 643
Pull-Replikation, WINS 492
PushPrinterConnections.exe 906

Q

Quota Management 814
Quotas 814

R

RADIUS-Proxy-Server 688
RADIUS-Remoteservergruppe 690
RAID 60
RAID-Controller 60
RAID-Level
Einfluss auf die Performance 120
RDP-Protokoll 1080
Read Only Domain Controller 252
Rechenzentrum 91
Feuer, Wasser 92
räumliche Anforderungen 93
Redundanz 96
Stromversorgung 94
Zugangskontrolle 91
Rechnen macht erfolgreich 119
Rechteverwaltungsdienste 641
Redundanz
IIS 1024
ReFS 865
regsvr32 schmmgt.dll 235
Remote-Administration
IIS 1030

Remoteanforderungen ... 1026
RemoteApp- und Desktopverbindungen mit Windows 7 ... 1124
RemoteApp-Benutzerzuweisung ... 1093
RemoteApp-Manager ... 1091
RemoteApp-Programme ... 1090
Remotedesktopdienste ... 1057, 1108
Administration ... 1098
Aktivieren des Lizenzservers ... 1110
Anwendungen installieren ... 1084
Benutzeradministration ... 1104
Benutzerzugriff ... 1080
change user ... 1087
Clearinghouse ... 1113
Desktop bereitstellen ... 1088
Drucken ... 1115
Drucken, Gruppenrichtlinien ... 1120
Easy Print ... 1115
Farmen ... 1128
Fernsteuerung ... 1106
Gruppenrichtlinien ... 1084, 1107
Gruppenrichtlinien, Drucken ... 1120
Installation ... 1063
Installationsmodus ... 1087
iPhone ... 1080
Lizenzierung ... 1108
Lizenzmodell wählen ... 1100
Lokale Gruppe Remotedesktopbenutzer ... 1081
Loopbackverarbeitungsmodus ... 1107
Network Load Balancing ... 1128
Netzwerklastenausgleich ... 1128
Office installieren ... 1088
RDP-Protokoll ... 1080
Remote Control ... 1106
RemoteApp-Benutzerzuweisung ... 1093
RemoteApp-Programme ... 1090
Remotedesktopdienste, Drucken ... 1120
Remoteüberwachung ... 1105, 1106
Schlussbemerkung ... 1133
Sicherheitsvorkehrungen ... 1086
Startmenü, Windows 7/8 ... 1124
Thin Clients ... 1080
Überblick ... 1059
Verbindungsbroker ... 1128
Verwaltung ... 1098
Vorteile ... 1060
Web Access für Remotedesktop ... 1121
Windows 7/8 ... 1124
XPS-Viewer ... 1117
Remotedesktopdienste-Farmen ... 1128
Remotedesktopdienste-Verbindungsbroker ... 1128
Remotedesktopgateway ... 1064
Remotedesktoplizenzierung ... 1064
Remotedesktoplizenzierungs-Manager ... 1108
Remotedesktop-Sitzungshost ... 1064
Remotedesktop-Verbindungsbroker ... 1064
Remoteserver-Verwaltungstools, Active Directory-Verwaltungscenter ... 433
Remotezugriff ... 759
Replikation einrichten, Active Directory Lightweight Directory Services ... 514
Replikationstopologie, DFS ... 849
Resilient File System ... 865
Ressourcen-Manager für Dateiserver ... 814
Ressourcenmonitor ... 99
Ressourcenübersicht ... 99
Reverse-Lookupzone ... 469
Richtlinien
DNS ... 484
Richtwerte zur Performance ... 97
RID-Master ... 241
Rights Management Services ... 641
RMDS ... 814
RMS ... 641
RODC ... 252
Rollen ... 45
Core-Installationsoption ... 210, 217
Root CA ... 563
Rotational Latency ... 62
Rückblick ... 23
DOS ... 24
Microsoft BackOffice ... 28
Windows 3.0 ... 25
Windows Server 2003 R2 ... 33
Wolfpack ... 29

