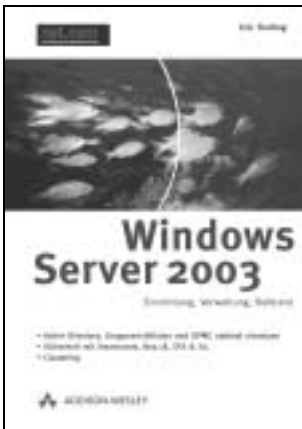


Active Directory

Netzwerke, Betriebssysteme, Sicherheit ... hierzu bietet Ihnen die Reihe net.com umfassende, praxisnahe Information. Neben Fragen der Systemverwaltung greift sie auch Themen wie Protokolle, Technologien und Tools auf. Profitieren Sie bei Ihrer täglichen Arbeit vom Praxiswissen unserer erfahrenen Autoren.



Windows Server 2003

Eric Tierling

1312 Seiten, € 59,95 [D]

ISBN 3-8273-2076-3

Ausführlich widmet sich dieses Buch allen wesentlichen Aspekten von Windows Server 2003 und all seiner Editionen. Active Directory, Gruppenrichtlinien, Windows NT-Domänenupgrade, TCP/IP-Dienste und Sicherheitsmerkmale sind detailliert beschrieben, um Unternehmen einen optimalen Einsatz zu ermöglichen. Clustering mit Netzwerklastenausgleich und Clusterdienst, E-Mail-Server, Group Policy Management Console, Terminaldienste, Remotedesktop und Webverwaltung, Volumen-Schatenkopie sowie die Smartcard-Integration und sichere Wireless-LAN-Unterstützung stellen weitere Highlights dieses Buches dar.



Firewalls illustriert

Jörg Fritsch,

Steffen Gundel

320 Seiten, € 44,95 [D]

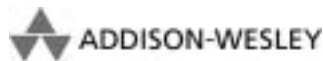
ISBN 3-8273-2043-7

Der Titel ist Programm – mithilfe von weit mehr als 100 Abbildungen erläutern die Autoren den Aufbau einer Firewall. Sie fangen mit einfachen Access-Listen an, und erweitern den Aufbau der Firewall sukzessive, damit Sie genau nachvollziehen können, wie eine Firewall Ihr Netzwerk schützt und welches dafür die optimale Größe ist.

Stephanie Knecht-Thurmann

Active Directory

Planung und praktischer Einsatz unter Windows 2000 und Windows 2003 Server



An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Bibliografische Information Der Deutschen Bibliothek

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

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 Hardware- und Softwarebezeichnungen, die in diesem Buch erwähnt werden, sind gleichzeitig auch eingetragene Warenzeichen oder sollten als solche betrachtet werden.

Umwelthinweis:

Dieses Buch wurde auf chlorfrei gebleichtem Papier gedruckt.

10 9 8 7 6 5 4 3 2 1

07 06 05 04

ISBN 3-8273-2130-1

© 2004 by Addison-Wesley Verlag,

ein Imprint der Pearson Education Deutschland GmbH,
Martin-Kollar-Straße 10–12, D-81829 München/Germany

Alle Rechte vorbehalten

Einbandgestaltung: atelier für gestaltung, niesner & huber, Wuppertal

Lektorat: Sylvia Hasselbach, shasselbach@pearson.de

Korrektur: Sandra Gottmann, Bonn

Herstellung: Claudia Bäurle, cbaeurle@pearson.de

Satz: MediaService, Siegen, www.media-service.tv

Druck und Verarbeitung: Kösel, Kempten (www.Koeselbuch.de)

Printed in Germany

Inhaltsverzeichnis

Vorwort	19
Teil A – Grundlagen	21
1 Ein Überblick über Active Directory und LDAP	23
1.1 Was bedeutet Active Directory?	23
1.1.1 Wie arbeitet ein Verzeichnisdienst?	23
1.2 Das Lightweight Directory Access Protocol (LDAP)	26
1.2.1 Die X.500- und LDAP-Standards	27
1.2.2 Die LDAP-Architektur	28
1.2.3 Die vier LDAP-Modelle	30
1.3 Die Architektur des Active Directory	40
1.3.1 Active Directory in der Betriebssystem-Architektur	40
1.3.2 Die Active Directory-Architektur	43
1.4 Die Features des Active Directory	45
2 Unterschiede zwischen Windows NT und Windows 2000/2003 Server	47
2.1 Domänenmodelle unter Windows NT	47
2.1.1 Domänenmodell mit einer Domäne	48
2.1.2 Domänenmodell mit einer Masterdomäne	48
2.1.3 Domänenmodell mit mehreren Masterdomänen	49
2.1.4 Domänenmodell mit gegenseitigen Vertrauensstellungen	50
2.2 Neuerungen in Windows 2000 und 2003 im Überblick	51
2.2.1 Unterschiede zwischen Windows 2000 und NT	51
2.2.2 Unterschiede zwischen Windows 2000 und 2003 Active Directory	54
2.2.3 Das Kerberos V5-Authentifizierungsprotokoll	57
3 Funktionsweise und Beschreibung des Active Directory	59
3.1 Domänen und Domänencontroller	59
3.2 Strukturen	61
3.2.1 Domänenstruktur (Tree)	62
3.2.2 Gesamtstruktur (Forest)	63
3.3 Der globale Katalog	64
3.3.1 Standorte von Katalogservern	65
3.4 Standorte	66
3.5 Organisationseinheiten	68
3.6 Objekte und Schema	70

3.7	Replikation	71
3.7.1	Multimaster-Replikation	71
3.7.2	Die Verzeichnispportionen oder Namenskontexte	72
3.7.3	Replikationstopologie	73
3.8	Zusammenarbeit mit anderen Betriebssystemen und Verzeichnisdiensten	75
3.8.1	ADSI-Clients für Windows 9x und NT	75
3.8.2	Unix und Linux	77
3.8.3	Microsoft BackOffice-Server und Active Directory	78
3.8.4	Grundlagen der Verzeichnisdienstzusammenarbeit	78
3.8.5	Novell Directory Services (NDS)	79
3.8.6	Features von ADSI	81
Teil B – Konzeption		83
4	Planung der Active Directory-Migration	85
4.1	Die Phasen der Migration und deren Milestones	86
4.1.1	Die Planungsphase	87
4.1.2	Die Designphase	88
4.1.3	Die Testphase	89
4.1.4	Der Rollout	89
4.2	Ausblicke und Möglichkeiten	90
4.2.1	Single Sign-on- und Single Point of Access-Strategie	90
4.2.2	Datenübernahme aus Datenbanken und Verzeichnissen – Metadirectories	92
4.2.3	Erstellen eines Asset-Managements im Active Directory	94
5	Die Planungsphase	97
5.1	Zieldefinition	97
5.2	Das Bilden des Projektteams	98
5.3	Erstellen eines Zeitplans	100
5.4	Bestandsaufnahme	101
5.4.1	Standorte der Organisation	101
5.4.2	Hardware-Landschaft	102
5.4.3	Netzwerktechnisches	104
5.4.4	Applikationsbezogenes	105
5.4.5	Arbeitsplatz- und Benutzerbezogenes	107
6	Die Designphase	109
6.1	Der Architekturplan	110
6.1.1	Domänen und Strukturen	110
6.1.2	DNS und Active Directory-Objektnamen	112
6.1.3	Organisationseinheiten	116
6.1.4	Standorte	117
6.1.5	Replikation	118
6.1.6	Gruppen und Gruppenrichtlinien	119

6.1.7	Sicherheit	120
6.1.8	Hardware- und Netzwerkanforderungen	124
6.1.9	Definition von Standards	125
6.1.10	Spätere Planungen	125
6.2	Die Migrations- und Koexistenzstrategie	126
6.2.1	Die Koexistenz mit Novell NetWare und Unix	127
6.2.2	Die Migrationsreihenfolge der Clients und Server	129
6.2.3	Möglichkeiten einer heterogenen Windows-Umgebung	130
6.3	Der Disaster Recovery-Plan	132
6.4	Betriebsführungskonzept und -handbuch	133
6.4.1	Betriebsführungskonzept	134
6.4.2	Betriebsführungshandbuch	134
7	Die Testphase	135
7.1	Design des Testcenters und Auswahl der Mitglieder des Testteams	135
7.2	Was wird getestet?	136
7.3	Die Testmatrix	137
8	Rollout und Migrationsabschluss	139
8.1	Der Rollout des Piloten	139
8.2	Der endgültige Rollout	140
8.3	Der Migrationsabschluss	141
Teil C – Praxis		143
9	Installation	145
9.1	Starten des Installationsassistenten	145
9.2	Die Active Directory-Installation	146
9.2.1	Die Installation einer neuen Domäne	146
9.2.2	Eine neue untergeordnete Domäne in einer Domänenstruktur einrichten	153
9.2.3	Erstellen einer neuen Domänenstruktur in einer vorhandenen Gesamtstruktur	155
9.2.4	Die Installation zusätzlicher Domänencontroller	156
9.3	Deinstallation des Active Directory	157
9.3.1	Die Deinstallation des Active Directory erzwingen	161
9.3.2	Herunterstufen eines Domänencontrollers über die Registry	162
9.4	Die Installation zusätzlicher Domänencontroller	162
9.4.1	Installation eines Active Directory-Replikats	163
9.4.2	Die netzwerkbasierte Active Directory-Installation	166
9.5	Domänenvorbereitung für Windows 2003-Domänencontroller mit ADPREP	166
9.5.1	ADPREP im Zusammenspiel mit weiteren Diensten	167

10 Die Betriebsmodi des Active Directory	169
10.1 Die Betriebsmodi im Überblick	169
10.1.1 Der gemischte Modus	169
10.1.2 Der einheitliche Modus	170
10.1.3 Wechsel des Betriebsmodus unter Windows 2000	170
10.1.4 Der Domänenfunktionsmodus Windows Server 2003	171
10.1.5 Der Gesamtstrukturfunktionsmodus Windows Server 2003	172
11 Die Betriebsmasterrollen	175
11.1 Die Betriebsmaster im Überblick	175
11.1.1 Die Betriebsmaster der Gesamtstruktur	175
11.1.2 Die Betriebsmaster der Domänenstruktur	176
11.1.3 Verteilen von Betriebsmasterrollen	178
11.1.4 Überprüfen und Ändern der Betriebsmasterrollen	179
11.1.5 Ausfälle von Betriebsmastern	183
12 Vertrauensstellungen	185
12.1 Grundlagen der Vertrauensstellungen	185
12.1.1 Transitive Vertrauensstellungen	186
12.1.2 Nicht transitive Vertrauensstellungen	187
12.1.3 Bidirektionale Vertrauensstellungen	187
12.1.4 Unidirektionale Vertrauensstellungen	187
12.1.5 Explizite Vertrauensstellungen	188
12.1.6 Erstellen expliziter Vertrauensstellungen	190
12.1.7 Erweiterte Vertrauensstellungen unter Windows Server 2003	192
13 Die Datenbank NTDS und der Systemdatenträger SYSVOL	197
13.1 NTDS und SYSVOL im Überblick	197
13.1.1 Die Verzeichnisdatenbank NTDS	197
13.1.2 Der Systemdatenträger SYSVOL	198
13.1.3 Verschieben von SYSVOL per Active Directory- Installations-Wizard	199
13.1.4 Manuelles Verschieben des SYSVOL-Ordners	200
13.1.5 Der Ordner Staging Area	205
13.1.6 Verschieben des Staging Area-Ordners	205
14 Standorte und Organisationseinheiten	207
14.1 Konfiguration von Standorten	207
14.1.1 Festlegen von Subnetzen	209
14.1.2 Erstellen von Standortverknüpfungen	212
14.1.3 Einrichten von Standortlizenzservern	213
14.1.4 Konfigurieren der Server am Standort	215
14.1.5 Ein Server als Mitglied mehrerer Standorte	216
14.2 Konfiguration von Organisationseinheiten	217

15	Einrichten von globalen Katalogservern	219
15.1	Verbesserungen unter Windows Server 2003	220
15.2	Replikation der globalen Katalogserver	221
15.3	Der Occupancy-Level des globalen Katalogservers	222
16	DNS und Active Directory	223
16.1	Das Prinzip von DNS	223
16.1.1	Was bedeutet Namensauflösung?	226
16.1.2	Wie funktionieren DNS-Abfragen?	227
16.2	DNS-Zonen	229
16.2.1	Forward Lookup-Zonen	230
16.2.2	Funktionsweise des Forward Lookup	233
16.2.3	Reverse Lookup-Zonen	235
16.2.4	Funktionsweise des Reverse Lookup	237
16.2.5	Ressourceneinträge	238
16.2.6	Delegieren von Zonen	240
16.2.7	DNS-Weiterleitungen	241
16.3	Zonenübertragungen	241
16.3.1	Die DNS-Benachrichtigungsliste	243
16.4	Dynamisches DNS	244
16.4.1	Einrichten von dynamischem DNS	245
16.5	Standorte von DNS-Servern	246
16.6	Fehlersuche bei DNS-Problemen	247
16.6.1	Das DNS-Ereignisprotokoll	247
16.6.2	Das DNS-Logfile	247
16.6.3	DNS-Befehlszeilenprogramme	249
16.6.4	DNS-Fehlerszenarien	251
17	Die Replikation	255
17.1	Der Replikationsablauf im Detail	255
17.1.1	Die Metadaten zur Replikationssteuerung	255
17.1.2	Das Ändern der Metadaten während der Replikation	257
17.1.3	Die Replikation eines Objekts	260
17.1.4	Die Linked-Value Replication unter Windows Server 2003	265
17.1.5	Synchronisieren der Systemzeit zwischen Domänencontrollern	266
17.1.6	Beschleunigen der Replikation	267
17.1.7	Bearbeiten der Replikationszeiten über die Registry	268
17.2	Standortübergreifende Replikation	269
17.2.1	Standortverknüpfungsattribute	270
17.2.2	Standortverknüpfungsbrücken (Site Link Bridges)	273
17.2.3	Bridgehead-Server	275
17.2.4	Einstellungen standortübergreifender Replikationstopologie	276
17.2.5	Wann wird welcher Replikationszeitplan benutzt?	278

17.3	Fehler bei der Replikation	279
17.3.1	Mögliche Replikationskonflikte	279
17.3.2	Replikationsprobleme mit DNSLint beheben	282
17.3.3	Fehlerbehebung bei der Replikation	283
17.3.4	FRS-Fehler im Ereignisprotokoll	284
18	Benutzer, Gruppen und Profile	287
18.1	Arten von Benutzerkonten	287
18.1.1	Domänenbenutzerkonten	287
18.1.2	Lokale Benutzerkonten	287
18.1.3	Integrierte Benutzerkonten	288
18.1.4	Das Zusammenspiel zwischen einer Domäne und Arbeitsgruppe	289
18.2	Einrichten von Benutzerkonten	289
18.2.1	Einrichten von Benutzerkonten	289
18.2.2	Eigenschaften von Benutzerkonten	292
18.2.3	Die tägliche Arbeit mit Benutzerkonten	297
18.2.4	Einrichten von Computerkonten	298
18.2.5	Die tägliche Arbeit mit Computerkonten	298
18.2.6	Verhindern von Änderungen der Benutzerattribute	299
18.3	Benutzerprofile und Basisverzeichnisse	301
18.3.1	Arten von Benutzerprofilen	301
18.3.2	Checkliste zum Einrichten von Benutzerprofilen	303
18.3.3	Einrichten eines servergespeicherten Profils	304
18.3.4	Einrichten eines verbindlichen Profils	306
18.3.5	Probleme mit lokalen Profilen nach der Migration – SID-History	307
18.3.6	Einrichten von Basisverzeichnissen	309
18.4	Grundlagen zu Benutzergruppen	310
18.4.1	Grundlegendes zu Gruppen	310
18.4.2	Gruppentypen und Gruppenbereiche	310
18.4.3	Standardmäßig vorhandene Gruppen	311
18.5	Planen und Einrichten von Gruppen	314
18.5.1	Welche Art von Gruppe soll verwendet werden?	314
18.5.2	Einrichten und Bearbeiten von Gruppen und Gruppeneigenschaften	316
18.6	Spezielle Optionen für Administratoren	317
18.6.1	Die Option Ausführen als	317
18.6.2	Verwenden von RUNAS	318
19	NTFS-Berechtigungen, Datenträgerkontingente und DFS	319
19.1	NTFS Ordner- und Dateiberechtigungen	319
19.1.1	Was bedeuten ACL, ACE, DACL und SACL?	319
19.1.2	Rechte für NTFS-Ordner und -Dateien	320
19.1.3	Spezielle NTFS-Berechtigungen	323
19.1.4	Verschieben und Kopieren von Ordnern und Dateien	326
19.1.5	Berechtigungsvererbung	326
19.1.6	Ändern der DACLs mit CACLS	327

19.2	Planen und Erstellen von Freigaben	328
19.2.1	Erstellen von Freigaben	330
19.2.2	Administrative Freigaben	331
19.2.3	Rechte für Freigaben und NTFS-Rechte kombinieren	332
19.3	Datenträgerkontingente	332
19.4	Das Distributed File System (DFS)	333
19.4.1	Einrichten eines DFS-Stammes	334
19.4.2	Einrichten einer DFS-Verknüpfung	337
19.4.3	Einrichten von DFS-Ordern	338
19.4.4	Festlegen der DFS-Replikation	338
19.5	Fehlersuche bei Berechtigungen und DFS	339
20	Gruppenrichtlinien	341
20.1	Grundlegendes zu Gruppenrichtlinien	341
20.1.1	Windows NT-Systemrichtlinie und Windows 2000 / 2003-Gruppenrichtlinie	341
20.1.2	Update der Windows 2000-Gruppenrichtlinien um XP-Features	343
20.1.3	Was bedeuten GPO, GPC und GPT?	345
20.1.4	Verarbeiten und Vererben von Gruppenrichtlinien	346
20.1.5	Öffnen und Bearbeiten der GPOs	347
20.1.6	Inhalte eines GPOs	348
20.1.7	Abarbeiten der Gruppenrichtlinien für Computer und Benutzer	351
20.1.8	Spezielle Optionen für Gruppenrichtlinien	353
20.1.9	Mehrere Anmeldungen unter Windows XP, bis ein GPO wirksam wird	354
20.1.10	Konflikte von GPO-Einstellungen vorhersagen – RSoP in Windows XP / 2003	355
20.2	Erstellen von Gruppenrichtlinien	358
20.2.1	Implementierungsstrategie für Gruppenrichtlinien	359
20.2.2	Erstellen eines GPO	361
20.2.3	Bearbeiten von GPOs	362
20.2.4	Zuweisen von GPOs	366
20.2.5	Spezielle An- und Abmeldeskripte	368
20.2.6	Gruppenrichtlinien für Organisationseinheiten sinnvoll planen	369
20.3	Die GPMC unter Windows Server 2003	371
20.3.1	Die Administration über die GPMC	373
20.3.2	Erstellen, Löschen und Verknüpfen von GPOs	374
20.3.3	Backup von GPOs	377
20.3.4	Wiederherstellung von GPOs	380
20.3.5	Kopieren von GPOs	383
20.3.6	Import und Export von GPOs	384
20.3.7	Migrationstabellen	386
20.3.8	Erstellen von HTML-Berichten	391
20.3.9	Gruppenrichtlinienmodellierung und -ergebnisse	391
20.3.10	Aufgabendelegierung	400
20.3.11	WMI-Filter	403

