Carlo Westbrook

Buch+

Active Directory
in Windows Server 2012 R2

Handbuch für die Planung und den praktischen Einsatz in Windows-Netzwerken

- Einführung & Grundlagen
- Planung, Aktualisierung & Migration
- Implementierung, Verwaltung & Wartung

Behandelt auch **Windows Server 2012 und Windows 10**

CertPro® PRESS - *Professional Learning*

Carlo Westbrook

Active Directory
in Windows Server 2012 R2

Planung und praktischer Einsatz in Windows-Netzwerken

CertPro PRESS
ein Imprint von CertPro® Limited

Bibliografische Informationen der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über *http://dnb.d-nb.de* abrufbar.

Die Informationen in diesem Produkt werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt. Bei der Zusammenstellung von Texten und Abbildungen wurde mit größter Sorgfalt vorgegangen. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Für Verbesserungsvorschläge und Hinweise auf Fehler sind Verlag und Herausgeber dankbar.

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Die gewerbliche Nutzung der in diesem Produkt gezeigten Modelle und Arbeiten ist nicht zulässig.

Fast alle Hard- und Softwarebezeichnungen und weitere Stichworte und sonstige Angaben, die in diesem Buch verwendet werden, sind als eingetragene Marken geschützt. Da es nicht möglich ist, in alle Fällen zeitnah zu ermitteln, ob ein Markenschutz besteht, wird das ®-Symbol in diesem Buch nicht verwendet.

Print-Ausgabe: ISBN 978-3-9447-4902-0
ebook-Ausgabe (PDF): ISBN 978-3-9447-4907-5
ebook-Ausgabe (EPUB): ISBN 978-3-9447-4908-2

Copyright © 2016 by CertPro Press-Verlag,
ein Imprint der CertPro® Limited, Im Pflänzer 14, D-55545 Bad Kreuznach/Germany.
Alle Rechte vorbehalten.
Einbandgestaltung: Carlo Westbrook, CertPro® Limited
Bilder und Grafiken: CertPro® Limited
Herstellung: CertPro® Limited
Druck und Verarbeitung: BoD GmbH, Hamburg
ebook-Distribution: libreka! GmbH, Frankfurt am Main
Printed in Germany

Auf einen Blick

Teil 1 - Einführung und Grundlagen

1 Einführung in Windows Server 2012 R2 33
2 Einführung in Active Directory 51
3 Sicherheit in Active Directory-Domänendienst-Umgebungen 123

Teil 2 - Planung, Aktualisierung und Migration

4 Planung einer Active Directory-Domänendienste-Infrastruktur 156
5 Aktualisierung vorhandener Gesamt- und Domänenstrukturen 223
6 Migration von Gesamtstrukturen und Domänen 237

Teil 3 - Implementierung, Verwaltung und Wartung

7 Installation und Konfiguration von Windows Server 2012 R2..... 259
8 Implementierung und Verwaltung von Domain Name System (DNS) 292
9 Implementieren der Active Directory-Domänendienste (AD DS)..... 322
10 Verwalten der Betriebsmasterrollen 354
11 Verwaltung globaler Katalogserver..... 373
12 Erstellen und Verwalten von Organisationseinheiten..... 381
13 Delegierung der Verwaltungsfunktionalität 395
14 Erstellen und Verwalten von Active Directory-Objekten..... 404
15 Erstellen und Verwalten von Gruppenrichtlinienobjekten 459
16 Verwaltung der Benutzerumgebung mit Gruppenrichtlinienobjekten..... 526
17 Planung und Einsatz von Kennworteinstellungen..... 565
18 Schreibgeschützte Domänencontroller..... 572
19 Domänencontroller unter Server Core..... 603
20 Verwaltung von Standorten und Replikation 631
21 Wartung und Diagnose der Active Directory-Domänendienste..... 645
22 Sichern und Wiederherstellen der Active Directory-Domänendienste..... 660
23 Weitere Active Directory-Dienste..... 685

Stichwortverzeichnis..... 691

Website zum Buch

Liebe Leserin, lieber Leser,

zu diesem Buch bieten wir Ihnen zusätzliche Materialien, wie z. B. Zusatzdokumentation, Beispieldateien, die Sie bei Bedarf gerne direkt aus unserer Verlagswebsite im Internet herunterladen können unter:

http://www.CertPro-Press.de/9020.html

Inhaltsverzeichnis

Der Autor 28
Vorwort 29
Aufbau des Buches 30
Konventionen und Symbole 30
Teil 1: Einführung und Grundlagen 31
1 Einführung in Windows Server 2012 R2 33
1.2 Unterstützte Serverrollen und -funktionen 34
1.2.1 Unterstützte Serverrollen 34
1.2.1 Unterstützte Features (Funktionen) 36
1.3 Neuerungen und Verbesserungen 39
1.3.1 Der Anmeldebildschirm 39
1.3.2 Die grafische Benutzeroberfläche 40
1.3.3 Der grafische Server-Manager 41
1.3.4 Server Core - Grafikoberfläche nachträglich aktivierbar 42
1.3.5 Neuerungen im Windows-Explorer 43
1.3.6 Die Windows PowerShell 4.0 44
1.3.7 Active Directory-Verwaltungscenter 44
1.3.8 Active Directory-Papierkorb - jetzt grafisch 45
1.3.9 Verbesserte Kennwortrichtlinienverwaltung 46
1.3.10 Active Directory-basierte Aktivierung 47
1.3.11 Klonen von Domänencontrollern 47
1.3.12 Dynamische Zugriffssteuerung 48
1.3.13 Essentials Experience - für kleine Firmen und Institutionen 48
Merkmale der Essentials Experience-Serverrolle 48
1.3.14 Weitere Verbesserungen und Neuerungen 50
1.4 Zusammenfassung 50
2 Einführung in Active Directory 51
2.1 Was ist ein Verzeichnisdienst? 51
2.2 Merkmale der Active Directory-Domänendienste 52
2.3 Der X.500-Standard und die Microsoft Active Directory-Domänendienste 52
2.3.1 Das Lightweight Directory Access Protocol (LDAP) 54

2.3.2 Der Namenskontext ... 54
Distinguished Name (DN) ... 55
Relative Distinguished Name (RDN) ... 55
LDAP Uniform Resource Locator (URL) ... 55
User Principal Name (UPN) ... 56
2.3.3 Das Kerberos-Protokoll ... 56
2.4 Die Architektur ... 57
2.5 Die physikalischen Komponenten der Active Directory-Domänendienste ... 58
2.5.1 Die Datenbank ... 59
Aufteilung in einzelne Partitionen ... 59
Replikation der Partitionsinhalte ... 60
Das Datenspeicherungsmodell ... 61
Schnittstellen für den Datenbankzugriff ... 62
Die Datenbankdateien ... 63
Die Extensible Storage Engine (ESE) ... 64
Der Ablauf von Transaktionen ... 65
2.5.2 Domänencontroller ... 66
2.5.3 Schreibgeschützte Domänencontroller ... 66
Einsatzzweck von RODCs ... 66
Weitere Funktionen ... 68
Zwischenspeichern von Kennwörtern auf RODCs ... 68
Delegierung der Verwaltungsberechtigung ... 68
Einschränkungen schreibgeschützter Domänencontroller ... 68
2.5.4 Die Betriebsmasterrollen ... 69
Gesamtstrukturweite Betriebsmasterrollen ... 69
Domänenweite Betriebsmasterrollen ... 70
Tools zur Verwaltung der Betriebsmasterrollen ... 71
2.5.5 Der globale Katalog ... 72
Globaler Katalog und der Infrastruktur-Master ... 74
2.5.6 Zwischenspeichern der universellen Gruppenmitgliedschaft ... 75
Vorteile ... 76
Ablauf des Anmeldevorgangs ... 76
2.5.7 Der Replikationsdienst ... 77
Die Replikationstopologie ... 78
Inter-Site Topology Generator ... 80
Replikation der Inhalte von Verzeichnispartitionen ... 80

Multimaster-Replikation ... 81
Dringlichkeitsreplikation (Urgent Replication) ... 81
Lokale USN ... 82
Replikationskonflikte ... 83
Replikation zwischen Standorten ... 84
Optimierung des Client-Anmeldeverkehrs ... 84
2.6 Die logischen Komponenten der Active Directory-Domänendienste ... 84
2.6.1 Das Active Directory-Schema ... 86
Gründe für die Änderung des Active Directory-Schemas ... 87
Tools zum Verwalten des Active Directory-Schemas ... 88
2.6.2 Verzeichnispartitionen ... 88
Tools zum Verwalten von Verzeichnispartitionen ... 89
2.6.3 Gesamtstrukturen ... 89
2.6.4 Vertrauensstellungen ... 91
Bidirektionale, transitive Vertrauensstellungen ... 92
Gesamtstrukturvertrauensstellung ... 93
Verknüpfte Vertrauensstellung ... 94
Externe Vertrauensstellung ... 95
Bereichsvertrauensstellung ... 96
Tools zum Verwalten von Vertrauensstellungen ... 96
2.6.6 Domänen ... 97
Tools zum Verwalten von Domänen ... 99
2.6.7 Authentifizierung und Autorisierung ... 99
Der Authentifizierungsprozess ... 99
Der Autorisierungsprozess ... 100
2.6.8 Organisationseinheiten ... 102
Beispiel für die Strukturierung von Organisationseinheiten ... 103
Delegierung der Verwaltungsberechtigung ... 104
Tools zum Verwalten von Organisationseinheiten ... 104
2.6.9 Standorte ... 105
Tool zum Verwalten von Active Directory-Standorten ... 106
2.6.10 Subnetz ... 106
Beispiel für den Einsatz von Subnetzen in Active Directory-Domänen ... 107
Tool zum Verwalten von Subnetzen ... 107
2.7.3 Heraufstufen einer Domänen- oder Gesamtstrukturfunktionsebene ... 111
Heraufstufen der Domänenfunktionsebene ... 112

Heraufstufen der Gesamtstrukturfunktionsebene ... 112
2.8 Active Directory- Domänendienste und das Domain Name System (DNS) ... 113
2.8.1 Die DNS-Namenszonen ... 114
Forward-Lookup-Zone ... 114
Reverse-Lookup-Zone ... 115
2.8.2 DNS-Zonentypen ... 115
2.8.3 Standardspeicherorte für DNS-Zonendaten ... 116
2.8.4 Dynamische oder statische Registrierung ... 116
DNS und DHCP ... 117
2.8.4.2 Sichere dynamische Aktualisierung ... 118
2.8.5 DNS-Ressourceneinträge ... 118
2.8.6 SRV-Einträge ... 119
Arten von Diensteinträgen ... 120
2.9 Zusammenfassung ... 122
3 Sicherheit in Active Directory-Domänendienst-Umgebungen ... 123
3.1 Grundlagen ... 123
3.1.1 Sicherheitsprinzipale ... 123
Beispiel für eine Sicherheitskennung (SID) ... 124
Standardmäßige Sicherheitskennungen ... 124
Löschen von Objekten ... 125
Discretionary Access Control List (DACL) ... 126
System Access Control List (SACL) ... 127
3.1.3 Authentifizierung & Autorisierung ... 127
3.1.4 Zugriffstoken ... 128
3.1.5 Kerberos V5-Protokoll ... 128
Kerberos - unterstützte Verschlüsselungstypen ... 130
Festlegen der AES-Verschlüsselung für Kerberos ... 130
Standardmäßiger Fallback zu NTLM ... 131
Kerberos-Konfiguration unter Windows Server 2012 (R2) ... 131
Ports für die Kerberos-Authentifizierung ... 132
Tools für die Kerberos-Verwaltung und -Problembehandlung ... 133
3.1.6 NTLM-Protokoll ... 133
Situationen für die Verwendung des NTLM-Protokolls ... 133
Vergleich von LM, NTLM und NTLMv2 ... 134
Verhindern der Zwischenspeicherung von LM-Hashes ... 134
Konfiguration der Lan Manager-Authentifizierungsebene ... 136

3.2 Domänensicherheit ... 138
3.2.1 Vordefinierte Sicherheit ... 138
3.2.2 Microsoft Security Compliance Manager (SCM) 3.0 ... 139
Problemloser Export in Gruppenrichtlinienobjekte möglich ... 140
Enthaltene Tools ... 141
3.3.2 Sicherheitsrichtlinien für Domänencontroller ... 142
Standardmäßige Gruppenrichtlinienobjekte ... 142
3.3.3 SMB - Zugriff auf Freigaben erst ab Version 2.0 ... 142
3.3.4 Domänencontroller als Server Core-Installation ... 143
Grafische Benutzeroberfläche nachträglich wieder aktivierbar ... 143
3.3.5 Dynamische Zugriffssteuerung ... 144
3.3.6 Verbesserte Kennwortrichtlinienverwaltung ... 144
Funktionsweise ... 145
Auswertelogik ... 145
Schritte zum Erstellen abgestimmter Kennwortrichtlinien ... 147
Anzeigen der auf einen Benutzer angewandten abgestimmten Kennwortrichtlinien ... 147
3.3.7 Sicherheitsgruppe „Protected Users" ... 149
Vordefinierte Schutzfunktionen ... 149
Voraussetzungen für den erweiterten Schutz ... 150
3.3.8 Überwachung der Active Directory-Domänendienste ... 150
Konfiguration der erweiterten Überwachungsrichtlinien ... 150
Zusätzliche Konfiguration für die erweiterte Überwachung ... 151
Aktivierung der Überwachung einzelner Active Directory-Objekte ... 152
Dokumentation der Änderungen in der Ereignisanzeige ... 153
3.4 Zusammenfassung ... 153
Teil 2: Planung, Aktualisierung und Migration ... 155
4 Planung einer Active Directory-Domänendienste-Infrastruktur ... 156
4.1 Planung der Active Directory-Domänendienste ... 156
4.1.1 Der Masterplan ... 157
4.1.2 Sammeln von Informationen über das Unternehmen ... 158
Sammeln und Analysieren von Unternehmensanforderungen ... 159
4.1.4 Dokumentation der vorhandenen Netzwerkinfrastruktur ... 160
Projektvorbereitende Dokumentation ... 161
4.2 Analysieren der Entwurfsoptionen ... 162
4.2.1 Eine oder mehrere Gesamtstrukturen? ... 163

Maximale Anzahl an Domänen ... 163
Maximale Anzahl an Domänencontrollern ... 163
Maximale Anzahl an Active Directory-Objekten ... 163
4.2.2 Gesamtstrukturmodelle ... 164
Organisations-Gesamtstrukturmodell ... 164
Ressourcen-Gesamtstrukturmodell ... 164
Gesamtstrukturmodell mit eingeschränktem Zugriff ... 165
4.2.3 Gesamtstrukturübergreifende Vertrauensstellung ... 166
SID-Filterung ... 166
Authentifizierungsoptionen ... 167
UPN-Suffix-Routing ... 167
4.2.4 Entwerfen einer Domänenstruktur ... 168
Das Domänenmodell ... 168
Anzahl der erforderlichen Domänen ... 170
Die Stammdomäne der Gesamtstruktur ... 171
Die Domänen- und Gesamtstrukturfunktionsebene ... 172
Strategien für die Planung von DNS-Namensräumen ... 177
Merkmale der verschiedenen Namensstrategien ... 178
Empfehlungen für die Namensvergabe ... 179
4.2.6 Entwerfen einer Standorttopologie ... 180
Standorte (Sites) ... 180
Subnetz ... 181
Standortverknüpfung (Site Link) ... 181
Standortverknüpfungsbrücke (Site Link Bridge) ... 183
Replikationsprotokolle ... 184
Bridgeheadserver ... 185
4.3 Platzierung von Domänencontrollern ... 186
4.3.1 Empfehlungen für die Anzahl von Domänencontrollern ... 186
4.3.2 Schreibgeschützte Domänencontroller ... 186
Voraussetzung für den Einsatz von RODCs ... 187
RODC als globaler Katalogserver ... 188
RODC und die Zwischenspeicherung der universellen Gruppenmitgliedschaft ... 189
RODC und die Betriebsmasterrollen (FSMO-Roles) ... 189
RODC und die Bridgehead-Server ... 189
Delegierung von RODCs ... 189
Schreibgeschützter DNS ... 190

4.3.3 Platzieren globaler Katalogserver ... 190
Globaler Katalog und der Anmeldeprozess ... 191
Globaler Katalog und die Infrastrukturmasterrolle ... 192
Der globale Katalog und Remote-Standorte ... 192
Richtlinien für die Platzierung von globalen Katalogservern ... 192
4.3.4 Platzieren der Betriebsmasterrollen ... 193
Standardmäßige Platzierung von Betriebsmasterrollen ... 193
Richtlinien für die Platzierung von Betriebsmasterrollen ... 194
Active Directory-Gesamtstruktur mit einer einzigen Domäne ... 194
Active Directory-Gesamtstruktur mit mehreren Domänen ... 195
4.4 Entwerfen einer Verwaltungsinfrastruktur ... 196
4.4.1 Bestimmen eines Verwaltungsmodells ... 196
Verwaltungsmodelle ... 197
Weitere Gesichtspunkte für die Auswahl eines Verwaltungsmodells ... 198
4.4.2 Planen einer Struktur für Organisationseinheiten ... 198
4.4.3 Delegieren der Verwaltungsfunktionalität ... 200
Vererbung der Verwaltungsberechtigung ... 200
Empfehlungen für den Entwurf von Organisationseinheitenstrukturen ... 201
4.5 Entwerfen von Strukturen für die Verwendung von Gruppenrichtlinienobjekten ... 201
4.5.1 Empfehlungen für die Planung der Struktur der Organisationseinheiten für die Verwendung von Gruppenrichtlinienobjekten ... 202
4.6 Entwerfen einer Strategie für Objekte ... 202
4.6.1 Benutzerobjekte ... 202
Unterschiede zwischen lokalen und Domänenbenutzerkonten ... 202
Eindeutigkeit anhand von Benutzerobjekten ... 203
Namensstrategie ... 203
Teilzeitkräfte, externe Mitarbeiter, Praktikanten und Dienstkonten ... 204
Benutzerprinzipalnamen (UPN) ... 204
Entwerfen einer Kennwortrichtlinie für Benutzerobjekte ... 204
4.6.2 InetOrgPerson-Objekte ... 205
4.6.3 Kontaktobjekte ... 206
4.6.4 Gruppenobjekte ... 206
Gruppentypen ... 207
Konvertierung von Gruppen ... 207
Gruppenbereiche ... 207
Delegierung der Verwaltung der Gruppenmitgliedschaft ... 209

Active Directory-Standardgruppen ... 209
4.6.5 Planungsstrategien für Gruppen ... 214
Die "A-G-DL-P"-Regel ... 214
Die „A-G-G-DL-P"-Regel ... 215
Die „A-G-U-DL-P"-Regel ... 215
Die „A-G-L-P"-Regel ... 216
Die „A-G-P"-Regel ... 217
Verwendung neuer oder vorhandener Gruppen? ... 217
4.6.6 Besondere Identitäten ... 217
4.6.7 Computerobjekte ... 218
Sicherheit durch Kennwortvereinbarung ... 218
Zurücksetzen von Computerkonten ... 219
Standardcontainer für Computerobjekte ... 219
Speicherung von Computerobjekten ... 220
4.6.8 Druckerobjekte ... 220
Gruppenrichtlinien für die Druckerkonfiguration ... 222
Druckerstandorte ... 222
4.6.9 Freigegebene Ordner-Objekte ... 222
4.7 Zusammenfassung ... 222
5 Aktualisieren vorhandener Gesamt- und Domänenstrukturen ... 223
5.1 Planen der Aktualisierungspfade ... 223
5.1.1 Unterstützte Aktualisierungspfade zu Windows Server 2012 R2 ... 224
5.1.2 Unterstützte Aktualisierungspfade zu Windows Server 2012 ... 225
5.2 Planen der Domänen- und Gesamtstrukturfunktionsebene ... 226
5.2.1 Vergleich der Domänen- und Gesamtstrukturfunktionsebenen ... 226
5.2.2 Mitgliedsserver und Clientcomputer ... 230
Windows 8/8.1 und Windows 10 als Clientbetriebssystem ... 231
5.3 Der Aktualisierungsvorgang ... 231
5.3.1 Aktualisierung des Betriebssystems der Domänencontroller ... 232
5.3.2 Domänenaktualisierung durch das Hinzufügen von Windows Server 2012 R2 bzw. Windows Server 2012-Domänencontrollern ... 233
5.3.3 Vorbereitung der Active Directory-Umgebung ... 233
Vorbereitung der Active Directory-Gesamtstruktur ... 234
Vorbereitung der Active Directory-Domäne ... 235
Vorbereitung der Domänen für den Einsatz eines RODCs ... 235

Aktualisieren der Berechtigungen für DNS-Anwendungsverzeichnispartitionen mittels adprep.exe ... 236
5.4 Zusammenfassung ... 237
6 Migration von Gesamtstrukturen und Domänen ... 237
6.1 Mögliche Migrationspfade ... 238
6.1.1 Neustrukturierung ... 238
SID-History und der Zugriff auf Ressourcen ... 240
6.2 Gesamtstrukturübergreifende Migration ... 240
6.2.1 Einrichtung der neuen Gesamtstruktur ... 241
6.2.2 Erstellen von Benutzerkonten für den Migrationsvorgang ... 241
6.2.3 Einrichtung von Vertrauensstellungen ... 242
6.2.4 Installation des Active Directory Migration Tools (ADMT) ... 242
Mögliche Migrationsschritte mit ADMT ... 243
Migration von Benutzerkontenkennwörtern ... 244
6.2.5 Aktivierung der Überwachung in der Quell- und Zieldomäne ... 244
6.2.6 Migration der Gruppen ... 245
6.2.7 Migration der Benutzerkonten ... 247
Migration von Benutzerkonten in der Praxis ... 248
6.2.8 Migration der Computerkonten ... 248
6.2.9 Migration der Dienstkonten ... 250
6.2.10 Migration der Domänenressourcen der Quell- zur Zieldomäne ... 251
6.2.11 Auflösung der alten Gesamtstruktur ... 251
6.3 Gesamtstrukturinterne Migration ... 251
6.3.1 Wichtiger Unterschied zur gesamtstrukturübergreifenden Migration ... 252
6.4 Alternative zur Migration: Gesamtstrukturvertrauensstellungen ... 252
6.4.1 Vor- und Nachteile ... 253
6.4.2 Einrichtung von Gesamtstrukturvertrauensstellungen ... 254
6.5 Zusammenfassung ... 255
Teil 3: Implementierung, Verwaltung und Wartung ... 257
7 Installation und Konfiguration von Windows Server 2012 R2 ... 259
7.1 Neuinstallation oder Aktualisierung? ... 259
7.2 Neuinstallation von Windows Server 2012 R2 ... 259
7.2.1 Voraussetzungen ... 260
Hardwareanforderungen ... 260
7.2.2 Bestimmen der zu verwendenden Betriebssystemedition ... 261

Verfügbare Betriebssystemeditionen ... 261
Enthaltene Virtualisierungsrechte ... 262
Erweiterbarkeit der Virtualisierungsrechte ... 263
Spätere Aktualisierung von Standard- auf Datacenter-Lizenz ... 263
Spätere Aktualisierung von Essentials- auf Standard-Lizenz ... 264
7.2.3 Digital signierte Treiber erforderlich ... 264
7.2.4 Schritte zur Vorbereitung der Installation ... 265
7.2.5 Installationsschritte ... 266
7.2.6 Unbeaufsichtigte Installation ... 271
7.3 Konfigurationsschritte nach der Installation ... 271
7.3.1 Systemeigenschaften im Server-Manager ... 271
7.3.2 Schritte zur Konfiguration der Systemeigenschaften ... 273
7.4 Aktivierung des Betriebssystems ... 273
7.4.1 Produktaktivierung oder „Volume Activation" ... 274
Volumenaktivierung (Volume Activation) ... 274
7.4.2 Aktivierung über Active Directory ... 275
7.4.3 (Einzel-)Produktaktivierung ... 276
Aktivierung über das Internet ... 276
Telefonische Aktivierung ... 277
Aktivierung über die Kommandozeile ... 278
7.4.4 Erneute Aktivierung? ... 278
7.5 Aktualisierung vorhandener Serversysteme ... 278
7.5.1 Unterstützte Aktualisierungspfade ... 279
7.5.2 Notwendige Schritte vor der Aktualisierung ... 280
7.5.3 Digital signierte Treiber erforderlich ... 282
7.5.4 Vorbereitung der Active Directory-Umgebung ... 283
Vorbereitung der Active Directory-Gesamtstruktur (forestprep) ... 284
Vorbereitung der Active Directory-Domäne (domainprep) ... 284
7.5.5 Durchführung der Serveraktualisierung ... 284
7.5.6 Überprüfung der erfolgreichen Aktualisierung ... 291
7.6 Zusammenfassung ... 292
8 Implementierung und Verwaltung von Domain Name System (DNS) ... 292
8.1 Installation der DNS-Serverrolle ... 293
8.1.2 Installationsschritte ... 294
8.2 DNS-Namenszonen ... 295