S

Sammlungssatz ... 104
SAN ... 65
Servervirtualisierung ... 1242
SAN Storage ... 803
SAN-Architektur ... 69
Scale-out ... 1241
Scale-up ... 1241
Schattenkopien ... 809
Schema ... 232
Schema-Manager ... 235
Schemamaster ... 243
schmmgt.dll ... 235
Schreibgeschützte Domänencontroller ... 252

sconfig.cmd ... 211
SCSI-Protokoll ... 66
SCVMM ... 1303
Secure Socket Tunneling Protocol ... 774
Self-Healing NTFS ... 812
Server
Aufgaben und Rollen ... 43
DNS ... 462
wiederherstellen ... 1233
Serverarchitektur ... 58
Serverhardware ... 55
64-Bit-Welt ... 57
Architektur ... 58
EMT64 ... 57
Festplatten ... 60
Hauptspeicher ... 59
IA32-Prozessoren ... 56
Prozessoren ... 55
RAID-Controller ... 60
x64 ... 57
Serversysteme
AWE ... 56
ECC ... 59
EM64T ... 57
EPIC ... 57
IA64 ... 57
IOPS ... 62
RAID ... 60
SAS ... 63
SATA ... 63
SCSI ... 63
Stepping ... 59
x64 ... 57
Servervirtualisierung ... 1237, 1241
Hyper-V ... 1247
Marktüberblick ... 1239
Performance ... 1244
Planung ... 1244
SAN ... 1242
Scale-out vs. Scale-up ... 1241
Vorteile ... 1238
Service Locator Records ... 383
Service Principal Name ... 1184
Service Principal Names ... 173, 176, 980
Service Resource Records ... 471
setspn.exe ... 174
SHA ... 680
SharePoint Foundation ... 1045
SharePoint, Warum SharePoint? ... 1046
Sichere E-Mail ... 528
signieren ... 529
verschlüsseln ... 528
Sicherheit
ASP.NET ... 927
Gruppenrichtlinien ... 323
IIS ... 1007
Sicherung ... 1225
Sicherungszeitplan ... 1225
Signatur, Windows PowerShell ... 1369
Single Sign On ... 519
Site-Local Addresses ... 148
Sitzungszustand ... 1021
Skripte ... 1368
slmgr ... 207
Smartcard ... 532
SOAP-Protokoll ... 912
Softgrid ... 1063
Softwareverteilung, Gruppenrichtlinien ... 369
SoH ... 680
Spanned Volume ... 797
Special Addresses ... 148
Speicherberichteverwaltung ... 824
Speicherpools ... 865
Sperrliste ... 616
Sperrlisteneinträge ... 578, 579
Sperrlisten-Verteilungspunkt ... 581
Spiegeln ... 799
SPN ... 173, 176, 980, 1184
SSL-Verschlüsselung ... 1007
SSoH ... 680
SSTP ... 756, 774
Troubleshooting ... 778
Zertifikatsperrliste ... 574
Stammhinweise, DNS ... 465
Stammzertifizierungsstelle ... 563
Standardauthentifizierung ... 962
Standardkompilierung
ASP.NET ... 922
Standardkompilierung ... 922
Standardverbindungs-URL ... 1095
Standort, ADS ... 262
Starter-Gruppenrichtlinienobjekte ... 331
Stateful ... 153
Stateless ... 152
Statement of Health ... 680
Statistik, Active Directory-Rechteverwaltungsdienste ... 672
Stelleninformationen ... 581, 614
Stepping ... 59
Storage
Blocklevel-Zugriff ... 65
Cloning ... 80
Controller-basierte Spiegelung ... 72