20.4	Ordnerverwaltung über Gruppenrichtlinien	405
20.4.1	Ordnerumleitung	405
20.4.2	Probleme bei der Ordnerumleitung unter Windows XP	409
20.4.3	Offline-Inhalte von Ordnern	409
20.5	Softwareverwaltung und -verteilung über Gruppenrichtlinien	413
20.5.1	Der Prozess der Softwareverteilung	413
20.5.2	Einrichten des Softwareverteilungspunktes und administratives Setup	416
20.5.3	Festlegen der Installationsoptionen	418
20.5.4	Zuweisen und Veröffentlichen von Paketen	419
20.5.5	Allgemeine Einstellungen an den Applikationspaketen	421
20.5.6	Bearbeiten und Entfernen von Applikationspaketen	422
20.5.7	Strategie zur Konfiguration der Softwareinstallation	426
20.6	Windows Installer-Technologie und Repaketierung	426
20.6.1	Windows Installer-Technologie	426
20.6.2	Repaketierung	428
20.7	Erstellen einer .mst-Datei (Transform-File)	429
20.8	Verteilen von mmcs	429
20.9	Fehlersuche bei Gruppenrichtlinien	430
20.9.1	Inkonsistenz bei Gruppenrichtlinien nach der Migration	432
21	Administrative Aufgaben am Active Directory	435
21.1	Veröffentlichen von Objekten und Netzwerkdiensten	435
21.2	Die Suchfunktion im Active Directory	436
21.3	Verschieben von Objekten	438
21.4	Löschen von Objekten – Tombstoning	439
21.5	Delegieren der Active Directory-Verwaltung	440
21.5.1	Der Assistent zur Verwaltungsdelegierung	440
21.5.2	Die Berechtigungsvererbung funktioniert nicht immer	442
21.5.3	Objektberechtigungen mit DSACLs bearbeiten	444
21.6	Backup des Active Directory	445
21.6.1	Planen einer Backup-Strategie	446
21.6.2	Backup-Programme von Drittanbietern	448
21.6.3	Wiederherstellen eines Teil-Backups	448
21.6.4	Backup der Active Directory-Gruppenrichtlinien	449
21.7	Wiederherstellen des Active Directory	450
21.7.1	Die nicht autorisierende Wiederherstellung	451
21.7.2	Die autorisierende Wiederherstellung	452
21.7.3	Ein allgemeiner Disaster Recovery-Plan	455
21.7.4	Domänencontroller-Wiederherstellung via Neuinstallation und Backup	457
21.8	Defragmentieren der Active Directory-Datenbank	459
21.8.1	Die Online-Defragmentierung	459
21.8.2	Die Offline-Defragmentierung	460
21.8.3	Die Größe der Datenbankdatei NTDS.DIT	460

21.9	Active Directory-Kontingente unter Windows Server 2003	461
21.10	Regelmäßige administrative Aufgaben	464
21.10.1	Tägliche Aufgaben	465
21.10.2	Wöchentliche Aufgaben	465
21.10.3	Monatliche Aufgaben	465
21.10.4	Aufgaben bei Bedarf	466
21.11	Das Umbenennen von Domänen	467
21.11.1	Umbenennen einer Windows 2003-Domäne	467
21.11.2	Umbenennen einer Windows 2000-Domäne im einheitlichen Modus	467
21.11.3	Umbenennen einer Windows 2000-Domäne im gemischten Modus	468
22	Überwachung und Sicherheit	471
22.1	Überwachungsrichtlinien	471
22.1.1	Einrichten von Überwachungsrichtlinien	471
22.1.2	Überwachungsrichtlinien für Domänencontroller	472
22.1.3	Überwachungsrichtlinien für Mitgliedsserver und Clients	473
22.2	Zugriffsüberwachung auf Active Directory-Ressourcen	473
22.2.1	Zugriffsüberwachung für Active Directory-Objekte	473
22.2.2	Zugriffsüberwachung für Dateien und Ordner	474
22.3	Die Sicherheitsrichtlinien	475
22.4	Richtlinien zur Softwareeinschränkung unter Windows Server 2003	477
22.4.1	Die Hashregeln	477
22.4.2	Die Internetzonenregeln	478
22.4.3	Die Pfadregeln	479
22.4.4	Die Zertifikatsregeln	480
22.4.5	Die Priorität der Regeln	481
22.5	Die Sicherheitsvorlagen	482
22.5.1	Arbeiten mit einer Sicherheitsvorlage	483
22.6	Die Sicherheitskonfiguration und -analyse	485
22.6.1	Die Sicherheitsanalyse	486
22.7	Die Konfiguration des Kerberos-Protokolls	487
22.8	Der Systemmonitor und die Leistungsprotokolle	488
22.8.1	Die Ereignisanzeige	491
22.8.2	Aktivieren des Diagnostic-Event-Logging	492
23	Die Windows-eigenen Active Directory-Support-Tools	493
23.1	Support-Tools für das Windows 2000 und Windows 2003 Active Directory	493
23.1.1	ACLDIAG	495
23.1.2	ADSIEDIT	496
23.1.3	ADSIZER	499
23.1.4	DCDIAG	501

23.1.5	DNSCMD	503
23.1.6	DOMMON	505
23.1.7	DSACLS	506
23.1.8	DSASTAT	508
23.1.9	DUMPFMOS	509
23.1.10	FAZAM 2000	509
23.1.11	GPOTOOL	511
23.1.12	GPRESULT	512
23.1.13	GUID2OBJ	513
23.1.14	LDP	514
23.1.15	MOVETREE	516
23.1.16	NETDIAG	517
23.1.17	NETDOM	518
23.1.18	NTDSUTIL	520
23.1.19	PERMS	524
23.1.20	REPADMIN	525
23.1.21	REPLMON	527
23.1.22	SDCHECK	528
23.1.23	User State Migration Tool	529
23.1.24	ADCheck (NetIQ)	531
23.2	Neue Support-Tools für das Windows 2003 Active Directory	532
23.2.1	RENDOM für Windows Server 2003	532
23.2.2	RedirUsr und RedirComp	543
24	Das Active Directory-Schema	545
24.1	Allgemeines zum Active Directory-Schema	545
24.1.1	Die Active Directory-Klassen	546
24.1.2	Die Active Directory-Attribute	549
24.1.3	Das abstrakte Schema	552
24.1.4	Die mmc Active Directory-Schema	552
24.2	Warum Änderungen durchführen?	553
24.2.1	Einschränkungen bei der Schemaerweiterung	555
24.2.2	Der Schema-Cache	555
24.2.3	Festlegen und Zuweisen von Object Identifiern (OIDs)	556
24.3	Das Ändern des Schemas	557
24.3.1	Hinzufügen neuer Klassen und Attribute	559
24.3.2	Namensregeln für Schema-Objekte	563
24.3.3	Klassen- und Attributprüfung bei Schemaänderungen	564
24.3.4	Deaktivieren von Klassen und Attributen	564
24.3.5	Dokumentieren der Änderungen	565
24.4	Dokumentation von Änderungen mit Schemadocfile.exe	566
24.5	Schemaänderungen als potenzielle Fehlerquelle	569

25 Import und Export der Active Directory-Umgebung	571
25.1 Das Format LDIF und LDIF-Dateien	571
25.2 Das Tool LDIFDE	572
25.2.1 Im- und Export von Active Directory-Objekten zwischen Domänen	574
25.2.2 Export von Objekten aus einer Gesamtstruktur	576
25.2.3 Ändern von Benutzerattributen	576
25.2.4 Anlegen und Löschen von Benutzern	578
25.2.5 Setzen von Passwörtern	578
26 Visualisierung und Design der Active Directory-Umgebung in Microsoft Visio	581
26.1 Microsoft Visio und Active Directory	581
26.1.1 Importieren von Active Directory-Objekten	582
26.1.2 Bearbeiten und Neuerstellen von Objekten	584
26.1.3 Bearbeiten des Active Directory-Schemas	586
26.1.4 Exportieren von Objekten ins Active Directory	588
26.1.5 Strukturdesign der Active Directory-Umgebung	588
27 Migration und Update von Windows NT zu Active Directory	589
27.1 Warum auf Windows 2000 oder 2003 aktualisieren?	589
27.1.1 Die Entscheidung: Migration oder Update	590
27.2 Allgemeine Planung einer Migration	591
27.2.1 Vorbereitung der Domänenstruktur	591
27.2.2 Standardisierung des Netzwerks auf TCP/IP	592
27.2.3 Die DNS-Struktur	593
27.2.4 Die SID-Probleme	593
27.3 Welches DNS-Modell ist das Beste?	594
27.3.1 Windows 2000/2003 beinhaltet den kompletten DNS-Stamm	594
27.3.2 Windows 2000/2003 beinhaltet eine untergeordnete Zone	595
27.3.3 Ein Unix-Server beinhaltet den Windows 2000/2003-Stamm	595
27.4 Migrationsmodelle für NT-Domänen	596
27.4.1 Vorbereiten der Migration	596
27.4.2 Vorbereiten des Updates	597
27.4.3 Was geschieht beim Update auf dem PDC?	598
27.4.4 Verschiedene Wege zur neuen Gesamtstruktur	599
27.4.5 Domänenstruktur und Verwaltungsvorgaben	602
27.5 Das Active Directory Migration Tool (ADMT)	603
27.5.1 Features	604
27.5.2 Voraussetzungen	606
27.5.3 Features des ADMT Version 2.0	607
27.5.4 Weitere Migrationstools	607
27.6 Die Migration gleichnamiger NT-Benutzergruppen	608

27.7	Die manuelle Migration	608
27.7.1	Verschieben von Benutzern	609
27.7.2	Verschieben von Benutzergruppen	609
27.7.3	Verschieben von Computern	610
27.7.4	Verschieben von Mitgliedsservern	610
27.7.5	Löschen von Domänen	611
27.8	Nach der Migration	611
27.8.1	Aktualisieren der ACLs und Löschen der SID-History	611
27.8.2	Ein Netzwerk ohne NetBIOS	612
27.8.3	Aktualisierte Domänencontroller und die Client-Anmeldung	612
28	Der Active Directory-Anwendungsmodus (AD/AM) des Windows Server 2003	615
28.1	Überblick über den AD / AM	615
28.1.1	Funktionsweise und Architektur des AD / AM	616
28.1.2	Einsatzmöglichkeiten des AD / AM	618
28.1.3	Installation des AD / AM	620
28.2	Die Verwaltungswerkzeuge des AD / AM	626
28.2.1	ADAMSetup	626
28.2.2	Adamuninstall	626
28.3	Verwalten einer AD / AM-Instanz	627
28.3.1	Auflisten der Verzeichnispartitionen und Namensräume einer AD / AM-Instanz	628
28.3.2	Den Dienst der AD / AM-Instanz verwalten	628
28.3.3	Den Port der AD / AM-Instanz ändern	629
29	Koexistenz mit Unix, Linux und MacOS	631
29.1	Die Benutzerverwaltung unter Unix	631
29.2	Die Windows Services for Unix (SFU)	632
29.2.1	Server / Client / Gateway for NFS	633
29.2.2	Server for PCNFS	635
29.2.3	User Name Mapping	636
29.2.4	Password-Synchronisation	637
29.2.5	Server for NIS	637
29.2.6	Konfiguration des NFS-Servers	639
29.3	Das Freeware-Tool AD4Unix	641
29.4	Der OpenLDAP-Client	643
29.5	Unix-Authentifizierung am Active Directory über pam_ldap	643
29.5.1	Konfiguration der Datei /etc/ldap.conf	644
29.5.2	Authconfig	645
29.5.3	Konfiguration der Datei /etc/pam.d/login	645
29.5.4	Authentifizierung über pam_ldap und SSL	646
29.5.5	Authentifizierung über stunnel	646

29.6	Unix-Authentifizierung am Active Directory über nss_ldap	647
29.7	Samba 3.0 und Active Directory	648
29.8	Unix-basierte DNS-Server im Active Directory	650
29.8.1	Dynamische Aktualisierungen zulassen	651
29.8.2	Inkrementelle Zonenübertragungen	652
29.8.3	Überprüfen der DNS-Einstellungen mit Dlint	652
29.9	MacOS-Clients im Active Directory	652
29.9.1	Die Services for Macintosh (SFM)	653
29.9.2	Freigaben für Macintosh-Clients	654
29.9.3	Authentifizierung der Macintosh-Clients an der Domäne	655
29.9.4	Die standardmäßige Apple-Authentifizierung	656
29.9.5	Die Microsoft UAM-Authentifizierung	657
29.10	Die Anmeldung am Active Directory über MacAdministrator	658
29.11	Verbindung von MacOS X-Clients mit dem Active Directory	659
30	Metadirectory-Services	661
30.1	Der Zweck eines Metadirectories	661
30.2	Microsoft Identity Integration Server 2003 (MIIS)	661
30.2.1	Die Architektur des MIIS 2003	662
30.2.2	Die Installation des MIIS 2003	664
30.3	Der Identity Manager	665
30.3.1	Management Agents (MA)	666
30.3.2	Run Profiles für Management Agents	676
30.3.3	Rules Extensions	680
30.3.4	Metaverse Designer	681
30.3.5	Metaverse Search	683
30.3.6	Joiner	684
31	Active Directory und Firewalls	687
31.1	Portbelegung eines Domänencontrollers im Active Directory	687
31.1.1	Tools zur Portüberwachung	689
31.2	Die Konfiguration von Firewalls für RPC-Aufrufe	690
31.2.1	Einschränken der dynamisch zugewiesenen RPC-Ports	690
31.2.2	RPC-Aufrufe über IPSec	692
31.2.3	Zulassen dynamischer RPC-Aufrufe	697
31.3	Die Konfiguration von Firewalls für Domänen und Vertrauensstellungen	698
31.4	Active Directory- und Firewall-Szenarien	700
31.4.1	Zwei durch eine Firewall getrennte Gesamtstrukturen	700
31.4.2	Mehrere durch Firewalls getrennte Domänen	701
31.4.3	Durch eine Firewall abgetrennte Mitgliedsserver	702

32 ADSI-Skripte	703
32.1 Einführung in ADSI und ADSI-Skripte	703
32.1.1 ADSI-Skripte unter Windows	703
32.1.2 Methoden und Eigenschaftsmethoden	705
32.1.3 IADs-Schnittstellen	707
32.1.4 Namensräume und ProgIDs	709
32.1.5 Zugriff auf Objekte	709
32.1.6 Authentifizierung bei der Verbindung zum Verzeichnisserver	710
32.1.7 Konventionen für Variablenpräfixe	712
32.2 ADSI-Skripte zur Benutzerverwaltung	713
32.2.1 Anlegen und Löschen eines Benutzerkontos	714
32.2.2 Die Schnittstelle IADsUser	714
32.2.3 Komplexe Benutzerkonten anlegen	715
32.2.4 Ändern von Benutzerattributen	716
32.2.5 Weitere Beispiele	717
32.3 ADSI-Skripte für Zugriff, Überwachung und Sicherheit	718
32.3.1 Erstellen eines ACEs	718
32.3.2 AccessMask	719
32.3.3 AceFlags	721
32.3.4 AceType	722
32.3.5 Flags: ObjectType, InheritedObjectType	723
32.3.6 Trustee	724
32.3.7 Beispiel	725
32.4 ADSI-Skripte zum Ändern des Schemas	726
32.4.1 Herstellen einer Verbindung zum Schema	726
32.4.2 Neue Schemaattribute und -klassen erstellen	727
32.4.3 Die Windows-GUI modifizieren und erweitern	729
32.4.4 Display Specifier für Klassen und Attribute	730
32.4.5 Erweitern der Kontextmenüs	731
32.4.6 Definieren eigener Registerkarten	732
32.4.7 Anlegen selbst definierter Assistenten	732
32.4.8 Container und Endknotenobjekte	733
33 Auflistung der erwähnten RFCs	735
33.1 Standards für Windows 2000 / 2003 sowie Active Directory	735
33.2 In diesem Buch referenzierte RFCs	736
34 Verweise auf weitere Programme	739
35 Glossar	743
Stichwortverzeichnis	773

Vorwort

Durch die Implementierung von Active Directory unter Windows 2000/2003 wird es in bisher nicht da gewesener Form möglich, Netzwerk-Strukturen in Unternehmen und Organisationen so zu gestalten, dass diese den realen Gegebenheiten weitgehend entsprechen. Komplexe Berechtigungen von Usern, entsprechend ihrer Funktion oder ihres Standortes, lassen sich definieren und vieles mehr. Diese Funktionen in ihrer Vielfalt als eine Referenz darzustellen wäre der Thematik nicht gerecht geworden. So entschied ich mich für eine Dreiteilung des Buches.

Der erste Teil gibt einen allgemeinen Überblick über die Grundlagen und Funktionen von Active Directory. Hier kann sich der Leser rasch einen Überblick über die neuen Technologien verschaffen. Im zweiten Teil wird ein komplettes Migrationskonzept für die Umstellung eines bestehenden Netzwerks auf Active Directory vorgestellt. Sie erhalten allgemeine Hinweise zum Erstellen eines Projektplans über mehrere Phasen. Der dritte Teil schließlich vermittelt die technische Seite der Implementierung. Sie erhalten hier ausführliche Konfigurationsanleitungen in einem breit gefächerten Feld von der Installation des Active Directory über Einstellungen zu DNS-Zonen, Replikationsplänen, Gruppenrichtlinien, Active Directory-Support-Tools, ADSI-Skripten oder Metadirectory Services.

Die Zielgruppe ist durch diesen Aufbau sehr weit gestreut. In der Einführung finden sowohl ein Einsteiger in das Thema Active Directory als auch ein bereits erfahrener NT-Administrator die Grundkonzepte anschaulich erklärt, da hier ausschließlich die Neuerungen in Windows 2000/2003 und nicht Windows-Grundlagen an sich erklärt werden. Der zweite Teil richtet sich sowohl an IT-Entscheider im Unternehmen als auch an die technische IT-Crew. Für die Planung der Migration muss ein Team aus Technikern und Nichttechnikern gebildet werden. Dieser Teil bezieht sich entsprechend auf die projektbezogene Arbeit. Der dritte Teil ist in erster Linie für Administratoren interessant, die mit dem neuen Werkzeug in der Praxis arbeiten. Selbst für Umsteiger aus der Windows NT-Welt bietet Windows 2000/2003 noch genügend Neuerungen.

An dieser Stelle möchte ich mich besonders bei meiner Lektorin Frau Hasselbach für die gute Zusammenarbeit bedanken. Auch meinem Ehemann danke ich für seine Ideen, seine kompetente und konstruktive Kritik und sein Verständnis. Danke auch Ihnen, liebe Leserin, lieber Leser. Sie werden hoffentlich viel Nutzen aus diesem Buch ziehen. Bei Fragen und Schwierigkeiten zum Thema bin ich für Sie da. Besuchen Sie auch meine Homepage <http://www.knecht-consult.de> zum Thema Active Directory.

Teil A – Grundlagen

Über diesen Teil

Das Buch beginnt mit einem theoretischen Einführungsteil in die Thematik Active Directory. Hier finden Sie eine Fülle von Grundlagen, die Ihnen später das Verständnis für die Konzeption und die praktische Umsetzung von Active Directory erleichtern werden.

Im ersten Kapitel dieses Teils werden Ihnen die Grundlagen von Active Directory vorgestellt. Sie erfahren hier, wie ein Verzeichnisdienst im Allgemeinen und Active Directory im Speziellen arbeiten. Bei der Beschreibung von Active Directory muss auch LDAP, das Lightweight Directory Access Protocol, näher vorgestellt werden. LDAP ist das Zugriffsprotokoll für Active Directory. Sie erfahren hier viele Details über die Historie und Architektur von LDAP. Weiterhin wird Ihnen auch das Architekturmodell von Active Directory sowie die Integration von Active Directory in die Betriebssystemarchitektur von Windows 2000/2003 vorgestellt.