8.2.1 Zonentypen ... 295
8.2.2 Forward-Lookup-Zonen ... 296
8.2.3 Reverse-Lookup-Zonen ... 296
8.3 Standardzonen ... 296
8.3.1 Primäre Standardzonen ... 297
8.3.2 Sekundäre Standardzonen ... 297
8.3.3 Erstellen von primären DNS-Namenszonen ... 297
8.3.4 Erstellen von sekundären DNS-Namenszonen ... 298
8.3.5 Umwandeln einer sekundären in eine primäre Namenszone ... 300
8.3.6 Active Directory-integrierte Zonen ... 300
8.3.7 Einrichten und Verwalten von Stub-Zonen ... 303
8.3.8 Einrichten und Verwalten von Reverse-Lookupzonen ... 305
8.4 Zonenübertragung ... 307
8.4.1 Konfiguration der Zonenübertragung ... 309
8.4.2 BIND-Sekundärzonen ... 310
8.4.3 Zonenreplikation im Vergleich zur Zonenübertragung ... 310
8.4.4 Speicherung von DNS-Namenszonen in Anwendungsverzeichnispartitionen ... 311
Erstellen einer Anwendungsverzeichnispartition ... 311
Speicherung von Zonendaten in einer Anwendungsverzeichnispartition ... 312
8.5 Verwalten von DNS-Einträgen ... 312
8.5.1 Manuelles Erstellen von DNS-Einträgen ... 313
8.5.2 Dynamische Aktualisierung ... 313
8.5.3 DNSUpdateProxy ... 314
8.5.4 Alterungs- und Aufräumprozess ... 315
Konfiguration des Alterungs- und Aufräumvorgangs für eine DNS-Namenszone ... 315
Aktivierung des automatischen Aufräumvorgangs bei veralteten Ressourceneinträgen ... 316
8.6 Manuelles Löschen von DNS-Einträgen ... 317
8.7 WINS-Forward-Lookup ... 317
8.8 Bedingte Weiterleitungen ... 318
8.9 Starten und Beenden des DNS-Dienstes ... 320
8.10 Entfernen von DNS-Namenszonen ... 320
8.11 Entfernen der DNS-Dienste ... 321
8.12 Zusammenfassung ... 322
9 Implementieren der Active Directory-Domänendienste (AD DS) ... 322

9.1 Installationsarten ... 323
9.2 Vorbereitende Schritte zur Installation ... 323
9.3 Installationsmethoden ... 324
9.3.1 Installation über den Server-Manager ... 324
Schritt 1: Installation der Serverrolle ... 324
Schritt 2: Heraufstufen des Servers zu einem Domänencontroller ... 326
9.3.2 Installation mithilfe der Windows PowerShell ... 330
9.3.3 Unbeaufsichtigte Installation ... 331
9.4 Überprüfung der erfolgreichen Installation ... 333
9.5 Installation von einem Medium ... 334
9.5.1 Erstellen eines Installationsmediums ... 334
Erstellen eines Installationsmediums mittels Ntdsutil.exe ... 334
Schritte zur Installation von einem Medium ... 336
9.6 Entfernen der Active Directory-Domänendienste ... 342
9.6.1 Vorbereitung des Herunterstufens eines Domänencontrollers ... 342
9.6.2 Herunterstufen eines Domänencontrollers ... 343
9.6.3 Entfernen der Active Directory-Domänendienste als Rolle ... 347
9.6.4 Entfernen der Active Directory-Domänendienste erzwingen ... 350
Auswirkungen nach dem erzwungenen Herabstufen eines Domänencontrollers ... 351
Bereinigung der Metadaten ... 352
9.6 Zusammenfassung ... 353
10 Verwaltung der Betriebsmasterrollen ... 354
10.1 Betriebsmasterrollen in einer Active Directory-Gesamtstruktur ... 354
10.1.1 Schemamaster ... 354
10.1.2 Domänennamenmaster ... 355
10.1.3 PDC-Emulator ... 356
10.1.4 RID-Master ... 357
10.1.5 Infrastrukturmaster ... 357
Infrastrukturmaster und der globale Katalog ... 358
10.2 Verschieben von Betriebsmasterrollen ... 359
10.2.1 Gründe für das Verschieben von Betriebsmasterrollen ... 359
10.2.2 Auswirkungen auf die Active Directory-Infrastruktur ... 359
Übergabe der Rollen beim Herunterstufen ... 359
10.2.3 Notwendige Berechtigungen ... 360
10.2.4 Ermitteln des Rolleninhabers der Betriebsmasterrollen ... 360

Ermitteln des Schemamaster-Rolleninhabers ... 361
Domänennamenmaster ... 363
PDC-Emulator ... 363
RID-Master ... 364
Infrastrukturmaster ... 364
10.2.5 Übertragen der Betriebsmasterrollen ... 364
Übertragung der Betriebsmasterrollen mittels Windows PowerShell ... 365
Schemamaster ... 366
Domänennamenmaster ... 367
PDC-Emulator, RID-Master und Infrastrukturmaster ... 367
10.3 Übernahme der Betriebsmasterrollen bei Ausfall des aktuellen Rolleninhabers . 368
10.3.1 Gründe für die Übernahme der Betriebsmasterrollen ... 369
10.3.2 Mögliche Auswirkungen des Ausfalls ... 370
10.3.3 Übernehmen der Betriebsmasterrollen ... 371
Übernahme der Betriebsmasterrollen mittels Windows PowerShell erzwingen ... 371
Übernahme der Betriebsmasterrollen mittels ntdsutil.exe erzwingen ... 372
10.4 Zusammenfassung ... 372
11 Verwaltung globaler Katalogserver ... 373
11.1 Funktionen des globalen Katalogservers ... 373
11.2 Ausfall eines globalen Katalogservers ... 374
11.3 Zuweisen der Funktion als globaler Katalogserver ... 374
11.4 Anpassen des globalen Katalogs ... 376
11.5 Zwischenspeichern der universellen Gruppenmitgliedschaft ... 379
11.6 Zusammenfassung ... 380
12 Erstellen und Verwalten von Organisationseinheiten ... 381
12.1 Planen und Erstellen von Organisationseinheiten ... 381
12.2 Werkzeuge zum Erstellen und Verwalten von Organisationseinheiten ... 382
12.3 Erstellen von Organisationseinheiten ... 383
12.3.1 Erstellen im Active Directory-Verwaltungscenter ... 383
12.3.2 Erstellen mittels MMC-Snap-In ... 384
12.3.3 Organisationseinheit erstellen mit dsadd.exe ... 384
12.3.4 Erstellen mittels Ldifde.exe ... 386
12.3.5 Verwenden der Eingabedatei mit Ldifde.exe ... 387
12.3.6 Erstellen mittels Windows Script Host ... 388
12.3.7 Erstellen mittels Windows PowerShell ... 389

12.4 Löschen von Organisationseinheiten 390
12.4.1 Löschen im Active Directory-Verwaltungscenter 390
12.4.2 Löschen mittels MMC-Snap-In 391
12.4.3 Löschen mittels von dsrm.exe 392
12.4.4 Löschen mittels Windows PowerShell 393
12.5 Verwaltung der Attributwerte von Organisa-tionseinheiten 393
12.6 Zusammenfassung 395
13 Delegierung der Verwaltungsfunktionalität 395
13.1 Schritte zur Delegierung der Verwaltungsberechtigung 396
13.2 Vererbung der Verwaltungsberechtigung 397
13.2.1 Blockieren der Vererbung der Verwaltungsberechtigung 397
Schritte zum Blockieren der Vererbung 397
13.3 Überprüfen der Delegierung der Verwaltungsberechtigung 398
13.3.1 Effektive Berechtigungen 399
13.4 Beendigung der Delegierung der Verwaltungsberechtigung 400
13.5 Bereitstellen angepasster Verwaltungskonsolen 400
13.5.1 Erstellen einer angepassten Verwaltungskonsole 401
13.6 Zusammenfassung 403
14 Erstellen und Verwalten von Active Directory-Objekten 404
14.1 Benutzerobjekte 404
14.1.1 Tools zum Erstellen und Verwalten von Benutzerobjekten 404
14.1.2 Erstellen von Benutzerobjekten mittels MMC-Snap-In 406
14.1.3 Erstellen von Benutzerobjekten im grafischen Active Directory-Verwaltungscenter (AD AD) 406
14.1.4 Erstellen von Benutzerobjekten mittels dsadd.exe 408
14.1.5 Erstellen von Benutzerobjekten mittels csvde.exe 409
Die Eingabedatei 409
Befehlsausführung 410
Nachteil bei der Verwendung von csvde.exe 410
14.1.6 Erstellen von Benutzerobjekten mittels ldifde.exe 411
Die Eingabedatei 411
Befehlsausführung 412
Nachteil bei der Verwendung von ldifde.exe 412
14.1.7 Erstellen von Benutzerobjekten mit net user 413
14.1.8 Erstellen von Benutzerobjekten mittels Windows Script Host (WSH) 413

Die Scriptdatei ... 413
Ausführung von WSH-Scripts ... 414
14.1.9 Erstellen von Benutzerobjekten mittels Windows PowerShell ... 415
14.2 Kontingente in Active Directory ... 415
14.2.1 Einrichtung und Verwaltung ... 416
14.2.2 Erstellen eines neuen Kontingenteintrags ... 416
14.2.3 Anzeige aller vorhandenen Kontingenteinträge ... 417
Ermitteln der Besitzer der meisten Active Directory-Objekte ... 417
14.2.4 Ändern vorhandener Kontingenteinträge ... 417
14.2.5 Löschen von Kontingenteinträgen ... 418
14.3 Verwalten von Benutzerobjekten ... 418
14.3.1 Attribut-Editor ... 418
14.3.2 Kopieren von Benutzerkonten ... 419
Pfadangaben in Benutzerkontenvorlagen ... 420
Empfehlungen für das Erstellen und Verwenden von Benutzerkontenvorlagen ... 420
14.3.3 Entsperren von Benutzerkonten ... 421
14.3.4 Zurücksetzen der Benutzerkontenkennwörter ... 422
14.3.5 Deaktivieren bzw. Aktivieren von Benutzerkonten ... 424
14.3.6 Löschen von Benutzerkonten ... 425
Schutz vor versehentlichem Löschen ... 425
14.4 Benutzerprofile und Basisverzeichnisse ... 426
14.5 Dienstkonten ... 427
14.5.1 Standardmäßig vorhandene Dienstkonten ... 427
14.5.2 Gruppenverwaltete Dienstkonten (Group Managed Service Accounts, gMSA) 428
Vorbereitung für den Einsatz gruppenverwalteter Dienstkonten (gMSA) ... 428
Speicherort gruppenveralteter Dienstkonten ... 429
Erstellen gruppenverwalteter Dienstkonten ... 429
Schritte zur Verwendung gruppenverwalteter Dienstkonten ... 430
Grafische Verwaltung mittels Managed Service Accounts GUI ... 431
14.6 InetOrgPerson-Objekte ... 431
14.8 Gruppenobjekte ... 432
14.8.1 Gruppentypen ... 433
14.8.2 Gruppenbereiche ... 433
14.8.3 Vordefinierte Gruppen ... 434
Standardgruppen im Builtin-Container ... 435

Standardgruppen im Users-Container ... 437
14.8.4 Gruppenstrategien ... 438
14.8.5 Erstellen und Verwalten von Gruppenobjekten ... 441
Erstellen von Gruppenobjekten mittels MMC-Snap-In ... 442
Erstellen von Gruppenobjekten im grafischen Active Directory-Verwaltungscenter (AD AC) ... 443
Erstellen von Gruppenobjekten mittels dsadd.exe ... 443
Erstellen von Gruppenobjekten mit der Windows PowerShell ... 444
14.9 Computerobjekte ... 445
14.9.1 Erstellen von Computerobjekten ... 445
Erstellen von Computerobjekten mittels MMC-Snap-In ... 446
Erstellen von Computerobjekten mittels Windows PowerShell ... 447
Erstellen von Computerobjekten mittels net computer ... 447
14.9.2 Berechtigung zum Hinzufügen von Arbeitsstationen zur Domäne ... 449
14.9.3 Verwalten von Computerobjekten ... 449
14.10 Verwaltung von Druckerobjekten ... 452
14.11 Veröffentlichung von freigegebenen Ordnern ... 454
14.12 Suche nach Objekten ... 457
14.12.1 Gespeicherte Abfragen ... 457
14.13 Zusammenfassung ... 459
15 Erstellen und Verwalten von Gruppenrichtlinienobjekten ... 459
15.1 Einführung und Funktionsweise ... 460
15.1.1 Konfigurierbare Einstellungen ... 461
15.1.2 Speicherorte von Gruppenrichtlinienobjekten ... 462
15.1.3 Komponenten der Gruppenrichtlinienvorlagen ... 464
15.1.4 Neuerungen in Windows Server 2012 R2 ... 465
15.1.5 Die Richtlinienverarbeitungsfolge ... 466
15.1.6 Die Gruppenrichtlinienverarbeitung ... 468
15.2 Der Gruppenrichtlinienaktualisierungsprozess ... 470
15.2.1 Dynamische Aktualisierung ... 470
15.2.2 Manuelle Aktualisierung ... 475
Gruppenrichtlinienupdate - aus der grafischen Konsole ... 475
15.3 Loopbackverarbeitungsmodus ... 477
15.4 Die Gruppenrichtlinienverwaltungskonsole (GPMC) ... 479
15.4.1 Verwaltungsmöglichkeiten ... 479

15.4.2 Installation der Gruppenrichtlinienverwaltungskonsole (GPMC) 480
15.5 Arbeiten mit Gruppenrichtlinienobjekten 482
15.5.1 Erstellen eines neuen Gruppenrichtlinienobjekts 482
15.5.2 Bearbeiten von Gruppenrichtlinienobjekten 483
15.5.3 Löschen von Gruppenrichtlinienobjekten 484
15.5.4 Wiederherstellen der Standardrichtlinienobjekte 485
15.6 Starter-Gruppenrichtlinienobjekte 486
15.6.1 Einrichten des Speicherorts für Starter-Gruppenrichtlinienobjekte 486
15.6.2 Erstellen von Starter-Gruppenrichtlinienobjekten 487
15.6.3 Bearbeiten eines Starter-Gruppenrichtlinienobjekts 488
15.6.4 Löschen eines Starter-Gruppenrichtlinienobjekts 489
15.6.5 Exportieren und Importieren von Starter-Gruppenrichtlinienobjekten 489
15.6.6 Erstellen eines neuen Gruppenrichtlinienobjekts aus einem Starter-Gruppenrichtlinienobjekt 491
15.7 Verknüpfen von Gruppenrichtlinienobjekten 493
15.7.1 Erstellen der Verknüpfung eines Gruppenrichtlinienobjekts mit einer Organisationseinheit (OU) 493
15.7.2 Löschen der Verknüpfung eines Gruppenrichtlinien-objekts 494
15.7.3 Deaktivieren einer Gruppenrichtlinienverknüpfung 495
15.7.4 Festlegen der Verknüpfungsreihenfolge 496
15.8 Gruppenrichtlinienvererbung 497
15.8.1 Vererbung deaktivieren 498
15.8.2 Erzwingen von Gruppenrichtlinien 499
15.9 Filterung von Gruppenrichtlinienobjekten 500
15.9.1 Die Sicherheitsfilterung 500
15.9.2 Die WMI-Filterung 502
15.10 Delegieren der Gruppenrichtlinienverwaltung 507
15.10.1 Delegierungsumfang 507
15.10.2 Delegierungsmöglichkeiten 507
15.10.3 Berichterstellung und Auswertung 510
15.10.4 Gruppenrichtlinien dokumentieren 520
15.10.5 Sichern und Wiederherstellen von Gruppenrichtlinienobjekten 522
15.11 Zusammenfassung 525
16 Verwaltung der Benutzerumgebung mit Gruppenrichtlinienobjekten 526

16.1 Konfigurieren der Gruppenrichtlinieneinstellungen ... 527
16.1.1 Konfiguration von Einzelwerten ... 527
16.1.2 Konfiguration von Mehrfachwerten ... 528
16.2 Die Erweiterungen für Gruppenrichtlinienvoreinstellungen ... 529
16.2.1 Windows-Einstellungen ... 530
16.2.2 Systemsteuerungseinstellungen ... 530
16.2.3 Beispiel für die Anwendung von Windows-Einstellungen ... 532
16.2.4 Zielgruppenadressierung ... 534
16.3 Bereitstellen und Anwenden von Skripts mithilfe von Gruppenrichtlinien ... 537
16.3.1 Beispiel für ein Anmeldeskript ... 538
16.3.2 Anwenden eines Anmeldeskripts ... 539
16.3.3 Speicherorte von Skriptdateien ... 540
16.3.4 Überlegungen zur Planung von Skriptdateien ... 540
16.4 Konfigurieren der Ordnerumleitung ... 541
16.4.1 Vorteile der Orderumleitung ... 542
16.4.2 Umleitbare Ordner ... 543
16.4.3 Zieldefinition der Ordnerumleitung ... 544
16.4.4 Weitere, konfigurierbare Einstellungen ... 545
16.4.5 Sicherheitsaspekte bei der Orderumleitung ... 547
16.4.6 Beispiele für die Konfiguration der Ordnerumleitung ... 548
16.5 Konfigurieren der Benutzerumgebung ... 549
16.5.1 Administrative Vorlagen ... 550
Administrative Vorlagen als XML-Dateien ... 551
Speicherort von .ADMX-Vorlagen ... 551
Verbesserungen bei der Verwendung von ADMX-Vorlagen ... 552
Hinzufügen von Gruppenrichtlinienvorlagen für Windows 10-Computer ... 553
Einrichten eines zentralen Speichers ... 554
16.5.2 Klassische administrative Vorlagen ... 555
Standardmäßige ADM-Vorlagen ... 556
Erstellen von eigenen administrativen Vorlagen (ADM-Dateien) ... 558
Konvertierung der klassischen administrativen Vorlagen ... 558
Hinzufügen oder Entfernen von klassischen administrativen Vorlagen ... 559
Filtern von administrativen Vorlagen ... 561
16.6 Zusammenfassung ... 564
17 Planung und Einsatz von Kennworteinstellungen ... 565

17.1 Funktionsweise ... 566
17.1.1 Auswertelogik ... 567
17.2 Schritte zum Erstellen von Objekten für Kennworteinstellungen ... 569
17.3 Anzeigen der auf einen Benutzer angewandten Kennworteinstellungen ... 569
17.4 SpecOps Password Policy Basic ... 571
17.5 Zusammenfassung ... 572
18 Schreibgeschützte Domänencontroller ... 572
18.1 Vorteile beim Einsatz von RODCs ... 573
18.2 Einschränkungen beim Einsatz von RODCs ... 574
18.3 Platzierung von RODCs ... 575
18.4 Bereitstellen schreibgeschützter Domänencontroller (RODCs) ... 575
18.4.1 Überprüfung der Gesamtstrukturfunktionsebene ... 576
18.4.2 Aktualisieren der Berechtigungen für DNS-Anwendungsverzeichnispartitionen ... 577
18.4.3 Installation eines RODC unter Windows Server 2012 R2 ... 578
Installationsschritte ... 578
Heraufstufen des Servers zu einem RODC ... 580
18.4.4 Delegierung der Installation von RODCs ... 585
18.4.5 Durchführung der delegierten RODC-Installation ... 588
18.5 Verwaltung schreibgeschützter Domänencontroller ... 592
18.5.1 Verwaltung der Kennwortreplikationsrichtlinie ... 592
Steuerung der Replikation von Kennwörtern ... 593
Attribute für die Steuerung der Kennwortreplikation ... 594
18.6 Konfigurieren der Kennwortreplikationsrichtlinie für einen RODC ... 595
18.7 Anzeige der auf einem RODC zwischengespeicherten Anmeldeinformationen ... 596
18.8 Überprüfung der für einen RODC authentifizierten Konten ... 597
18.9 Auffüllen des Kennwortcache für RODCs ... 598
18.9.1 Schritte zum Auffüllen des Kennwortcache ... 598
18.10 Überprüfen den Kennwortzwischenspeicherung für einzelne Benutzer ... 599
18.11 Zurücksetzen von zwischengespeichertern Kennwörtern ... 600
18.12 Konfiguration zur Aufteilung der Administratorrolle auf RODCs ... 601
18.13 Zusammenfassung ... 602
19 Domänencontroller unter Server Core ... 603
19.1 Hardware-Anforderungen ... 604

19.2 Schritte zur Vorbereitung der Installation 604
19.3 Installationsschritte 605
19.4 Unbeaufsichtigte Installation 608
19.4.1 Vorteile der unbeaufsichtigten Installation 608
19.5 Erstkonfiguration 609
19.5.1 Festlegen des Administratorkennworts 609
19.5.2 Konfiguration einer statischen IP-Adresse 610
Konfiguration mithilfe der Windows PowerShell 611
Konfiguration mithilfe von sconfig 613
Konfiguration mithilfe von netsh 614
19.5.3 Umbenennen des Servers 614
Ändern des Servernamens mithilfe der Windows PowerShell 615
Ändern des Servernamens mithilfe von sconfig 615
Ändern des Servernamens mithilfe von netdom 615
19.5.4 Beitreten zu einer Active Directory-Domäne 616
Beitritt zu einer Active Directory-Domäne mithilfe der Windows PowerShell 616
Beitritt zu einer Active Directory-Domäne mithilfe von sconfig 617
Beitritt zu einer Active Directory-Domäne mithilfe von netdom 617
19.5.5 Aktivieren von Windows Server 2012 R2 als Server Core 618
19.5.6 Remoteaktivierung 618
19.5.7 Konfigurieren der Remoteverwaltung 619
Remoteverwaltung mithilfe von sconfig konfigurieren 619
Remoteverwaltung der Firewall-Konfiguration 620
19.6 Hinzufügen der grafischen Benutzeroberfläche unter Server Core 620
19.6.1 Wechsel von der Server Core-Installation zu einer Serverinstallation mit grafischer Benutzeroberfläche 621
19.7 Entfernen der grafischen Benutzeroberfläche 623
19.8 Server Core als DNS-Server 624
19.8.1 Installation der DNS-Serverrolle 625
19.8.2 Verwaltung des Server Core als DNS-Server 625
Alternative Verwaltung mittels dnscmd.exe 626
Alternative Verwaltung mittels Windows PowerShell 626
19.8.3 Entfernen der DNS-Serverrolle 626
19.9 Server Core als Domänencontroller 627
19.9.1 Heraufstufen über den grafischen Server-Manager 627

19.9.2 Unbeaufsichtigte Installation der Active Directory-Domänendienste mittels dcpromo.exe ... 628
Beispiel für die Datei Unattend.txt ... 628
19.9.3 Heraufstufen über die Windows PowerShell ... 629
Installation der Serverrolle der Active Directory-Domänendienste (AD DS) mittels Windows PowerShell ... 629
Heraufstufen des Serversystems zu einem Active Directory-Domänencontroller mittels Windows PowerShell ... 629
19.10 Zusammenfassung ... 630
20 Verwaltung von Standorten und Replikation ... 631
20.1 Standorte und die Replikation ... 631
20.2 Erstellen eines Active Directory-Standorts ... 632
20.3 Erstellen eines Subnet-Objektes ... 632
20.4 Erstellen einer Standortverknüpfung ... 633
20.4.1 Hinzufügen eines Standorts zu einer Standortverknüpfung ... 634
20.4.2 Entfernen von Standorten aus einer Standortverknüpfung ... 635
20.5 Planen der Replikation zwischen Active Directory-Standorten ... 636
20.5.1 Notwendige Kommunikationsports für die Replikation ... 637
20.5.2 Replikationstransport ... 637
Konfiguration des Zeitplans für die standortübergreifende Replikation ... 638
Konfiguration der Häufigkeit der standortübergreifende Replikation ... 639
20.6 Überprüfung und Problembehandlung ... 639
20.6.1 Standortermittlung mit nltest.exe ... 640
20.6.2 Überprüfung der Replikation mit Repadmin.exe ... 640
20.6.3 Überprüfung der Replikation mit Dcdiag.exe ... 641
20.6.4 Überprüfung der Replikation mit Windows PowerShell ... 642
20.6.5 Überprüfung der Replikation mit dem AD Replication Status Tool ... 642
20.6.6 LDAP-Echtzeitüberwachung mit ADInsight ... 643
20.6.7 ADExplorer ... 643
20.6.8 Überprüfung des Ereignisprotokolls ... 643
20.7 Zusammenfassung ... 644
21 Wartung und Diagnose ... 645
21.1 Überwachung der Active Directory-Domänendienste ... 645
21.1.1 Überwachung und Diagnose mithilfe der Ereignisan-zeige ... 646
Zu überwachende Ereignisprotokolle ... 647

Ereignisdetails anzeigen ... 648
21.1.3 Überwachung mithilfe der Konsole Leistung ... 649
Hinzufügen von Indikatoren ... 650
21.1.4 Zuverlässigkeitsüberwachung ... 650
21.1.5 Sammlungssätze ... 651
21.2 Wartung der Active Directory-Domänendienste ... 653
21.2.1 Garbage Collection ... 653
21.2.2 Online- und Offline-Defragmentierung ... 654
Online-Defragmentierung ... 654
Offline-Defragmentierung ... 655
Integritätsprüfung der Active Directory-Datenbank ... 657
Semantik-Prüfung der Active Directory-Datenbank ... 657
Verschieben der AD-Datenbank und -Protokolldateien ... 658
21.3 Zusammenfassung ... 659
22 Sichern und Wiederherstellen der Active Directory-Domänendienste ... 660
22.1 Active Directory-Datensicherung ... 660
22.1.1 Unterstützte Sicherungstypen ... 660
22.1.2 Mögliche Wiederherstellungsarten ... 661
22.2 Installation der Windows Server-Sicherung ... 661
22.2.1 Datensicherung und Wiederherstellung mit der Windows PowerShell ... 662
22.3 Durchführung der Datensicherung ... 662
22.3.1 Vollständige Serversicherung eines Domänencontrollers ... 662
22.3.2 Ungeplante Sicherung wichtiger Volumes eines Domänencontrollers ... 663
22.4 Planen der täglichen Sicherung eines Domänencontrollers ... 663
22.4.1 Online-Sicherung ... 664
22.5 Durchführung der Datenwiederherstellung ... 665
22.5.1 Vollständige Serverwiederherstellung eines Domänencontrollers ... 665
Voraussetzungen für das Ausführen einer vollständigen Wiederherstellung eines Domänencontrollers ... 666
22.5.2 Active Directory aus der Datensicherung wiederherstellen ... 666
Ausführen einer nicht autorisierenden Wiederherstellung der Active Directory-Domänendienste (AD DS) ... 666
Vorgehensweise für die Durchführung einer nicht autorisierenden Wiederherstellung der Active Directory-Domänendienste (AD DS) ... 668
Ausführen einer autorisierenden Wiederherstellung gelöschter Active Directory-Objekte ... 673
22.5.3 Reanimieren von Tombstone-Objekten ... 675

Verwenden von Ldp.exe zum Reanimieren von Tombstone-Objekten 676
Verwenden von AdRestore.exe zum Reanimieren von Tombstone- Objekten 678
22.6 Active Directory-Papierkorb - jetzt grafisch 679
22.6.1 Schritte zum Aktivieren des Active Directory-Papierkorbs 680
Aktivierung des Active Directory-Papierkorbs mittels Windows Power-Shell 682
22.6.2 Anzeigen und Wiederherstellen gelöschter Active Directory-Objekte 682
Anzeigen und Wiederherstellen mittels Windows PowerShell 682
22.7 Installation der AD-Domänendienste (AD DS) von einer Sicherung 683
22.7.1 Verschiedene Installationsmedien 683
22.7.2 Erstellen eines Installationsmediums 684
22.7.3 Einrichten eines neuen Domänencontrollers mithilfe eines Installationsmediums 685
22.8 Zusammenfassung 685
23 Weitere Active Directory-Dienste 685
23.1 Die Dienste im Überblick 686
23.2.1 Active Directory Lightweight Directory Services (AD LDS) 686
23.2.2 Active Directory-Zertifikatdienste (AD CS) 687
23.2.3 Active Directory-Rechteverwaltungsdienste (AD RMS) 688
Rechtevergabe auf digitale Inhalte 688
23.2.4 Active Directory-Verbunddienste (AD FS) 689
Unterstützte Szenarien der AD FS 689
23.3 Zusammenfassung 689
Stichwortverzeichnis 691

Der Autor

Carlo Westbrook ist seit fast 30 Jahren u. a. als IT-Trainer, Senior Consultant sowie als Learning Consultant und Kursdesigner für technische Kurse & Workshops tätig. Als Fachautor publizierte er neben einer Vielzahl an Fachbüchern u. a. auch Fachbeiträge bei verschiedenen Verlagen.
Zu seinen Schwerpunkten zählen u.a. die Windows-Betriebssysteme, Active Directory, Exchange Server, Cloud-Dienste, die Microsoft System Center-Technologien und IT-Sicherheit.