Storage (Forts.)
controller-basierte Virtualisierung ... 80
Copy-on-Write-Snapshot ... 76
DAS ... 65
FibreChannel ... 66
host-basierte Spiegelung ... 74
In-Band-Virtualisierung ... 81
Initiator ... 69
iSCSI ... 65, 68
Multipathing ... 71
NAS ... 65
Out-of-Band-Virtualisierung ... 82
Redundante Storage-Systeme ... 71
SAN ... 65
SAN-Architektur ... 69
SAN-basierte Virtualisierung ... 80
SCSI-Protokoll ... 66
Snapshotting ... 75
Target ... 69
Virtualisierung ... 80
Volume Shadow Copy Services ... 77
Write Penalty ... 120
Storage Spaces ... 865
Störfall vs. Notfall ... 1142
Stripesetvolume ... 797
System Center Virtual Machine Manager 2008
Bibliotheken ... 1325
Hosts verwalten ... 1323
System Center Virtual Machine Manager 2012 ... 1303
Architektur ... 1304
virtuelle Maschinen verwalten ... 1324
System Center Virtual Machine Manager 2012 → SCVMM
System Center Virtual Machine Manager 2012 → VMM
System Center Virtual Machine Manager, Migration von VMs ... 1354
System Health Agents ... 680
Systemintegritätsprüfungen ... 682, 700
Systemmonitor ... 97
Protokoll erstellen ... 104
Sammlungssatz ... 104
Systempartition ... 114

T

Target ... 69
Terminaldienste ... 1057
Gruppenrichtlinien ... 373
Loopbackverarbeitungsmodus ... 372
TGT ... 169
Ticket Granting Service ... 169
Ticket Granting Ticket ... 169
Top-down-System ... 1053
Transactional NTFS ... 812
Transition Addresses ... 148
Tree ... 224
Treiber, Drucken ... 896
Troubleshooting, Active Directory-Domänendienste ... 412
Tunneling-Protokolle ... 756

U

Überblick, Editionen ... 51
Über-Provisionierung ... 869
Umstrukturieren, Active Directory-Domänendienste ... 418
Unicast ... 147
Unique Local Addresses ... 148, 150
Universal Group Membership Caching ... 237
Universale Gruppe ... 378
Universelle Gruppen ... 231
Unmanaged Applications ... 188
Unternehmenswissen ... 1047, 1048
Updates genehmigen ... 746
Upgrade, Active Directory-Domänendienste ... 392
URL-Autorisierung ... 1005
Use License ... 644
useAppPoolCredentials ... 1217
User-CAL ... 53

V

Verbindungsanforderungsrichtlinien ... 682, 696
Verbindungs-Manager-Verwaltungskit ... 781
Verbunddienst ... 521
Verbunddienstproxy ... 521
Vererbung, Gruppenrichtlinien ... 320
Verfügbarkeit, Active Directory-Domänendienste ... 243
Verschieben der Betriebsmasterrollen ... 244
Verschlüsselung ... 525
Verteiltes Dateisystem ... 828
Vertriebsleiterbeispiel ... 1054
Verwalteter Pipelinemodus ... 933
Verwaltungscenter ... 432
Virtualisierung, Storage ... 80
Virtuelle Maschinen, Migration ... 1354

Virtuelles Verzeichnis ... 943, 957
Visual Studio Professional ... 915
Visual Web Developer ... 915
VMM ... 1304
Volume Shadow Copy Service ... 77, 809
Volumenlizenz-Datenträger ... 208
Volumes
  vergrößern ... 802
  verkleinern ... 802
Voraussetzungen
  Active Directory-Papierkorb ... 424
  Active Directory-Verwaltungscenter ... 443
Vorinstallierter Schlüssel ... 771
Vorkompilierung
  ASP.NET ... 922, 925
Vorrang, Gruppenrichtlinien ... 323
Vorteile, Windows PowerShell ... 1361
VPN
  automatischer Modus ... 780
  CMAK ... 781
  Connection Manager Administration Kit ... 781
  EAP ... 770
  einrichten ... 764
  Einwahlberechtigung ... 768
  Extensible Authentication Protocol ... 770
  Gateway-Architektur ... 757
  IKEv2 ... 756
  IPSec ... 771
  L2TP ... 756, 771
  PPTP ... 756, 769
  Pre-Shared Key ... 771
  PSK ... 771
  Secure Socket Tunneling Protocol ... 774
  Server, Grundkonfiguration ... 759
  SSTP ... 756, 774
  Tunneling-Protokolle ... 756
  Verbindungs-Manager-Verwaltungskit ... 781
  vorinstallierter Schlüssel ... 771
  VPN-Server, Grundkonfiguration ... 759
VPN-Verbindungen ... 88
VSS → Volume Shadow Copy Service