Besonders für Umsteiger aus der Welt von Windows NT ist das zweite Kapitel interessant. Hier werden die Neuerungen einer Active Directory-Domänenlandschaft gegenüber den Windows NT-Domänenmodellen vorgestellt sowie die neuen Features in Windows 2000 aufgelistet. Ein eigenes Kapitel beschreibt die Neuerungen des Windows 2003 Server Active Directory gegenüber Windows 2000.

Das dritte Kapitel stellt alle Begrifflichkeiten und Schlagwörter im Zusammenhang mit Active Directory vor und erläutert diese ausführlich. Im technischen Teil (Teil C) wird immer wieder auf die Grundlagen dieses Kapitels verwiesen. Weiterhin erfahren Sie viel Wissenswertes über die Zusammenarbeit von Active Directory mit Clients älterer Windows-Versionen sowie Clients anderer Betriebssysteme wie Novell NetWare oder Unix.

1 Ein Überblick über Active Directory und LDAP

In diesem Kapitel erfolgt eine Einführung in die Thematik Active Directory. Zunächst wird eine kurze, allgemein gültige Beschreibung von Active Directory an sich sowie der Funktionsweise eines Verzeichnisdienstes detailliert erläutert. Das primäre Zugriffsprotokoll für Active Directory ist LDAP (Lightweight Directory Access Protocol). Dieses Protokoll wird in seiner Historie, Architektur sowie seinen Modellen vorgestellt. Anschließend wird die Architektur von Active Directory selbst erläutert. Zusammenfassend werden am Ende die in Active Directory enthaltenen und gegenüber Windows NT-Domänen neuen Kernfeatures präsentiert.

1.1 Was bedeutet Active Directory?

Microsoft vollzog mit Active Directory in Windows 2000 den Einstieg in die Welt der Verzeichnisdienste. Bereits länger am Markt vertreten ist Novell Directory Service (NDS) der Firma Novell NetWare. Active Directory basiert auf InternetStandardtechnologien. Es ist vollständig in das Betriebssystem Windows 2000 / 2003 Server integriert. Mit Active Directory wird das Domänenmodell von Windows NT erweitert. Das primäre Zugriffsprotokoll für Active Directory ist LDAP (Lightweight Directory Access Protocol) in der Version 3.

1.1.1 Wie arbeitet ein Verzeichnisdienst?

Ein Verzeichnisdienst arbeitet vergleichbar mit einem Telefonbuch. In einem Telefonbuch ist mit jedem Namenseintrag eine bestimmte Telefonnummer verknüpft. Außerdem können Sie dort weitere optionale Informationen wie z.B. die Adresse eines Teilnehmers finden. Im Verzeichnisdienst sind die Objekte der Netzwerkressourcen wie z.B. Benutzer, Drucker, Datenbanken usw. mit Informationen verknüpft. Diese Informationen enthalten z.B. den Namen des Objekts, den Standort und viele objektspezifische Informationen. Je mehr optionale Informationen Sie bei den Eigenschaften eines Objekts angeben, desto schneller und präziser kann das Objekt später von den Netzwerkbenutzern gefunden werden – auch wenn dies natürlich beim einmaligen Einpflegen der Objekte in die Datenbank mehr Zeit in Anspruch nimmt.

Wenn der Name eines Objekts im Verzeichnis bekannt ist, z.B. der Benutzername, kann eine dazugehörige Information wie z.B. eine E-Mail-Adresse direkt bezogen werden. Dies entspricht dem Nachschlagen eines bekannten Namens in einem herkömmlichen Telefonbuch, um die zugeordnete Telefonnummer zu erhalten. Damit sind die Nachschlagefunktionen des Verzeichnisses aber noch nicht erschöpft. Angenommen, Sie kennen nicht exakt den Namen eines Objekts, dafür aber einige Informationen; dann werden alle Objekte im Verzeichnis nach diesen Kriterien durchsucht. Dieser Vorgang entspricht

dem Nachschlagen in den Gelben Seiten. Dieses Verzeichnis verwenden Sie, wenn Sie nicht den genauen Namen kennen. Sie finden dann eine Liste aller Einträge, auf die Ihre Suchkriterien zutreffen. Das Verzeichnis ist den Gelben Seiten aber insofern überlegen, dass diese nur nach vordefinierten Einträgen durchsucht werden können, während Sie im Verzeichnis selbst die Kriterien bestimmen können, nach denen Sie suchen möchten.

Ein Verzeichnisdienst ermöglicht es, alle Netzwerkobjekte zentralisiert zu verwalten. Im Active Directory können Informationen über Benutzer, Server, Computer, Drucker usw. an einer Stelle gepflegt und verwaltet werden, die Informationen können aber von allen Benutzern im gesamten Netzwerk abgerufen werden. Dadurch wird sowohl das Verwalten als auch das Finden der Netzwerkressourcen stark vereinfacht.

Im Verzeichnis werden die Objekte gespeichert. Ein Objekt ist eine gespeicherte Information, die mit einer Netzwerkressource verknüpft ist. Um die Ressourcen den Netzwerkbenutzern oder auch Applikationen zur Verfügung stellen zu können, wird der Verzeichnisdienst benötigt. Hierbei handelt es sich um einen Netzwerkdienst, der für die Identifikation der Ressourcen zuständig ist, damit die Benutzer auf diese zugreifen können. Im Active Directory können Millionen von Objekten gespeichert werden. Deshalb muss jedes einzelne Objekt eindeutig gekennzeichnet und referenziert sein, damit es gefunden werden kann. Dafür hat jedes einzelne Objekt in Active Directory eine eindeutige Kennung, die als GUID (Globally Unique Identifier) bezeichnet wird. Bei dem GUID handelt es sich um einen Wert von 128 Bit Länge. Dieser Wert wird jedem Objekt beim Erstellen zugeteilt.

Es gibt zwei Arten von Active Directory-Objekten: Container und Nicht-Container. Die Nicht-Container werden auch Endknoten oder Leafs genannt. Ein Container enthält weitere Container oder Endknoten, ein Endknoten kann keine weiteren Objekte enthalten. Ein Beispiel für einen Container ist eine Organisationseinheit. In dieser befinden sich Computer, Benutzer usw. Ein Beispiel für einen Endknoten ist ein Benutzer. Auch Computer werden als Endknoten klassifiziert, obwohl sie rein theoretisch auch Objekte, wie z.B. Drucker, enthalten könnten.

Da das Verzeichnis oftmals auch als Datenbank oder Verzeichnisdatenbank bezeichnet wird, sollen grundlegend die Unterschiede zwischen diesen beiden Begriffen klargestellt werden. Ein Verzeichnis bietet Funktionen, die weit über die der herkömmlichen relationalen Datenbanken hinausgehen. Ein großer Unterschied besteht darin, dass die Informationen aus einem Verzeichnis weitaus öfter abgerufen als geändert werden. In einer Datenbank werden vermehrt aktualisierte Daten geschrieben. Deshalb sollten in einem Verzeichnis also die Such- und Lesefunktionen gegenüber der Schreibfunktion optimiert sein. Der Lesezugriff geschieht schließlich durch alle Benutzer des Verzeichnisses, während der Schreibzugriff auf die Administratoren beschränkt ist. Es werden Daten im Verzeichnis gespeichert, die relativ statisch sind, da sie nicht oft Änderungen unterworfen sind. Die Verzeichnisbenutzer können hundert Mal, wenn nicht sogar noch öfter die E-Mail-Adresse eines bestimmten Benutzers abfragen, während diese im selben Zeitraum vom Administrator höchstwahrscheinlich nicht geändert wird.

Ein zweiter Unterschied zwischen Verzeichnis und Datenbank besteht im Zugriff auf die jeweilige Komponente. Auf eine Datenbank wird meist mittels einer standardisierten, komplexen SQL-(Structured Query Language-)Abfrage zugegriffen. Hiermit werden zwar komplexe Abfragen und Updates der Datenbank ermöglicht, aber leider geschieht

dies auf Kosten von Komplexität und Größe der Applikation. Verzeichnisse wie das Active Directory benutzen das LDAP-Protokoll zum Zugriff. Hierbei handelt es sich um ein einfaches, optimiertes und schlankes Protokoll. Ausführlich wird LDAP im nächsten Kapitel beschrieben.

Der Zugriff auf Informationen im Verzeichnis erfolgt über das Client-Server-Kommunikationsmodell. Dabei darf eine Applikation auf einem Client, die Informationen aus dem Verzeichnis benötigt, nicht direkt auf das Verzeichnis auf dem Server zugreifen. Es wird eine ein??? API (Application Programming Interface) aufgerufen, die über eine entsprechende Meldung einen neuen Prozess aufruft, den Directory Client, der die weitere Anfrage über das TCP/IP-Protokoll durchführt. Der direkte Zugriff auf das Verzeichnis erfolgt über den Directory Server. Über diesen Mechanismus wird schließlich in umgekehrter Reihenfolge die Information an die Applikation zurückgeschickt. Diesen Vorgang soll die Abbildung 1.1 verdeutlichen.

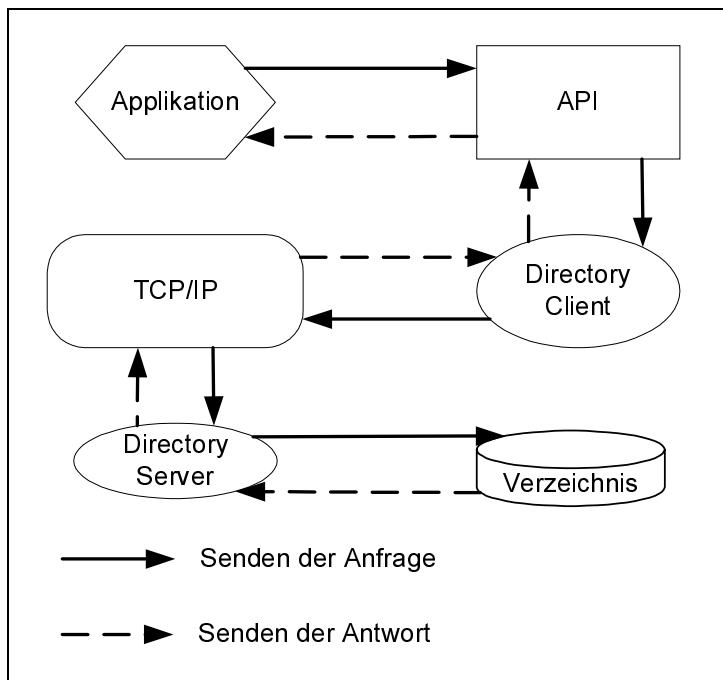


Abbildung 1.1: Der Zugriff auf das Verzeichnis

Ein Verzeichnisdienst ist nur ein Beispiel für die Client-Server-Kommunikation. Weitere Dienste sind z.B. der Druckdienst, der Webservice usw. Sie können alle auf einem Computer gemeinsam vorhanden sein.

Auch die Sicherheit der im Verzeichnis gespeicherten Objekte muss kurz angesprochen werden. Es muss möglich sein, dass alle Verzeichnisbenutzer öffentliche Informationen wie etwa die E-Mail-Adresse eines Kollegen finden können, weiterhin z.B. Mitglieder der Personalabteilung weitere Informationen wie etwa die komplette Privatanschrift lesen können, aber nur die Administratoren die Möglichkeit haben, diese Einträge zu

verändern. Diese Steuerung des Objektzugriffs erfolgt über Access Control Lists. Zu jedem Objekt wird automatisch eine Liste generiert, in der eingetragen wird, welche Benutzer welche Zugriffsrechte für das Objekt besitzen.

1.2 Das Lightweight Directory Access Protocol (LDAP)

Für die Kommunikation zwischen den Active Directory Clients und Servern bei der Netzwerkanmeldung oder dem Auffinden von Ressourcen wird LDAP in der Version 3.0 als das Standardzugriffsprotokoll benutzt. In diesem Kapitel wird Ihnen zunächst eine Übersicht über die Entwicklung von LDAP gegeben. Danach erfolgt eine Übersicht über die definierten LDAP-Standards. Auch der architektonische Aufbau sowie das LDAP-Modell werden ausführlich erläutert.

Bereits in den 70er-Jahren wurde klar, dass aufgrund der zunehmenden Entwicklung von Kommunikations- und Computertechnologien ein Standard geschaffen werden musste, da viele Komponenten untereinander inkompatibel waren. Es gab zwei verschiedene Versuche, die Datenkommunikation zu standardisieren. Ein Ergebnis war das siebenschichtige OSI-Referenzmodell der Datenkommunikation. Die untersten Schichten beschreiben den physikalischen Transport, die oberen Schichten den Transport über die Anwendungsprotokolle. Verantwortlich für die Entwicklung dieses Modells waren das CCITT (Comité Consultatif International Téléphonique et Télégraphique, dann ITU-T (International Telecommunications Union – Telecommunication Standardization Sector) und die ISO (International Standards Organization). Bei diesem Ansatz wurden keine Implementierungen benötigt. Die Transportkommunikation wurde von Grund auf an sich beschrieben.

Der zweite Standard wurde von IAB (Internet Architecture Board) sowie IETF (Internet Engineering Task Force) entwickelt. Alle entwickelten Standards wurden in Form von RFCs (Request for Comment) veröffentlicht. Zwischenzeitlich gibt es über 3200 dieser RFCs. Sie finden das jeweilige Dokument, indem Sie im Internet nach RFC <Nummer> suchen. Im Praxisteil C wird an einigen Stellen auf diese RFCs verwiesen. Nachdem sich diese Standards bewährt haben, werden Sie zu endgültigen Standards (STDs). Bei diesem Ansatz wurden Technologien implementiert und nach positiven Tests als Standard definiert. Da sich das Internet und dessen TCP/IP-Protokoll rasch weiterentwickelten, wurden auf dieser Grundlage weitere Netzwerkprotokolle und -produkte entwickelt.

Die OSI-Protokolle widmeten sich eher Thematiken für große verteilte Systeme, die sich rasch auf dem Internetsektor entwickelten. Eines dieser Gebiete waren auch die Verzeichnisdienste. Bereits 1988 hatte die CCITT den X.500-Standard entwickelt. Dieser erhielt 1990 die ISO-Norm, um genau zu sein ISO 9594 (Data Communications Network Directory Recommendation X.500 – X.521). Bis heute wird dieser Standard als X.500 bezeichnet.

1.2.1 Die X.500- und LDAP-Standards

Bereits 1990 wurde in X.500 der Standard definiert, Einträge im Verzeichnis hierarchisch in einen Namensraum zu gliedern. Da dieser Namensraum bereits in der Lage war, eine große Menge an Informationen zu beinhalten, war auch eine umfangreiche Suchfunktion integriert. Für die Kommunikation zwischen dem Client und Server wurde das Vorgängerprotokoll von LDAP, nämlich DAP (Directory Access Protocol) definiert. DAP benötigte jedoch noch den kompletten OSI-Stack. Damit wurden jedoch sehr viele Ressourcen belegt. Aufgrund dieser Tatsache wurde LDAP als das „leichtgewichtige“ DAP entwickelt. Bei seiner Geburt hieß LDAP zunächst „Lightweight Access Protocol“ (siehe RFC 1487), erst später erhielt es den endgültigen Namen „Lightweight Directory Access Protocol“ (siehe RFC 1777). LDAP benötigt nicht mehr den kompletten OSI-Stack, sondern nur den weniger ressourcenintensiven TCP/IP-Protokoll-Stack. Die ursprüngliche Version war LDAP 2.0. Heute wird LDAP in der Version 3.0 eingesetzt. Dessen Features werden in RFC 2252 definiert.

Die wichtigsten Änderungen zwischen Version 2.0 und 3.0 sind in den folgenden Punkten vorgenommen worden: Verbesserte Suchfunktion wie benutzerdefinierte Suche mit wählbarer Sortierreihenfolge der Ergebnisse, Weiterleitungsverweise von einem Server, der die angeforderten Daten nicht besitzt, zu einem weiteren Server, Verwendung des UTF-8-Standards, sodass für alle Attribute in den Textstrings internationale Zeichen verwendet werden können, sowie Verbesserung der Sicherheit durch Einsatz der erweiterten SASL-(Simple Authentication and Security Layer-)Authentifizierung. Eine Beschreibung aller dieser neuen Features sowie weiterer technischer Spezifikationen befindet sich in den RFCs 2251 bis 2256.

LDAP ist ein Kommunikationsprotokoll, das den Transport sowie das Message-Format definiert, das die Clients für den Zugriff auf ein Verzeichnis benutzen, das nach dem X.500-Standard arbeitet. Die gesamte Kommunikation des LDAP läuft über den Port 389. Im LDAP-Protokoll wird festgelegt, wie der Zugriff auf die Active Directory-Server erfolgen darf, welche Verzeichnisaktionen gestattet sind, welche freigegebenen Daten benutzt werden dürfen oder wie ein sicherer Zugriff durchgeführt werden soll. Über LDAP werden Verwaltung, Abfragen und Auflistungen der Objekte durchgeführt.

In Abbildung 1.1 haben Sie gesehen, dass eine Applikation nicht direkt auf die Verzeichnisdaten zugreifen darf, sondern der Zugriff über eine API gesteuert wird, die über eine Message aufgerufen wird. Hierbei handelt es sich um eine LDAP-API, die von einer LDAP-Message initiiert wird. Der LDAP-Client kann direkt über TCP/IP auf das Verzeichnis des LDAP-Servers zugreifen.

Ursprünglich lagen die Verzeichnisse auf X.500-Servern. Diese waren jedoch nicht in der Lage, LDAP-Messages zu verstehen. Die LDAP-Messages mussten für die X.500-Server für die Kommunikation über OSI aufbereitet werden. Also muss der LDAP-Client über ein Gateway mit dem X.500-Server kommunizieren. Dieses Gateway war der LDAP-Server, der mit dem LDAP-Client per TCP/IP und mit dem X.500-Server über OSI kommuniziert. Im Laufe der Zeit wurden weniger X.500-Server eingesetzt, sodass der LDAP-Server selbst das Verzeichnis enthalten konnte, auf das der LDAP-Client direkt zugreifen kann. Damit wurde der ohnehin ressourceträchtige OSI-Protokoll-Stack für LDAP überflüssig. Abbildung 1.2 zeigt die beiden Zugriffsmöglichkeiten des LDAP-Clients.