Vorwort

Mit Windows Server 2012 R2 hat Microsoft wieder einmal einen Meilenstein in der Betriebssystementwicklung für Serversysteme geschaffen. Die darin enthaltenen Rollen und Funktionen wurden gegenüber den Vorversionen nicht nur optimiert, sondern gleich um eine Vielzahl weiterer, für die tägliche Praxis sicher notwendige Dienste und Funktionen erweitert. Mit Windows Server 2012 R2 orientierte sich Microsoft auch wieder direkt an der aktuellen Entwicklung in Richtung des „Cloud Computing". Das Betriebssystem lässt sich problemlos in Private, Public oder auch Hybrid-Cloud-Umgebungen betreiben. Die dazu mitunter notwendige Anbindung der Active Directory-Domänendienste an die Microsoft Cloud-Dienste im Internet, z. B. für die Verwendung von Office 365 oder Exchange Online, wird in den Online-Inhalten des Buches in einem Zusatzkapitel Schritt für Schritt erklärt. Problemlos lässt sich das neue Serverbetriebssystem aber auch parallel zu älteren Windows-Server-betriebssystemen, wie z. B. Windows Server 2012 oder auch Windows Server 2008 (R2) einsetzen, was in diesem Buch ebenso berücksichtigt wurde.

Da die Active Directory-Domänendienste für immer mehr der BackOffice-Produkte - nicht nur von Microsoft - die eigentliche „Basis" für die Authentifizierung und auch Autorisierung darstellen, ist es umso notwendiger, sich von Grunde auf bis ins Detail mit diesen zu befassen. Aus diesem Grund ist das Buch in insgesamt drei verschieden Abschnitte unterteilt. Der erste Teil des Buches beschreibt die wichtigsten Neuerungen in Windows Server 2012 R2 sowie auch in Windows Server 2012, und geht auf die Grundlagen und Funktionen der in Windows Server 2012 R2 unter Active Directory zusammengefassten Dienste und Funktionen ein. Im zweiten Teil des Buches werden dann die Konzepte für die erfolgreiche Planung der Bereitstellung von Windows Server 2012 R2 in neue und auch bereits existierende Unternehmensnetzwerke vorgestellt. Im dritten Teil finden Sie die notwendigen Schritte zur Bereitstellung, Konfiguration, Verwaltung und Wartung der Active Directory-Domänen-dienste mitsamt der darin enthaltenen Rollen und Funktionen.

Die Inhalte des Buches sind so verfasst, dass Einsteiger, aber auch Active Directory-Profis darin das notwendige Wissen rund um die Active Directory-Domänendienste unter Windows Server 2012 R2 finden.

An dieser Stelle möchte ich mich bei meiner Familie für ihre Unterstützung während der Zeit der Erstellung dieses Buches bedanken. Natürlich möchte ich mich auch bei Ihnen, liebe Leser, für den Kauf dieses Buches bedanken und wünsche Ihnen nun eine interessante Zeit beim Lesen.

Ihr Carlo Westbrook

Aufbau des Buches

Das Buch ist zur besseren Übersicht in insgesamt drei verschiedene Teile gegliedert. Die einzelnen Teile unterscheiden sich in ihrer inhaltlichen Ausrichtung, bauen fachlich jedoch aufeinander auf. Insgesamt finden Sie in diesem Buch die folgenden Teile:

Teil 1 - Einführung und Grundlagen

Teil 2 - Planung, Aktualisierung und Migration

Teil 3 - Bereitstellung, Verwaltung und Wartung

Konventionen und Symbole

Um bestimmten Textpassagen dieses Buches etwas hervorzuheben, habe ich die folgenden typografischen Konventionen und Symbole verwendet:

Konvention	Bedeutung
`befehl`	Stellt die Befehlssyntax oder auch Befehlsausführung von Kommandozeilen- oder Windows PowerShell-Befehlen dar.
Weiter	Kennzeichnet die Ausführung einer bestimmten Programmfunktion, beispielsweise den Mausklick auf eine Schaltfläche.
HINWEIS	Weist auf einen allgemeinen Hinweis zu bestimmten Themenbereichen hin.
WICHTIG!	Gibt einen Hinweis auf wichtige Funktionen oder auch Situationen, die unbedingt beachtet werden sollten.
VORSICHT!	Kennzeichnet Informationen oder auch Situationen, die ein Risiko oder eine Bedrohung darstellen können.
PRAXISTIPP!	Kennzeichnet Tipps für die praktische Anwendung bzw. Umsetzung.
INTERNET	Weist auf weitere Informationsquellen zu bestimmten Themenbereichen im Internet hin.

Teil 1

Einführung und Grundlagen

Die drei Kapitel im Teil 1 dieses Buches sind nicht nur für Einsteiger von Interesse. Auch geschulte Administratoren finden hier ebenso bereits wertvolle Informationen, um die Active Directory-Domänendienste unter Windows Server 2012 R2 oder unter Windows Server 2012 effizient zu planen, einzusetzen und zu betreiben.

Nach der Einführung in die Neuerungen rund um Windows Server 2012 R2 im ersten Kapitel erhalten Sie anschließend einen einführenden Überblick über die Protokolle, Dienste und Komponenten der Active Directory-Domänendienste sowie deren Funktionsweise.

Das letzte der drei Kapitel in diesem Abschnitt gibt letztlich einen Überblick über die konfigurierbare Sicherheit in den Umgebungen der Active Directory-Domänendienste.

Dieser erste Teil dieses Buches unterteilt sich in die folgenden Kapitel:

- **Kapitel 1 – Einführung in Windows Server 2012 (R2)** Lernen Sie die Neuerungen und Verbesserungen rund um Windows Server 2012 R2 und Windows Server 2012 kennen. (*ab Seite 33*)
- **Kapitel 2 – Funktionsweise und Beschreibung des Active Directory** Neben der Einführung in Active Directory werden die Komponenten, Protokolle und Dienste der Active Directory-Domänendienste unter Windows Server 2012 (R2) sowie auch die Funktionsweisen der einzelnen Komponenten vorgestellt. (*ab Seite 51*)

- **Kapitel 3 – Sicherheit in Umgebungen der Active Directory-Domänendienste** Dieses Kapitel beschreibt die grundsätzlichen Sicherheitsfunktionen, den Authentifizierungsvorgang mitsamt der dafür konfigurierbaren Sicherheitsebenen, die Domänencontrollersicherheit sowie auch die Möglichkeit der Überwachungsmöglichkeiten der Active Directory-Domänendienste. (*ab Seite 123*)

1 Einführung in Windows Server 2012 R2

Microsoft hat wieder sehr viel Fleiß in die Entwicklung des Windows Server 2012 R2 (Release 2) gesteckt. Dies zeigt sich in den vielen Verbesserungen und Ergänzungen, die in das Betriebssystem eingeflossen sind. Insbesondere fallen diese Änderungen im direkten Vergleich zu Windows Server 2008 R2 auf, denn zum direkten Vorgänger, dem Windows Server 2012 hingegen fallen diese eher marginal aus. Einige der Neuerungen und Verbesserungen nimmt man jedoch erst wahr, wenn man sich intensiver mit dem neuen Betriebssystem befasst. Gleich noch mit Windows Server 2012 hatte Microsoft jedoch bereits das Angebot der dazu verfügbaren Editionen im Vergleich mit älteren Windows-Serverbetriebssystemen verändert.

1.1 Verfügbare Editionen

Anders als noch bei Windows Server 2008 R2 hat Microsoft, beginnend bereits mit Windows Server 2012, lediglich noch vier direkte, unterschiedliche Betriebssystemeditionen von Windows Server 2012 R2 veröffentlicht. Die zuvor zum Beispiel noch erhältliche *Enterprise Edition* existiert nicht mehr. Die Editionen von Windows Server 2012 R2 richten sich in erster Linie nach der Größe des Unternehmens, sowie nach dem möglichen Bedarf an Virtualisierung und Cloud Computing.

Windows Server 2012 R2 wird von Microsoft in den folgenden Editionen angeboten:

Edition	Einsatzbereich	Enthaltene Funktionen
Datacenter	Große virtualisierte Private- und Hybrid-Cloud-Umgebungen	Vollständige Windows Server-Funktionalität
Standard	Unternehmensweiter Einsatz in kleinen, mittleren und großen Unternehmen, Behörden und Institutionen	Vollständige Windows Server-Funktionalität
Essentials	Kleine und mittlere Unternehmen	Eingeschränkte Windows Server-Funktionalität, unterstützt maximal 25 Benutzer und 50 Geräte.
Foundation	Einstiegsserver für kleine Unternehmen, Kanzleien und Freiberufler	Grundlegende Windows Server-Funktionalität, unterstützt bis zu 15 Benutzer.

Tabelle 1.1: *Verfügbare Editionen von Windows Server 2012 R2*

HINWEIS: Die Windows Server 2012 R2 Essentials Edition wird von Microsoft als der Nachfolger des Microsoft Small Business Server 2011 Standard/Essentials angeboten, und ist für die Verwendung Cloud-basierter Dienste konzipiert. Im Vergleich zum SBS 2011 enthält die Essentials Edition jedoch die zuvor noch im Umfang enthaltenen Exchange- und SQL-Server-Funktionalitäten nicht mehr. Diese Produkte müssen – alternativ zur Nutzung der von Microsoft angebotenen Cloud-basierten Dienste – bei Bedarf nunmehr zusätzlich beschafft und lizenziert werden.

Seitens der im Umfang enthaltenen Serverrollen und -funktionen gibt es unter Windows Server 2012 R2 keinen Unterschied zwischen der Standard Edition zur Datacenter Edition. So unterstützt selbst die Standard Edition u. a. auch das Failover-Clustering. Lediglich in den Virtualisierungsrechten unterscheiden sich die beiden Betriebssystem-Editionen. Im Vergleich dazu fehlen in Windows Server 2012 R2 Essentials unter anderem die Virtualisierungsunterstützung mit Hyper-V oder auch die Active Directory-Verbunddienste (engl. *Active Directory Federation Services, AD FS*). Der Windows Server 2012 R2 Foundation ist als „Einstiegsserver" noch weiter eingeschränkt und lediglich als OEM-Version (*Original Equipment Manufacture*) verfügbar.

1.2 Unterstützte Serverrollen und -funktionen

Windows Server 2012 R2 enthält eine Vielzahl der in den Computernetzwerken von Unternehmen notwendigen Serverrollen und -funktionen. Der jeweilige Umfang unterscheidet sich dabei zwischen den jeweiligen Betriebssystem-Editionen von Windows Server 2012 R2, und wird Ihnen in den nachfolgenden Tabellen verdeutlicht.

1.2.1 Unterstützte Serverrollen

Die folgende Tabelle enthält eine Übersicht über die in den verschiedenen Editionen von Windows Server 2012 R2 enthaltenen Serverrollen:

Unterstützte Serverrolle	Foundation	Essentials	Standard	Datacenter
Active Directory Lightweight Directory Services (AD LDS)	●	●	●	●
Active Directory-Domänendienste (AD DS)	● (max. 15 Benutzer)	● (max. 25 Benutzer und 50 Geräte)	●	●
Active Directory-Rechteverwaltungsdienste (AD RMS)	●	●	●	●

Unterstützte Serverrolle	Foundation	Essentials	Standard	Datacenter
Active Directory-Verbunddienste (AD FS)	●	●	●	●
Active Directory-Zertifikatdienste (AD CS)	●	●	●	●
Anwendungsserver	●	●	●	●
Datei- und Speicherdienste	●	●	●	●
DHCP-Server	●	●	●	●
DNS-Server	●	●	●	●
Druck- und Dokumentdienste	●	●	●	●
Faxserver	●	●	●	●
Hyper-V			●	●
Netzwerkrichtlinien- und Zugriffsdienste	●	●	●	●
Remotedesktopdienste	●	●	●	●
Remotezugriff	●	●	●	●
Volumenaktivierungsdienste	●	●	●	●
Webserver (IIS)	●	●	●	●
Windows Server Essentials-Umgebung			●	●
Windows Server Update Services (WSUS)			●	●
Windows-Bereitstellungsdienste (WDS)	●	●	●	●

Tabelle 1.2: *Unterstützte Serverrollen in den verschiedenen Editionen von Windows Server 2012 R2*

1.2.1 Unterstützte Features (Funktionen)

Die folgende Tabelle enthält eine Übersicht der in den verschiedenen Editionen von Windows Server 2012 R2 enthaltenen Features (Funktionen):

Unterstützte Features (Funktionen)	Foundation	Essentials	Standard	Datacenter
.NET Framework 3.5-Funktionen	●	●	●	●
.NET Framework 4.5-Funktionen	●	●	●	●
Benutzer-oberfläche und Infrastruktur	●	●	●	●
BitLocker-Laufwerks-verschlüsselung	●	●	●	●
BitLocker-Netzwerk-entsperrung	●	●	●	●
BranchCache	●	●	●	●
Client für NFS	●	●	●	●
Data Center Bridging	●	●	●	●
Einfache TCP/IP-Dienste	●	●	●	●
Erweitertes Speichern	●	●	●	●
Failoverclustering			● (max. 64 Knoten)	● (max. 64 Knoten)
Freihand- und Handschriftdienst	●	●	●	●
Gruppenricht-linienverwaltung	●	●	●	●
Hostfähiger Webkern für	●	●	●	●

Unterstützte Features (Funktionen)	Foundation	Essentials	Standard	Datacenter
Internetinformationsdienste				
IIS-Erweiterungen für OData Services for Management	●	●	●	●
Intelligenter Hintergrundübertragungsdienst (Background Intelligent Transfer Service, BITS)	●	●	●	●
Interne Windows-Datenbank	●	●	●	●
Internetdruckdienstclient	●	●	●	●
IP-Adressverwaltungsserver (IPAM-Server)	●	●	●	●
iSNS-Serverdienst	●	●	●	●
LPR-Portmonitor	●	●	●	●
Media Foundation	●	●	●	●
Message Queuing	●	●	●	●
Multipath-E/A	●	●	●	●
Netzwerklastenausgleich	●	●	●	●
Peer Name Resolution-Protokoll	●	●	●	●
RAS-Verbindungs-Manager-Verwaltungskit (CMAK)	●	●	●	●
Remotedifferenzialkomprimierung	●	●	●	●
Remoteserver-Verwaltungstools	●	●	●	●
Remoteunterstützung	●	●	●	●

Unterstützte Features (Funktionen)	Foundation	Essentials	Standard	Datacenter
RPC-über-HTTP-Proxy	•	•	•	•
SMB-Bandwith Limit			•	•
SMTP-Server	•	•	•	•
SNMP-Dienst	•	•	•	•
Standardbasierte Windows-Speicherverwaltung	•	•	•	•
Telnet-Client	•	•	•	•
Telnet-Server	•	•	•	•
TFTP-Client	•	•	•	•
Unterstützung für die SMB 1.0/CIFS-Dateifreigabe (nur *OPTIONAL* - standardmäßig deakt.)	(•)	(•)	(•)	(•)
Verbesserte Windows-Audio-/Video-Streaming	•	•	•	•
Windows Identity Foundation 3.5	•	•	•	•
Windows PowerShell	•	•	•	•
Windows Search	•	•	•	•
Windows Server-Migrationstools	•	•	•	•
Windows Server-Sicherung	•	•	•	•
Windows-Biometrieframework	•	•	•	•
Windows-Feedbackweiterleitung	•	•	•	•
Windows-Prozessaktivierungsdienst	•	•	•	•

Unterstützte Features (Funktionen)	Foundation	Essentials	Standard	Datacenter
Windows-TIFF-IFilter	•	•	•	•
WinRM-IIS-Erweiterungen	•	•	•	•
WINS-Server	•	•	•	•
WLAN-Dienst	•	•	•	•
WoW64-Unterstützung	•	•	•	•
XPS-Viewer	•	•	•	•

Tabelle 1.3: *Unterstützte Features in den verschiedenen Editionen von Windows Server 2012 R2*

WICHTIG! Wie in der oberen Tabelle zu ersehen ist, unterstützt Windows Server 2012 R2 *SMB 1.0-Freigaben* lediglich noch *optional*. Bei Bedarf kann man diese Unterstützung in der Windows-Registry des Serverbetriebssystems aktivieren.

Darüber hinaus wurden der *Windows System Ressourcen-Manager (WSRM)*, sowie auch die *Windows Services for Unix (Unterstüzung POSIX-kompatibler Anwendungen)* vollständig aus dem Umfang von Windows Server 2012 R2 entfernt.

1.3 Neuerungen und Verbesserungen

Im Vergleich zu Windows Server 2008 R2 hat Microsoft in Windows Server 2012, sowie auch in Windows Server 2012 R2 (Release 2) wiederum eine Vielzahl an Neuerungen und auch Verbesserungen eingearbeitet. Die Verwaltung der neuen Serverbetriebssysteme wurde an die Anforderungen in modernen Computernetzwerken angepasst und verbessert. Die Möglichkeit der zentralen Verwaltung von Serversystemen stand insbesondere bei der Entwicklung und Optimierung des Server-Managers sicher bedeutend im Fokus. Microsoft hat auch viele der zuvor bereits vorhandenen Serverrollen und -funktionen vielfach überarbeitet und optimiert. Viele der Neuerungen und Verbesserungen werden Ihnen in den nächsten Seiten dieses Fachbuches vorgestellt.

1.3.1 Der Anmeldebildschirm

Nach der Installation von Windows Server 2012 R2 (Release 2) fällt auf, dass Microsoft mögliche Neuerungen nicht nur innerhalb des Serverbetriebssystems eingearbeitet hat. Auch der *Startbildschirm* zeigt sich in neuem Gewand. Deutlich sichtbar ist dabei die Anzeige für Datum und Uhrzeit.

Nach dem gleichzeitigen Drücken der Tasten **Strg**, **Alt** und **Entf** sich dann der überarbeitete Anmeldebildschirm. Wenn man Zeichen in das darin enthaltene Kennwortfeld eingegeben hat, so kann man dies durch einen Klick auf das daneben enthaltene Symbol kontrollieren. Solange man die Maustaste gedrückt hält, werden die in das Kennwortfeld eingegebenen Zeichen im Klartext angezeigt. Hierdurch lässt sich problemlos feststellen, ob man sich bei der Eingabe des Benutzerkennworts womöglich vertan hat.

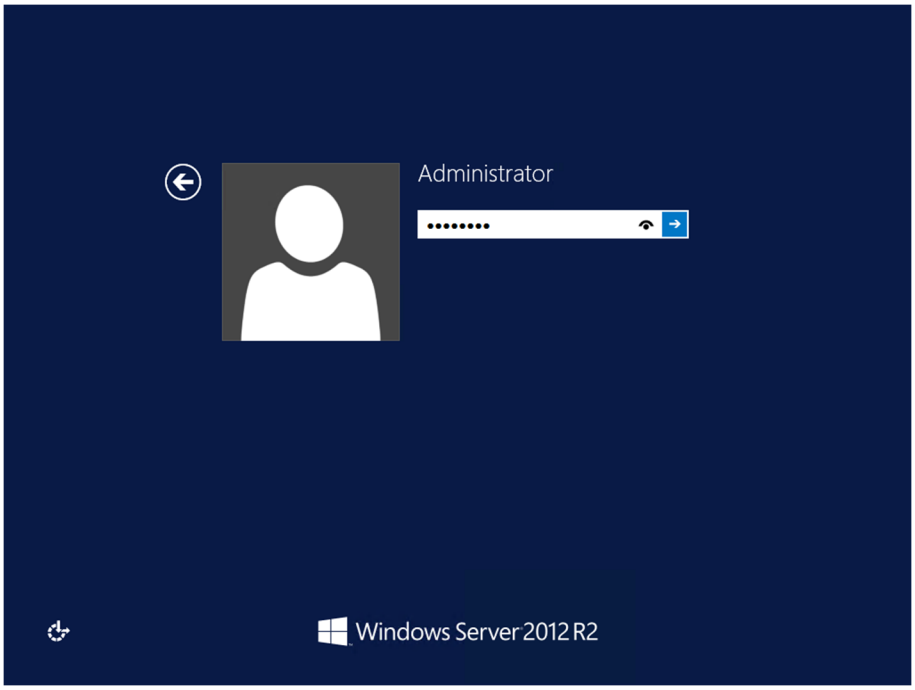

Abbildung 1.1: *Der Anmeldebildschirm von Windows Server 2012 R2*

Die Funktion für die visuelle Kontrolle des im Kennwortfeld eingegebenen Kennworts findet sich parallel auch in Windows 8, Windows 8.1 und auch Windows 10, wodurch sich die Anzahl von Kontosperrungen von Benutzerkonten durch die Falscheingabe von Kennwörtern - und somit auch der damit verbundene Supportaufwand - möglicherweise reduzieren lassen kann.

1.3.2 Die grafische Benutzeroberfläche

Gleich nach der Anmeldung an Windows Server 2012 R2 als Server mit grafischer Benutzeroberfläche startet automatisch der grafische Server-Manager. Am unteren Rand fällt in der unter Windows-Betriebssystemen gewohnten Taskleiste auf, dass Microsoft den Startknopf unter Windows Server 2012 R2, sowie parallel auch unter Windows 8.1 wieder hinzugefügt hat. Das von früheren Windows-Version gewohnte Startmenü ist unter dem aktuellen Windows-Serverbetriebssystem nicht enthalten. Es findet sich im Gegensatz dazu ein auf die wichtigsten Funktionen hin reduziertes (Ersatz-)Startmenü, das durch einen Klick mit der rechten Maustaste auf den Startknopf angezeigt wird.

Unter dem Serverbetriebssystem wie parallel auch unter Windows 8.1 findet sich ein auf die mögliche „*Touch*"-Steuerung abgestimmter Startbildschirm (technisch engl. *Modern UI*), in dem sich standardmäßig bereits einige Verknüpfungen befinden. So steht zum Beispiel bereits eine entsprechende Kachel (engl. *Tile*) zum Aufruf der Systemsteuerung, der Windows PowerShell, der Verwaltung, sowie auch des Internet Explorers bereit.

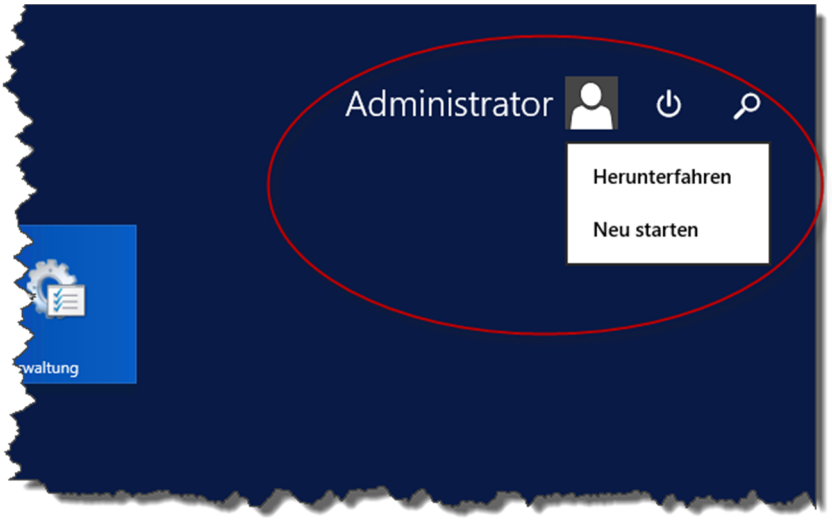

Abbildung 1.2: *Verknüpfungen im Startbildschirm von Windows Server 2012 R2 mit Update (1)*

In der grafischen Benutzeroberfläche des Startbildschirms hat Microsoft unter Windows Server 2012 R2 und Windows 8.1 auch die zuvor bereits unter Windows 8 bzw. Windows Server 2012 zur Navigation eingeführte, sogenannte „Charms"-Leiste integriert. Hierüber besteht neben der Maussteuerung auch die Möglichkeit, das Serversystem beispielsweise von einem Tablet-PC mit Touch-Bildschirm oder vergleichbaren Geräten mit den Fingern zu steuern.