W

W3SVC ... 931
w3wp.exe ... 931
WAN-Miniport-Treiber ... 756
Warteschlange ... 116
Wartungsservergruppen ... 682
Warum eine neue Server-Version? ... 23
Warum SharePoint? ... 1046
WAS ... 931
WCF ... 197
Web Access für Remotedesktop ... 1064, 1121
  Konfiguration ... 1123
web.config ... 919
Weboberfläche
  Active Directory-Zertifikatdienste ... 560
Webserver ... 909, 946
  Best Practice Analyzer ... 1042
  BPA ... 1042
  IIS ... 909
Website ... 943, 949
Website/Webseite, Begriffsdefinition ... 914
Webverwaltungsdienst ... 1032
Weiterleitungen, DNS ... 464
Wiederherstellung ... 1229
  eines Servers ... 1233
Wiederherstellungszeit ... 1137
Windows 1, 2 und 3 ... 23
Windows 2000 Server ... 31
Windows 7/8, Remotedesktopdienste ... 1124
Windows Communication Foundation ... 197
Windows Firewall
  Basiskonfiguration ... 716
  Gruppenrichtlinien ... 725
  Isolierungsregel ... 722
  Konfigurationshinweise ... 727
  Profile ... 716
  Regeln ... 715
Windows NT 3.1 Advanced Server ... 25
Windows NT 4 Server ... 29
Windows NT Server 3.5 ... 27
Windows PowerShell ... 1361
  Alias ... 1364, 1367
  Ausführungsrichtlinie ... 1369
  Cmdlets ... 1364
  Entwicklungsumgebung ... 1374
  Grundlagen ... 1364
  Pipelines ... 1372
  Profile.ps1 ... 1370
  Signatur ... 1369
  Skripte ... 1368
  Vorteile ... 1361
Windows PowerShell Integrated Scripting Environment ... 1374
Windows PowerShell → PowerShell
Windows Presentation Foundation ... 197
Windows Script Host ... 1361
Windows Server 2003 ... 31
Windows Server 2008 ... 33

Windows Server 2008 R2 ..... 33, 34
Windows Server 2012 R2, Neuerungen 40
Windows Server 2012, Neuerungen 36
Windows Server Update Services 729
Windows Workflow Foundation 197
Windows-Authentifizierung 972
Windows-Firewall 713
Regeln im Detail 718
Windows-PowerShell, Modul für Active Directory 446
Windows-Prozessaktivierungsdienst 931
WINS 491
DHCP 480
Wireless Authentification 534
WMI-Filter 365
Wolfpack 29
Word-Dokument schützen 662
Worst-Case-Fall 1137
WPF 197
Write Penalty 120
WS-Federation 519
WSH 1361
WSUS 729
automatische Genehmigung 746
Berichte 754
Erstkonfiguration 736
Funktionsweise 729
Gruppen 743
Gruppenrichtlinien 750
Installation 731
Konfiguration 741
Updates genehmigen 746
Updates manuell genehmigen 748
Windows Server Update Services 729
wuauclt 751
WWF 197
WWW-Publishing-Dienst 931

X

x64 57
XenApp 1059
XPS 889
XPS-Viewer 1117

Z

Zeitdienst 387
Zeitsynchronisation 388
Zentraler Netzwerkrichtlinienserver 686
Zentraler Speicherort, Gruppenrichtlinien 340
Zertifikat überprüfen 585
Zertifikatdatenbank wiederherstellen 543
Zertifikatdienste 525
Zertifikate, Cache 588
Zertifikatgültigkeit überprüfen 582
Zertifikatsperrliste 574, 604
DirectAccess 574
Funktionsweise 576
Gültigkeit 582
ISA Server 589
Zertifikatvorlagen 551
Zertifizierungspfad 550
Zertifizierungsstelle, OCSP anpassen 600
Zonen, Netzwerkdienste 456
Zonentypen, DNS 457
Zugriff auf Stelleninformationen 581
Zusammenspiel mit anderen Microsoft-Produkten 48
Zusätzliche Domänencontroller einrichten 308
Zuverlässigkeit und Leistung 97
Zweistufige Architektur implementieren 602