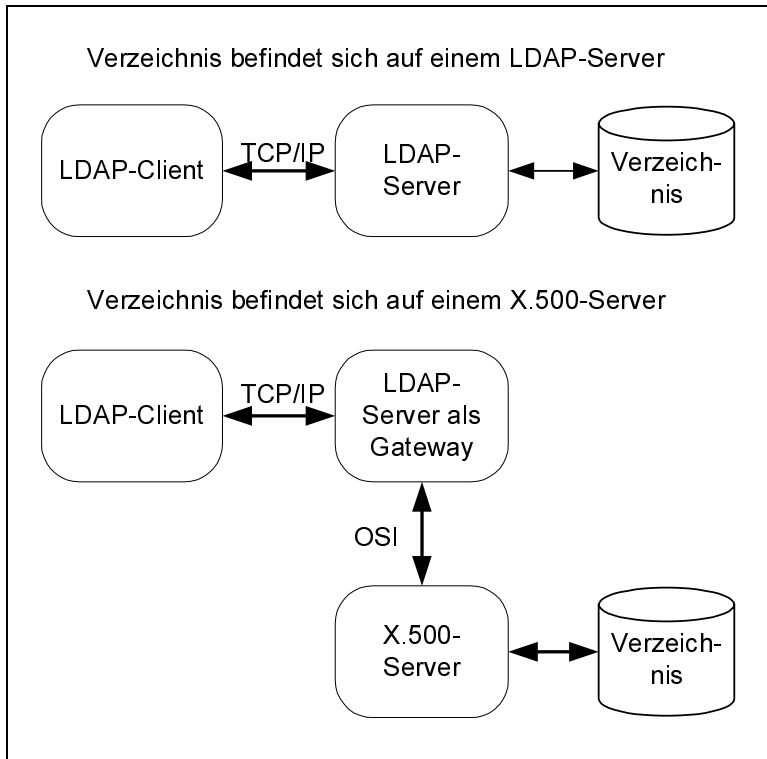


Abbildung 1.2: Zugriff des LDAP-Clients auf das Verzeichnis

Für den LDAP-Client macht es keinen Unterschied, für welche Funktion auf einem Server das LDAP-Protokoll vorhanden ist, ob es sich also um einen LDAP-Server handelt, der das Verzeichnis direkt bereitstellt, oder um einen Gateway-Server, über den man auf das Verzeichnis eines X.500-Servers zugreift.

LDAP hat sich zu einem offenen Industriestandard entwickelt. Über dieses Protokoll können Produkte verschiedener Hersteller in verschiedenen Betriebssystemen miteinander kommunizieren und, vergleichbar dem http-Standard des Internets, damit eine globale Verzeichnisstruktur unterstützen.

1.2.2 Die LDAP-Architektur

Dieses Kapitel stellt Ihnen das logische Modell von LDAP vor. Wie bereits erwähnt, ist LDAP das Zugriffsprotokoll für X.500-basierte Verzeichnisdienste. Gegenüber DAP und OSI bietet LDAP mit Active Directory die folgenden Verbesserungen: LDAP benutzt TCP/IP und nicht den ressourcenintensiven OSI-Protokoll-Stack. Das Funktionsmodell ist vereinfacht und um selten gebrauchte Funktionen erleichtert worden. Außerdem werden normale Zeichenketten zur Darstellung der Daten benutzt und nicht mehr komplizierte Syntaxen wie ASN.1 (Abstract Syntax Notation).

Über LDAP wird die Meldung definiert, die zwischen einem LDAP-Client und LDAP-Server ausgetauscht wird. Über die Meldung seitens des Clients wird die durchzuführende Handlung wie das Suchen oder Löschen eines Objekts angegeben, seitens des Servers die daraus resultierenden Antworten sowie das Format der transportierten Daten. Der Transport der Daten geschieht über das TCP/IP-Protokoll. Für das Design von Active Directory ist wichtig zu wissen, wie das Verzeichnis aufgebaut ist, welche Operationen durchgeführt werden können oder wie Daten auf dem Transport geschützt sind.

Jede Kommunikation zwischen einem LDAP-Client und Server läuft identisch ab. Sie kann in drei Schritte unterteilt werden:

1. Der LDAP-Client stellt die Verbindung zum Server her. Dabei gibt der Client für den Server die IP-Adresse oder den Host-Namen sowie den TCP-Port (389) des LDAP-Servers an. Die Authentifizierung kann auf dreierlei Weise erfolgen: über anonyme Authentifizierung mit Standardzugriffsrechten, der Client kann sich über einen Benutzernamen und Passwort authentifizieren, oder die Verbindung kann verschlüsselt erfolgen.
2. Der Client greift nun auf die Verzeichnisdaten zu. Der Zugriff kann als Schreib- oder Lesevorgang erfolgen. Am häufigsten werden Suchvorgänge sein. Dabei kann ein Benutzer über boolesche Operatoren bestimmen, welche Informationen herausgefiltert werden sollen.
3. Nach Ende der durchgeführten Aktion wird die Verbindung zum Server beendet.

Da LDAP auf dem X.500-Modell basiert, werden dementsprechend die Daten im Verzeichnis als Einträge gespeichert und organisiert. Ein Eintrag ist die Basiseinheit für die gespeicherten Informationen im Verzeichnis. Jeder Verzeichniseintrag beschreibt ein einzelnes Objekt. Jedes Objekt besitzt einen eindeutigen definierten Namen (= Distinguished Name, DN), der sich seinerseits aus einer Reihe von relativ definierten Namen (= Relative Distinguished Name, RDN) zusammensetzt. Diese Namenskette ist vergleichbar mit einem Verzeichnispfad im Windows-Explorer. Diese Objekte werden in einer hierarchischen Baumstruktur angeordnet, die auf den DNs der Objekte basieren. Diese Baumstruktur wird auch Directory Information Tree (DIT) genannt.

Jeder Eintrag besteht aus ein oder mehr Attributen zur Beschreibung des Eintrags. Jedes Attribut besteht aus einem Typ und einem Wert. Diesen Aufbau verdeutlicht Abbildung 1.3.

In unserem Beispiel sind die Attribute Nachname und E-Mail-Adresse herausgegriffen. Die Syntax des Attributs Nachname bestimmt, dass es sich dabei um einen alphanumerischen String handelt. Es können in einer E-Mail-Adresse Buchstaben, Zahlen oder auch Sonderzeichen wie ein Bindestrich (-) vorkommen.

Durch die Verzeichniseinträge wird ein Objekt näher beschrieben. Dabei beschreibt eine Objektklasse ein Objekt. Die Objektklasse Benutzer wird z.B. durch die Attribute Nachname und E-Mail-Adresse beschrieben. Jede Objektklasse hat seine eigenen Attribute, und jedes Attribut hat seinen eigenen Wert. So werden Sie beispielsweise in einem Drucker-Objekt nicht die Attribute Nachname und E-Mail-Adresse finden, sondern eher ein Attribut Farbdrucker. Alle diese Objektklassen und in ihnen mögliche Werte werden als das Active Directory-Schema bezeichnet.



Benutzer-Objekt

DN = RDN.RDN.RDN.RDN
 = PeterMustermann.vertrieb.firma.de
 = eindeutiger Name

Objekt-Einträge

	Typ	Wert
Attribut 1: Nachname	String	Mustermann
Attribut 2: E-Mail-Adresse	String	p.mustermann@ vertrieb.firma.de

Abbildung 1.3: Der Aufbau eines Objekt-Eintrags

Weiterhin wird über LDAP festgelegt, welche Handlungen an einem Verzeichnis-Eintrag vollzogen werden können. Hierzu zählen das Hinzufügen, Löschen, Ändern und Umbenennen eines Eintrags, wobei schreibend auf das Verzeichnis zugegriffen wird, sowie das Suchen und Vergleichen eines Eintrags. Hier erfolgt nur ein lesender Zugriff auf die Verzeichnisdaten.

1.2.3 Die vier LDAP-Modelle

Als Nächstes werden die vier Modelle beschrieben, auf denen LDAP basiert. Dabei handelt es sich um das Informations-, Namens-, Funktions- und Sicherheitsmodell. Die einzelnen Modelle beschreiben LDAP in folgenden Punkten (siehe Tabelle 1.1):

Modell	Beschreibung
Informationsmodell	Strukturbeschreibung der Informationen, die im Verzeichnis gespeichert werden
Namensmodell	Beschreibt, wie die Informationen im Namensraum aufgebaut und organisiert sind
Funktionsmodell	Beschreibt, welche Operationen an den Informationen vollzogen werden können, z.B. Löschen usw.
Sicherheitsmodell	Beschreibt, wie der Zugriff auf die Informationen geschützt wird

Tabelle 1.1: Die vier LDAP-Modelle

Das Informationsmodell

Durch jeden Eintrag im Active Directory wird ein bestimmtes Objekt repräsentiert. Dabei kann es sich um Benutzer, Drucker, Domänen usw. handeln. Jeder Eintrag setzt sich aus einer bestimmten Anzahl von Attributen zusammen, und jedes dieser Attribute hat einen Typ sowie einen oder mehrere dazugehörige Werte. So kann z.B. das Attribut „E-Mail-Adresse“ mehrere Werte haben, wenn ein Benutzer über mehrere Adressen verfügt. Alle Werte eines Attributs müssen jedoch vom gleichen Typ sein. Über die Syntax des Attributs wird bestimmt, welche Zeichen für einen Wert zugelassen sind. Bei einer Telefonnummer werden dies nur Zahlen sein, bei einem Vor- oder Nachnamen nur Buchstaben und u.U. Sonderzeichen.

Außerdem wird über die Syntax festgelegt, wie sich die einzelnen Zeichen der Attribute bei bestimmten Verzeichnis-Operationen wie etwa dem Suchvorgang verhalten sollen. Bei dem Beispiel der Telefonnummer kann über die Syntax Folgendes festgelegt werden:

Die Werte dürfen ausschließlich die Ziffern 0 bis 9 umfassen sowie Leerzeichen und Bindestriche. Wenn mehrere Werte vorhanden sind, werden die Einträge lexikografisch geordnet. Leerzeichen und Bindestriche (um eine Durchwahl zu kennzeichnen) werden ignoriert, da bei einer Suchanfrage nur die Zahl-Zeichen miteinander verglichen werden. Somit ist es gleichgültig, ob eine Telefonnummer in der Form 9988776, 99 88 776 oder 9988-776 angegeben ist.

Tabelle 1.2 gibt Ihnen einen Überblick über einige wichtige Syntaxen, die für LDAP entwickelt worden sind.

Syntax	Beschreibung
Dn	DistinguishedName. Hierbei handelt es sich um einen im gesamten Verzeichnis eindeutigen Namen, der sich aus einer Reihe relativ definierter Namen (RDN) zusammensetzt, z.B. PeterMustermann.vertrieb.firma.de.
Cn	CommonName. Dies ist der Benutzername, also Peter Mustermann.
Sn	Surname. Hierbei handelt es sich um den Nachnamen, also Mustermann.
Bin	Binary Information. Es wird ein Binärwert angegeben.
Ces	Case exact string. Während des Vergleichs wird zwischen Groß- und Kleinschreibung unterschieden wie z.B. bei Passwörtern.
Cis	Case ignore string. Hierbei wird nicht zwischen Groß- und Kleinschreibung unterschieden.
Tel	Telefonnummer. Die Zeichenkette wird als Text behandelt, wobei Leerzeichen und Bindestriche beim Vergleich ignoriert werden.

Tabelle 1.2: LDAP-Beispielsyntaxen

Zusätzlich kann festgelegt werden, wie viele Zeichen ein Wert haben oder wie groß ein Wert insgesamt sein darf. Wenn Sie z.B. ein Geburtsdatum angeben, wird der Wert nie mehr als zehn Zeichen umfassen, selbst wenn Sie die folgende Schreibweise benutzen: 16.05.1975. Fügen Sie zu einem Objekt beispielsweise ein Foto hinzu, so können Sie bestimmen, dass eine Gesamtgröße von z.B. 15 kb nicht überschritten werden darf. Diese Reglementierungen dienen dazu, dass nicht unnötig Speicherplatz verschwendet wird.

Weiterhin ist im Active Directory-Schema festgelegt, welche Werte für die Attribute eines Objekts erforderlich und welche optional sind. Bei einem Benutzerobjekt muss zwangsläufig der Nachname eingetragen werden, während der Wert des Attributs „Beschreibung“ optional ist.

Das Namensmodell

Alle Einträge werden in einer Baumstruktur angeordnet, die sich Directory Information Tree (DIT) nennt. Die Anordnung basiert auf den jeweiligen eindeutigen DN's der Objekte. Der DN setzt sich aus einer Kette von durch Kommata getrennten RDN's zusammen, wobei jeder RDN einer Hierarchieebene im DIT entspricht. Jeder RDN wird aus den Attributen eines Eintrags hergeleitet. Sehen wir uns dieses Verfahren am DN eines Computers an, der über die folgenden Merkmale verfügt: Der Computer heißt „Archimedes“, befindet sich in einer Organisationseinheit „Finanzen“ in der Domäne „firma.de“. Jeder dieser Namensteile ist ein RDN. Der DN wird automatisch gebildet, sobald ein Objekt erstellt wird. Der definierte Name für unser Beispiel lautet also DN = RDN1,RDN2,RDN3,RDN4, z.B. DN: cn=Archimedes,dc=firma,dc=de

Die Bedeutungen der Attribute cn und dc werden in der nächsten Tabelle beschrieben. Sie müssen diese Namen selbstverständlich nicht in diesem Format ins Active Directory einpflegen. Aus den Attributen, die Sie dort mit Werten füllen, wird automatisch ein DN im LDAP-konformen Format gebildet. Erst wenn Sie Ihr Schema erweitern oder ändern, müssen Sie LDAP-konform arbeiten. Das Support-Tool LDP (siehe Kapitel 23.1.14) bietet zudem die Möglichkeit, in einer grafischen Oberfläche direkt auf LDAP-Ebene zu arbeiten.

Die höchste Ebene im DIT ist das Länderkürzel, die niedrigste der Name des Objekts. Der DN setzt sich aus den RDN's zusammen, die von der niedrigsten DIT-Ebene zur höchsten hin zusammengesetzt und gelesen werden. Die Tiefe des DIT ist nicht eingeschränkt. Sie können also so viele Hierarchieebenen bilden, wie sie für die Abbildung Ihrer Unternehmensstruktur notwendig sind. Bedenken Sie aber auch, dass mit zunehmender Tiefe auch die Unübersichtlichkeit zunimmt. Ebenfalls gibt es keine Beschränkung für die Breite des DIT. Sie können also auf einer Hierarchieebene beliebig viele Domänen, Organisationseinheiten, Benutzer usw. einrichten.

Tabelle 1.3 zeigt Ihnen die wichtigsten Attributtypen. Bei keinem dieser Attributtypen wird zwischen Groß- und Kleinschreibung unterschieden.

Zeichenkette	Attributtyp
Dc	Domain Component: Name der Domänenbestandteile
Cn	Common Name: Objektname
C	Country: Ländername
St	StateOrProvinceName: Name eines Bundeslandes
L	LocalityName: Name einer Stadt
O	OrganizationName: Firmenname
Ou	OrganizationalUnit: Name der Organisationseinheit
Uid	UserID

Tabelle 1.3: Die wichtigsten Attributtypen

Da sich auf einem einzelnen LDAP-Server möglicherweise nicht der komplette DIT, sondern nur die Einträge für untere Hierarchieebenen befinden, in denen er eigenständige Einträge besitzt, müssen die Server untereinander verlinkt sein, damit alle Informationen im Verzeichnis gefunden werden können. Ein Server muss in seinem DIT nicht alle übergeordneten Einträge speichern. Der oberste Eintrag, den ein Server besitzt, wird auch als Suffix oder Naming Context (Namenskontext) bezeichnet.

Auf Abbildung 1.4 sehen Sie Server 1, der das Suffix `dc=firma,dc=de` trägt. Dies sind die obersten Einträge des DIT. Dieser Server speichert jedoch nicht selbst die Einträge für `ou=marketing,dc=firma,dc=de`, sondern verweist auf einen zweiten Server, der über diese Informationen verfügt. Dieser Verweis wird auch als „Referral“ bezeichnet. Server 2 beginnt mit dem DIT ab der Hierarchieebene „marketing“. Er besitzt keine Einträge für `dc=firma,dc=de`. Innerhalb der OU „Marketing“ befinden sich diverse Objekte. Herausgegriffen sind das Benutzerobjekt `cn=Peter Mustermann` und das Computerobjekt `cn=Archimedes`.

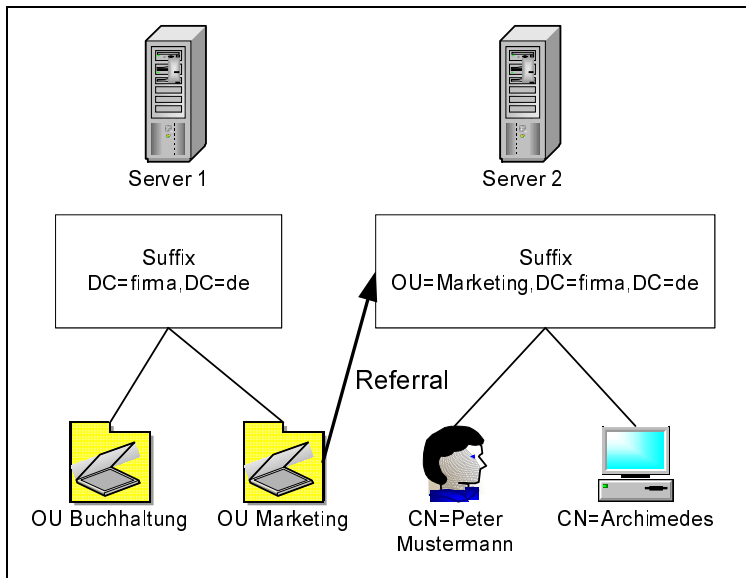


Abbildung 1.4: Der DIT auf mehreren Servern verteilt

Damit ein Benutzer alle Einträge im Verzeichnis auffinden kann, sind die Referrals wichtig. Hierbei handelt es sich um einen Link auf einen zweiten Server, der den DIT für das gesuchte Objekt beherbergt. Angenommen, ein Benutzer sucht den Computer „Archimedes“ in der Organisationseinheit „Marketing“. Würde diese Suche auf die Einträge von Server 1 beschränkt sein, könnte das Computerobjekt nicht gefunden werden. Auf Server 1 ist jedoch ein Link gespeichert, der auf die Organisationseinheit verweist. Dieser Link führt direkt zu den gespeicherten Einträgen für die OU.

Fragt nun ein Client einen Server nach einem bestimmten Objekt, kann die Antwort der Link sein. Der Link wird vom Server nicht weiter verfolgt, sondern an den Client übergeben. Der Client folgt dann direkt dem im Link angegebenen Pfad, um das Objekt zu finden. Von dem im Link angegebenen Server wird die Antwort zurück an den Client gesendet.

Bei diesem Link handelt es sich um den Eintrag in der Objektklasse „Referral“ mit dem Attribut `ref`. Der Wert ist die entsprechende LDAP-URL auf einen Server. Über die Referrals ist es möglich, Informationen über einen weit verzweigten DIT über mehrere Server zu finden.

Schließlich muss auch jeder LDAP-Server Informationen über sich selbst bereitstellen. Hierzu wird ein spezieller Eintrag mit dem Namen Root-DSE (Directory Service Entry) benutzt. Der DN ist ein leerer Wert (Null-Wert), er besitzt lediglich einige Attribute. Im Root-DSE sind die folgenden Informationen über jeden Server enthalten:

- ▶ Die unterstützte(n) LDAP-Version(en)
- ▶ Liste der unterstützten SASL-Sicherheitsmechanismen
- ▶ Liste der alternativen LDAP-Server
- ▶ Die Liste der Suffixe / Namenskontexte, die der Server speichert
- ▶ Den DN eines speziellen Eintrags, der alle dem Server bekannten Objektklassen sowie Schema-Attribute auflistet
- ▶ Eine Liste der unterstützten Erweiterungen des LDAP-Protokolls

Das Funktionsmodell

LDAP gibt die Operationen vor, die an den im Verzeichnis gespeicherten Objekten vorgenommen werden können. Dazu zählen Abfrage-, Update- sowie Authentifizierungsvorgänge. Jede dieser Operationen kann mehrere Vorgänge beinhalten. Darüber soll die folgende Tabelle Aufschluss geben:

Operation	Beschreibung
Abfrage	Umfasst die Such- und Vergleichsfunktionen, um Informationen aus dem Verzeichnis zu beziehen.
Update	Unter dieser Operation werden alle Vorgänge zusammengefasst, die ein Objekt aktualisieren. Dazu zählen das Hinzufügen, Ändern, Löschen und Verschieben von Objekten.
Authentifizierung	Umfasst alle Operationen zur Verbindungsherstellung und Trennung zu und von einem LDAP-Server sowie das Durchsetzen der Zugriffsrechte und Schutz der Informationen.