1.3.3 Der grafische Server-Manager

Der bereits seit Windows Server 2008 auf den Serversystemen als zentrale Verwaltungskonsole enthaltene Server-Manager wurde bereits unter Windows Server 2012 nochmals völlig überarbeitet. Neben einer neu konzipierten Oberfläche findet man darin nicht nur verbesserte, sondern auch viele neue Funktionen. So kann man im grafischen Server-Manager unter Windows Server 2012 R2 nicht nur andere Serversysteme im Netzwerk remoteverwalten, sondern auch Serverrollen und -features über das Netzwerk auf anderen Servern installieren bzw. bei Bedarf auch wieder entfernen.

HINWEIS: Im Vergleich zu Windows Server 2012 finden sich im grafischen Server-Manager unter Windows Server 2012 R2 (Release 2) prinzipiell keine Änderungen.

Gleich nach dem Aufruf der grafischen Server-Manager-Konsole zeigt dieser das Dashboard, in dem man u. a. einen Überblick über die damit verwalteten Server und Serverrollen erhält.

Über die automatisch eingerichteten, bidirektionalen und transitiven Vertrauensstellungen zwischen den einzelnen Domänen einer Struktur der Gesamtstruktur können alle vorhandenen Benutzer im Bedarfsfall die Zugriffsmöglichkeit auf prinzipiell alle vorhandenen Ressourcen erhalten.

Gesamtstrukturvertrauensstellung

Seit der Einführung von Windows Server 2003 ist es möglich, zwischen zwei unterschiedlichen Active Directory-Gesamtstrukturen eine Gesamtstrukturvertrauensstellung (engl. *Forest Trust*) einzurichten. Diese kann unidirektional oder auch bidirektional eingerichtet werden, sodass der Zugriff auf Ressourcen entweder einseitig oder gegenseitig möglich wird.

Die Gesamtstrukturvertrauensstellungen werden immer zwischen den Stammdomänen der jeweiligen Active Directory-Gesamtstrukturen eingerichtet. Wenn hierbei jedoch eine Active Directory Gesamtstruktur gleich auch mehreren anderen Gesamtstrukturen über die Gesamtstrukturvertrauensstellungen vertraut, so ist die Transitivität der Vertrauensstellung zueinander nicht nutzbar. Gesamtstrukturvertrauensstellungen gelten immer nur zwischen den jeweils bei der Einrichtung der Vertrauensstellung angegebenen Gesamtstrukturen (sprich: eine Art „Punkt-zu-Punkt-Vertrauen“).

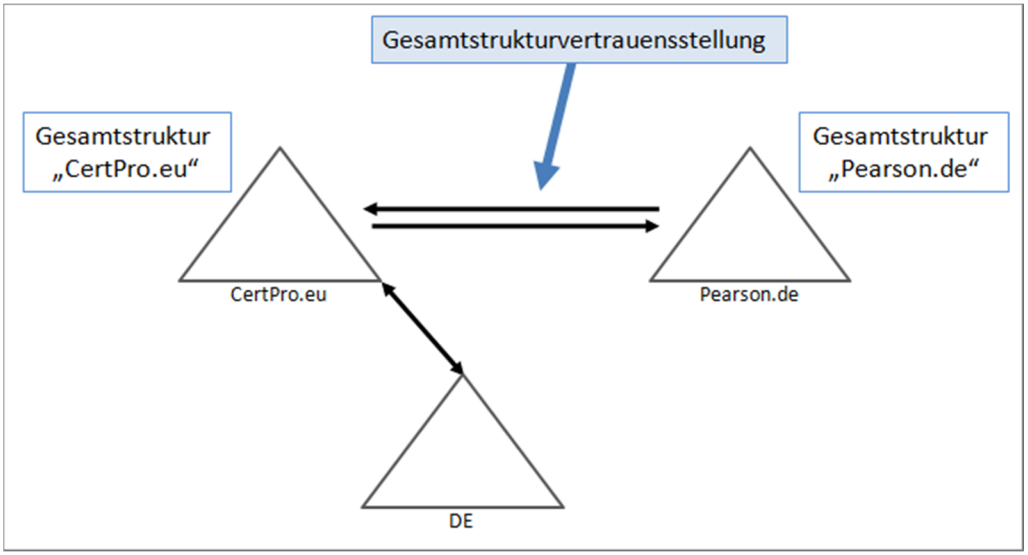

Abbildung 2.19: *Gegenseitige Gesamtstrukturvertrauensstellung zwischen zwei verschiedenen Active Directory-Gesamtstrukturen*

Gesamtstrukturvertrauensstellungen können sehr dienlich sein, wenn bisherige, unterschiedliche Active Directory-Gesamtstrukturen beispielsweise durch die Fusion zweier Firmen zu einem großen Netzwerk zusammenwachsen sollen. Wenn die vorhandenen Gesamtstrukturen, beispielsweise wegen der notwendigen, administrativen Autonomie, erhalten bleiben sollen, so kann man zumindest den gegenseitigen Zugriff mit dieser Art von Vertrauensstel-

lung sicherstellen. Die Gesamtstrukturvertrauensstellungen werden transitiv eingerichtet, sodass über das Vertrauen zwischen den jeweiligen Stammdomänen der Gesamtstrukturen der Zugriff auf Ressourcen ebenso auf die jeweils untergeordneten Domänen ermöglicht wird.

Filterung mittels Namensuffix-Routing

Die Reichweite einer Gesamtstrukturvertrauensstellung kann durch das sogenannte *Namensuffix-Routing* beschränkt werden. Hierbei kann man bestimmte, untergeordnete Domänen oder auch weitere Active Directory-Strukturen einer Active Directory-Gesamtstruktur aus der Nutzungsmöglichkeit der Gesamtstrukturvertrauensstellung zwischen zwei Gesamtstrukturen ausschließen. Ausschlaggebend ist hierbei der zur Filterung angegebene Name bei der Konfiguration des Namensuffix-Routings.

Das Namensuffix-Routing kann für bestimmte Domänennamen aktiviert bzw. deaktiviert werden. Bei der Deaktivierung des Namensuffix-Routings für bestimmte Domänen anhand derer Domänensuffix wird deren Mitgliedern der Zugriff auf die in der vertrauen den Gesamtstruktur vorhandenen Ressourcen verwehrt. Das Namensuffix-Routing kann im Bedarfsfall sogar direkt auf Ebene der Stammdomäne der Gesamtstruktur für die gesamten darin befindlichen Domänen deaktiviert werden.

Das Namensuffix-Routing wird mittels der Konsole *Active Directory-Domänen und Vertrauensstellungen* direkt in der Konfiguration für die Gesamtstrukturvertrauensstellung aktiviert bzw. deaktiviert.

Standardmäßig ist das Namensuffix-Routing innerhalb einer Gesamtstrukturvertrauensstellung zwischen zwei Active Directory-Gesamtstrukturen für alle Domänennamen aktiviert.

INTERNET: Weitere Informationen zu den Konfigurationsmöglichkeiten des Namensuffix-Routings unter Windows Server 2012 (R2) erhalten Sie im Internet unter:

https://technet.microsoft.com/en-us/library/cc731648.aspx

Verknüpfte Vertrauensstellung

In Active Directory-Gesamtstrukturen, die über mehrere physikalische Standorte verteilt sind und in denen auch gleich mehrere, untergeordnete Domänen vorhanden sind, kann man die zu beschreitenden Wege des Vertrauens mitunter verkürzen – durch die Einrichtung von verknüpften Vertrauensstellungen. Hierbei werden neben den ohnehin automatisch eingerichteten, transitiven Vertrauensstellungen zwischen den untergeordneten zu den übergeordneten Domänen innerhalb einer Active Directory-Gesamtstruktur noch zusätzliche, ebenso transitive Vertrauensstellungen zwischen bestimmten Domänen eingerichtet. Diese dienen oft dazu, um den langen Weg des Vertrauens, der standardmäßig immer über die jeweilige Stammdomäne der Active Directory-Struktur(en) führt, zu verkürzen.

Wenn sich beispielsweise zwei untergeordnete Active Directory-Domänen an einem, die Stammdomäne der betreffenden Active Directory-Struktur sich jedoch an einem anderen physikalischen Standort befindet, kann man die übermäßige Kommunikation zwischen den

Domänen über die WAN-Verbindung mitunter reduzieren. Hierzu kann man eine verknüpfte Vertrauensstellung direkt zwischen den beiden am gleichen physikalischen Standort befindlichen, untergeordneten Domänen einrichten.

INTERNET: Weitere Informationen zu verknüpften Vertrauensstellungen unter Windows Server 2012 (R2) findet man im Internet unter:

https://technet.microsoft.com/de-de/library/cc754538.aspx

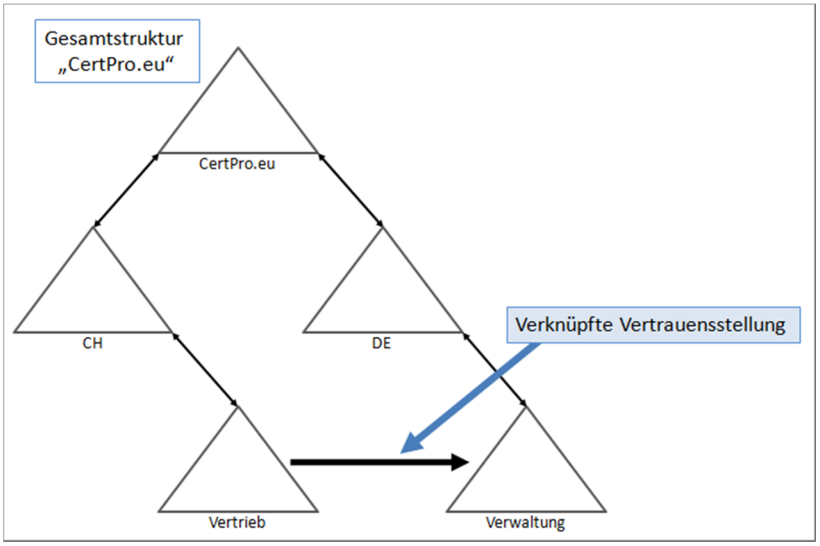

Abbildung 2.20: *Verknüpfte, unidirektionale Vertrauensstellung zwischen zwei untergeordneten Domänen innerhalb einer Active Directory-Gesamtstruktur*

Externe Vertrauensstellung

Eine externe Vertrauensstellung dient in der Praxis dazu, den Zugriff zwischen Domänen verschiedener Gesamtstrukturen oder auch zwischen einer Windows NT 4.0- und einer Windows Server 2012 R2-Active Directory-Domäne über die betreffende Vertrauensstellung zu ermöglichen. Externe Vertrauensstellungen sind grundsätzlich nicht transitiv, können jedoch bidirektional eingerichtet werden, sodass bei Bedarf ein gegenseitiger Zugriff auf Ressourcen ermöglicht wird.

INTERNET: Weitere Informationen zur Konfiguration externer Vertrauensstellungen unter Windows Server 2012 (R2) findet man im Internet unter:

https://technet.microsoft.com/de-de/library/cc732859.aspx

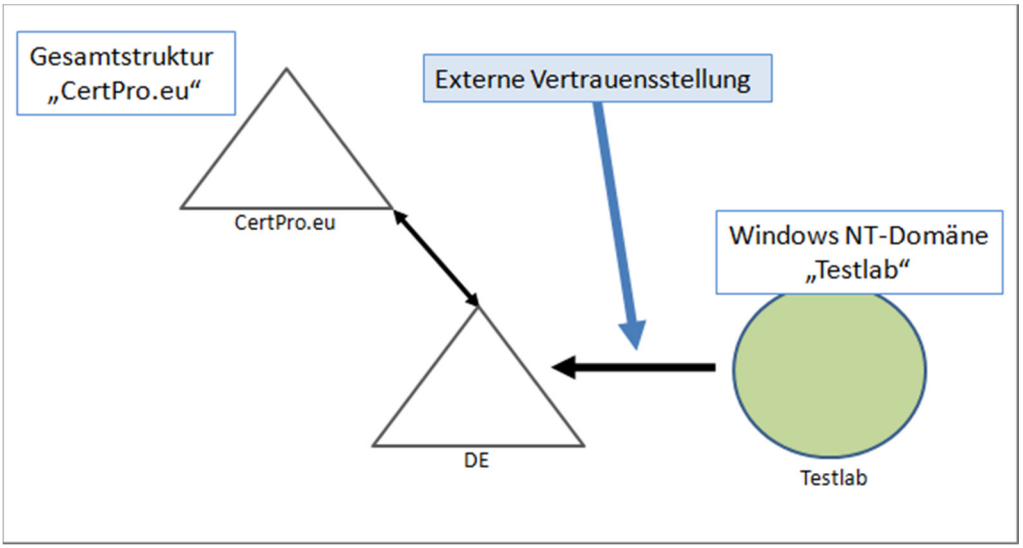

Abbildung 2.21: *Externe, unidirektionale Vertrauensstellung zwischen einer Windows NT-Domäne und einer untergeordneten Domäne einer Active Directory-Gesamtstruktur*

Bereichsvertrauensstellung

Eine Bereichsvertrauensstellung dient in der Praxis dazu, den Zugriff zwischen verschiedenen Verzeichnisdiensten, die Kerberos als Authentifizierungsprotokoll verwenden, beispielsweise einer Active Directory-Gesamtstruktur und einem *LDAP-Bereich* unter *Unix/Linux* (*OpenLDAP* oder Ähnlichem), zu ermöglichen. Diese Art von Vertrauensstellung, prinzipiell vergleichbar mit der externen Vertrauensstellung in Abbildung 2.22, wird im Englischen auch als *Realm Trust* bezeichnet. Sie kann unidirektional oder bidirektional sowie transitiv oder nicht transitiv eingerichtet werden.

INTERNET: Weitere Informationen zur Konfiguration von Bereichsvertrauensstellungen (engl. *Realm Trusts*) unter Windows Server 2012 (R2) findet man im Internet unter:

https://technet.microsoft.com/de-de/library/cc731297.aspx

Tools zum Verwalten von Vertrauensstellungen

Zur Verwaltung von Vertrauensstellungen in einer Active Directory-Domänendienste-Infrastruktur stehen die folgenden Tools zur Verfügung:

- Active Directory-Domänen und -Vertrauensstellungen
- Netdom.exe

2.6.5 Domänenstrukturen

Eine Domänenstruktur (engl. *Tree*) stellt den Teilbereich einer Gesamtstruktur der Active Directory-Domänendienste (*Active Directory Domain Services, AD DS*) dar. Eine Domänenstruktur beschreibt einzelne oder auch mehrere, über Vertrauensstellungen zusammenhängende Domänen, die einem bestimmten Namensraum entsprechen. Die in Domänenstrukturen untergeordneten Domänen führen den Namensraum der jeweils übergeordneten Domäne fort. Hierzu ein Beispiel:

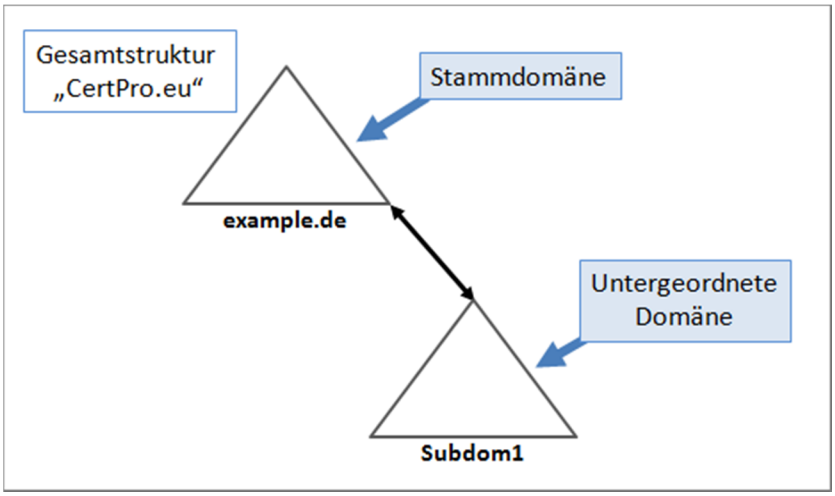

Abbildung 2.22: *Beispiel einer Active Directory-Stammdomäne mit einer weiteren, untergeordneten Domäne*

Die Stammdomäne einer Active Directory-Gesamtstruktur wird mit dem Namen *example.de* eingerichtet. Wenn man zu dieser Domäne nun eine untergeordnete Domäne hinzufügt, so führt diese den bereits definierten Namen fort. Wenn die untergeordnete, neue Domäne nun den Domänennamen *Subdom1* erhalten soll, so setzt sich ihr vollständiger Name wie folgt zusammen: *Subdom1.example.de*

2.6.6 Domänen

Eine Active Directory-Domäne stellt eine Gruppe von Computern (sprich: Domänencontrollern) dar, die eine gemeinsame Verzeichnisdatenbank unter einem einheitlichen Namenskontext nutzen. Eine Domäne definiert die Sicherheitsgrenzen, in denen gemeinsame Sicherheitsrichtlinien für die darin enthaltenen Objekte wie beispielsweise Benutzer- oder Computerobjekte genutzt werden. Die Namen von Domänen müssen in der Netzwerkumgebung eindeutig sein und bauen auf den Namensauflösungsdiensten des DNS (*Domain Name System*) auf. Hierbei kommen in der Regel sogenannte vollqualifizierte Domänennamen (engl. *Fully Qualified Domain Name, FQDN*) zum Einsatz. Wenn die Active Directory-Domäne gleichsam intern wie auch im Internet vertreten sein soll, so sollte der entsprechend übergeordnete Domänenname bei der zuständigen Registrierungsstelle registriert werden. Somit kann die Verwendbarkeit des Domänennamens einer Active Directory-Gesamtstruktur eines Unternehmens im Internet sichergestellt werden.

PRAXISTIPP! Die Domänenregistrierung für .de-Domänen kann in Deutschland unter anderem bei der DeNIC (***http://www.denic.de***) erfolgen. Für internationale Namen wie beispielsweise die .com- oder .org-Domänen ist die InterNIC zuständig (***http://www.internic.net***).

Domänen können als Domänenstrukturen in Hierarchien angeordnet werden. Die oberste Domäne wird hierbei als *Stammdomäne der Domänenstruktur*, die darunter liegenden Domänen werden als *untergeordnete Domänen* bezeichnet. Die erste Domäne, die man in einer Active Directory-Umgebung installiert, wird als *Stammdomäne der Gesamtstruktur* bezeichnet.

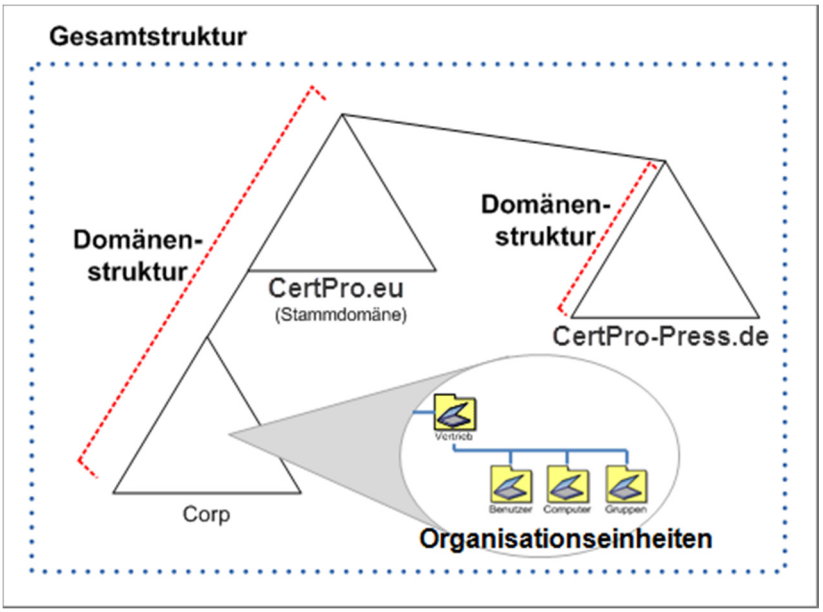

Abbildung 2.23: *Active Directory-Domänen innerhalb verschiedener Domänenstrukturen einer Active Directory-Gesamtstruktur*

Domänen können sich über mehrere Standorte erstrecken. In der Verzeichnisdatenbank der Active Directory-Domänendienste (*Active Directory Domain Services, AD DS*) werden die domäneninternen Objekte, wie beispielsweise Benutzer-, Computerobjekte, Gruppen, Organisationseinheiten (*OUs*), Gruppenrichtlinien, Drucker und veröffentlichte freigegebene Ordner gespeichert. Diese Verzeichnisdatenbank befindet sich auf den Domänencontrollern und wird zwischen diesen durch Replikationsvorgänge ständig abgeglichen.

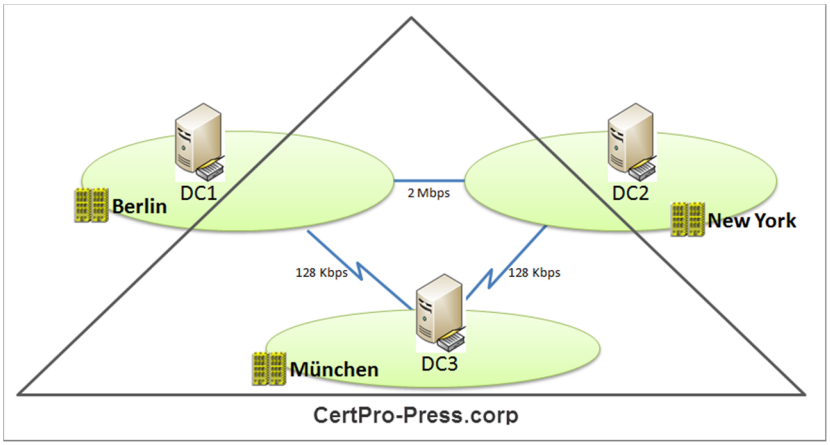

Abbildung 2.24: *Erstreckung einer Active Directory-Domäne über mehrere physikalische Standorte*

Tools zum Verwalten von Domänen

Zum Verwalten von Domänen der Active Directory-Domänendienste (*Active Directory Domain Services, AD DS*) bzw. der darin enthaltenen Objekte können u. a. die folgenden Tools eingesetzt werden:

- Grafisches *Active Directory-Verwaltungscenter*
- Konsole *Active Directory-Benutzer und -Computer*
- Konsole *Active Directory-Domänen und -Vertrauensstellungen*
- DS-Tools (dsadd.exe, dsmod.exe, dsmove.exe, dsquery.exe, dsrm.exe)
- CSVde.exe
- LDIFde.exe
- ADSIEdit.msc
- LDP.exe
- Netdom.exe
- Windows PowerShell

2.6.7 Authentifizierung und Autorisierung

Die Benutzeranmeldung sowie der Zugriff auf Ressourcen in einer Active Directory-Domänendienste-Umgebung werden anhand von zwei unterschiedlichen, nacheinander folgenden Prozessen geregelt:

Der Authentifizierungsprozess

Bei der Authentifizierung wird die Identität eines Benutzers anhand eines vorweg definierten Benutzerkontos der betreffenden Domäne oder eines lokalen Benutzerkontos in Verbindung mit dem jeweils persönlichen Kennwort überprüft.

Windows Server 2012 R2 unterstützt zur Authentifizierung eine Vielzahl an Protokollen (sog. Authentifizierungsprotokolle). Als Standardauthentifizierungsprotokoll kommt in Domänenumgebungen mit Clients und Servern ab Windows 2000 das Kerberos Version 5(*V5*)-Protokoll zum Einsatz. Aus Gründen der Abwärtskompatibilität zu älteren Client- und Server-Betriebssystemen, wie zum Beispiel Windows NT 4.0, werden jedoch noch weitere Authentifizierungsprotokolle unterstützt. Hierzu zählen beispielsweise das Lan-Manager-Protokoll (*LMProtokoll*), das NT-Lan-Manager-Protokoll (*NTLM*) und das NT-Lan-Manager-Protokoll Version 2 (*NTLMv2*).

Mit Sicherheitsrichtlinien in Gruppenrichtlinienobjekten einer Domäne ist es möglich, die Authentifizierungsebene festzulegen, um die Sicherheit gegenüber möglichen Man-in-the-Middle-Angriffen durch das Mitlesen der übermittelten Authentifizierungsinformationen zu erschweren.

Als Alternative zu den herkömmlichen Authentifizierungsmethoden über den Benutzernamen und das Benutzerkennwort können auch digitale Zertifikate für die Authentifizierung von Benutzern und Computern verwendet werden. Dies erfordert jedoch die Integration der Active Directory-Zertifikatdienste (*Active Directory Certificate Services, AD CS*) in die Domänenumgebung. Auf lange Sicht hin wird sich diese Art der Authentifizierung in Netzwerken wohl durchsetzen.

Die Windows Server 2012 R2-Verbunddienste (*Active Directory Federation Services, AD FS*) können verwendet werden, um die Authentifizierung sogar beispielsweise auf Partnerfirmen über das Internet auszuweiten.

HINWEIS: Selbst wenn ein Benutzer gegenüber einem Domänencontroller erfolgreich authentifiziert werden konnte, muss er für den eigentlichen Ressourcenzugriff zusätzlich noch autorisiert werden. Beispielsweise kann einem Benutzer trotz erfolgreicher Authentifizierung durch fehlende Autorisierung dennoch die Anmeldung an einer spezifischen Arbeitsstation im Netzwerk verweigert werden.

Der Autorisierungsprozess

Im zweiten Schritt folgt nach der erfolgreichen Authentifizierung eines Benutzers nun die Autorisierung. Hierbei wird anhand des bei der Authentifizierung verwendeten Benutzerkontos die Berechtigung für beispielsweise die lokale Anmeldung auf dem betreffenden Computer sowie auch die Berechtigung für Zugriffe auf Netzwerkressourcen überprüft.

Zur Überprüfung der Autorisierung eines Benutzers werden die folgenden Komponenten verwendet:

Komponente	Beschreibung
Sicherheitskennung (Security Identifier, SID)	Beim Erstellen eines Benutzerkontos wird dem Objekt eine eindeutige Sicherheitskennung (SID) zugeordnet.

Komponente	Beschreibung
Sicherheitstoken (Security Token)	Nach der erfolgreichen Anmeldung eines Benutzers wird diesem ein Sicherheitstoken ausgestellt, das die Sicherheitskennung des Benutzers sowie aller Sicherheitsgruppen enthält, welcher der Benutzer angehört. Darüber hinaus sind in dem Sicherheitstoken die dem Benutzer zugeordneten Benutzerrechte enthalten.
Zugriffskontrollliste (Access Control List, ACL)	Liste von Einträgen (sog. *Access Control Entries, ACEs*), anhand derer der Zugriff auf Ressourcen geregelt werden kann. Mit den Einträgen in den ACLs kann der Zugriff auf die betreffende Ressource genehmigt oder verweigert werden. Beim Zugriff auf Ressourcen im Netzwerk wird das Sicherheitstoken des Benutzers auf Übereinstimmung mit den Einträgen der jeweiligen Zugriffskontrollliste verglichen. Bei den ACLs unterscheidet man zwischen: Discretionary Access Control List (DACL) für die eigentliche Zugriffssteuerung und Security Access Control List (SACL) für die Steuerung der Überwachung des Zugriffs auf Ressourcen.

Tabelle 2.3: *Komponenten zur Überprüfung der Autorisierung eines Benutzers*

Beispiel für den Anmeldevorgang in einer Domäne

Nachfolgend sehen Sie ein vereinfachtes Beispiel für den Anmeldevorgang eines Benutzers in einer Domänenumgebung:

Die Schritte im Einzelnen:

1. Ein Benutzer gibt seine Anmeldedaten in das Anmeldefenster ein.
2. Das lokale Sicherheitsteilsystem (engl. *Local Security Authority, LSA*) des betreffenden Rechners nimmt die Anmeldeinformationen des Benutzers entgegen und sendet diese an einen Domänencontroller.
3. Der betreffende Domänencontroller überprüft die Anmeldedaten des Benutzers anhand des jeweiligen Domänenbenutzerkontos.
4. Nach erfolgreicher Authentifizierung generiert der Domänencontroller ein Sicherheitstoken, in dem die Sicherheitskennung des Benutzerkontos sowie aller Sicherheitsgruppen, denen der Benutzer zugeordnet ist, enthalten ist, und sendet dieses an den betreffenden Computer zurück.

Gruppenname	Beschreibung
Server-Operatoren	Mitglieder dieser Gruppe können Domänenserver verwalten.
Sicherungs-Operatoren	Mitglieder dieser Gruppe können Daten sichern und wiederherstellen, sowie sich am System lokal anmelden.
Terminalserver-Lizenzserver	Mitglieder dieser Gruppe können Benutzerkonten in Active Directory für Nachverfolgungs- und Berichtszwecke mit Informationen zur Lizenzausstellung aktualisieren.
Windows-Autorisierungszugriffsgruppe	Mitglieder dieser Gruppe haben Zugriff auf das berechnete Attribut „*tokenGroupsGlobalAndUniversal*“ für Benutzerobjekte.
Zertifikatdienst-DCOM-Zugriff	Mitglieder dieser Gruppe sind berechtigt, eine Verbindung mit den Zertifizierungsstellen im Unternehmen herzustellen.
Zugriffssteuerungs-Unterstützungsoperatoren	Mitglieder dieser Gruppe können remote Autorisierungsattribute und -berechtigungen für Ressourcen auf dem Computer abfragen.

Tabelle 4.5: *Standardmäßige Gruppen im Container „Builtin“*

Neben den standardmäßigen Gruppen im *Builtin*-Container sind in Active Directory-Domänen noch weiter Gruppen vorhanden. Diese befinden sich im Container *Users* der Domäne.

Active Directory-Gruppen im Users-Container

Die im Container ***Users*** einer Active Directory-Domäne vorhandenen Gruppen werden zur Rechte- und Berechtigungsvergabe innerhalb der Domäne verwendet.

Die folgende Tabelle enthält eine Übersicht über die standardmäßig vorhandenen Gruppen des ***Users***-Containers einer Active Directory-Domäne.

Gruppenname	Beschreibung
Abgelehnte RODC-Kennwortreplikationsgruppe	Mitglieder, deren Kennwörter nicht auf schreibgeschützten Domänencontrollern (RODCs) repliziert werden.
DNSAdmins	Mitglieder dieser Gruppe können DNS-Objekte in der Domäne verwalten.
DNSUpdateProxy	Mitglieder dieser Gruppe (typischer Weise DHCP-Server) können im Namen anderer Clients dynamische Aktualisierungen in der DNS-Datenbank vornehmen.

Gruppenname	Beschreibung
Domänen-Admins	Mitglieder dieser Gruppe besitzen administrative Rechte und Berechtigungen innerhalb der Active Directory-Domäne.
Domänen-Benutzer	Alle Benutzerkonten in dieser Domäne.
Domänencomputer	Alle Arbeitsstationen und Mitgliedsserver in dieser Domäne.
Domänencontroller	Alle Domänencontroller in dieser Domäne.
Domänen-Gäste	Alle Gäste dieser Domäne.
Klonbare Domänencontroller	Mitglieder dieser Gruppe sind Domänencontroller, die geklont werden.
Organisations-Admins	Mitglieder dieser Gruppe besitzen administrative Rechte in der Active Directory-Gesamtstruktur.
Protected Users	Mitglieder dieser Gruppe erhalten zusätzlichen Schutz vor Sicherheitsbedrohungen.
RAS- und IAS-Server	Server in dieser Gruppe können auf die RAS-Eigenschaften von Benutzern zugreifen.
Richtlinien-Ersteller-Besitzer	Mitglieder dieser Gruppe können Gruppenrichtlinienobjekte in der Domäne erstellen oder ändern.
Schema-Admins	Mitglieder dieser Gruppe können Änderungen im Schema der Active Directory-Gesamtstruktur vornehmen.
Schreibgeschützte Domänencontroller	Mitglieder dieser Gruppe sind schreibgeschützte Domänencontroller in der Domäne.
Schreibgeschützte Domänencontroller der Organisation	Mitglieder dieser Gruppe sind schreibgeschützte Domänencontroller im Unternehmen.
WinRMRemoteWMIUsers_	Mitglieder dieser Gruppe können über Verwaltungsprotokolle auf WMI-Ressourcen zugreifen (z. B. WS-Verwaltung über den Windows-Remoteverwaltungsdienst). Dies gilt nur für WMI-Namespaces, die dem Benutzer Zugriff gewähren.
Zertifikatherausgeber	Mitglieder dieser Gruppe können Zertifikate innerhalb von Active Directory veröffentlichen.
Zulässige RODC-Kennwortreplikationsgruppe	Mitglieder, deren Kennwörter auf schreibgeschützte Domänencontroller (RODCs) repliziert werden.

Tabelle 4.6: *Standardmäßige Gruppen im Container „Users“*

4.6.5 Planungsstrategien für Gruppen

Die Planungsstrategie für die Verwendung von Gruppen in einer Active Directory-Gesamtstruktur sollte möglichst transparent gehalten sein. Es ist sicher empfehlenswert, sich an grundlegende Standardregeln zu halten.

Die "A-G-DL-P"-Regel

Die einfachste Regel beschreibt sich mit A-G-DL-P. Die Abkürzungen stehen hierbei für:

A = Accounts (deutsch: Benutzerkonten)

G = Global Groups (deutsch: Globale Gruppen)

DL = Domain local Group (deutsch: Domänenlokale Gruppe)

P = Permission (deutsch: Berechtigung)

Die Regel übersetzt die empfohlene Gruppenstrategie, der man sicher die effektivste und effizienteste Verwaltung von Active Directory-Objekten im Zugriff auf Ressourcen nachsagen kann.

Bei dieser Strategie werden die Benutzerkonten (***A***) in globale Gruppen (***G***) zusammengefasst. Diese wiederum werden zum Mitglied der domänenlokalen Gruppen (***DL***), welchen man letztlich die Berechtigung (***P***) zuordnet.

Wenn man in dieser Gruppenstrategie nun ein Benutzerkonto als Mitglied einer der betreffenden globalen Gruppen (***G***) definiert, so erhält der Benutzer die der domänenlokalen Gruppe (***DL***) zugeordneten Berechtigungen an der jeweiligen Ressource. Die Gruppenverschachtelung macht es möglich.

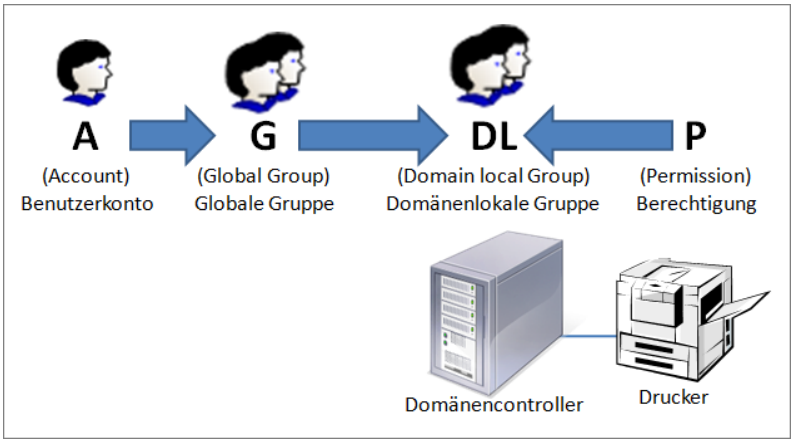

Abbildung 4.20: *A-G-DL-P-Verfahren für den Zugriff auf eine Ressource*

Je nachdem, wie die Active Directory-Umgebung eines Unternehmens strukturiert ist, kann es von Vorteil sein, noch weitere Regeln für die effektivste Gruppenverschachtelung zu nutzen.

Die „A-G-G-DL-P"-Regel

Diese Regel beschreibt die Verschachtelung von globalen Gruppen in andere globale Gruppen derselben Active Directory-Domäne. So kann man beispielsweise viele globale Vertriebsgruppen (*G Vertrieb Nord, G Vertrieb Mitte, G Vertrieb Süd*) zu einer einzigen globalen Vertriebsgruppe (*G Gesamtvertrieb*) zusammenfassen, wenn man Ressourcen für alle Mitglieder einer verstreuten Vertriebsabteilung gemeinsam bereitstellen möchte.

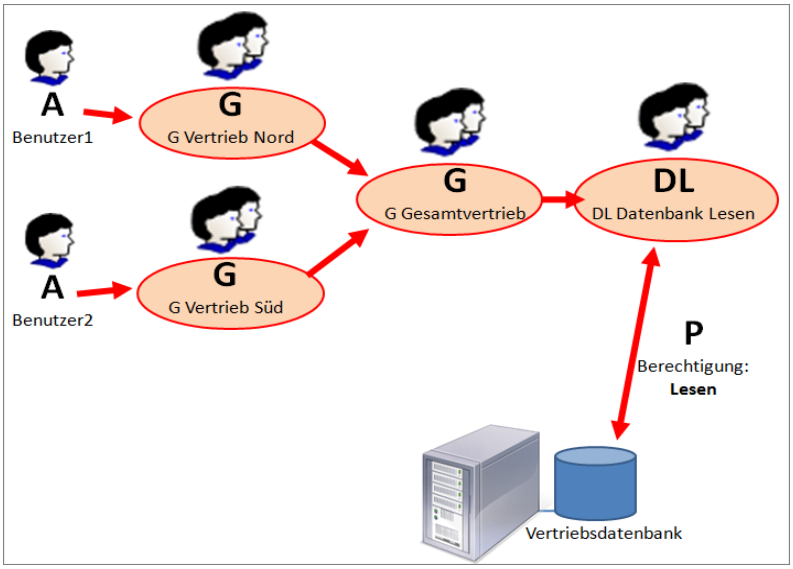

Abbildung 4.21: *Verschachtelung mehrerer globaler Gruppen innerhalb einer Active Directory-Domäne nach A-G-G-DL-P für den Zugriff auf eine Vertriebsdatenbank*

Die „A-G-U-DL-P"-Regel

Diese Regel findet ihren Nutzen in sehr großen Active Directory-Gesamtstrukturen mit mehreren Domänen. Wenn man beispielsweise allen Benutzern verschiedener Domänen einer Gesamtstruktur den gemeinsamen Zugriff auf Ressourcen ermöglichen möchte, so kann man die vorhandenen, globalen Gruppen zu einer einzigen, universellen Gruppe zusammenfassen. Diese universelle Gruppe verschachtelt man dann jeweils einmalig in die für die Ressourcenzugriffe bereitgestellte, domänenlokale Gruppe.

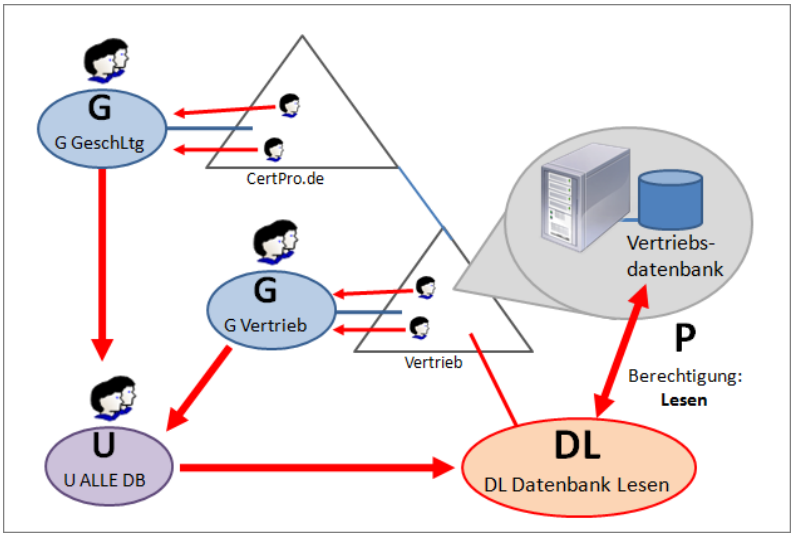

Abbildung 4.22: *Beispiel für die mögliche Gruppenverschachtelung mehrerer globaler Gruppen verschiedener Domänen in eine universelle Gruppe zwecks Verschachtelung in eine domänenlokale Gruppe*

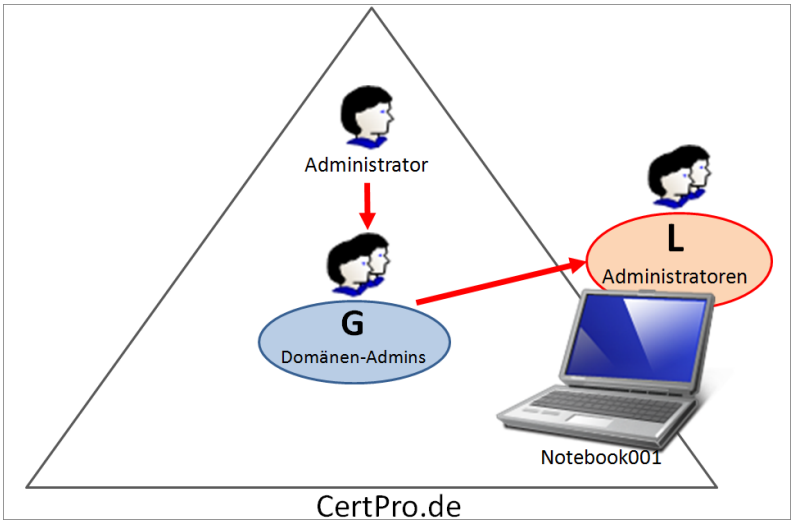

Abbildung 4.23: *Standardmäßige Gruppenverschachtelung der globalen Gruppe der Domänen-Admins in die lokale Gruppe der Administratoren auf einem Clientcomputer als Mitglied einer Active Directory-Domäne*

Die „A-G-L-P"-Regel

Wenn sich eine zu verwaltende Ressource lokal auf einem der in der Domäne enthaltenen Computer befindet, so kann man sich der vorhandenen oder gar neu zu erstellenden, lokalen

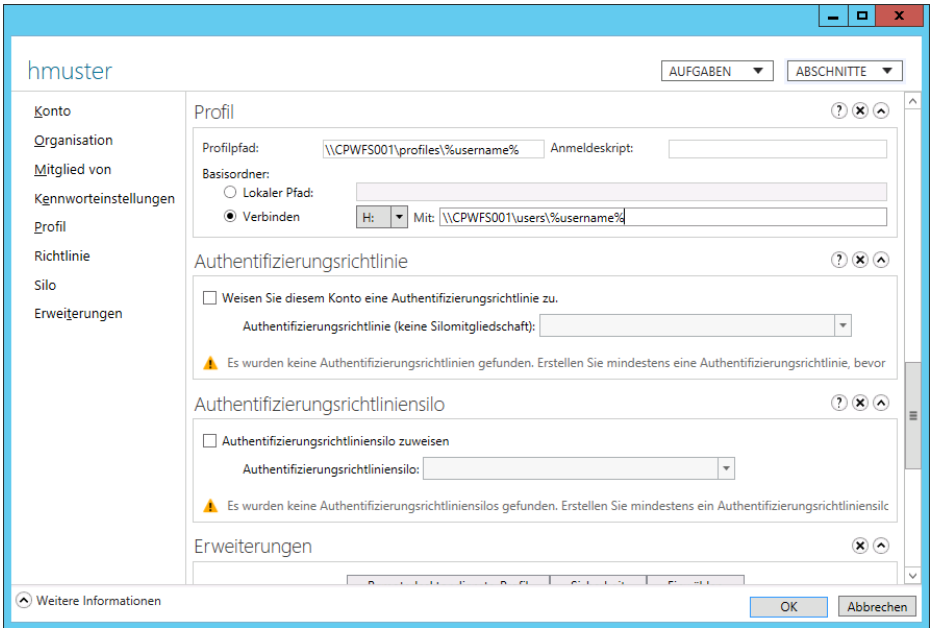

Abbildung 14.18: *Pfadangaben für den Benutzerprofilpfad und den Basisordner*

14.5 Dienstkonten

Neben den für die Authentifizierung und Autorisierung von Benutzern verwendeten Benutzerobjekten kommen in Active Directory-Gesamtstrukturen häufig auch Dienstkonten zum Einsatz. Diese werden für die Ausführung bestimmter Dienste wie beispielsweise die SharePoint-Dienste, SQL-Datenbanken usw. benötigt. Solchen Benutzerkonten, die man als Dienstkonten bezeichnet, sollte man ein komplexes und langes Kennwort zuordnen.

WICHTIG! Ein Benutzerobjekt, das als Dienstkonto innerhalb einer Active Directory-Gesamtstruktur eingesetzt wird, sollte über ein komplexes Kennwort verfügen.

14.5.1 Standardmäßig vorhandene Dienstkonten

Windows Server 2012 R2 stellt standardmäßig bereits bestimmte Dienstkonten bereit:

- **System**
- **Lokaler Dienst**
- **Netzwerkdienst**

Diesen speziellen Dienstkonten wurden standardmäßig bereits die für die Ausführung von Diensten notwendigen Rechte zugewiesen. Ihnen können durch die Administratoren keine Kennwörter zugewiesen werden. Eine weitergehende Verwaltung der standardmäßigen Dienstkonten ist prinzipiell nicht vorgesehen.

14.5.2 Gruppenverwaltete Dienstkonten (Group Managed Service Accounts, gMSA)

Im Gegensatz zu den standardmäßig vorhandenen Dienstkonten, die beim Einrichten der Active Directory-Domäne automatisch angelegt werden, kann man auf Domänencontrollern unter Windows Server 2012 R2 oder auch Windows Server 2012 eigene, bei Bedarf auch mehrfach verwendbare, gruppenverwaltete Dienstkonten (engl. *group Managed Service Accounts, gMSA*) erstellen und nach Bedarf einsetzen.

Eingeführt wurden die verwalteten Dienstkonten (engl. *Managed Services Accounts, MSA*) bereits unter Windows Server 2008 R2 und Windows 7. Der Vorteil dieser verwalteten Dienstkonten liegt darin, dass die Passwortverwaltung innerhalb der Domäne automatisch stattfindet. Durch den Einsatz eines Dienstprinzipialnamens (engl. *Service Principal Name, SPN*) ist auch die Delegierung von verwalteten Dienstkonten an andere Administratoren möglich.

Unter Windows Server 2012 R2 wurden diese Dienstkonten in ihrer Einsatzmöglichkeit nochmals erweitert, und können als gruppenverwaltete Dienstkonten nunmehr parallel gleich auf mehreren Servern eingesetzt werden. Dies ermöglicht zum Beispiel die Verwendung eines einzelnen, gruppenverwalteten Dienstkontos (gMSA) auf mehreren Servern innerhalb einer SQL-Datenbankserverfarm.

HINWEIS: Gruppenverwaltete Dienstkonten werden standardmäßig nur über die Windows PowerShell erstellt und verwaltet. Um gruppenverwaltete Dienstkonten in Domänen mit Windows Server 2008- bzw. Windows Server 2008 R2-Domänencontrollern nutzen zu können, muss zuvor das Active Directory-Schema auf Windows Server 2012 R2 aktualisiert werden. Zusätzlich muss mindestens ein Domänencontroller unter Windows Server 2012 R2 ausgeführt werden.

Kennwörter der gruppenverwalteten Dienstkonten werden, wie dies auch bei Computerobjekten in den Active Directory-Domänen automatisch verwaltet. Das Kennwort erhält hierbei eine Länge von 240 Buchstaben, Zahlen und Sonderzeichen, und wird zudem standardmäßig bereits gegen mögliche Angriffe stark verschlüsselt.

Vorbereitung für den Einsatz gruppenverwalteter Dienstkonten (gMSA)

Der Einsatz gruppenverwalteter Dienstkonten (gMSA) erfordert zunächst die Vorbereitung der betreffenden Active Directory-Domäne. In dieser muss mit einem Windows PowerShell-Befehl zunächst ein neuer Master-Schlüssel für das Erstellen neuer gruppenverwalteter Dienstkonten bereitgestellt werden. Verwenden Sie dazu den folgenden Befehl:

```
Add-KdsRootKey -EffectiveImmediately
```

Standardmäßig dauert es insgesamt 10 Stunden, bis der neue Master-Schlüssel in der Domäne erstellt ist, und man beginnen kann, verwaltete Dienstkonten anzulegen. In Testumgebungen kann man diese zeitliche Verzögerung mithilfe des folgenden Befehls umgehen:

```
Add-KdsRootKey -EffectiveImmediately ((Get-Date).addhours(-10))
```

Speicherort gruppenveralteter Dienstkonten

Gruppenverwaltete Dienstkonten (gMSA) werden in der jeweiligen Active Directory-Domäne in der Organisationseinheit *Managed Service Accounts* gespeichert. Um diesen in der Konsole *Active Directory-Benutzer und -Computer* anzuzeigen, müssen in dieser über die *Ansicht* noch die e*rweiterten Features* aktiviert werden.

Erstellen gruppenverwalteter Dienstkonten

Zum Erstellen gruppenverwalteter Dienstkonten (gMSA) steht standardmäßig lediglich die Windows PowerShell mit dem Cmdlet `New-ADServiceAccount` zur Verfügung.