Tabelle 1.4: Die von LDAP definierten Operationen

Zunächst werden kurz die Update- und Authentifizierungsoperationen näher beschrieben. Da die häufigste dieser Operationen die Suche und der Vergleich sind, werden diese ausführlichst danach beschrieben.

Bei Update-Operationen werden die Verzeichnisinhalte geändert. Die folgend definierten Operationen sind möglich:

Operation	Beschreibung
Add	Es werden neue Einträge im Verzeichnis erstellt.
Delete	Vorhandene Einträge werden aus dem Verzeichnis entfernt.
Modify	Es werden die Attribute und Werte eines Eintrags geändert. Dazu zählen das Hinzufügen, Löschen sowie Modifizieren von Attributen.
Modify DN	Hierbei wird entweder der am weitesten links stehende RDN, also der Objektname, geändert, oder aber ein kompletter DN-Eintrag wird an eine andere Stelle im DIT verschoben.

Tabelle 1.5: Die Update-Operatoren

Die Authentifizierungs-Operationen werden beim Herstellen und Beenden einer Verbindung zum LDAP-Server durchgeführt. Die Sitzung selbst kann auf verschiedenen Sicherheitsleveln basieren. Es sind eine unsichere anonyme Sitzung, eine durch den Client passwort-authentifizierte Sitzung oder auch eine verschlüsselte Sitzung möglich. Die folgenden Authentifizierungs-Operationen sind möglich:

Operation	Beschreibung
Bind	Hierdurch wird die Sitzung initiiert. Der Client lässt sich dabei vom Server authentifizieren.
Unbind	Die Sitzung zwischen Client und Server wird beendet.
Abandon	Der Client kann den Server auffordern, eine noch ausstehende Operation aufzugeben.

Tabelle 1.6: Die Authentifizierungs-Operatoren

Die häufigste aller Operationen ist die Suche von Informationen im Verzeichnis. Aufgrund der großen Flexibilität in der Suche sind auch die Optionen sehr komplex. Beim Suchvorgang stellt der Client eine Anfrage an einen LDAP-Server. Der DIT des Servers wird nach den Informationen durchsucht, die mit den vom Benutzer vorgegebenen Kriterien übereinstimmen. Die Vorgänge des Lesens und Auflistens der gefundenen Informationen sind im Suchvorgang integriert. Sie gelten unter LDAP nicht als separate Operation.

Bei einer Suche können die folgenden Kriterien vorgegeben werden:

- ▶ Der Startpunkt der Suche im DIT
- ▶ Wie tief im DIT gesucht werden soll
- ▶ Welche Attribute ein Eintrag haben muss, damit es als Treffer gewertet werden kann
- ▶ Welche Attribute für die gefundenen Einträge zurückgegeben werden

Es könnten also z.B. folgende Kriterien für eine Suche vorgegeben werden:

- ▶ Finden der E-Mail-Adresse von cn=Peter Mustermann,ou=marketing,dc=firma,dc=de
- ▶ Finden der E-Mail-Adresse und der Handynummer von allen Personen in der Organisationseinheit Marketing, deren Nachname mit N beginnt und bei denen eine Privatadresse eingetragen ist.

Um eine Suche durchzuführen, müssen Parameter angegeben sein. Sobald ein Benutzer Suchkriterien über die GUI eingibt (siehe Abbildung 1.5), werden daraus LDAP-Abfragen generiert.



Abbildung 1.5: Suchkriterien für eine Suche im Verzeichnis

Angenommen, ein Benutzer hat eine Suche nach einer Person definiert, bei der für das Ergebnis zwei Kriterien erfüllt sein müssen. Erstens muss der Vorname der Person mit A beginnen, und zweitens muss in der E-Mail-Adresse die Zeichenfolge marketing vorkommen. Die folgenden Parameter müssen für eine Suche angegeben werden:

- ▶ Der Startpunkt für die Suche. Ein DN gibt den Startpunkt an, der auch Base Object genannt wird. Es kann im gesamten Verzeichnis oder nur in einer bestimmten Domäne gesucht werden.
- ▶ Die Tiefe der Suche im DIT vom Startpunkt aus gerechnet. Dafür gibt es drei Möglichkeiten: baseObject, singleLevel oder wholeSubtree. Bei baseObject wird nur das Basisobjekt, also der Startpunkt durchsucht, singleLevel durchsucht nur die direkt vom Basisobjekt abstammenden Einträge ohne das Basisobjekt selbst, und wholeSubtree durchsucht alle vom Basisobjekt abstammenden Einträge einschließlich des Basisobjekts selbst. Enthält ein Server nicht das Basisobjekt, wird der Referral auf einen anderen Server zurückgegeben. Ein Referral kann im Suchergebnis zusammen mit anderen Einträgen ausgegeben werden, die den Suchkriterien entsprechen. Diese Referrals werden dann als „Continuation References“ bezeichnet, da sie angeben, an welchem Punkt die Suche nach dem gewünschten Objekt fortgesetzt werden kann. Der Benutzer kann selbst entscheiden, ob er den Referrals weiter folgen will, um einen Eintrag zu finden.
- ▶ Über Suchfilter werden die Kriterien festgelegt, die ein Eintrag erfüllen muss, damit er als Ergebnis wiedergegeben wird. Für die Suchfilter werden Boolesche Operatoren benutzt. Bei der Feststellung jedes Attributwerts wird überprüft, ob er größer, kleiner oder gleich usw. dem vorgegebenen Kriterium ist. Die folgende Tabelle gibt eine Übersicht über die Operatoren der Filter, die für die Suche verwendet werden können. Bei dem Suchfilter cn=Archimedes ist cn das Attribut, = der Operator und Archimedes der Wert.

Operator	Beschreibung	Beispiel
=	Es werden nur die Einträge ausgegeben, deren Attribute gleich dem Wert sind. Der * kann als Wildcard für einen beliebigen String stehen.	cn=Archimedes gibt nur die Einträge aus, deren CN-Attribut den Wert Archimedes besitzt. cn=Ar* findet Archimedes und Aristoteles.
> =	Es werden die Einträge ausgegeben, deren Attribute größer oder gleich dem Wert sind.	cn > =Archimedes gibt alle Einträge von Archimedes bis Z* aus.
< =	Es werden die Einträge ausgegeben, deren Attribute kleiner oder gleich dem Wert sind.	cn < = Archimedes gibt alle Einträge von A* bis Archimedes aus.
= *	Es werden alle Einträge ausgegeben, die für das betreffende Attribut einen beliebigen Wert gesetzt haben.	CN= * gibt alle Einträge aus, die das Attribut CN besitzen.
~ =	Es werden die Einträge ausgegeben, deren Attribute annähernd mit dem angegebenen Wert übereinstimmen. Dieser Algorithmus wird bei Wörtern angewendet, die sich fonetisch ähneln.	~ = Archimedes wird den Eintrag Archimedes finden.

Tabelle 1.7: Suchfilter-Operatoren

Diese Operatoren können zusätzlich noch mit Booleschen Operatoren kombiniert werden, um komplexere Abfragen zu gestalten und Suchfilter miteinander zu verknüpfen. Es gibt drei Boolesche Operatoren, die in der folgenden Tabelle beschrieben werden.

Operator	Beschreibung	Syntax	Beispiel
&	Gibt die Einträge zurück, die in allen gewählten Filtern zutreffen.	(& (Filter1) (Filter2) (Filter3))	(&(cn=Archimedes) (ou=marketing) (dc=firma): gibt alle Einträge mit dem Namen Archimedes in der OU Marketing der Domäne Firma aus.
	Gibt die Einträge zurück, die mindestens in einem Filter zutreffen.	((Filter1) (Filter2) (Filter3))	((cn=Archimedes) (cn=Platon)): gibt alle Einträge mit dem Namen Archimedes oder Platon aus.
!	Gibt die Einträge zurück, für die der Filter nicht zutrifft. Hierbei kann immer nur ein Filter angegeben werden.	(! (Filter))	(!(cn=Archimedes): gibt alle Einträge aus, die nicht den Namen Archimedes tragen.

Tabelle 1.8: Die Booleschen Operatoren

Bei der Suche werden die Attribute und Werte miteinander verglichen. Verfügt ein Eintrag über den gesuchten Wert, gibt der Vergleichsvorgang TRUE aus. Ist im Eintrag nicht der gesuchte Wert enthalten, wird FALSE ausgegeben.

- Es wird festgelegt, welche Attribute eines gefundenen Eintrags dem Benutzer angezeigt werden, wenn der Eintrag über mehrere Attribute verfügt. Damit kann es dem Benutzer ermöglicht werden, nur die Attribute zu sehen, die für ihn interessant sind.
- Die Aliasnamen für Einträge können als Verweis verwendet werden oder nicht. D.h., es wird unterschieden, ob der Aliaseintrag selbst oder der Eintrag, auf den durch das Alias gezeigt wird, für die Suche benutzt wird. Wenn Aliasnamen nicht als Verweise angesehen werden, sind sie ein alternativer Name für das Objekt. Wird ein Aliasname als Verweis angesehen, können die Aliasnamen selbst anstatt des Eintrags durchsucht werden.
- Der Benutzer kann für jede Suche das Größenmaximum des Suchergebnisses sowie die maximale Suchzeit für die Einträge bestimmen. Serverseitig können diese Limits aber weiter herabgesetzt werden. Die Beschränkungen sind sinnvoll bei einer Suche in umfangreichen Verzeichnisstrukturen.

Das Sicherheitsmodell

Das letzte zu beschreibende Modell ist das Sicherheitsmodell. Das Sicherheitsmodell basiert auf der Bind-Operation, siehe Tabelle 1.6. Da es verschiedene Authentifizierungsverfahren des Clients gibt, gibt es auch verschiedene Sicherheitsmechanismen. Der Client kann zur Authentifizierung an den Server seinen DN sowie das Passwort im Klartext senden. Das Senden von Passwörtern im Klartext sollte aber nur dann durchgeführt werden, wenn während des Sendevorgangs gewährleistet ist, dass das Passwort nicht von unautorisierten Dritten abgefangen werden kann. Wenn der Client keinen DN und kein Passwort zur Authentifizierung angibt, eröffnet der LDAP-Server eine anonyme Sitzung.

Die dritte Möglichkeit besteht in einer verschlüsselten Sitzung. LDAP in der Version 2.0 verwendete dazu Kerberos. Dieses Verfahren wurde in der Version 3.0 durch SASL (Simple Authentication and Security Layer) abgelöst. Hierbei handelt es sich um ein Authentifizierungs-Framework, das viele verschiedene Methoden der Authentifizierung bietet.

In SASL werden alle Verbindungsprotokolle, so auch LDAP (z.B. aber auch POP3 und SMTP), als ein Profil dargestellt, und jedes dieser Profile wird als Protokollerweiterung betrachtet. Über diese Erweiterung wird die Zusammenarbeit zwischen Protokoll und SASL ermöglicht. Die Protokolle müssen für die Zusammenarbeit um einen bestimmten Befehl erweitert sein, um den Authentifizierungsmechanismus zu identifizieren und den gegenseitigen Austausch der Authentifizierung durchzuführen. Zusätzlich kann – aber muss nicht – ein Sicherheits-Layer ausgehandelt werden, um die Daten nach erfolgreicher Authentifizierung zu verschlüsseln und damit eine sichere Sitzung abzuhalten.

Die gewählte Sicherheitsmethode wird von drei Parametern beeinflusst. Dabei handelt es sich um den DN, den Mechanismus sowie die Identifizierungsdaten. Der DN gibt den Verzeichniseintrag an, über den Sie die Verbindung herstellen möchten. Dabei kann es sich um eine User-ID mit zugehörigem Passwort handeln. Über den Mechanismus (Mechanism) wird die zu verwendende Sicherheitsmethode angegeben. Dabei kann es sich z.B. um Kerberos, GSSAPI oder EXTERNAL handeln. Zu EXTERNAL zählt auch der unter LDAP am

häufigsten benutzte Mechanismus SSL (Secure Socket Layer) bzw. dessen Nachfolger TLS (Transport Layer Security). Um herauszufinden, welche SASL-Mechanismen der LDAP-Server unterstützt, geben Sie folgende URL in die Adresszeile eines Webbrowsers ein:

Ldap://<Name des LDAP-Servers>/?supportedsaslmecanismus

Die Identifizierungsdaten (Credentials) umfassen beliebige Daten, über die der DN identifiziert werden kann. Das Format ist abhängig vom gewählten Sicherheitsmechanismus.

Die SASL-Bindung ruft eine bestimmte API-Funktion auf. Dabei rufen die Applikationen der LDAP-Clients den SASL-Protokolltreiber auf dem Server auf. Dieser Treiber verbindet sich mit der im SASL-Mechanismus definierten Authentifizierungsmethode, um die für den Client erforderlichen Authentifizierungsinformationen zu beziehen. SASL ist der Vermittler zwischen der Authentifizierungsmethode und dem Protokoll.

Die Verbindung zwischen dem LDAP-Client und -Server ist nur während der Aushandlung des Sicherheitsmechanismus noch nicht geschützt. Ist jedoch ein Mechanismus ausgehandelt, ist die Verbindung gegen Angriffe von außen geschützt.

Wie bereits erwähnt, werden in SASL die SSL- und TLS-Mechanismen meistens für LDAP benutzt. Deshalb sollen SSL und TLS kurz vorgestellt werden. TLS ist der Nachfolger von SSL. TLS bietet aber vollständige Abwärtskompatibilität zu SSL in der Version 3.0. Beide Mechanismen arbeiten nach demselben Verfahren, sodass in den nächsten Absätzen auch TLS gemeint ist, wenn nur von SSL die Rede ist. Über das SSL-Protokoll sind sowohl Authentifizierung als auch Datensicherheit möglich. SSL kann von jeder TCP/IP-Applikation benutzt werden, um die Verbindung zu sichern, da der TCP/IP-Socket gekapselt wird. Der SSL-Layer liegt über dem TCP/IP-Layer des Netzwerkprotokolls. Dieser SSL-Mechanismus wird von den darüber liegenden Protokollen wie LDAP, http oder SMTP benutzt.

SSL verwendet das Verfahren eines öffentlichen Schlüssels für die Authentifizierung und den Datenaustausch zwischen Client und Server. Es wird ein Schlüsselpaar privater und öffentlicher Schlüssel verwendet, die gegenseitig die verschlüsselten Daten wieder entschlüsseln können. Das Schlüsselpaar aufseiten des Servers wird beim Einrichten eines Servers automatisch generiert.

Es werden nun die Schritte beschrieben, die nach der Aushandlung der SSL-Verbindung zwischen Client und Server ablaufen. Der Vorgang lässt sich in sechs Schritte untergliedern:

1. Der Client teilt dem Server mit, dass er eine SSL-Sitzung eröffnen möchte.
2. Der Server antwortet mit einem Zertifikat, das u.a. folgende Dinge beinhaltet: den öffentlichen Schlüssel des Servers, die Identität des Clients, für den das Zertifikat herausgegeben wurde, den Namen des Zertifikatherausgebers sowie die Gültigkeitsdauer des Zertifikats.
3. Der Client sendet eine Anforderung an den Server, damit dieser seine Identität beweist. Damit wird festgestellt, ob das Zertifikat wirklich vom Server gesendet wurde.
4. Der Server sendet eine Message, die mit seinem privaten Schlüssel verschlüsselt ist als Bestätigung seiner Identität. Der Client entschlüsselt diese mit dem öffentlichen Schlüssel des Servers aus Schritt 2. Ist die Entschlüsselung erfolgreich, wird die Identität des Servers anerkannt, und die Authentifizierung ist abgeschlossen.

5. Nun müssen sich Client und Server auf einen Sicherheitsschlüssel, d.h. ein symmetrisches Schlüsselpaar, einigen, über das die Daten verschlüsselt werden. Der Client generiert einen der symmetrischen Schlüssel und verschlüsselt diesen mit dem öffentlichen Schlüssel des Servers aus Schritt 2 und schickt ihn an den Server. Diesen Sicherheitsschlüssel kann nur der Server mit seinem privaten Schlüssel öffnen.
6. Der Server entschlüsselt den Sicherheitsschlüssel und sendet eine zufällige Testmessage an den Client, die mit dem Sicherheitsschlüssel verschlüsselt wurde. Damit zeigt der Server, dass ihn der Sicherheitsschlüssel vom Client ordnungsgemäß erreicht hat. Danach kann die Kommunikation mithilfe des symmetrischen Sicherheitsschlüssels beginnen.

1.3 Die Architektur des Active Directory

Im Folgenden wird zuerst die Active Directory-Architektur innerhalb der Windows 2000-Betriebssystem-Architektur beschrieben. Danach wird die Architektur des Active Directory an sich vorgestellt.

1.3.1 Active Directory in der Betriebssystem-Architektur

Dieses Kapitel beschreibt, in welchen Bereichen der Zugriffsmodi des Betriebssystems Active Directory ausgeführt wird. Um dies zu verstehen, muss ein wenig weiter ausgeholt werden und als kleiner Exkurs ein Überblick über das Windows 2000-Architekturmodell erfolgen.

Eines sei noch vorweg gesagt: In diesem Kapitel erwartet Sie eine Fülle von Fachbegriffen, die nicht alle bis ins Detail erläutert werden. Für die in diesem Kapitel erwähnten und nicht detailliert beschriebenen Begriffe der Windows 2000-Architektur sei auf die Windows 2000-Hilfe verwiesen. Hierbei handelt es sich um Komponenten, die in eine allgemeine Windows 2000-Beschreibung gehören, aber nicht in ein Active Directory-Handbuch, da sie sich nicht speziell auf diese Thematik beziehen. Lediglich die Komponenten, die von Active Directory benutzt werden, werden ausführlicher erläutert.

Als Einführung finden Sie einen grafischen Überblick über den Aufbau des Betriebssystems Windows 2000 und der darin enthaltenen Komponenten. Die von Active Directory benutzten Komponenten sind darin hervorgehoben. So können alle nachfolgenden Beschreibungen anhand des Bildes (siehe Abbildung 1.6) verifiziert werden.