Die vollständige Syntax des Cmdlets lautet:

```
New-ADServiceAccount [-Name] <string> [-AccountExpirationDate
<System.Nullable[System.DateTime]>] [-AccountNotDelegated
<System.Nullable[bool]>] [-AccountPassword <SecureString>]
[-AuthType {<Negotiate> | <Basic>}] [-Certificates <string[]>]
[-Credential <PSCredential>] [-Description <string>] [-Display-
Name <string>] [-Enabled <System.Nullable[bool]>] [-HomePage
<string>] [-Instance <ADServiceAccount>] [-OtherAttributes
<hashtable>] [-PassThru <switch>] [-Path <string>] [-SamAc-
countName <string>] [-Server <string>] [-ServicePrincipalNames
<string[]>] [-TrustedForDelegation <System.Nullable[bool]>]
[-Confirm] [-WhatIf] [<CommonParameters>]
```

INTERNET: Detaillierte Informationen zur Syntax des Cmdlet `New-ADServiceAccount` erhält man über den Befehl **`Get-Help New-ADServiceAccount`** oder alternativ im Internet auf der Website von Microsoft unter:

https://technet.microsoft.com/en-us/library/ee617211.aspx

Um ein neues, gruppenverwaltetes Dienstkonto anzulegen, geben Sie den folgenden Befehl in der Windows PowerShell ein, und drücken Sie die Eingabetaste:

`New-ADServiceAccount` *"<Name des Dienstkontos>"*

Alternativ kann man ein neues, gruppenverwaltetes Dienstkonto beim Anlegen auch gleich registrieren, sowie den damit verbundenen Dienstprinzipalnamen (engl. Service Principal Name, SPN) erstellen lassen. Dies wird im folgenden Beispiel ersichtlich:

`New-ADServiceAccount` *SQLSvc* **`-PrincipalsAllowedToRetrieveMana-gedPassword`** *SQLSVR* **`-ServicePrincipalNames`** *„MSSQLSVC/SVR1.Cert-Pro.intra"*

In diesem Beispiel wird ein neues, gruppenverwaltetes Dienstkonto erstellt, den Computern als Mitgliedern der Gruppe *SQLSVR* das Recht eingeräumt, das Kennwort für das Dienstkonto anzufordern, und letztlich wird das Dienstkonto mit einem Dienstprincipalname in Active Directory registriert. Der Schalter **-PrincipalsAllowedToRetrieveManagedPassword** bestimmt hierbei, wer das dem Dienstkonto zugewiesene Kennwort verwenden darf.

HINWEIS: Mit dem Cmdlet **Get-ADServiceAccount** kann man sich vorhandene, gruppenverwaltete Dienstkonten anzeigen lassen. Änderungen an gruppenverwalteten Dienstkonten hingegen kann man mit dem Cmdlet **Set-ADServiceAccount** durchführen, und zum Löschen steht das Cmdlet **Remove-ADServiceAccount** in der Windows PowerShell von Windows Server 2012 R2 bereit.

Schritte zur Verwendung gruppenverwalteter Dienstkonten

Die folgenden, einzelnen Schritte sind zum Verwenden von gruppenverwalteten Dienstkonten (gMSA) notwendig:

1. Anlegen des gruppenverwalteten Dienstkontos in der Active Directory-Domänen, sowie Verbinden des Dienstkontos mit dem Computerkonto.
   Im folgenden Beispiel wird ein neues, gruppenverwaltetes Dienstkonto angelegt, und der Sicherheitsgruppe „Domänencontroller" der Domäne für die mögliche Verwendung durch diese Server entsprechend zugeordnet:
   New-ADServiceAccount -Name *MyDomSVC* **-DNSHostName** *MyDomSVC.CertPro.intra* **-PrincipalsAllowedToRetrieveManagedPassword** *„Domänencontroller"*
   Der Schalter **-PrincipalsAllowedToRetrieveManagedPassword** bestimmt, wer das dem Dienstkonto zugewiesene Kennwort verwenden darf.
2. Installieren des verwalteten Dienstkontos auf dem betreffenden Computer. Hierfür verwendet man den folgenden Befehl in der Windows PowerShell:
   Install-ADServiceAccount <*gMSA-Name*>
3. Anpassen der Einstellungen des Dienstes, der Rolle oder der Anwendung zur Verwendung des gruppenverwalteten Dienstkontos.

Der Name des gruppenverwalteten Dienstkontos wird gefolgt von einem $-Zeichen (wie zum Beispiel *MyDomSVC$*) in das entsprechende Feld in der Anwendung oder den Eigenschaften des Dienstes eingetragen. Das Kennwortfeld bleibt hierbei leer, da die Kennwortverwaltung im Hintergrund völlig automatisch durchgeführt wird.

INTERNET: Ein umfangreiches Beispiel für das Erstellen und Zuordnen von gruppenverwalteten Dienstkonten unter Windows Server 2012 R2 bzw. Windows Server 2012 findet man auf der Website von Microsoft im Internet unter:

https://blogs.technet.microsoft.com/askpfeplat/2012/12/16/windows-server-2012-group-managed-service-accounts/

Grafische Verwaltung mittels Managed Service Accounts GUI

Im Internet steht ein grafisches Tool mit dem *Namen Managed Service Accounts GUI* zur grafischen Verwaltung der gruppenverwalteten Dienstkonten zum kostenfreien Download zur Verfügung.

INTERNET: Das Tool *Managed Service Accounts GUI* dient dazu, verwaltete Dienstkonten unter Windows Server 2008 R2, sowie auch gruppenverwaltete Dienstkonten unter Windows Server 2012 und Windows Server 2012 R2 zu erstellen und zu verwalten. Herunterladen kann man dieses Tool kostenfrei im Internet unter:

http://www.cjwdev.co.uk/Software/MSAGUI/Info.html

14.6 InetOrgPerson-Objekte

Als Alternative zu den standardmäßig genutzten Benutzerkontenobjekten in Active Directory stehen seit der Einführung von Windows Server 2003 auch die so genannten InetOrgPerson-Objekte zur Verfügung. Microsoft hat diese Objekte in die Active Directory-Domänendienste integriert, um eine nahtlosere Integration und Kommunikation mit anderen X.500-Verzeichnisdiensten zu ermöglichen. InetOrgPerson-Konten können, wie auch standardmäßige Benutzerobjekte in Active Directory, beispielsweise mittels des MMC-Snap-In *Active Directory-Benutzer und -Computer* erstellt und verwaltet werden. InetOrgPerson-Objekte stellen eine untergeordnete Klasse der in Active Directory verwendeten Benutzerobjekte dar, wonach sie ebenso wie diese beispielsweise auch in Zugriffskontrolllisten (*Access Control Lists, ACLs*) für die Steuerung der Zugriffsberechtigungen, oder auch für Anmelde- und Authentifizierungsvorgänge verwendet werden können.

Die Klasse *InetOrgPerson* ist im Schema des Active Directory bereits seit Windows Server 2003 enthalten und steht für die Verwendung bereit.

14.7 Kontakt-Objekte

Neben den bisher benannten Benutzer- und InetOrgPerson-Objekten ist es bereits seit Active Directory unter Windows 2000 Server möglich, Kontakt-Objekte in der Datenbank der Active Directory-Domänendienste (*Active Directory Domain Services, AD DS*) anzulegen und zu nutzen.

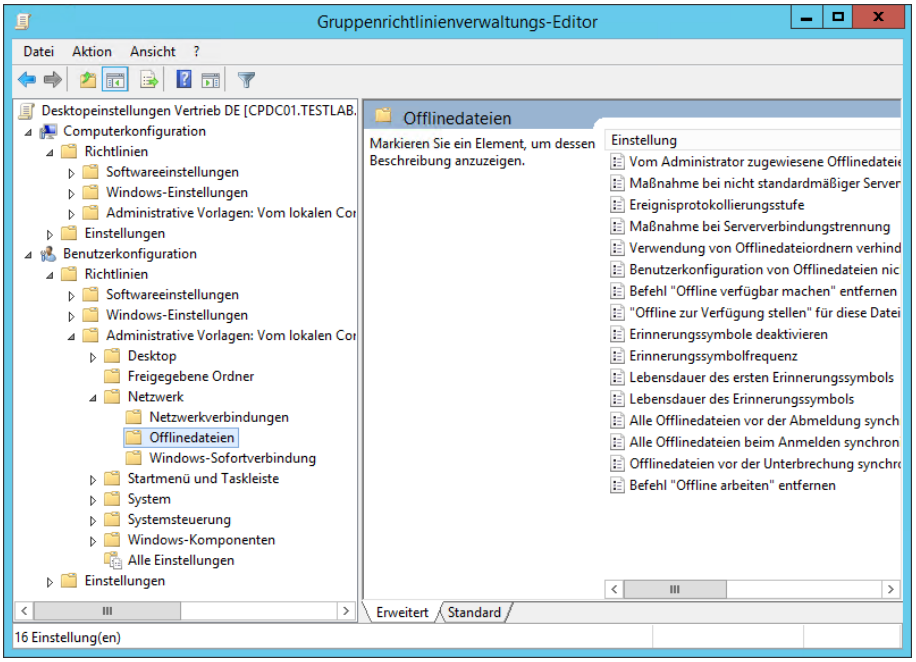

Abbildung 16.11: *Konfigurierbare Richtlinien innerhalb der administrativen Vorlagen auf Ebene der Computerkonfiguration in der Konsole Gruppenrichtlinienverwaltung*

Administrative Vorlagen als XML-Dateien

Mit der Einführung von Windows Vista wurde das Konzept der Anwendung von administrativen Vorlagen unter Windows vollständig überarbeitet. Nicht dass Windows Vista einfach neue Vorlagen mit sich brachte, nein - die seit Windows Vista bzw. Windows Server 2008 enthaltenen, administrativen Vorlagen sind im XML-Format als .ADMX-Dateien einheitlich in englischer Sprache gespeichert. Um einen jeweils länderbezogenen Einsatz der administrativen Vorlagen in Gruppenrichtlinienobjekten zu ermöglichen, existieren neben den ***ADMX-Dateien*** ebenso noch ***ADML-Dateien*** als Sprachdateien für die jeweiligen, von Microsoft für das jeweilige Betriebssystem unterstützten Landessprachen.

Speicherort von .ADMX-Vorlagen

Die neuen administrativen Vorlagen werden seit Windows Vista und Windows Server 2008, sowie in allen nachfolgenden Windows-Betriebssystemen lokal im folgend Pfad gespeichert:

```
C:\Windows\PolicyDefinitions
```

Unterhalb dieses Ordners findet sich ein jeweils sprachenbezogener, weiterer Ordner (bspw. **`de-DE`** für den Speicherort der deutschen, oder **`en-US`** für den Speicherort der englischen ADML-Datei), in dem die für die administrativen Vorlagen verwendbaren Übersetzungen bereitgestellt werden. Hierdurch ist es möglich, die Gruppenrichtlinien in allen z. B. von

Windows 7, Windows 8/8.1, Windows 10 oder auch Windows Server 2012 (R2), und Windows Server 2016 unterstützten Landessprachen „lesbar" bereitzustellen. Dies freut selbst in Deutschland eine Vielzahl an Administratoren, da diese nach eigener Aussage teils selbst ungern mit englischen administrativen Vorlagen arbeiteten (beispielsweise die administrativen Vorlagen für die Anpassung von Office 2000 oder 2003). Wenn man eine der in den administrativen Vorlagen vorhandenen Richtlinien aufgrund eines möglichen Übersetzungsfehlers falsch definieren würde, so könnte dies mitunter sehr „fürchterliche" Auswirkungen auf die jeweiligen Benutzer und/oder Computer der betreffenden Domäne haben.

Die neuen, XML-basierten, administrativen Vorlagen werden von den Betriebssystemen unter Windows erst seit Windows Vista und Windows Server 2008, sowie allen nachfolgenden Windows-Betriebssystemen verarbeitet. Ältere Windows-Betriebssysteme können diese Art von administrativen Vorlagen nicht verarbeiten. Anders hingegen sieht es mit den „klassischen" administrativen Vorlagen aus. Wenn man in einer Domäne unter Windows Server 2003 die klassischen, administrativen Vorlagen verwendet, so sind die neueren Betriebssysteme seit Windows Vista und Windows Server 2008 in der Regel sehr wohl in der Lage, die darin enthaltenen Richtlinien zu verarbeiten. Aber lassen Sie uns erst einmal den Begriff „klassisch" im Bezug auf administrative Vorlagen erörtern.

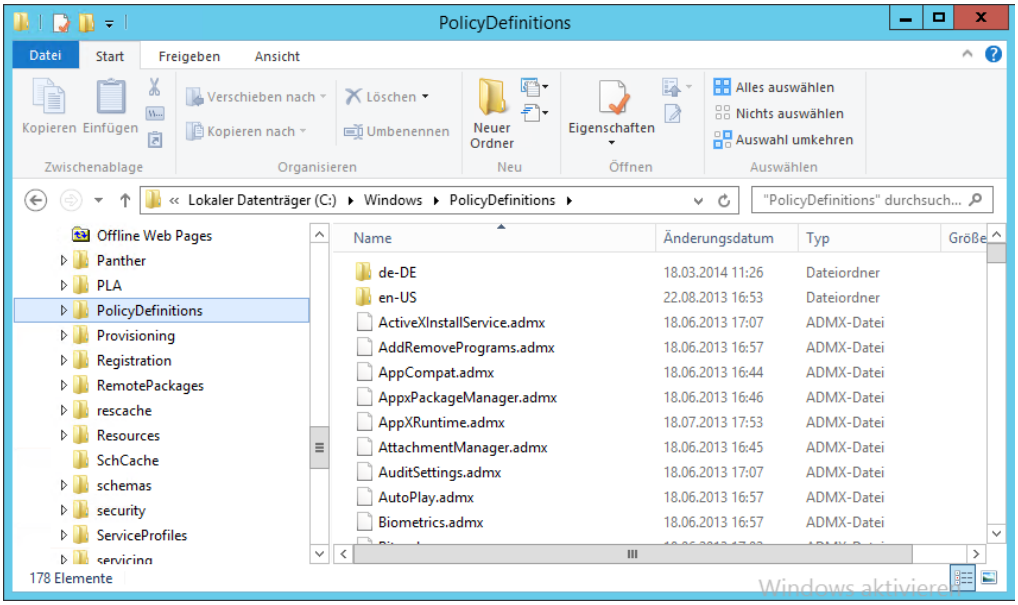

Abbildung 16.12: *Speicherort der administrativen Vorlagen (.ADMX-Dateien) unter Windows Server 2012 R2*

Verbesserungen bei der Verwendung von ADMX-Vorlagen

Bei der Verwendung der klassischen administrativen Vorlagen wurden unter den älteren Windows-Betriebssystemen die in den Gruppenrichtlinienobjekten verwendeten ADM-

Dateien jeweils in das SYSVOL-Verzeichnis des betreffenden Domänencontrollers kopiert, auf welchem das Gruppenrichtlinienobjekt bearbeitet wurde. Diese ADM-Dateien mussten dann anschließend an jeden anderen Domänencontroller in der Domäne repliziert. Hierzu wurde insbesondere in großen Netzwerkumgebungen eine große Menge an Netzwerkbandbreite, sowie auch Festplattenspeicher für die Speicherung von nicht selten dutzenden bis zu hunderten von Gruppenrichtlinienobjekten verschwendet. Seit der Einführung von Windows Vista hat Microsoft hier endlich eine Verbesserung geschaffen.

Wenn man ein domänenbasiertes Gruppenrichtlinienobjekt auf einem Server unter Windows Server 2008 (R2), Windows Server 2012 (R2), Windows 2016 oder auf der Arbeitsstation unter Windows 7, 8/8.1 oder Windows 10 erstellt, so werden die administrativen Vorlagen für die in dem Gruppenrichtlinienverwaltungs-Editor (bzw. Gruppenrichtlinienobjekt-Editor) angezeigten Richtlinien standardmäßig aus dessen jeweils lokalem Verzeichnis *C:\Windows\PolicyDefinition* geladen. Die ADMX- und die zugehörigen ADML-Dateien werden nicht in das Verzeichnis SYSVOL auf dem Domänencontroller kopiert. Auf diese wird lediglich lokal verwiesen, wodurch die Netzwerkbelastung und auch der Speicherverbrauch für die Bereitstellung von mitunter vielen hunderten Gruppenrichtlinien reduziert werden.

Hinzufügen von Gruppenrichtlinienvorlagen für Windows 10-Computer

Windows 10 wurde bekanntlich nach Windows 8.1 und Windows Server 2012 R2 auf den Markt gebracht. In dem neuesten Betriebssystem finden sich viele Neuerungen und Verbesserungen, die sich auch in den lokalen Gruppenrichtlinieneinstellungen des jeweiligen Computersystems unter Windows 10 verwalten lassen. Erst einmal problematisch ist wiegt hierbei der Umstand, dass die Domänencontroller unter Windows Server 2012 R2 mit den ganzen Neuerungen in Windows 10 richtlinientechnisch betrachtet noch nicht viel anfangen können.

Damit man die neuen Einstellungen in den Gruppenrichtlinien von Windows 10 auch zentral mittels Gruppenrichtlinienobjekten in einer Active Directory-Domäne verwalten kann, muss man sich zunächst die von Microsoft dazu veröffentlichten Gruppenrichtlinienvorlagen aus dem Internet herunterladen.

INTERNET: Die Administrativen Vorlagen der Gruppenrichtlinieneinstellungen für Windows 10 kann man kostenfrei aus dem Internet herunterladen unter:

https://www.microsoft.com/de-DE/download/details.aspx?id=48257

Nach dem Herunterladen kann man diese einfach auspacken und in das entsprechende Verzeichnis auf dem Domänencontroller kopieren unter:

C:\Windows\PolicyDefinitions

Nach dem Kopieren der Administrativen Vorlagen-Dateien für Windows 10 stehen diese gleich beim nächsten Aufruf der Konsole Gruppenrichtlinienverwaltung zur Verfügung, und können ganz nach Bedarf auf Computersysteme unter Windows 10 angewendet werden.

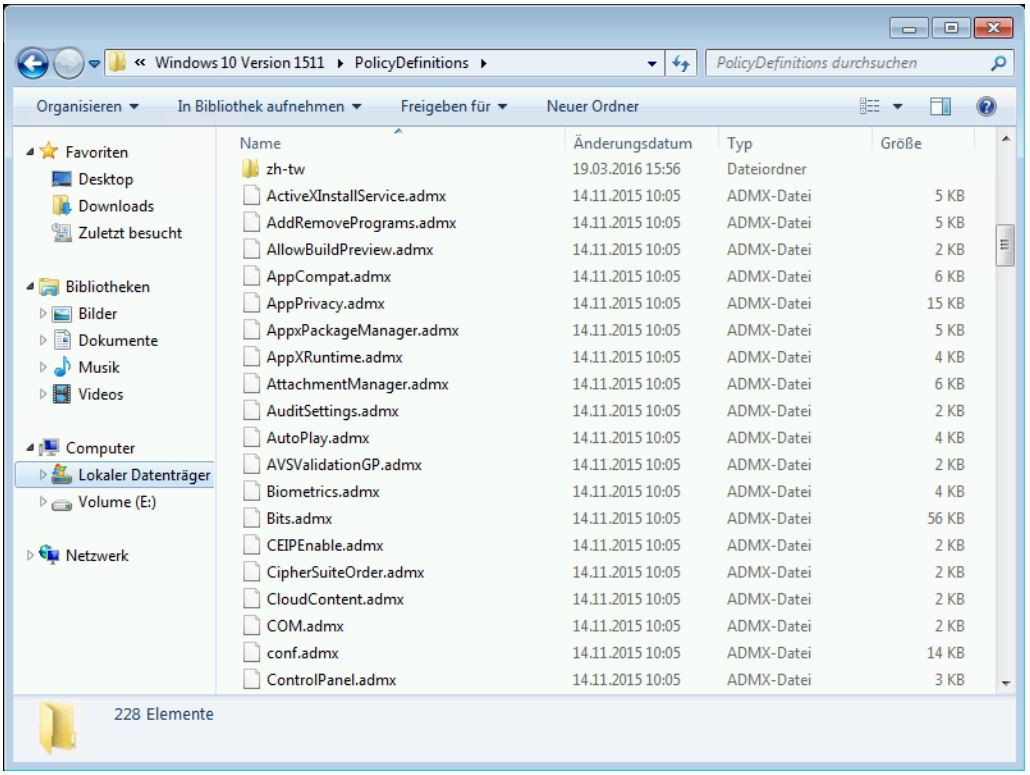

Abbildung 16.13: *Administrativen Vorlagen (.ADMX- und -ADML-Dateien) für Windows 10*

Einrichten eines zentralen Speichers

Bereits schon seit der Einführung von Windows Vista und Windows Server 2008 unterstützen die Windows-Betriebssysteme die Einrichtung eines zentralen Speichers, der als Repository für administrative Vorlagen dient. Dieser Speicher dient als Netzwerkspeicherort für alle offiziellen ADMX- und ADML-Dateien (und alle benutzerdefinierten ADMX- und ADML-Dateien, die man selbst erstellt hat). Somit wird die wirksame Kontrolle der ADMX-Dateien für die Bearbeitung von Gruppenrichtlinien möglich. Nach dem Einrichten eines zentralen Speichers verweist die anschließende Bearbeitung von Gruppenrichtlinien, z.B. unter Windows 7 oder Windows Server 2012 (R2), automatisch auf diesen und nutzt somit die netzwerkbasierten Versionen statt der jeweils lokal gespeicherten Versionen. Die Inhalte des Verzeichnisses *SYSVOL* werden zwischen allen Domänencontrollern der jeweiligen Domäne automatisch repliziert.

Das Einrichten eines zentralen Speichers kann mit einfachen Schritten durchgeführt werden. Gehen Sie wie folgt vor, um einen zentralen Speicher auf einem Domänencontroller zu erstellen:

1. Öffnen Sie den Windows Explorer und navigieren Sie zum freigegebenen Ordner ***sysvol*** (standardmäßig ***C:\Windows\SYSVOL\sysvol***).

HINWEIS: Die Konsole *Gruppenrichtlinienverwaltung* verbindet sich beim Start standardmäßig mit dem Domänencontroller, der als *PDC-Emulator* konfiguriert ist. Deshalb sollte man auch den zentralen Speichers auf diesem Server erstellen. Die darin nachfolgend enthaltenen Richtlinienvorlagen können auf diesem Server noch vor der Replikation des SYSVOL-Verzeichnisses zu anderen Domänencontrollern bei der Bearbeitung von Gruppenrichtlinienobjekten aus dem zentralen Speicher genutzt werden.

2. Erstellen Sie in dem Ordner ***sysvol*** ein neues Verzeichnis mit der Namensbezeichnung ***PolicyDefinitions***.
3. Kopieren Sie den kompletten Inhalt des lokal vorhandenen Ordners **C:\Windows\PolicyDefintions** einer Arbeitsstation unter Windows 8/8.1 oder 10 bzw. eines Serversystems unter Windows Server 2012 (R2) (inklusive aller darin enthaltenen Dateien) mitsamt der darin ebenso enthaltenen, untergeordneten Verzeichnisse für die jeweiligen Sprachversionen (beispielsweise **de-DE**) und deren gesamten Inhalt (sprachabhängige ADML-Dateien) in den im Ordner ***sysvol*** neu angelegten Ordner ***PolicyDefinitions***.

Beim nächsten Aufruf der Konsole ***Gruppenrichtlinienverwaltung*** erkennt diese den vorweg eingerichteten zentralen Speicher im SYSVOL-Verzeichnis auf dem Domänencontroller und verwendet dann die auf dem Server bereitgestellten Richtlinienvorlagen bei der anschließenden Gruppenrichtlinienverwaltung. Die auf dem jeweiligen, für das Erstellen und Verwalten von Gruppenrichtlinien genutzten Rechner lokal gespeicherten administrativen Vorlagen werden dabei vollständig ignoriert.

16.5.2 Klassische administrative Vorlagen

Bereits in den früheren Windows-Betriebssystemen, wie Windows 2000 wurden administrative Vorlagen verwendet, um bestimmte Richtlinieneinstellungen im Netzwerk bereitzustellen. Diese wurden als administrative Vorlagen in einem bestimmten, programmierähnlichen Inhaltsformat bereitgestellt, in dem es galt, sich an bestimmten, vordefinierten Abschnitten und Kategorien zu orientieren. Da ein solcher Aufbau von administrativen Vorlagen bereits bei der ursprünglichen Einführung von Gruppenrichtlinien bereitgestellt und verarbeitet wurde, bezeichnet man diese als „klassische", administrative Vorlagen.

Die klassischen administrativen Vorlagen werden als .ADM-Dateien gespeichert und können zu den Gruppenrichtlinienobjekten in einer Active Directory-Domäne hinzugefügt oder bei Bedarf auch aus diesen entfernt werden.

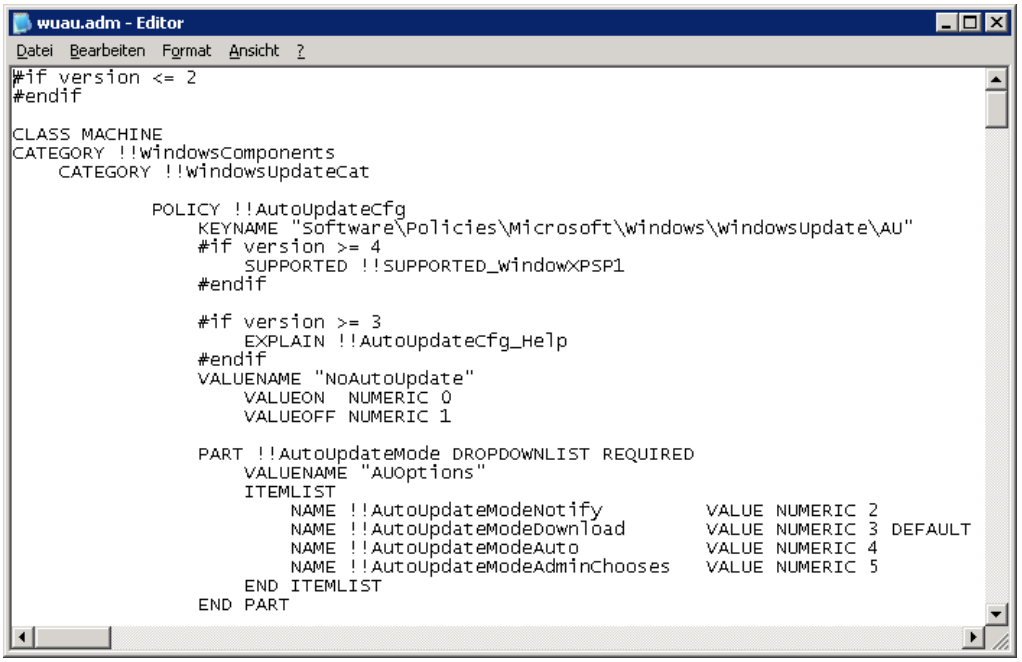

Abbildung 16.14: *Beispiel für den Aufbau einer klassischen administrativen Vorlage (Datei WUAU.ADM) unter Windows Server 2003*

Standardmäßige ADM-Vorlagen

Windows Server 2003 enthält bereits verschiedene administrative Vorlagendateien. Diese werden standardmäßig im Pfad ***%SystemRoot%\Inf*** (standardmäßig *C:\Windows\Inf*) gespeichert. Die folgende Tabelle enthält eine Übersicht, sowie den Verwendungszweck der in Windows Server 2003 standardmäßig vorhandenen, klassischen, administrativen Vorlagen (ADM-Dateien):

Vorlagendatei	Verwendungszweck
Conf.adm	Stellt Einstellungen für NetMeeting bereit.
Inetset.adm und Inetres.adm	Stellen Einstellungen im Rahmen der Internet Explorer-Wartung direkt über die administrativen Vorlagen bereit.
System.adm	Dies ist die umfangreichste und komplexeste Vorlage, mit der die meisten der möglichen Einstellungen zum System, dem Internet Explorer und weiteren Komponenten bereitgestellt werden.
Wmplayer.adm	Stellt Einstellungen für den Windows Media Player bereit.
Wuau.adm	Mit dieser Vorlage werden Einstellungen der clientseitigen Konfiguration für die Verwendung von Windows Server Update Services (WSUS) sowie auch der Software Update Services (SUS) bereitgestellt.

spielsweise erstellt man Active Directory-Standorte um den Clientanmeldeverkehr für Mitarbeiter an einem kleineren Unternehmensstandort mit geringer WAN-Bandbreite zum Firmenhauptsitz zu steuern.

20.2 Erstellen eines Active Directory-Standorts

Standardmäßig wird in einer neuen Implementierung einer Active Directory-Gesamtstruktur ein Standort mit dem Namen „***Standardname-des-ersten-Standorts***" (engl. *Default-First-Site-Name*) erstellt. Diesem Standort werden alle in der Gesamtstruktur installierten Domänencontroller aller vorhandenen Domänen zugeordnet. Im Bedarfsfall kann man (insbesondere für kleinere Standorte mit geringer WAN-Bandbreite) jederzeit neue Active Directory-Standorte erstellen. Einem solchen Standort ordnet man in der Regel nachfolgend ein oder mehrere Domänencontroller bzw. Server mit bestimmten Active Directory-basierten Applikationen zu.

Um einen neuen Active Directory-Standort einrichten zu können, muss man mindestens Mitglied der Gruppe der Organisations-Admins oder Domänen-Admins der Stammdomäne der Gesamtstruktur bzw. einer entsprechend delegierten Sicherheitsgruppe sein. Gehen Sie wie folgt vor, um einen neuen Active Directory-Standort unter Windows Server 2012 R2 zu erstellen:

1. Öffnen Sie die Konsole *Active Directory-Standorte und -Dienste*.
2. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf *Standorte (Sites)*, und wählen Sie im Kontextmenü den Eintrag **Neuer Standort...**
3. Geben Sie im Feld *Name* den gewünschten Namen des neuen Standorts ein.
4. Klicken Sie unter *Verknüpfungsnam*E auf ein Standortlinkobjekt (bspw. *DEFAULTIPSITELINK*), und klicken Sie dann auf **OK**.

Nachfolgend erscheint ein Hinweis, dass der Active Directory-Standort erstellt wurde. Darüber hinaus wird man u. a. darauf hingewiesen, dass man die in dem Standort vorhandenen Subnetze dem Subnetz-Container zufügen soll. Die notwendigen Konfigurationsschritte hierzu erfahren Sie in den nächsten Seiten.

HINWEIS: Der Name eines Active Directory-Standorts darf keine Leerzeichen enthalten. Man kann mehrere Begriffe innerhalb des Namens jedoch problemlos mit einem Bindestrich (-) miteinander verbinden. Beispielsweise kann der Name „*Standort München*" nicht verwendet werden, jedoch akzeptiert Active Directory den Namen in der Schreibform als „*Standort-München*". Dies sollten Sie bei der Standortplanung berücksichtigen.

20.3 Erstellen eines Subnet-Objektes

Um eine Standortzuordnung von Client- und Serversystemen zu ermöglichen, muss man die in dem jeweils physikalischen Standort vorhandenen IP-Subnetze als Active Directory-Objekte anlegen und dabei dem jeweiligen Active Directory-Standort zuweisen. Neu ist seit

Windows Server 2008 und höher hierbei die Unterstützung von IPv6-Subnetzen neben den bisher verwendeten IPv4-Subnetzen.

HINWEIS: Um neue Active Directory-Subnetze einrichten zu können, muss man mindestens Mitglied der Gruppe der *Organisations-Admins* oder Domänen-Admins der *Stammdomäne der Gesamtstruktur* bzw. einer entsprechend delegierten Sicherheitsgruppe sein.

Gehen Sie wie folgt vor, um ein neues Subnet-Objekt in Active Directory unter Windows Server 2012 R2 zu erstellen:

1. Öffnen Sie die Konsole *Active Directory-Standorte und -Dienste*.
2. Doppelklicken Sie in der Konsolenstruktur auf den Container **Standorte (Sites)**, klicken Sie dann mit der rechten Maustaste auf **Subnetze (Subnets)**, und wählen Sie im Kontextmenü den Eintrag **Neues Subnetz...**
3. Geben Sie im Feld *Präfix* das zutreffende ***IP-Adresspräfix*** an, klicken Sie im Abschnitt *Standortobjekt für dieses Präfix auswählen* auf den gewünschten Standort, und dann auf **OK**.

20.4 Erstellen einer Standortverknüpfung

Nachdem in der Active Directory-Gesamtstruktur neue Active Directory-Standorte erstellt wurden, ist es nun an der Zeit, diese logisch miteinander zu verknüpfen. In Active Directory-Standorten, welche mithilfe einer Standortverknüpfung (*Site Link*) direkt miteinander verbunden sind, nutzen die Domänencontroller diese Verknüpfungen für die Replikation untereinander. Man definiert anhand der Standortverknüpfungen die möglichen Replikationspfade.

Wie bereits bei den Standorten und den Subnetzen muss man auch zum Erstellen von Standortverknüpfungen mindestens Mitglied der Gruppe der Organisations-Admins oder Domänen-Admins der Stammdomäne der Gesamtstruktur bzw. einer entsprechend delegierten
Sicherheitsgruppe sein.

Um eine neuen Standortverknüpfung (*Site Link*) in einer Active Directory-Gesamtstruktur einzurichten, gehen Sie wie folgt vor:

1. Öffnen Sie die Konsole *Active Directory-Standorte und -Dienste*.
2. Erweitern Sie in der Konsolenstruktur den Container *Sites (Standorte), Inter-Site-Transports (Standortübergreifender Transport)* und klicken Sie mit der rechten Maustaste auf **IP** oder **SMTP**. Wählen Sie im Kontextmenü den Eintrag **Neue Standortverknüpfung...**
3. Geben Sie im Feld *Name* den Namen der neu zu erstellenden Standortverknüpfung (*Site Link*) an.
4. Markieren Sie im linken Feld unter *Standorte außerhalb dieser Standortverknüpfung* die gewünschten Standortnamen und klicken Sie dann auf **Hinzufügen**.
5. Klicken Sie zum Abschluss auf **OK**.

Die neue Standortverknüpfung (*Site Link*) wird nach dem Erstellen in der Konsole *Active Directory-Standorte und -Dienste* angezeigt.

Natürlich kann es nachfolgend jederzeit notwendig werden, weitere Active Directory-Standorte zu einer bereits vorhandenen Standortverknüpfung hinzuzufügen bzw. diese aus der entsprechenden Standortverknüpfung zu entfernen. Wie bereits beim Erstellen von Standorten, Subnetzen und Standortverknüpfungen muss man auch zum Verwalten von Standortverknüpfungen mindestens Mitglied der Gruppe der *Organisations-Admins* oder *Domänen-Admins* der *Stammdomäne der Gesamtstruktur* bzw. einer entsprechend delegierten Sicherheitsgruppe sein.

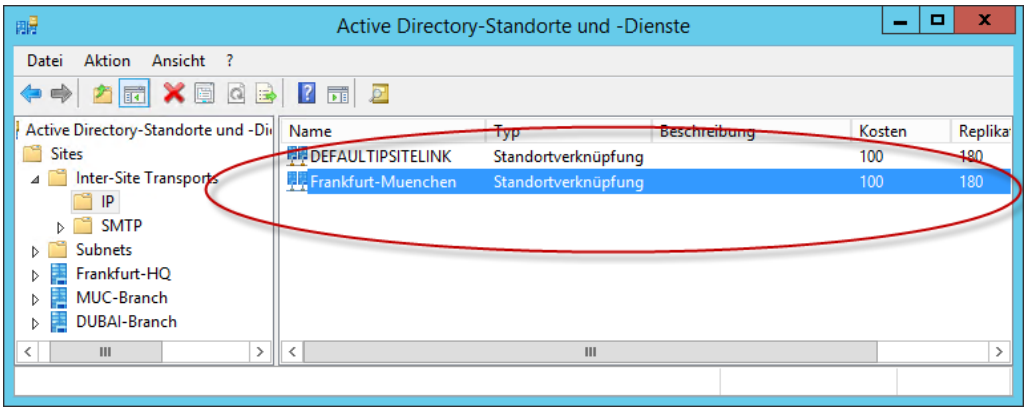

Abbildung 20.1: *Neu erstellte Standortverknüpfung (Site Link)*

20.4.1 Hinzufügen eines Standorts zu einer Standortverknüpfung

Gehen Sie wie folgt vor, um einen Standort zu einer bestehenden Standortverknüpfung hinzufügen:

1. Öffnen Sie die Konsole *Active Directory-Standorte und -Dienste*.
2. Erweitern Sie in der Konsolenstruktur die Container *Sites (Standorte)*, *Inter-Site-Transports (Standortübergreifender Transport)* und *IP* (oder *SMTP*).
3. Klicken Sie mit der rechten Maustaste auf das entsprechende Standortverknüpfungsobjekt, und wählen Sie im Kontextmenü den Eintrag **Eigenschaften**
4. Klicken Sie im Feld *Standorte außerhalb dieser Standortverknüpfung*: den gewünschten Standortnamen an, und klicken Sie dann auf **Hinzufügen**.

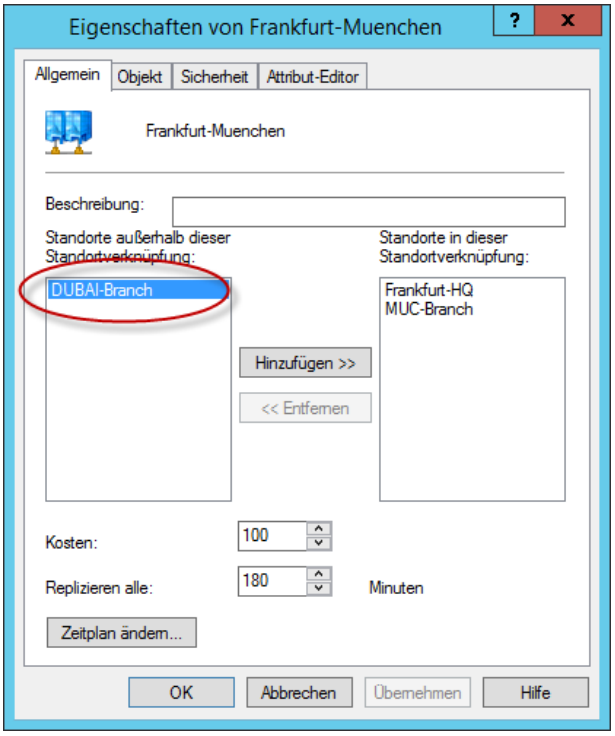

Abbildung 20.2: *Auswahl eines Standorts außerhalb der Standortverknüpfung*

5. Der Standort wird in der Liste der *Standorte in dieser Standortverknüpfung* angezeigt.
6. Klicken Sie zum Abschluss auf **OK**.

20.4.2 Entfernen von Standorten aus einer Standortverknüpfung

Gehen Sie wie folgt vor, um einen Standort aus einer bestehenden Standortverknüpfung zu entfernen:

1. Öffnen Sie die Konsole *Active Directory-Standorte und -Dienste*.
2. Erweitern Sie in der Konsolenstruktur die Container *Sites (Standorte)*, *Inter-Site-Transports (Standortübergreifender Transport)* und IP (oder SMTP).
3. Klicken Sie mit der rechten Maustaste auf das entsprechende Standortverknüpfungsobjekt, und wählen Sie im Kontextmenü den Eintrag ***Eigenschaften***
4. Klicken Sie im Feld *Standorte in dieser Standortverknüpfung:* den gewünschten Standortnamen an, und klicken Sie dann auf ***Entfernen***.

„Windows Server 2008 R2" der Active Directory-Gesamtstruktur. Dies bedeutet, dass sich alle Domänen innerhalb der Active Directory-Gesamtstruktur in der *Domänenfunktionsebene „Windows Server 2008 R2"* und damit ebenso auch alle Domänencontroller mindestens auf Ebene des Betriebssystems Windows Server 2008 R2, Windows Server 2012 oder Windows Server 2012 R2 befinden müssen. Erst dann kann man den Active Directory-Papierkorb u. a. im Active Directory-Verwaltungscenter (AD AC) oder alternativ mithilfe der Windows PowerShell aktivieren.

WICHTIG! Das Aktivieren des Active Directory-Papierkorbs in einer Active Directory-Gesamtstruktur kann zu einem späteren Zeitpunkt nicht mehr rückgängig gemacht werden.

22.6.1 Schritte zum Aktivieren des Active Directory-Papierkorbs

Gehen Sie wie folgt vor, um den Active Directory-Papierkorb im Active Directory-Verwaltungscenter (AD AC) auf einem Server unter Windows Server 2012 R2 zu aktivieren:

1. Melden Sie sich als *Administrator* am Domänencontroller an.
2. Öffnen Sie den *Server-Manager* (soweit dies nicht automatisch geschieht) über einen Klick in der *Taskleiste* auf das **Symbol für den Server-Manager** bzw. im *Startbildschirm* auf die entsprechende **Kachel**.
3. Klicken Sie oben im *Server-Manager* auf **Tools**, und dann auf Active Directory-**Verwaltungscenter**.
4. Klicken Sie im Active Directory-Verwaltungscenter mit der rechten Maustaste auf den *Domänennamen*, und wählen Sie im Kontextmenü die Option **Papierkorb aktivieren...**

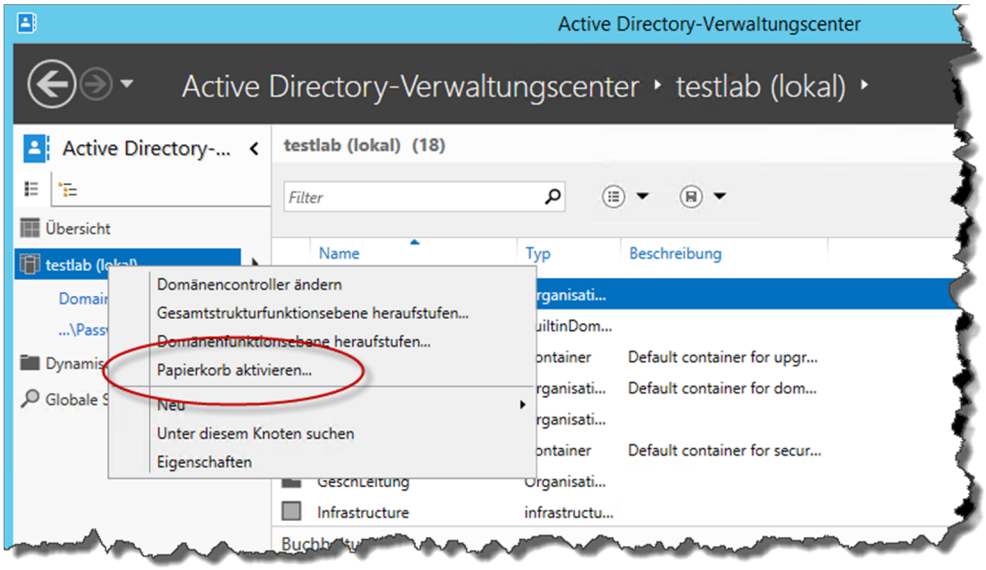

Abbildung 22.6: *Aktivieren des Active Directory-Papierkorbs im Active Directory-Verwaltungscenter von Windows Server 2012 R2*

5. Bestätigen Sie die Meldung, dass der Papierkorb nach der Aktivierung nicht mehr deaktiviert werden kann, durch einen Klick auf **OK**.
6. Bestätigen Sie den Dialog zur notwendigen Aktualisierung des Active Directory-Verwaltungscenters mit einem Klick auf **OK**.

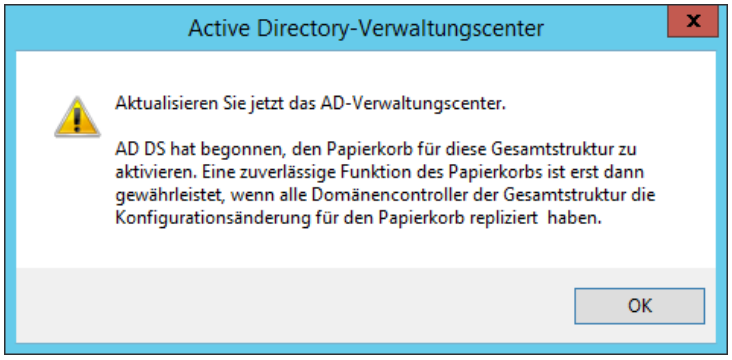

Abbildung 22.7: *Hinweis auf die Notwendigkeit der Aktualisierung des Active Directory-Verwaltungscenters während der Aktivierung des Active Directory-Papierkorbs*

HINWEIS: Nach der Aktivierung des Active Directory-Papierkorbs muss, wie dies in der vorangegangenen Meldung auch aufgezeigt wurde, die Replikation in der Active Directory-Gesamtstruktur zwischen den einzelnen, darin vorhandenen Domänencontrollern durchgeführt werden. Erst im Anschluss ist sichergestellt, dass man (versehentlich) gelöschte Active Directory-Objekt zuverlässig wieder herstellen kann.

Aktivierung des Active Directory-Papierkorbs mittels Windows PowerShell

Alternativ zur Aktivierung des Active Directory-Papierkorbs im Active Directory-Verwaltungscenter kann dies ebenso auch in der Windows PowerShell unter Windows Server 2012 R2 erfolgen. Verwenden Sie dazu den folgenden Befehl:

```
Enable-ADOptionalFeature –Identity 'CN=Recycle Bin Feature,
CN=Optional Features,CN=Directory Service,CN=Windows NT,
CN=Services,CN=Configuration,DC=CertPro,DC=local' –Scope
ForestOrConfigurationSet –Target 'certpro.local'
```

HINWEIS: In dem aufgeführten Beispiel wird der Active Directory-Papierkorb für die Domäne *CertPro.local* als optionales Features aktiviert. Um diesen Befehl anwenden zu können, muss zuvor das Active Directory-Modul für Windows PowerShell geladen werden.

22.6.2 Anzeigen und Wiederherstellen gelöschter Active Directory-Objekte

Die gelöschten Objekte in den Active Directory-Domänendiensten (AD DS) unter Windows Server 2012 R2 werden nach der Aktivierung des Active Directory-Papierkorbs im Active Directory-Verwaltungscenter unterhalb der jeweiligen Domäne im Container *Deleted Objects* angezeigt.

Die gelöschten Active Directory-Objekte lassen sich i.d.R. problemlos mittels eines Klicks mit der rechten Maustaste, und der Auswahl der entsprechenden Option *Wiederherstellen*... bzw. *Wiederherstellen in*... aus dem Papierkorb (sprich: dem Container „*Deleted Objects*") zurückholen. Die Option *Wiederherstellen in*... ermöglicht es alternativ, das zuvor gelöschte Active Directory-Objekt bei Bedarf in einem anderen als dem ursprünglichen Container in der Active Directory-Datenbank wieder herzustellen.

Anzeigen und Wiederherstellen mittels Windows PowerShell

Alternativ zum grafischen Active Directory-Papierkorb kann man gelöschte Objekte auch mithilfe der Windows PowerShell anzeigen oder auch gleich wiederherstellen lassen. Verwenden Sie zum Anzeigen eines gelöschten Objekts einfach den folgenden Befehl:

```
Get-ADObject -Filter {displayName -eq „Carlo Westbrook"}
-IncludeDeletedObjects
```

Um ein gelöschtes Objekt wieder herzustellen, kann man einfach den folgenden Befehl verwenden:

ADM-Vorlagen · 558
ADMX-Vorlagen · 552
  Speicherort von · 551
adprep · 573
Adprep /domainprep · 235, 284
Adprep /forestprep · 234, 284
adprep.exe · 234, 236, 283, 284
adprep32.exe · 234, 283
AdRestore.exe · 678
Aktivierung · 273
Aktualisierungspfade · 279
Alterungs- und Aufräumprozess · 121, 315
Anforderungsfilter · 562
Anmeldebildschirm · 291
Anmeldeskripts
  Anwenden von · 539
Anmeldeversuch · 356
Anwendungs- und Dienstprotokolle · 292
Anwendungsverzeichnispartition · 573
  Berechtigungen für DNS · 577
Attribut · 595
Attribut-Editor · 418
Authentifizierte Konten · 597
Authentifizierung · 356
Autorisierenden Wiederherstellung · 673
Autoritätsursprung (SOA) · 309

B

Backup Domain Controllers, BDCs Siehe Sicherungsdomänencontroller ·
Backup-GPO · 523
Base Line · *Siehe* Basislinie
Basisline · 649
Basisverzeichnisse · 426
Bedingte Weiterleitungen · 318
Benutzer · 210
Benutzeranmeldung · 593
Benutzerkonten
  Deaktivieren bzw. Aktivieren von · 424
  Entsperren von · 421
  Kopieren von · 419
  Löschen von · 425
Benutzerkontenkennwörter · 574
Benutzerobjekte · 202, 418
  Erstellen von · 415
Benutzerprofile · 426
Besondere Identitäten · 217
Betriebsmasterrollen · 69, 193, 575
  Übertragen der · 364
  Verschieben von · 359
  Verwaltung der · 354
Betriebssystemeditionen · 261
BIND-Sekundärzonen · 310
BIND-Server · 310
BIND-Versionen · 310
BIOS · 266
Boot-Laufwerk · 266
Boot-Menü · 666

C

CA · *Siehe* Zertifizierungsstelle
CAB-Dateien · 486
Certificate Authority · *Siehe* Zertifizierungsstelle
Circular Logging · 660
Clientanmeldeverkehr · 632
Client-Side Extensions, CSEs · 529
Closed Set · 252
Clusterdienste-Informationen · 667
COM+-Klassenregistrierungsdatenbank · 667
Common.adm · 557
Computerkonto · 302
Computerobjekte · 218
  Verwalten von · 449
Conf.adm · 556
ConfirmGc · 332
control
  intl.cpl · 603
  timedate.cpl · 603
ConvertTo-SecureString · 630
cscript · 603
csvde.exe · 409, 441

D

Datacenter-Lizenz · 263
DATENSAMMLERSÄTZE · 652
Datensicherung · 666
  Durchführung der · 662

Datenspeicherungsmodell · 61
Datenwiederherstellung
Durchführung einer · 665
Dcdiag.exe · 641, 646
DcGPOFix.exe · 485
dcpromo.exe · 323, 627, 668
Unbeaufsichtigte Installation mittels · 628
Default Domain Controllers Policy · 142, 460
Default Domain Policy · 142, 460
DefaultGateway · 612
DEFAULTIPSITELINK · 632
delegierte RODC-Installation
Durchführung · 588
Delegierung der Verwaltungsberechtigung
Beendigung der · 400
Delegierung der Verwaltungsfunktionalität · 395
Deleted Objects · 682
Desktopdarstellung · 620
DFS-Replikation · 643, 647
DHCP-Server · 314, 610
Dienste · 320
Diensteinträge (SRV Records) · 295
Dienstkonten · 250, 427
Disaster Recovery Plan · Siehe
Notfallwiederherstellungsplan
Discretionary Access Control List (DACL) · 126
Distinguished Name · 653
Distinguished Name (DN) · 55
Distributed COM-Benutzer · 210
DNSAdmins · 212
dnscmd.exe · 625, 626
DNS-Datenbank · 315
DNS-Dienste
Entfernen der · 321
DNS-Einträge · 312, 317
Manuelles Löschen von · 317
DNS-Namensräume · 177
DNS-Namenszonen · 295
Entfernen von · 320
DNS-Ressourceneinträge · 301
DnsServer · 626
DNS-Server
Schreibgeschützter · 574
Server Core als · 624, 625
DNS-Serverrolle
Entfernen der · 626
DNSUpdateProxy · 212, 314, 437
DNS-Zonentypen · 115
Domain Name System (DNS) · 292
Domain Naming Master Siehe
Domänennamenmaster ·
domainprep · 284
Domänen · 97
Domänen-Admins · 213, 360, 437, 594, 598, 634, 644
Domänenaktualisierung · 238
Domänenbenutzer · 213
Domänen-Benutzer · 437
Domänencomputer · 213, 437
Domänencontroller · 142, 213, 235, 284, 437, 594
Klonen von · 47
Maximale Anzahl · 163
Server Core als · 627
Sicherheit · 140
Domänencontroller ohne Schreibzugriff · 594
Domänenfunktionsebene · 112, 226
Domänenfunktionsebenen · 107
Domänengäste · 213
Domänen-Gäste · 437
Domänenkennung · 357
Domänenmodell · 168
Domänennamenmaster · 69, 354, 355
Domänennamensmaster · 193
Domänenstruktur
Entwerfen einer · 168
Domänenstrukturen · 96
Domänenvorbereitung · 235, 284
Dringlichkeitsreplikation (Urgent Replication) · 81
Druckerobjekte · 220
Druck-Operatoren · 210
dsadd · 443
dsadd.exe
Erstellen von Benutzerobjekten · 408
dsget · 417
dsmod.exe · 426
DSRM · *Siehe*
Verzeichnisdienstwiederherstellung-Modus
Dualcore-Prozessor · 260
Dynamische Aktualisierung · 313, 470
Dynamische Updates · 303
Keine · 313
Nicht sichere und sichere · 302, 314
Nur sichere · 302, 314
Dynamische Zugriffssteuerung · 48, 144