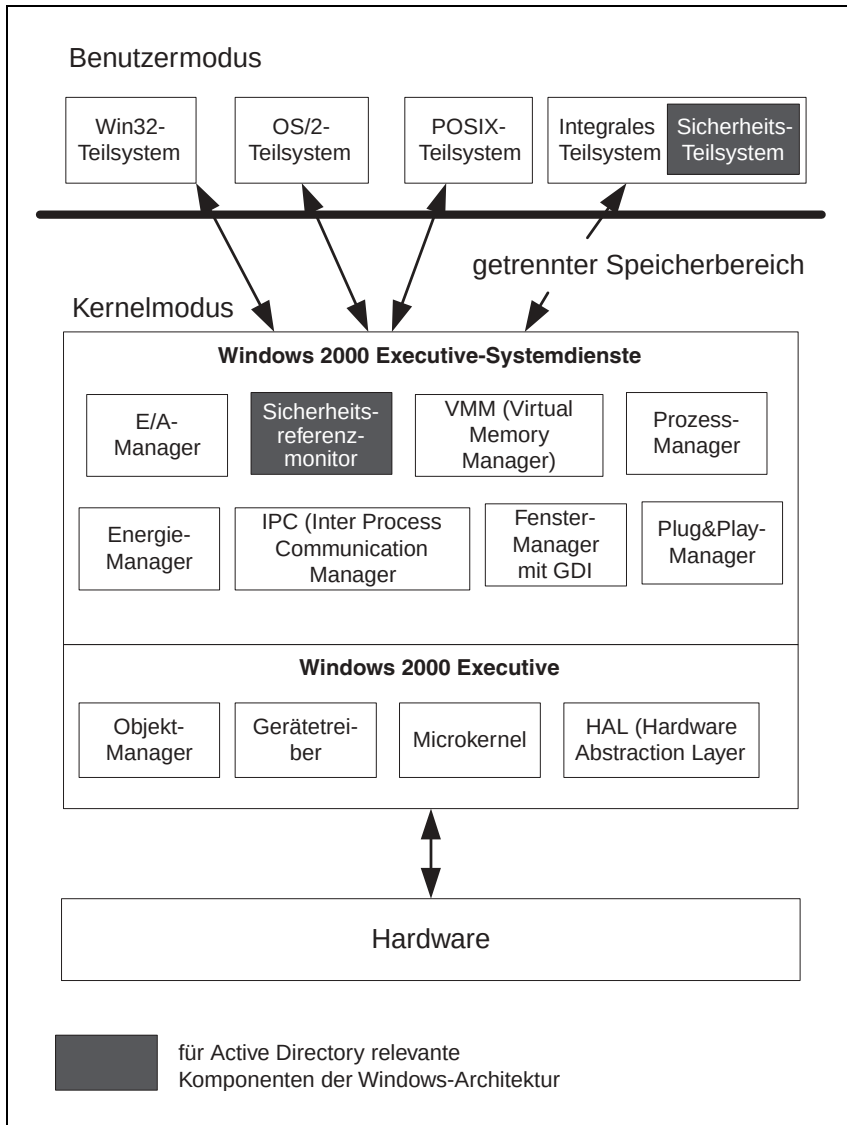


Abbildung 1.6: Die Windows 2000-Betriebssystemarchitektur

Die Windows 2000-Architektur teilt sich in zwei voneinander getrennte Schichten, in den Kernelmodus und den Benutzermodus.

Benutzermodus

Der Benutzermodus spaltet sich wiederum in die Bereiche Umgebungsteilsysteme und integrale Teilsysteme auf.

► Benutzermodus – Umgebungsteilsysteme

Unter Windows 2000 können Anwendungen ausgeführt werden, die eigentlich für andere Betriebssysteme geschrieben worden sind. Im Umgebungsteilsystem erfolgt eine Emulation dieser Betriebssysteme. Dies geschieht, indem die APIs (Application Programming Interfaces), die für die Anwendung erforderlich sind, unter Windows zur Verfügung gestellt werden. Die API-Aufrufe werden im Umgebungsteilsystem so konvertiert, dass Windows 2000 das Format der API verstehen kann. Diese Windows 2000-gerecht konvertierte API kann dann an die Executive im Kernelmodus weitergeleitet werden. Hierdurch wird sichergestellt, dass die Anwendungen nicht direkt auf Gerätetreiber und Hardware zugreifen können. Auch der Zugriff auf APIs für die Windows-Zwischenablage oder das Umschalten von Tasks wird unterbunden. Die Prozesse laufen alle mit einer niedrigeren Priorität als die des Kernelmodus. Es gibt die folgenden drei Umgebungsteilsysteme:

- Win32-Teilsystem: Für Windows 16-Bit- oder auf MS-DOS basierende Anwendungen wird eine Umgebung bereitgestellt.
- OS/2-Teilsystem: Bereitstellung von APIs für 16-Bit-OS/2-Anwendungen
- POSIX-Teilsystem (= Portable Operating System Interface for Unix): Bereitstellung von APIs für Unix-Anwendungen

► Benutzermodus – Integrale Teilsysteme

Das integrale Teilsystem umfasst eine große Anzahl wichtiger Betriebssystemfunktionen. Im Zusammenhang mit Active Directory ist nur das Sicherheitsteilsystem relevant. In diesem Teilsystem werden die folgenden Aktionen durchgeführt: Überprüfung, welche Systemressourcen überwacht werden, Überwachen von Benutzerkonten und den diesen erteilten Rechten sowie Überprüfung der Anmeldeauthentifizierung. Auch die Durchsetzung, Replikation und Zwischenspeicherung der Wiederherstellungsrichtlinie für Daten wird vom Sicherheitsteilsystem gesteuert.

Weitere wichtige Komponenten der integralen Teilsysteme sind z.B. die Dienste Arbeitsstation und Server.

Kernelmodus

Im Kernelmodus erfolgt ein direkter Zugriff auf die Hardware und Systemdaten. Die Ausführung erfolgt in einem getrennten Speicherbereich, da direkt auf den Arbeitsspeicher zugegriffen wird. Der Kernelmodus besteht aus vier Teilen: Windows 2000 Executive, Gerätetreiber, Mikrokern sowie HAL (Hardware Abstraction Layer).

► Kernelmodus – Windows 2000 Executive

Die Windows 2000 Executive besteht aus einem ganzen Satz von Komponenten. Die gesamte Executive ist zuständig für E/A-Vorgänge, Sicherheit und Objektverwaltung. Diese Komponenten werden unterteilt in Systemdienste, die sowohl Teilsystemen des Benutzermodus als auch Executive-Komponenten zur Verfügung stehen, und interne Routinen, die nur von Komponenten der Executive verwendet werden können. Der Objektmanager ist eine interne Routine und damit Teil der eigentlichen Executive. Er ist für die Verwaltung von Prozessen, Threads usw. zuständig. Die einzelnen Systemdienste sind: E/A-Manager, Sicherheitsreferenzmonitor, VMM (Manager des virtuellen Speichers, Prozess-Manager, Energie-Manager, IPC (Inter Process

Communication-Manager), Fenster-Manager mit GDI (Graphical Device Interface) sowie Plug and Play-Manager. Im Zusammenhang mit Active Directory ist von den Systemdiensten nur der Sicherheitsreferenzmonitor wichtig. Diese Komponente ist dafür zuständig, dass auf dem betreffenden lokalen Rechner die über Active Directory zugewiesene Sicherheitsrichtlinie durchgesetzt wird.

► **Kernelmodus – Gerätetreiber**

Durch die Gerätetreiber werden Treiberaufrufe vom Betriebssystem oder von Applikationen zur Steuerung der entsprechenden Hardwarekomponente in ausführbaren Maschinencode übersetzt, d.h. Assemblerbefehle. Treiber und Programme greifen unter Windows 2000 nie direkt auf die Hardware zu wie unter DOS, sondern immer über das Betriebssystem. Dies steigert die Systemstabilität und Sicherheit. Keine Applikation soll am OS vorbei operieren können.

► **Kernelmodus – Mikrokern**

Hierdurch erfolgt die Verwaltung des Mikroprozessors. Dies beinhaltet eine Synchronisation aller Windows 2000 Executive-Dienste und die Koordination aller E/A-Funktionen.

► **Kernelmodus – HAL**

Durch die HAL ist eine Portierung von Windows 2000 auf andere Hardwarearchitekturen möglich. Die HAL beinhaltet den hardwarespezifischen Code für die Kommunikation, IRQ-Steuerung usw. verschiedener Prozessortypen. Dadurch ist es z.B. möglich, Windows 2000 mit nur einer einzigen Windows 2000 Executive auch auf Alpha-Prozessoren zu betreiben.

1.3.2 Die Active Directory-Architektur

Auf diesen Erkenntnissen aufbauend erhalten Sie nun Einblick in die Architektur von Active Directory. Sie sehen zunächst ein Schaubild, anhand dessen Sie die nachfolgenden Informationen nachvollziehen können. Abbildung 1.7 zeigt eine Übersicht über das Active Directory-Schichtenmodell sowie der verwendeten Zugriffsmechanismen.

Active Directory gliedert sich in drei Schichten. In diesen Dienstsichten sind verschiedene Informationstypen enthalten, über die die Daten in der Active Directory-Datenbank gefunden werden. Über diesen Schichten liegen vier Zugriffsmechanismen für die Kommunikation zwischen den Clients und dem Verzeichnisdienst. Dabei handelt es sich um Protokolle und APIs.

Active Directory-Schichten

Es gibt die drei folgenden Active Directory-Schichten:

1. **DSA (Directory System Agent / Verzeichnissystem-Agent)**

Der DSA greift auf die Informationen der Active Directory-Datenbank zu. Diese Datenbank beinhaltet alle Informationen, die physisch auf einer Festplatte des Domänencontrollers gespeichert sind. Über den DSA wird den Clients einer der vier Zugriffsmechanismen für das Verzeichnis bereitgestellt. Diese werden im Absatz „Active Directory Zugriffsmechanismen“ erläutert. DSA ist Teil des lokalen Sicherheitsteilsystems im Benutzermodus des Betriebssystems.

2. Datenbankschicht

Die Datenbankschicht ist eine Pufferzone zwischen Applikationen, die auf die Datenbank zugreifen, und der Datenbank selbst. Die Aufrufe der Anwendungen können so nicht direkt an die Datenbank gesendet werden. Die Kommunikation wird über die Datenbankschicht umgeleitet.

3. ESE (Extensible Storage Engine / erweiterbares Speichermodul)

Über die ESE erfolgt eine direkte Kommunikation mit den Daten in der Verzeichnisdatenbank. Die Kommunikationsgrundlage bilden die relativ definierten Namen der Datenbankobjekte. Die ESE ist die einzige Schicht, die direkt auf die Datenbankdatei NTDS.DIT zugreifen kann.

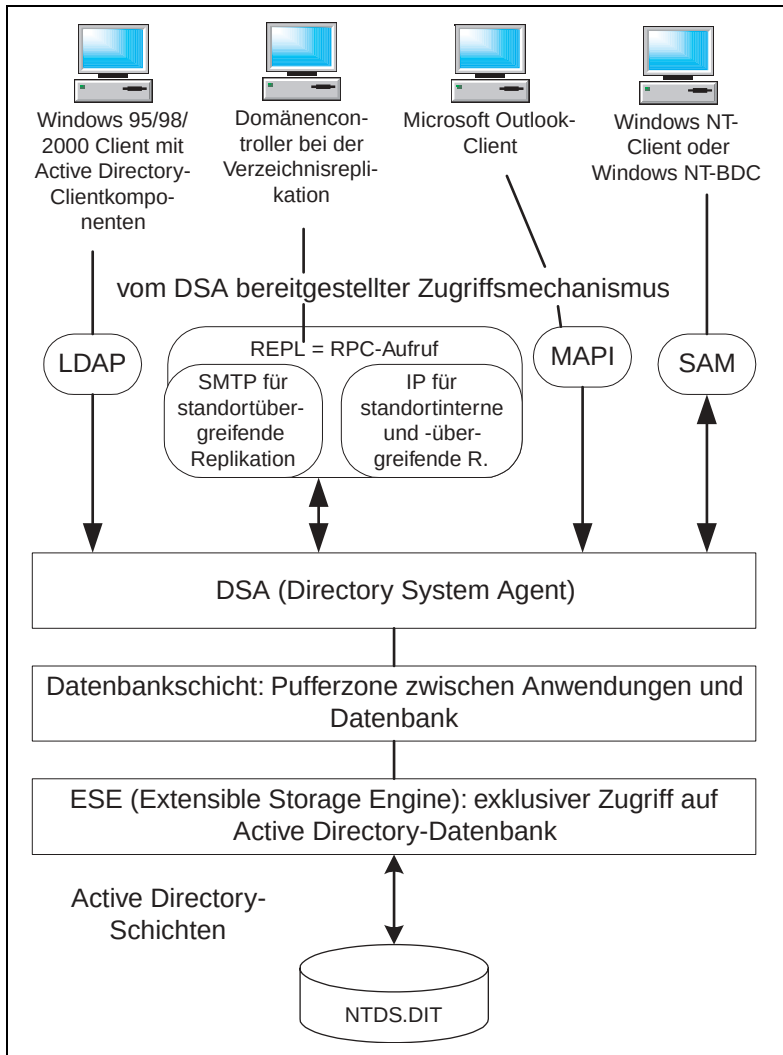


Abbildung 1.7: Übersicht über die Active Directory-Architektur

Active Directory-Zugriffsmechanismen

Vom DSA werden für die Clients verschiedene Zugriffsmechanismen bereitgestellt, über die die Clients auf Active Directory zugreifen können. Hierbei handelt es sich teils um Protokolle, teils um APIs. Diese vier Mechanismen sind:

1. LDAP

Die Windows-Clients, auf denen die Active Directory-Clientkomponenten entweder nativ oder über den ADSI-Client (siehe Kapitel 3.8.1) ausgeführt werden, benutzen das LDAP-Protokoll in der Version 3.0, um sich mit dem DSA zu verbinden. Active Directory unterstützt auch LDAP in der Version 2.0.

2. REPL (Replikation)

Bei der Verzeichnisreplikation verbinden sich die beteiligten DSAs untereinander. Hierbei wird eine proprietäre RPC-(Remote Procedure Call-)Schnittstelle verwendet wie SMTP (Simple Mail Transfer Protocol) oder IP (Internet Protocol). SMTP wird nur für die standortübergreifende Replikation verwendet, IP sowohl für die standortübergreifende als auch für die standortinterne Replikation.

3. MAPI (Messaging API)

Ein MAPI-Client ist beispielsweise ein Microsoft Outlook-Client. Dieser verbindet sich mit dem DSA über die Schnittstellen des RPC-Adressbuchdienstes. Über die MAPI-Schnittstelle gewährleistet Active Directory die Abwärtskompatibilität mit Exchange Server-Anwendungen.

4. SAM (Security Accounts Manager / Sicherheitskontenverwaltung)

Diesen Mechanismus benutzen Windows-Clients, die Windows NT 3.5x oder 4.0 ausführen. Wenn Sie in Ihrer Domäne im gemischten Modus (siehe Kapitel 10.1.1) noch BDCs mit Windows NT verwenden, benutzen auch diese für die Replikation diese Schnittstelle.

1.4 Die Features des Active Directory

Active Directory bietet die folgenden neuen, fest integrierten, aber dennoch flexibel gestaltbaren Features, die im Windows NT-Domänenmodell nicht verfügbar waren:

- ▶ Vereinfachen der Verwaltung durch Zentralisierung. Jede Domäne kann mehrere gleichrangige Domänencontroller enthalten. Dadurch werden die Änderungen, die Sie an einem Domänencontroller vornehmen, automatisch auf die anderen repliziert. Ein Administrator kann sich von einem beliebigen Computer im Netzwerk aus anmelden und von dort aus Ressourcen auf anderen Computern der Domäne verwalten.
- ▶ Delegation von bestimmten Verwaltungsoperationen vom zentralen Administrator an Unteradmins. Einem Benutzer wird von einer höheren Autoritätsebene gestattet, einen bestimmten Satz von Aktionen an einer festgelegten Gruppe von Objekten in einem zugewiesenen Abschnitt der Domänenstruktur durchzuführen. Hiermit erfolgt eine präzise Kontrolle darüber, wer welche Aktion ausführen darf, ohne dass dem Benutzer dafür höher privilegierte Benutzerrechte erteilt werden müssen.

- ▶ Speichern der Objekte in einer strukturierten Hierarchie, die die Unternehmensgliederung abbildet. Domänen können z.B. nach geografischen oder funktionellen Aspekten eingerichtet werden; in Organisationseinheiten kann die physische Struktur des Unternehmens, z.B. Einteilung in Etagen, abgebildet werden.
- ▶ Hohe Verfügbarkeit der Daten sowie Lastenverteilung durch Multimaster-Replikation des Verzeichnisses auf alle Domänencontroller. Dadurch wird das Verzeichnis einer größeren Gruppe von Benutzern zugänglich gemacht. Außerdem ist beim Ausfall eines Domänencontrollers ein hohes Maß an Redundanz geboten, da die Aktualisierung von Active Directory nicht mehr an einen PDC gebunden ist, sondern auf jedem beliebigen Domänencontroller durchgeführt werden kann.
- ▶ Einfacheres und schnelleres Finden der Ressourcen im Netzwerk: Es kann z.B. nach einem Netzwerkdrucker gesucht werden, auch wenn nicht die komplette Adresse bekannt ist. Geben Sie zur Suche nur Teile der Ihnen bekannten Eigenschaften ein, z.B. Duplex – ja oder nein, Farbe – ja oder nein usw.
- ▶ Hohe Skalierbarkeit. Die Active Directory-Datenbank hat eine viel höhere Kapazität als die Windows NT-Benutzerdatenbank. Es ist möglich, zunächst eine kleine Domänenstruktur mit vielleicht 200 Objekten zu erstellen, die später dynamisch mit dem Wachstum des Unternehmens auf Millionen von Objekten erweitert werden kann.
- ▶ Erweiterbarkeit und individuelle Anpassung des Active Directory-Schemas. Jedem Objekt können eigene Attribute hinzugefügt werden, die sehr unternehmensspezifisch sein können, so z.B. ein Attribut für zeichnungsberechtigt o. Ä. hinzufügen. Außerdem können Sie über die Dienstprogramme LDIFDE oder CSVDE Attribute und Objekte dem Schema hinzufügen.
- ▶ Unterstützung von Standards wie LDAP, NSPI (Name Service Provider Interface), HTTP und DNS. Active Directory unterstützt die Internetstandards und baut auf diesen auf. Durch die Unterstützung des LDAP 3.0 sowie NSPI-Standards ist die Zusammenarbeit mit anderen Verzeichnisdiensten sichergestellt, die ebenfalls diese Protokolle verwenden. Mit DNS wird das Internet-Namenskonzept in Windows 2000 integriert. Windows 2000 unterstützt sogar Dynamisches DNS (DDNS). Clients mit über DHCP bezogenen IP-Adressen können sich dadurch dynamisch beim DNS-Server registrieren. In einer reinen 2000-Umgebung kann der WINS-Namensdienst durch DDNS abgelöst werden, sofern nicht noch ältere Client-Server-Anwendungen den WINS-Dienst voraussetzen.
- ▶ Verbesserung der Sicherheit: Im Active Directory kann eine präzise Zugriffssteuerung nicht nur auf Objektebene, sondern sogar auf der Objekteigenschaftsebene festgelegt werden. Weiterhin können über Gruppenrichtlinien domänenweite Sicherheitsrichtlinien für die Benutzerkonten definiert werden.

2 Unterschiede zwischen Windows NT und Windows 2000/2003 Server

Als Grundlage für das Verständnis vieler Neuerungen an Active Directory sollte das herkömmliche Windows NT-Domänenmodell bekannt sein. Dieses wird zunächst vorgestellt, bevor dann die Unterschiede und Neuerungen von Windows 2000/2003-Active Directory zu Windows NT aufgelistet werden.