E

Effektive Berechtigungen · 399
Eingabemethode · 266
Einmalsicherung · 662
Ereignisablaufverfolgungssitzungen · 652
Ereignisanzeige · 291, 645
Ereignisdetails
  anzeigen · 648
Ereignisprotokoll · 644, 648
  Überprüfung der · 643
Ereignisprotokolle · 647
Ereignisprotokollleser · 210
Ersteller-Besitzer · 548
Erstellungen eingehender
  Gesamtstrukturvertrauensstellung · 210
Erstkonfiguration · 609
Erweiterungen für
  Gruppenrichtlinienvoreinstellungen · 529
Essentials Experience-Serverrolle
  Merkmale der · 48
Extensible Storage Engine (ESE) · 64

F

F8-Taste · 666, 668
Festplatte · 278
Fine Grained Password Policies · 571
Firewall-Konfiguration
  Remoteverwaltung der · 620
Flexible Single Master Operation Roles,
  FSMO-Roles Siehe Betriebsmasterrollen ·
forest Siehe Active Directory-Gesamtstruktur · ,
forestprep · 284
Forward-Lookup-Abfragen · 296
Forward-Lookup-Zone · 114
Forward-Lookup-Zonen · 296
Freigabeberechtigung · 547

G

Gabage Collection-Vorgang · 653
Garbage Collection · 653
Garbage Collection-Prozess · 654
garbageCollPeriod-Attribut · 654
Gäste · 210
Geplante Sicherung · 661, 662
Gesamtstrukturen · 89
Gesamtstrukturfunktionsebene · 226, 573
  Überprüfung der · 576
Gesamtstrukturfunktionsebenen · 109
Gesamtstrukturfunktionsebenenmodus · 679
Gesamtstrukturinterne Migration · 251
Gesamtstrukturübergreifende
  Vertrauensstellung · 166
Gesamtstrukturvertrauensstellung · 254
Gesamtstrukturvertrauensstellungen · 252
`Get-ADObject` · 682, 683
Get-ADReplicationFailure · 642
Get-ADReplicationPartnerMetadata · 642
Get-ADReplicationSite · 642
`Get-NetIPInterface` · 611
Get-WindowsFeature · 621
Get-WindowsImage · 622, 625
Global Unique Identifier · 653
Global Uniqueness ID Siehe Globaler
  Bezeichner ·
Globaler Bezeichner · 357
globaler Katalog · 72
Globaler Katalog · 358
globaler Katalogserver · 190
  Verwaltung · 373
Globaler Katalogserver · 574
GPResult.exe · 510
gpupdate.exe · 475
grafische Benutzeroberfläche
  Entfernen der · 623
Group Managed Service Accounts, gMSA · 428
Gruppen
  domänenlokale · 434
  globale · 434
  universelle · 434
Gruppenbereiche · 433
Gruppenobjekte · 206, 432
Gruppenrichtlinien
  Erzwingen von · 499
Gruppenrichtlinienaktualisierungsprozess · 470
Gruppenrichtliniencontainer · 462
Gruppenrichtlinieneinstellungen
  Konfigurieren der · 527
Gruppenrichtlinienergebnis-Assistent
  Verwenden des · 513
Gruppenrichtlinienmodellierungs-Assistent
  Verwendung des · 516
Gruppenrichtlinienobjekte

Arbeiten mit · 482
Bearbeiten von · 483
Löschen von · 484
Verknüpfung von · 493
Gruppenrichtlinienupdate · 465
Gruppenrichtlinienvererbung · 497
Gruppenrichtlinienverknüpfung
Deaktivieren der · 495
Gruppenrichtlinienverwaltung · 555
Delegierung der · 507
Gruppenrichtlinienverwaltungskonsole (GPMC) · 479
Gruppenrichtlinienvorlagen
Komponenten von · 464
Gruppenstrategien · 438
Gruppenverwaltete Dienstkonten · 428

H

Hardware-Komponenten · 278
Heraufstufen eines Serversystems · 294
Hinzufügen
von Serverrollen · 324
Histogrammleiste · 649
Hosteinträge (A-Records) · 295
Hyper-V-Administratoren · 435

I

IIS_IUSRS · 210
Implementierungsszenarien
Implementierungsszenarien · 689
Indikatoren
Hinzufügen von · 650
Inetcorp.adm · 557
InetOrgPerson-Objekte · 205, 431
Infrastructure Master Siehe
Infrastrukturmaster ·
Infrastrukturmaster · 71, 193, 354, 357
Inplace-Upgrade · 232
Install from Media (IFM) · 334
install.wim · 623
`Install-ADDSDomainController` · 630
Installationsarten · 323
Installations-DVD · 234, 235, 236, 266, 283
Installationsmedium
Erstellen eines · 334
InstallDNS · 332
Install-WindowsFeature · 330, 623, 625, 629
Internet Explorer · 621
Inter-Site Topology Generator · 80
IPSec-Verschlüsselung · 307
IPv4 Reverse-Lookupzone · 306
IPv6 Reverse-Lookupzone · 306
IPv6-Subnetze · 633
IPv6-Unterstützung · 465

K

Kennwortänderungen · 356
Kennwortcache · 598
Kennwortcache für RODCs
Auffüllen des · 598
Kennworteinstellungen
Auswertelogik · 567
Erstellen von Objekten für · 569
Funktionsweise · 567
Kennwörter · 592
Kennwortreplikation
Verwaltung der · 595
Kennwortreplikationsrichtlinie · 592, 595, 596
Verwaltung der · 592
Kennwortzwischenspeicherung
Überprüfen der · 599
Kerberos · 637
Kerberos V5-Protokoll · 128
Key Distribution Center, KDC · 128
Key Management Service, KMS Siehe
Schlüsselverwaltungsdienst ·
Klassische administrative Vorlagen · 555
Klist.exe · 133
Klonbare Domänencontroller · 438
Kommunikationsports · 637
Konfigurationsinformationen · 265, 280
Konsistenz · 657
Konsole Leistung · 645
Kontaktobjekte · 206
Kontakt-Objekte · 431
Konten-Operatoren · 210, 595
Kontingente · 415
krbtgt · 594
Kryptografie-Operatoren · 210

L

Langsame Netzwerkverbindung · 515
Latenz · 639
Laufwerkszuordnungen
  Konfiguration von · 532
LDAP · 637, 686
LDAP Uniform Resource Locator (URL) · 55
ldifde.exe · 411, 412, 441
Ldp.exe · 676
Leistungsprotokollbenutzer · 210
Leistungsüberwachung · 649
Leistungsüberwachungsbenutzer · 211
Lightweight Directory Access Protocol (LDAP) · 54
Liste der Namensserver · 308
Lokale USN · 82
Loopbackverarbeitungsmodus · 477

M

Managed Service Accounts GUI · 431
Man-in-the-Middle-Attacke · 307
Manuelle Sicherung · 660
Master-DNS-Server · 297, 307
Mehrfachaktivierungsschlüssel · 274
Mehrfachaktivierungsschlüssel (MAK) · 275
Messagingdienst · 638
Microsoft Azure · 664
Microsoft Disk Quota · 474
Microsoft Management Console (MMC) · 621
Microsoft Security Compliance Manager (SCM) · 139
Microsoft System Center Operations Manager (SCOM) · 648
Migrationspfade · 238
Mitgliedsserver · 230
msDS-NeverRevealGroup · 594
msDS-Reveal-OnDemandGroup · 594
Multimaster-Replikation · 81
Multiple Activation Key, MAK Siehe Mehrfachaktivierungsschlüssel ·

N

Namensauflösung · 295
Namensraum · 295
Namensuffix-Routing · 253
net stop ntds · 658
NetBIOS-Namensauflösung · 317
netdom · 614, 615
  query fsmo · 360
netdom.exe
  Beitreten zur Domäne mit · 617
  renamecomputer · 615
Netlogon · 333
netsh · 610, 614
Netzwerkfreigaben · 661
Netzwerkkonfigurations-Operatoren · 211
Neuinstallation
  des Servers · 278
Neustrukturierung · 238
`new-ADGroup` · 444
`New-ADServiceAccount` · 429
New-NetIPAdress · 611
Nicht autorisierende Wiederherstellung · 666, 670, 674
nltest.exe
  Standortermittlung mit · 640
Notfallwiederherstellungsplan · 660
`nslookup.exe` · 296
ntbackup.exe · 660
NTDS Quota · 418
ntds.dit · 63, 656
ntdsutil.exe · 365, 657
Ntdsutil.exe
  Installationsmedium · 683
NTFS formatiert · 323
NTLM-Protokoll · 133

O

Objektidentifikation · 357
Objektklassen und -attribute · 355
Objektreferenz · 357
Office SharePoint Server 2007 · 292
Offline-Defragmentierung · 655
Online-Backupagent · 664
Online-Defragmentierung · 654
Online-Sicherung · 664

Orderumleitung
Vorteile der · 542
Ordnerumleitung · 541, 548
Organisations-Admins · 213, 360, 594, 634
Organisationseinheiten
Erstellen von · 383
Löschen von · 390
Planen und Erstellen von · 381
Organisationseinheiten (OUs) · 102
Organizational Units, OUs Siehe Organisationseinheit ·

P

PDC-Emulator · 70, 193, 354, 356
PKI · 687
PolicyDefinitions · 555
Prä-Windows 2000-kompatibler Zugriff · 211
PrefixLength · 612
Primäre DNS-Namenszone · 320
Primary Domain Controller Emulator Siehe PDC-Emulator ·
Product Key · 618
Produktaktivierung · 274, 276
Protected Users · 149, 438
PTR Record · 313, 317

R

RAS- und IAS-Server · 213
Read-Only Domain Controller, RODC Siehe Schreibgeschützte Domänencontroller ·
RebootOnCompletion · 332
Relative Distinguished Name (RDN) · 55
Relative Identifier Master Siehe RID-Master ·
Remote Procedure Call · 637
Remoteaktivierung · 618
Remotedesktop-Benutzer · 211
Remoteverwaltung
Konfigurieren der · 619
Rename-Computer · 615
repadmin.exe · 598
Repadmin.exe · 640, 646
Überprüfung der Replikation mit · 640
Replikation · 595, 631, 637, 639
von Kennwörtern · 593
Replikationsdaten · 631
Replikationsdatenverkehr · 636
Replikationsdienst · 77
Replikationshäufigkeit · 636
Replikationsintervall · 636
Replikationskonfiguration · 638
Replikationskonflikte · 83
Replikationslatenz · 356
Replikationsoperator · 211
Replikations-Operator · 436
Replikationstransport · 637
Replikationsvorgänge · 574, 636
reset-ComputerMachinePassword · 452
Restart-Computer · 623, 630
Reverse-Lookup-Zone · 115
Reverse-Lookup-Zonen · 296, 305
Richtlinienaktualisierungsintervall · 471
Richtlinieneinstellungen · 562
Richtlinien-Ersteller-Besitzer · 213, 594
Richtlinienverarbeitungsfolge · 466
RID-Master · 70, 193, 354, 357
RID-Pool · 357
RODC
Platzierung von · 575
RODC-Filter · 574
Rollen und Features entfernen · 624
Rolleninhaber der Betriebsmasterrollen
Ermitteln des · 360
RPC · *Siehe* Remote Procedure Call

S

Sammlungssätze · 645, 651
Schema · 213
Schema-Administratoren · 355
Schema-Admins · 213, 360, 594
Schemamaster · 69, 193
Schema-Master · 354
Schlüsselverwaltungsdienst · 274
Schlüsselverwaltungsdienstschlüssel · 274
Schlüsselwortfilter · 562
Schreibbare Domänencontroller · 578
Schreibgeschützte Active Directory-Datenbank · 573
Schreibgeschützte Domänencontroller · 66, 186, 213
Schreibgeschützte Domänencontroller der Organisation · 213

schreibgeschützter Domänencontroller
Bereitstellen · 575
Verwaltung · 592
sconfig · 613
secedit.exe · 475
Security Identifier · 653
Security Identifier, SID Siehe Sicherheitskennung ·
Semantik-Prüfung · 657
Serielle Schnittstellen · 265, 280
Server Core · 42, 278
Aktivieren von · 618
Domänencontroller als · 143
Erstkonfiguration · 609
Hardware-Anforderungen · 604
unbeaufsichtigte Installation · 608
Serveraktualisierung · 284
SERVERDATACENTER · 625
Serverdokumentation · 333
Server-GUI-Mgmt-Infra · 623
Server-Gui-Shell · 623
Server-Manager · 41, 481, 620, 627
Server-Operatoren · 212, 436, 595
SERVERSTANDARD · 625
Serverwiederherstellung
vollständige · 665
`Set-ADObject` · 673
Set-DNSClientServerAddress · 612
Set-NetIPInterface · 613
Setup.exe · 285
Sichere dynamische Aktualisierung · 118
Sicherheitsfilterung · 500
Sicherheitsgruppe · 632
Sicherheitskennung · 357, 358
Sicherheitskennung (SID)
Beispiel für eine · 124
Sicherheitskonfigurations-Assistent · 141
Sicherheitsprinzipale · 123
Sicherungsdomänencontroller · 356
Sicherungsoperatoren · 212, 595
Sicherungs-Operatoren · 436, 663
SID-Filterung · 166
SID-History · 240
Single-Sign-On (SSO) · 52
Site Link · *Siehe* Standortverknüpfung
SITES · *Siehe* Standorte
Skriptdateien · 540
Speicherorte von · 540
slmgr.vbs · 278, 618
slmgr.vbs -ato · 618
SMB over IP · 637
SMTP · 638
SMTP-Replikation · 638
Software-Updates · 592
SpecOps Password Policy Basic · 571
Stammdomäne · 171
Standardmäßige ADM-Vorlagen · 556
Standardname-des-ersten-Standorts · 632
Standardrichtlinienobjekte · 485
Standardzonen · 296
primäre · 297
sekundäre · 297
Standorte · 631, 638
Standorte (Sites) · 180
Standorttopologie · 180
Standortübergreifende Replikation · 639
Zeitplan für die · 638
Standortverknüpfung · 633, 635
Erstellen einer · 633
Standortverknüpfung (Site Link) · 181
Standortverknüpfungsobjekt · 638
Starter-Gruppenrichtlinienobjekt · 491
Starter-Gruppenrichtlinienobjekte · 486
Importieren und Exportieren · 489
Start-Gruppenrichtlinienobjekte
Neuerungen in · 475
Steuerung der Kennwortreplikation
Liste der verweigerten Objekte · 594
Liste der zulässigen Objekte · 594
Stub-Zonen · 303, 317
Subnet-Objekt · 632
Subnets · *Siehe* Subnetze
Subnetz · 106
Subnetze · 633
System Access Control List (SACL) · 127
System.adm · 556
Systemmonitor · 649
Systemprotokoll · 647
systemstaterecovery · 670
Systemstatusdaten · 667
SYSVOL · 333, 462, 463

T

Tägliche Sicherung · 663
Taskleiste · 621
Telefonische Aktivierung · 277
Terminalserver-Lizenzserver · 212
Ticket-genehmigendes Ticket · 128
Tombstone · 653
Tombstone-Lebensdauer · 671
  ändern · 673
Tombstone-Objekte
  Reanimieren von · 675

U

Überprüfung der erfolgreichen Aktualisierung · 291
Überwachung · 649
Unattend.txt · 625, 628
Unattend.xml · 271
unbeaufsichtigte Installation · 627
Unbeaufsichtigte Installation · 271, 608
Ungeplante Sicherung · 662, 663
Unidirektionale Replikation · 573
Uninstall-WindowsFeature · 624, 627
UNIX/Linux-Servern · 310
Unterbrechungsfreie Stromversorgung Siehe USV-Geräte · ,
Unterstützte Sicherungstypen · 660
Update Sequence Number · 653
Upgrade-Vorgang · 290
UPN-Suffix-Routing · 167
User Principal Name (UPN) · 56
Users · 381
Users-Container · 315
USV-Geräte · 265, 280, 605

V

Veritas BackupExec · 664
Verknüpfungsreihenfolge
  Festlegen der · 496
Vertrauensstellungen · 91
  Bidirektionale, transitive · 92
Verwaltungsfunktionalität
  Delegierung der · 200
Verwaltungsinfrastruktur · 196
Verwaltungsmodell · 196
Verzeichnisdienst · 51
Verzeichnisdienstwiederherstellung-Modus · 666
Verzeichnispartitionen · 88
Virtualisierungsrechte · 262
Virusbefall · 278
Vollständige Serversicherung · 662
Vollständige Serverwiederherstellung · 661
Vollständige Sicherung
  eines Domänencontrollers · 662
Volume Activation · 274
Volume Activation Management Tool (VAMT) · 275
Volumenaktivierung · 274
Vorbereitende Schritte · 280

W

Währungsformat · 266
WAN-Bandbreite · 632
WAN-Verbindung · 575
WAP · *Siehe* Web Application Proxy
Wbadmin.exe · 663
Web Application Proxy · 689
Wiederherstellung des Systemstatus · 661
Wiederherstellung von Dateien · 661
Wiederherstellungsarten · 661
Windows 10 · 144, 231, 620
  Gruppenrichtlinienvorlagen für · 553
Windows 8-Shell · 621
Windows Azure Online Backup · 664
Windows Media Player · 621
Windows PowerShell · 44, 441
Windows Script Host (WSH)
  Erstellen von Benutzerobjekten · 413
Windows Server 2003 · 573
Windows Server Update Services (WSUS) · 286
Windows Server-Sicherung · 662
  Installation der · 661
Windows Store · 621
Windows System Image Manager (WSIM) · 271
Windows.adm · 557
Windows-Autorisierungszugriffsgruppe · 212

Windows-Einstellungen · 532
Windows-Explorer · 621
WindowsServerBackup · 662
Windows-Speicherdiagnose · 266, 281
Windows-Speicherdiagnosetool · 605
Windows-Update · 286
Windows-Wiederherstellungsdatenträger · 661
Winnt.adm · 557
WINS-Forward-Lookup · 317
WINS-Namensabfrage · 318
WINS-Server (Windows Internet Name Service) · 317
WMI-Abfrage · 535
WMI-Filter
  Abfragesyntax · 503
WMI-Filterung · 500, 502
Wmplayer.adm · 556
wscript.exe · 414

X

X.500-Standard · 52
x64-Prozessor · 266
x86-kompatible Treiber · 265, 281

Z

Zeigereintrag (engl. Pointer) · 305
Zeigereinträge (Pointer Records, kurz PTR) · 312
Zeitgeber · 356
zentraler Speicher
  Einrichten · 554
Zertifikatdienst-DCOM-Zugriff · 212
Zertifikate · 687
Zertifikatherausgeber · 213, 594
Zertifizierungsstelle · 687
Zielgruppenadressierung · 534, 536
Zielvolume · 664
Zonenaktualisierung · 317
Zonendatei · 306
Zoneninhalte · 321
Zonentypen · 295
  Active Directory-integrierte Zonen · 295
  Standardzonen (primär oder sekundär) · 295
  Stub-Zonen · 295
Zonenübertragung · 307
  inkrementell (IXFR) · 310
  vollständig (AXFR) · 310
Zugriffssteuerungsliste · 592
Zulässige RODC-Kennwortreplikationsgruppe · 213, 593
Zuverlässigkeits- und Leistungsüberwachung · 652
Zuverlässigkeitsüberwachung · 645, 650, 651
Zweigniederlassungen · 573
zwischengespeicherte Anmeldeinformationen
  RODC · 596
Zwischengespeicherte Kennwörter
  Zurücksetzen der · 600
Zwischenspeichern der universellen Gruppenmitgliedschaft · 75, 379
Zwischenspeichern von Anmeldeinformationen · 574

Nutzungsbedingungen | Haftungsbeschränkungen

1. Ihr Exemplar wird Ihnen ausschließlich für Ihre persönliche, nichtgewerbliche Nutzung zur Verfügung gestellt, wobei Einschränkungen gemäß diesen Nutzungsbedingungen und dem Urheberrecht Deutschlands sowie anderer Länder gelten.
2. Sie dürfen die nachfolgenden Handlungen weder selbst vornehmen noch von anderen vornehmen lassen:
   (a) Ihr Exemplar ganz oder in Teilen verändern, veröffentlichen, übertragen oder öffentlich wiedergeben oder davon abhängige eigene Werke erstellen, soweit dies nicht ausdrücklich nach diesen Nutzungsbedingungen oder den Schranken des Urheberrechts gemäß §§ 44a ff. UrhG erlaubt ist.
   (b) Das Exemplar ins Usenet oder auf eine externe Internetseite hochladen oder das Exemplar Dritten auf andere Weise zur Verfügung stellen, etwa über ein Intranet, einen öffentlichen oder privaten Hostingdienst, einem peer-to-peer Netzwerk, oder über RSS-Feeds, soweit dies nicht ausdrücklich von diesen Nutzungsbedingungen oder gemäß §§ 44a ff. UrhG erlaubt ist; und/oder
   (c) Dritten die Ihnen nach diesen Nutzungsbedingungen eingeräumten Rechte ganz oder teilweise übertragen, lizenzieren oder in anderer Form weitergeben.
3. Soweit dies nicht ausdrücklich in diesen Nutzungsbedingungen oder den Schranken des Urheberrechts gemäß §§ 44a ff. UrhG erlaubt ist, darf Ihr Exemplar nicht gespeichert, vervielfältigt oder auf beliebige Art und Weise übertragen werden, ohne dass der Urheberrechtsinhaber dies im Vorwege ausdrücklich schriftlich erlaubt hat. Der Händler und seine Zulieferer behalten sich sämtliche Rechte vor, die nicht ausdrücklich in diesen Nutzungsbedingungen eingeräumt werden. Der Händler oder seine Zulieferer sind Inhaber sämtlicher Ansprüche, urheberrechtlicher Nutzungsrechte und sonstiger geistiger Eigentumsrechte am Exemplar. Sie dürfen Urheberrechtshinweise oder andere Herkunftshinweise, die sich am Exemplar befinden, weder entfernen noch sonst unkenntlich machen.
4. Vorbehaltlich der Regelungen in Ziffer 6 bestätigen Sie, dass Sie Ihr Exemplar und dessen Inhalt auf eigene Gefahr verwenden und dass das Exemplar „wie besehen" zur Verfügung gestellt wird, ohne jegliche zusätzliche Versicherung oder Garantie irgendwelcher Art, ausdrücklich oder konkludent (sei es gewohnheitsrechtlich, gesetzlich oder auf sonstiger Grundlage). Soweit dies rechtlich möglich ist, schließen der Händler und seine Zulieferer jegliche Bedingungen, Versicherungen, Bestätigungen und Garantien aus (insbesondere auch konkludente Garantien bezüglich der Qualität oder der Eignung des Exemplars oder seines Inhalts für einen bestimmten Zweck).
5. Unbeschadet der Regelungen in Ziffer 6 bestätigen Sie und stimmen Sie zu, dass der Händler und seine Zulieferer nicht für folgende Ansprüche haftbar ist:
   (a) Direkte Verluste, Ansprüche, Schäden oder Verletzungen;
   (b) Indirekte Verluste, Ansprüche oder Schäden, oder jegliche Buszahlungen, atypische Schäden, beiläufig entstandene Schäden oder Folgeschäden jeder Art, die nicht unmittelbar mit dem Vorgang im Zusammenhang stehen, der Ihren Anspruch begründet hat;
   (c) Entgangene Gewinne oder Ersparnisse;
   (d) Verlust oder Beschädigung von Daten oder Informationen;
   (e) Verlust von Vertragsbeziehungen, Geschäft oder geschäftlichen Gelegenheiten oder
   (f) Schäden am Ruf oder Reputation; dies geltend in jedem Fall, unabhängig davon, ob unmittelbare oder mittelbare Schäden geltend gemacht werden und unabhängig davon, ob Ansprüche aus Vertrag, unerlaubter Handlung (insbesondere wegen Fahrlässigkeit), Gefährdungshaftung oder aus anderen Gründen hergeleitet werden, soweit sie im Zusammenhang mit diesem Exemplar oder dessen Inhalt und/oder jeglicher Nutzung derselben entstehen, auch soweit der Händler oder seine Zulieferer im Vorwege gewarnt wurden oder sich der Möglichkeit derartiger Verluste oder Schäden bewusst waren.
6. Keine Regelung dieser Nutzungsbedingungen verringert oder beseitigt eine Haftung seitens des Händlers oder dessen Zulieferer für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit oder für sonstige Schäden, die auf einer grob fahrlässigen Pflichtverletzung, auf Vorsatz oder einer arglistigen Täuschung seitens der jeweils haftenden Partei oder deren Erfüllungsgehilfen beruht oder für sonstige Haftungsansprüche, die nach deutschem Recht nicht ausgeschlossen oder eingeschränkt werden können.