2.1 Domänenmodelle unter Windows NT

Unter Windows NT gibt es insgesamt vier verschiedene Domänenmodelle. Domänen werden hier als Master- und Ressourcendomänen bezeichnet. Auf einer Masterdomäne befinden sich die Benutzerkonten. Die Masterdomäne umfasst den PDC sowie die BDCs, die die Anmeldeinformationen verarbeiten. Die Anzahl der Clients einer Domäne ist unter Windows NT dadurch begrenzt, dass die empfohlene Maximalgröße der Benutzerdatenbank 40 MB nicht übersteigen sollte. Diese 40 MB entsprechen ungefähr 40.000 Objekten. Aufgrund dieser Grenze mussten NT-Administratoren oftmals zusätzliche Domänen einrichten, die aber keineswegs in die logische Struktur des Unternehmens passten, sondern allein wegen der Größenbeschränkung eingerichtet werden mussten. Hier bringt nun Windows 2000 die entscheidende Veränderung. Im Active Directory können in einer einzelnen Domäne ein bis zwei Millionen Objekte gespeichert sein. Eine Gesamtstruktur kann bis zu zehn Millionen Objekte umfassen. Die empfohlene Maximalgröße der Datenbank liegt bei 70 Tbyte. Angenommen, ein weltweiter Konzern verfügt über 250.000 Computer und ebenso viele Benutzer. Damit haben sie erst 5% der maximal empfohlenen Datenbankgröße ausgenutzt. Weiter angenommen, dass weitere zwei Millionen Objekte wie Organisationseinheiten, freigegebene Verzeichnisse, Drucker, Kontakte usw. hinzukommen, so haben Sie dann mit insgesamt 2,5 Millionen Objekten erst 25% der Datenbank belegt.

Außerdem gab es zwischen den Master- und Ressourcendomänen keine automatischen Vertrauensstellungen. Diese mussten alle manuell erstellt werden, was einen enormen Zeitaufwand erforderte. Eine Masterdomäne kann mit beliebig vielen Ressourcendomänen zusammenarbeiten.

Es gibt unter Windows NT die folgenden vier Domänenmodelle:

1. Domänenmodell mit einer Domäne
2. Domänenmodell mit einer Masterdomäne
3. Domänenmodell mit mehreren Masterdomänen
4. Domänenmodell mit gegenseitigen Vertrauensstellungen

Diese werden nun kurz in ihrem Aufbau sowie der damit verbundenen Arbeit zum manuellen Erstellen der Vertrauensstellungen beschrieben.

2.1.1 Domänenmodell mit einer Domäne

Bei diesem Modell wird lediglich eine einzige Kontendomäne verwendet. Dieses Modell wird sich nur in kleinen Unternehmen finden, da die Benutzerdatenbank nicht die 40 MB-Grenze überschreiten darf.

In diesem Modell (siehe Abbildung 2.1) gibt es keine Vertrauensstellungen, da keine zwei Masterdomänen vorhanden sind. Die Masterdomäne ist hier gleichzeitig auch die Ressourcendomäne, also darf die Gesamtanzahl aller Netzwerkressourcen nicht über 40.000 liegen.



Abbildung 2.1: Domänenmodell mit einer Domäne

2.1.2 Domänenmodell mit einer Masterdomäne

Auch in diesem Modell (siehe Abbildung 2.2) wird nur eine Masterdomäne für die Benutzerkonten verwendet, also darf auch hier die Kontendatenbank maximal 40 MB umfassen. Allerdings werden hier mehrere Ressourcendomänen verwendet.

Zwischen der Masterdomäne und den Ressourcendomänen werden einseitige Vertrauensstellungen von den Ressourcendomänen zur Masterdomäne hin eingerichtet. Damit ist es möglich, den Mitgliedern der Masterdomäne Zugriffsrechte auf Ressourcen der Ressourcendomäne zu erteilen. Dadurch behalten die Administratoren der Ressourcendomänen die Autorität über ihre Domänen und müssen sie nicht an den Administrator der Masterdomäne abtreten.

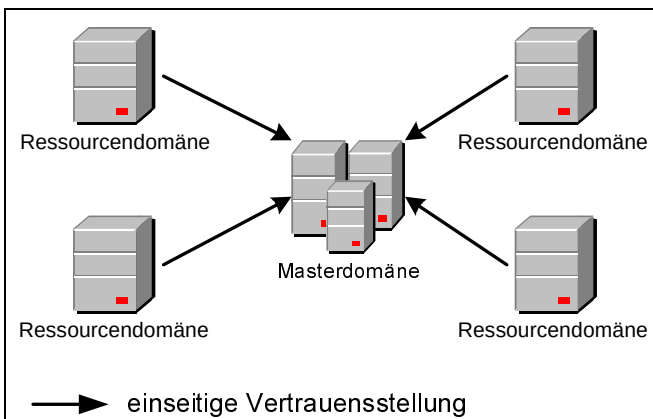


Abbildung 2.2: Domänenmodell mit einer Masterdomäne

2.1.3 Domänenmodell mit mehreren Masterdomänen

Dieses Modell (siehe Abbildung 2.3) gleicht dem eben beschriebenen Modell bis auf die Tatsache, dass hier aufgrund einer Benutzerdatenbankgröße von mehr als 40 MB mehrere Masterdomänen eingerichtet sind. Die Masterdomänen erhalten untereinander zweiseitige, gegenseitige Vertrauensstellungen. Die Ressourcendomänen haben einseitige Vertrauensstellungen zu allen Masterdomänen. Hierbei wird deutlich, dass viel Arbeit in das manuelle Erstellen der Vertrauensstellungen investiert werden muss. Die Anzahl der zu erstellenden Vertrauensstellungen zwischen den Masterdomänen untereinander berechnet sich nach der folgenden Formel:

$$(\text{Anzahl der Masterdomänen}) * (\text{Anzahl der Masterdomänen} - 1)$$

Die Anzahl der Vertrauensstellungen zwischen Masterdomänen und Ressourcendomänen wird nach der folgenden Formel errechnet:

$$(\text{Anzahl der Masterdomänen}) * (\text{Anzahl der Ressourcendomänen})$$

Angenommen, Ihr Unternehmen verfügt über fünf Masterdomänen und 100 Ressourcendomänen. Dann müssen Sie 20 Vertrauensstellungen zwischen den fünf Masterdomänen sowie 500 Vertrauensstellungen zwischen den Master- und Ressourcendomänen manuell einrichten.

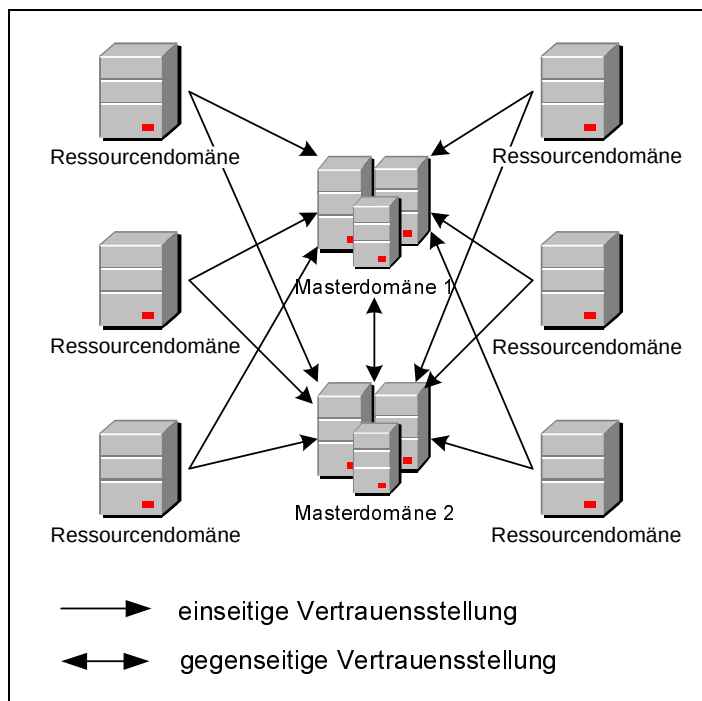


Abbildung 2.3: Domänenmodell mit mehreren Masterdomänen

2.1.4 Domänenmodell mit gegenseitigen Vertrauensstellungen

In diesem Modell (siehe Abbildung 2.4) bestehen zwischen sämtlichen Domänen vollständige gegenseitige Vertrauensstellungen. Damit kann ein Administrator jeder Domäne in jeder anderen Domäne Konten erstellen und Ressourcen verwalten und freigeben. Eine Domäne umfasst dabei eine kombinierte Benutzer- und Ressourcendomäne. In diesem Modell müssen Sie zwar innerhalb einer Domäne keine Vertrauensstellungen einrichten, aber es wird eine größere Gesamtanzahl von Domänen erforderlich, da die Einzeldomäne alle der 40-MB-Grenze unterliegen. Dadurch haben Sie es mit einer großen Anzahl nicht strukturiert angeordneter Domänen zu tun, für die Sie alle gegenseitige Vertrauensstellungen einrichten müssen.

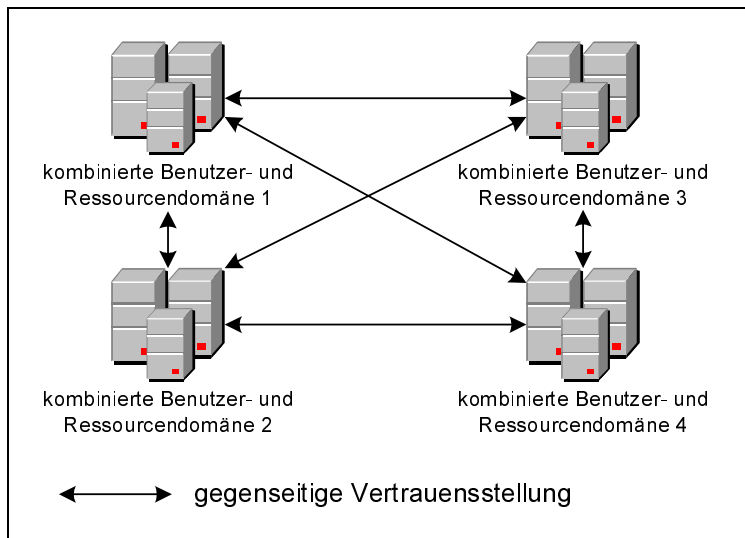


Abbildung 2.4: Domänenmodell mit gegenseitigen Vertrauensstellungen

Die beiden am weitesten verbreiteten Modelle dürften wohl in sehr kleinen Unternehmen das Modell 1 mit nur einer Domäne sein und in großen Unternehmen das Modell 3 mit mehreren Masterdomänen. Tabelle 2.1 gibt einen zusammenfassenden Überblick über die verschiedenen Domänenmodelle unter Windows NT.

Domänenmodell	Anzahl Master-domänen	Anzahl Ressourcen-domänen	Vertrauensstellungen
Mit einer Domäne	1	0	Keine
Mit einer Masterdomäne	1	Beliebig	Einseitig von Ressourcendomäne zu Masterdomäne
Mit mehreren Masterdomänen	Beliebig	Beliebig	Gegenseitig zwischen den Masterdomänen, einseitig von Ressourcendomäne zu Masterdomäne
Mit gegenseitigen Vertrauensstellungen	Beliebig	Beliebig	Gegenseitig zwischen allen Domänen

Tabelle 2.1: Die NT-Domänenmodelle

Das Domänenmodell unter Windows 2000 ist vergleichbar mit Modell 2, also einer Masterdomäne und mehreren Ressourcendomänen, wird aber nicht als Domänenmodell bezeichnet. Allerdings werden hier statt der Ressourcendomänen Organisationseinheiten verwendet.

2.2 Neuerungen in Windows 2000 und 2003 im Überblick

Sie haben bereits den entscheidenden Vorteil von Active Directory gegenüber Windows NT kennen gelernt, nämlich dass unter Windows 2000 quasi keine Größenlimitierung der Benutzerdatenbank vorgegeben ist. Damit entfällt das zwangsweise Neuerstellen von neuen Domänen, und stattdessen können Sie eine logische Domänenstruktur mit Organisationseinheiten erstellen.

2.2.1 Unterschiede zwischen Windows 2000 und NT

Aber dies ist selbstverständlich noch nicht die einzige Verbesserung oder Neuerung von Windows 2000. Die weiteren Unterschiede zwischen Windows NT und Windows 2000 werden in den folgenden Tabellen vorgestellt. Der Übersichtlichkeit halber werden die Unterschiede in die fünf Gruppen Domänenbezogen, Objekte, Datenbank, Schema und Netzwerk unterteilt.

Domänenbezogene Neuerungen

Windows NT	Windows 2000
Vier verschiedene Domänenmodelle; willkürliches Erstellen weiterer Domänen erforderlich, wenn Datenbankgröße überschritten war. Zeitaufwändiges, manuelles Einrichten von Vertrauensstellungen Bei der Installation muss entschieden werden, ob es ein PDC, BDC oder Mitgliedsserver werden soll. Ein Mitgliedsserver kann nicht zum PDC heraufgestuft werden. Die Replikation findet zwischen einem PDC und einer beliebigen Anzahl BDCs statt. Domänen sind die kleinste Einheit für die Delegierung der Administration. Domänen sind die kleinste Einheit für die Durchsetzung von Sicherheitsrichtlinien.	Hierarchische Gliederung der Domänen; NT-Ressourcendomänen werden von Organisationseinheiten abgelöst. Vertrauensstellungen zwischen Domänen in einer Gesamtstruktur werden automatisch erstellt. Es wird immer automatisch ein Mitgliedsserver installiert. Dieser kann über den Installationsassistenten für Active Directory zum Domänencontroller werden. Während der Installation wird die Position der Domäne in der Gesamtstruktur festgelegt. Die Replikation wird zwischen allen gleichrangigen Domänencontrollern durchgeführt. Es gibt keine PDCs und BDCs mehr. Objekteigenschaften sind die kleinste Einheit für die Delegierung der Administration. Organisationseinheiten sind die kleinste Einheit für die Durchsetzung von Sicherheitsrichtlinien über Gruppenrichtlinien.

Tabelle 2.2: Domänenbezogene Neuerungen

Objektbezogene Neuerungen

Windows NT	Windows 2000
Ein Objekt ist die kleinste Einheit, die repliziert werden kann. Wenn Sie beispielsweise nur den Nachnamen eines Benutzers ändern, wird das gesamte geänderte Benutzer-Objekt repliziert.	Eine Eigenschaft ist die kleinste replizierbare Einheit. Ändern Sie hier den Nachnamen des Benutzers, wird nur die geänderte Eigenschaft repliziert. Bei dieser Form des Byte-Level-Differencing wird der Netzwerkverkehr verringert, da eine geringe Datenmenge zu replizieren ist.

Tabelle 2.3: Objektbezogene Neuerungen

Datenbankbezogene Neuerungen

Windows NT	Windows 2000
Die Höchstgrenze für die Datenbank liegt bei 40 MB bzw. bei 40.000 Objekten.	Die Höchstgrenze für die Datenbank in einer Gesamtstruktur liegt bei 70 Tbyte bzw. bei 1 bis 2 Millionen Objekten in einer einzelnen Domäne oder 10 Millionen Objekten in der Gesamtstruktur.

Tabelle 2.4: Datenbankbezogene Neuerungen

Schemabezogene Neuerungen

Windows NT	Windows 2000
Das Schema ist fest vorgegeben und kann nicht geändert oder erweitert werden.	Das Active Directory-Schema ist durch das Hinzufügen neuer Klassen und Attribute individuell erweiterbar.

Tabelle 2.5: Schemabezogene Neuerungen

Netzwerkbezogene Neuerungen

Windows NT	Windows 2000
Die transportprotokollunabhängige NetBIOS-Schnittstelle ist das primäre Netzwerkprotokoll für alle Verbindungen. Verwendung von WINS für die NetBIOS-Namensauflösung und DNS für TCP/IP-Anwendungen. Damit verbunden ist die Pflege der WINS-Datenbank sowie der LMHOSTS-Tabellen. Authentifizierung erfolgt über NTLM (NT LAN-Manager).	Verwendung des TCP/IP-Protokolls Nur Verwendung von DNS, NetBIOS-Namensauflösung wird nicht verwendet. Zur Abwärtskompatibilität muss im gemischten Betriebsmodus ein WINS-Server betrieben werden. Im einheitlichen Modus muss kein WINS mehr vorhanden sein. Authentifizierung erfolgt über NTLM (NT LAN-Manager) oder das Kerberos V5-Protokoll. Dieses Protokoll wird im folgenden Kapitel näher beschrieben. NTLM-Authentifizierung ist im einheitlichen Betriebsmodus nicht mehr verfügbar.

Tabelle 2.6: Netzwerkbezogene Neuerungen

2.2.2 Unterschiede zwischen Windows 2000 und 2003 Active Directory

In diesem Kapitel werden die Unterschiede zwischen dem Windows 2000 und 2003 Active Directory vorgestellt. Diese Optimierungen werden sich besonders in mittleren und großen Umgebungen positiv auswirken.

Umbenennen von Domänen, sogar auf dem höchsten Level

Es ist im Windows 2003 Active Directory möglich, die Namen (DNS und / oder NetBIOS-Namen) vorhandener Domänen in einer Gesamtstruktur zu ändern. Das Umbenennen ist dabei auf jedem Domänen-Level möglich. So kann es notwendig werden, eine oder mehrere Domänen umzubenennen, wenn ein Unternehmen seinen Namen ändert oder durch eine Fusion ein neues Unternehmen hinzukommt, das zwar seine Struktur behält, aber den Namen ändert. So kann zwar auch die Stammdomäne innerhalb der Gesamtstruktur umbenannt werden, aber es ist nicht möglich, die alte Stammdomäne durch eine neue zu ersetzen. Das Umbenennen von Domänen wird mithilfe des Support-Tools *DOMAINRENAME* durchgeführt. Im Windows 2000 Active Directory konnte eine Domäne nur umbenannt werden, indem der Domänencontroller über *DCPROMO* zum Mitgliedsserver herabgestuft und anschließend wieder ein Active Directory installiert wurde. Allerdings gingen dabei sämtliche alten Active Directory-Daten verloren.

Vertrauensstellungen zwischen zwei Gesamtstrukturen

Transitive Vertrauensstellungen konnten im Windows 2000 Active Directory nur innerhalb von Domänen einer Gesamtstruktur automatisch hergestellt werden. Vertrauensstellungen zu Domänen einer anderen Gesamtstruktur waren nur manuell zwischen zwei Domänen herstellbar. Dabei handelt es sich jedoch um intransitive Vertrauensstellungen. Dies ist besonders dann eine Schwierigkeit, wenn es darum geht, neue Gesamtstrukturen in das bestehende Active Directory eingliedern zu müssen. Dies ist z.B. dann der Fall, wenn ein Unternehmen dazugekauft wird und dessen Active Directory-Struktur in die bestehende Struktur eingegliedert werden soll oder wenn aufgrund mangelhafter Planung mehrere Gesamtstrukturen im Netzwerk vorhanden sind, die nun doch zusammengeführt werden sollen. Im Windows 2003 Active Directory können jedoch auch transitive Vertrauensstellungen zwischen allen Domänen in zwei Gesamtstrukturen hergestellt werden. So können die Benutzer der Domäne *finanzen.firma.de* auf sämtliche Ressourcen der Domäne *werbung.filiale.de* zugreifen. Allerdings kann eine solche Vertrauensstellung nur zwischen zwei Gesamtstrukturen hergestellt werden. Verfügen Sie über drei oder mehr Gesamtstrukturen, so müssen Sie drei oder mehr Vertrauensstellungen einrichten. Dabei kann bestimmt werden, ob die Vertrauensstellungen nur in eine oder transitiv in beide Richtungen konfiguriert werden. Die Vertrauensstellungen zwischen Gesamtstrukturen vereinfachen die Planung und Migration einer Active Directory-Struktur.

Replikation

Auch im Bereich der Replikation wurden Änderungen zur Verbesserung der Performance durchgeführt. Diese Optimierungen sind auf den ersten Blick zwar nur kleine Details, aber besonders in großen Umgebungen machen sich diese Verbesserungen deutlich bemerkbar.

Verbesserungen der Inter-Site-Replikationstopologie

Eine wesentliche Verbesserung wurde an der standortübergreifenden Replikation vorgenommen, und zwar an der Berechnung der Inter-Site-Replikationstopologie. Der Effekt zeigt sich jedoch erst in größeren Unternehmen mit deutlich mehr als 1.000 Benutzern. Im Windows 2000 Active Directory wird die Replikationstopologie über den KCC-(Knowledge Consistency Checker-)Dienst berechnet. Allerdings sind die für die Berechnung verwendeten Algorithmen sehr prozessor- und speicherintensiv. Mit der Anzahl der Standorte steigt exponentiell auch die benötigte Rechenleistung. Verfügen Sie über mehr als 100 Standorte, so muss die Replikationstopologie manuell bestimmt werden, da eine automatische Berechnung unmöglich wird. Das Windows 2003 Active Directory verwendet zur Berechnung verbesserte Algorithmen, die nun vom ISTG-(Inter-Site-Topology-Generator-)Dienst durchgeführt werden. Allerdings ist die damit verbundene höhere Skalierbarkeit erst in einem reinen Windows 2003-Umfeld möglich. Weiterhin ist auch ein globaler Katalog für die Anmeldung nicht mehr an jedem Standort zwingend erforderlich. An jedem Standort musste unter Windows 2000 ein Teilreplikat aller Domänen vorhanden sein. Ein Domänencontroller unter Windows 2003 hingegen kann einen speziellen Cache aktivieren und verwenden, der Einträge für Mitgliederlisten aller universellen Gruppen enthält. Die Einträge im Cache werden während der Replikation aktualisiert. So kann sich ein Client authentifizieren, ohne dass an seinem Standort ein globaler Katalogserver vorhanden sein muss.

Verbesserte Replikation der Gruppenmitgliedschaften

Im Windows 2000 Active Directory wird grundsätzlich eine vollständige Liste aller Mitglieder einer Benutzergruppe an alle Domänencontroller repliziert, sobald Sie einer Gruppe einige neue Mitglieder hinzugefügt oder einige daraus gelöscht haben. Enthält eine Gruppe, z.B. die der Domänenbenutzer, mehrere 100 Mitglieder und wurden dabei lediglich drei Änderungen vorgenommen, so macht die Replikation der nicht geänderten Daten den größten Anteil aus und belastet unnötig das Netzwerk. Im Windows 2003 Active Directory werden nur noch die geänderten Daten der Gruppenmitgliedschaften repliziert und nicht mehr die kompletten Listen von Gruppenmitgliedern.

Allerdings arbeitet der Windows 2003-Server mit diesen Features nur in einer reinen 2003-Domänenumgebung. Unter Windows 2003 können Sie neben dem einheitlichen und gemischten als dritten Betriebsmodus den „Windows 2003-Betriebsmodus“ wählen. Dabei handelt es sich quasi um einen einheitlichen Modus, der ausschließlich Domänencontroller unter Windows 2003 erkennt und benutzt. Windows 2003-Server können zwar im gemischten oder einheitlichen Modus gemeinsam mit Windows 2000-Domänencontrollern innerhalb einer Domäne betrieben werden, aber in diesem Fall werden die neuen Features automatisch deaktiviert, und der Windows 2003-Domänencontroller verhält sich wie ein Windows 2000-Domänencontroller. Besonders in Unternehmen, die bereits

über ein Active Directory unter Windows 2000 verfügen, ist ernsthaft zu überlegen, ob die Verbesserungen im Windows 2003 Active Directory ein Update aller Server auf 2003 rechtfertigen oder nicht. Bei einer Neuimplementierung eines Active Directory ist der Einsatz des Windows 2003-Servers jedoch anzuraten.

Anwendungspartitionen

Neu beim Windows 2003-Server sind die Anwendungspartitionen. Dahinter verbergen sich spezielle Partitionen, in denen vom Active Directory verwendete Daten abgelegt werden. Bei diesen Daten kann es sich auch um dynamische Daten handeln. Ein gutes Beispiel dafür sind die Daten des Exchange Servers. Im Windows 2000 Active Directory werden die Exchange-Daten unmittelbar in der Domäne abgelegt. In einer Anwendungspartition sind diese Daten sauber von übrigen Daten getrennt. In diesen Partitionen können auch Daten eigener Anwendungen abgelegt werden. Die einzige Einschränkung besteht darin, dass keine sicherheits- und authentifizierungsbezogenen Objekte wie Benutzer oder Computer in einer Anwendungspartition gespeichert werden können. Anwendungspartitionen werden auch für systemeigene Bereiche wie DHCP, RAS oder RADIUS verwendet. Die Inhalte dieser Partitionen können nicht nur auf die Domänencontroller innerhalb einer Domäne, sondern auch auf alle Domänencontroller innerhalb der Gesamtstruktur repliziert werden.

Schemabezogene Neuerungen

Es können nun im Schema Attribute und Klassen neu definiert werden. Diese Definitionen können zusätzlich jederzeit außer Kraft gesetzt bzw. die Deaktivierungen wieder aufgehoben werden. Diese Funktion ist dann sehr nützlich, wenn Sie ein neues Objekt fehlerhaft erstellt haben. Es kann nun einfach deaktiviert und danach mit den korrekten Definitionen neu angelegt werden. Auch wenn Objekte von nicht mehr benutzten Anwendungen nicht mehr benötigt werden, ist eine Deaktivierung sinnvoll, damit die alten Objekte nicht mit denen einer neuen Anwendung in Konflikt treten.

Verbesserungen für die Administration

Die regelmäßig wiederkehrenden Administrationsaufgaben werden nun auch über die GUI vereinfacht. Bestes Beispiel dafür ist die GPMC (Group Policy Management Console, siehe Kapitel 20.3), mit der jetzt zentral alle Einstellungen an den Gruppenrichtlinien vorgenommen werden können. Bislang war es in vielen Bereichen einfacher, ein Skript zu erstellen, das für die Abarbeitung komplexer, wiederkehrender Aufgaben zuständig war. Der Windows 2003-Server bietet jedoch die Möglichkeit, einmal ausgeführte Abfragen und Aufgaben zu speichern. Dieser Menüpunkt befindet sich in jeder mmc. Zusätzlich ist innerhalb der mmcs auch die gleichzeitige Auswahl von mehreren Objekten sowie Drag&Drop möglich.

Authentifizierung

Im Windows 2003-Active Directory kann eine Authentifizierung über die Grenzen der Gesamtstruktur hinweg durchgeführt werden. Diese *Cross-Forest-Authentication* ermöglicht einen gesicherten Zugriff auf Ressourcen, wenn sich das Benutzerkonto in einer anderen Gesamtstruktur befindet als das Computerkonto. Dabei werden die Vorteile des

Single Sign-On ausgenutzt, da der Benutzer nur den Benutzernamen und das Kennwort seiner eigentlichen Domäne benötigt. Die Authentifizierung erfolgt über NTLM oder Kerberos. Kann bei der Authentifizierung der Benutzername auf dem lokalen Domänencontroller nicht aufgelöst werden, wird die Abfrage an den globalen Katalog gerichtet. Kann auch dort der Name nicht aufgelöst werden, wird die neue Funktion aufgerufen, wobei der Security Principal Name in allen Namensräumen der vertrauenden Gesamtstrukturen gesucht wird. Wird der Name in einer Gesamtstruktur gefunden, wird der Name dieser Gesamtstruktur als *Routing Hint* zurückgegeben, und der Zugriff kann erfolgen.

Durch die die Gesamtstruktur übergreifende Authentifizierung ist es für die Administratoren möglich, bestimmte Benutzer aus vertrauenden Gesamtstrukturen in lokale Gruppen oder ACLs aufzunehmen. Die zur Namens-SID-Übersetzung notwendigen APIs sind so erweitert worden, dass sie auch die Gesamtstruktur übergreifende Routing Hints verwenden können. Führen zwei Gesamtstrukturen die übergreifende Authentifizierung durch und benutzen dabei bidirektionale Vertrauensstellungen, so können auch IAS- und RADIUS-Server die Benutzerkonten der anderen Gesamtstruktur authentifizieren.

2.2.3 Das Kerberos V5-Authentifizierungsprotokoll

Das Kerberos V5-Authentifizierungsprotokoll ist ein festgelegter Industriestandard. Das Kerberos V5-Authentifizierungsprotokoll ist das primäre Authentifizierungsprotokoll in einer Windows 2000- und 2003-Domäne. Die NTLM-Authentifizierung wird nur bei nicht Windows 2000/XP-Clients bzw. von nicht Windows 2000/2003-Servern angewandt. Beim Kerberos-Verfahren erhalten die Benutzer über einen einzigen Anmeldevorgang Zugriff auf alle Ressourcen von Umgebungen, die Interoperabilität mit diesem Protokoll bieten. Außerdem werden die Kennwörter nicht im Klartext, sondern verschlüsselt über das Netzwerk gesendet.

Bei dieser Art der Authentifizierung werden so genannte Tickets für den Zugriff auf die Netzwerkdienste ausgestellt. Ein Ticket besteht aus verschlüsselten Daten, z.B. auch aus einem verschlüsselten Kennwort. Damit wird die Identität des Benutzers gegenüber dem Netzwerkdienst verifiziert und bestätigt. Dieser Vorgang der Authentifizierung läuft für den Benutzer unsichtbar ab.

Die Kerberos-Tickets werden in einem speziellen Teil des RAMs gecacht. Aus Sicherheitsgründen wird dieser Speicherbereich nicht in die Page-File ausgelagert und damit auf die Festplatte geschrieben. Hierin ist es auch begründet, dass nur Windows 2000/2003-Server diese Art der Authentifizierung unterstützen, da ausschließlich sie die Verwendung des speziellen Speicherbereichs durchführen können. Ältere Clients bieten diese Funktion nicht, auch nicht im Zusammenspiel mit dem ADSI-Client.

Zum Erstellen des Tickets muss auf jedem Domänencontroller der KDC-Dienst ausgeführt werden. KDC bedeutet Key Distribution Center/Schlüsselverteilungszentrum. Im KDC sind alle Kennwörter und Kontoinformationen der Clients gespeichert. Der KDC-Dienst ist in Active Directory integriert.

Bei der Kerberos V5-Authentifizierung werden die folgenden Schritte durchgeführt:

1. Der Clientbenutzer muss sich mit seinem Kennwort am KDC des Domänencontrollers authentifizieren.
2. Daraufhin erstellt der KDC ein ticketgenehmigendes Ticket für den Client. Dieses Ticket wird im Gruppenrichtlinien-Editor auch als Benutzerticket bezeichnet. Über den Gruppenrichtlinien-Editor können die Kerberos-Richtlinien für Benutzer- und Gruppenkonten geändert werden.
3. Mit diesem vorläufigen Ticket greift der Client auf den ticketgenehmigenden Dienst (TGS = Ticket Granting Service) zu. Der TGS ist fester Bestandteil der Kerberos V5-Authentifizierung auf dem Domänencontroller.
4. Daraufhin erstellt der TGS ein Diensticket für den Client.
5. Der Client übergibt dieses endgültige Ticket an den erforderlichen Netzwerkdienst. Dadurch wird die Identität des Benutzers und auch der Netzwerkdienste überprüft. Deshalb wird der Vorgang auch gegenseitige Authentifizierung genannt.

Die Kerberos-Dienste werden auf allen Windows 2000-Domänencontrollern installiert. Damit ist jeder Domänencontroller automatisch ein KDC. Der Kerberos-Client wird auf jedem Computer mit Windows 2000 Professional oder Server installiert. Wenn sich ein Client an der Domäne anmelden möchte, wird über den DNS-Dienst der nächste zur Verfügung stehende Domänencontroller mit KDC ermittelt. Sollte dieser Domänencontroller im Laufe der Client-Sitzung ausfallen oder aus anderen Gründen nicht mehr verfügbar sein, so wird von Windows 2000 ein anderer Domänencontroller als KDC zur Authentifizierung gesucht.

Die Kerberos V5-Authentifizierung beschränkt sich nicht nur auf Windows 2000-Domänen. In einer Windows 2000-Domäne können auch Konten für Unix-Server und -Clients angelegt werden, die dann über das Kerberos-Protokoll vom Windows-Domänencontroller authentifiziert werden können.

3 Funktionsweise und Beschreibung des Active Directory

Nachdem Sie in den vergangenen Kapiteln einen Einblick in die Funktionsweise des Verzeichnisdienstes sowie die Vorteile von Active Directory gegenüber Windows NT erhalten haben, werden hier die wesentlichen Komponenten und Begriffe von Active Directory wie Domänen, Strukturen, Replikation usw. vorgestellt.

3.1 Domänen und Domänencontroller

Während der Installation von Windows 2000 müssen Sie entscheiden, ob der Computer Mitglied einer Arbeitsgruppe oder Domäne werden soll. Die dritte Möglichkeit bei der Serverinstallation, das Einrichten einer Domäne, lassen wir hier zunächst außer Acht.

In einer Domäne werden im Gegensatz zur Arbeitsgruppe alle Konten und Ressourcen zentral verwaltet. Dies bedeutet, dass ein Benutzer mit einer einzigen Anmeldung an der Domäne automatisch Zugriff auf alle Ressourcen der kompletten Domäne erhält, für die er die entsprechenden Rechte hat. Die Anmeldung erfolgt ausschließlich am Domänencontroller der Domäne. Dort liegt die zentrale Datenbank, die die Einträge zu den Benutzerkonten, Rechten, Ressourcen usw. enthält. Ein Domänencontroller besitzt keine lokale Sicherheitsdatenbank. In einer einzelnen Domäne können bis zu zwei Millionen Objekte gespeichert werden.

Eine Windows 2000-Domäne kann mehrere gleichberechtigte Domänencontroller enthalten. Diese Domänencontroller gleichen automatisch ihre Datenbanken untereinander ab, sodass stets die aktuellen Informationen im Netzwerk zur Verfügung stehen. Dieser Vorgang wird als Replikation bezeichnet. Der Replikationsprozess wird ausführlich in Kapitel 3.7 beschrieben. Wenn Sie mehrere Domänencontroller einsetzen, erzielen Sie damit ein höheres Maß an Datenverfügbarkeit und Fehlertoleranz. Eine Domäne ist die Grundeinheit für Replikation und Sicherheit.

In einer Arbeitsgruppe kann sich jeder Benutzer nur lokal an seinem Rechner anmelden. Um dann beispielsweise auf einen Drucker oder freigegebenen Ordner zugreifen zu können, benötigt er separate Passwörter. Die lokalen Benutzerdaten und Ressourceninformationen befinden sich bei jedem Computer in der lokalen Sicherheitsdatenbank. Die Rechner arbeiten alle gleichberechtigt ohne einen Server in einem Peer-to-Peer-Netzwerk. Die Verwaltung von Benutzerkonten und Ressourcen kann hier nur dezentral auf den einzelnen Rechnern erfolgen.

Eine Domäne sollte immer einer Arbeitsgruppe vorgezogen werden, es sei denn, Sie haben spezielle Gründe, keine Domäne einzurichten. Dies könnte der Fall sein, wenn Sie nur über ein sehr kleines Netzwerk bis etwa 15 Clients verfügen oder aber die Windows-Clients ihre Anmeldung über einen Novell NetWare-Server durchführen.

Mit dem Einrichten des ersten Domänencontrollers einer Domäne wird gleichzeitig auch die Domäne selbst neu eingerichtet.

Wenn Sie bei der Installation eines 2000-Servers nicht die Option der Mitgliedschaft in einer Domäne oder Arbeitsgruppe wählen, sondern einen Domänencontroller anlegen wollen, so haben Sie damit jedoch noch kein Active Directory eingerichtet. Solange Sie auf dem Domänencontroller nicht den Installationsassistenten für Active Directory ausgeführt haben, verfügen Sie über eine Domäne, wie Sie sie aus einem Windows NT-Umfeld kennen. Diese Domäne ist zwar einsatzbereit, verfügt aber noch nicht über die Features von Active Directory. Der Installationsassistent für Active Directory übernimmt die Einstellungen der Betriebssysteminstallation wie etwa IP-Adresse, DNS-Server usw. und kombiniert diese mit den für Active Directory spezifischen Angaben des Benutzers wie Name der Domäne, Eingliederung in die Domänenstruktur usw.

Ein Domänencontroller ist in seiner Umgebung für die Anmeldung und Authentifizierung der Benutzer sowie das Durchsuchen des Verzeichnisses nach Objekten zuständig. Er speichert sämtliche Daten des Active Directory. Wenn Sie an einem beliebigen Domänencontroller Änderungen an Objekten vornehmen, so werden diese Änderungen automatisch an alle anderen Domänencontroller der Domäne repliziert. Hierbei spricht man von Multimaster-Replikation, da alle Domänencontroller gleichberechtigt sind. Jeder Domänencontroller verfügt über eine beschreibbare Kopie der Active Directory-Datenbank. Somit ist es gleichgültig, an welchem Domänencontroller die Änderungen vorgenommen werden. Wichtige Änderungen, wie etwa das Deaktivieren eines Kontos, werden sofort repliziert. Das Replikationsintervall ist ansonsten einstellbar.

Eine Domäne muss nicht identisch sein mit den physischen Grenzen eines Unternehmensstandorts. Es ist möglich, dass in einer Domäne Objekte aus mehreren physisch getrennten Standorten vorhanden sind.

Wenn kein Domänencontroller für einen Client verfügbar ist, so konnte unter Windows NT der Client nicht auf Netzwerkressourcen zugreifen. Diese Problematik wurde erkannt und unter Windows 2000 verbessert. Clients ab dem Betriebssystem Windows 2000 verwenden automatisch das Login-Caching.

Dabei wird bei jeder erfolgreichen Anmeldung an der Domäne auf dem Client das Login gecacht. Standardmäßig können bis zu zehn Einträge auf dem Client vorgehalten werden. Dieser Wert kann in den Sicherheitsrichtlinien modifiziert werden. Will sich dieser Client nun zu einem späteren Zeitpunkt erneut an der Domäne anmelden und kann dabei keine Verbindung zum Domänencontroller aufbauen, so kann er sich dennoch an der Domäne anmelden. Es werden aus dem Cache des Clients die Einstellungen von Rechten, Gruppenmitgliedschaft etc. des letzten erfolgreichen Anmeldens am Domänencontroller übernommen. Auch wenn diese Einträge auf dem Domänencontroller zwischenzeitlich geändert worden sind, sind die Einstellungen aus dem lokalen Cache für den Client gültig. Der Cache wird dann bei der nächsten erfolgreichen Verbindung zum Domänencontroller automatisch aktualisiert.

Innerhalb einer Domäne sind die folgenden Computertypen vertreten: mindestens ein oder mehrere Domänencontroller, Clientcomputer und optional Mitgliedsserver, die als Datei- oder Druckserver dienen können. Auf einem Mitgliedsserver befindet sich nicht

die Active Directory-Datenbank. Somit ist ein Mitgliedsserver auch kein Replikationspartner für Domänencontroller.

Abbildung 3.1 gibt einen Überblick über die Rollen von Computern in einer Windows 2000 Active Directory-Domäne.

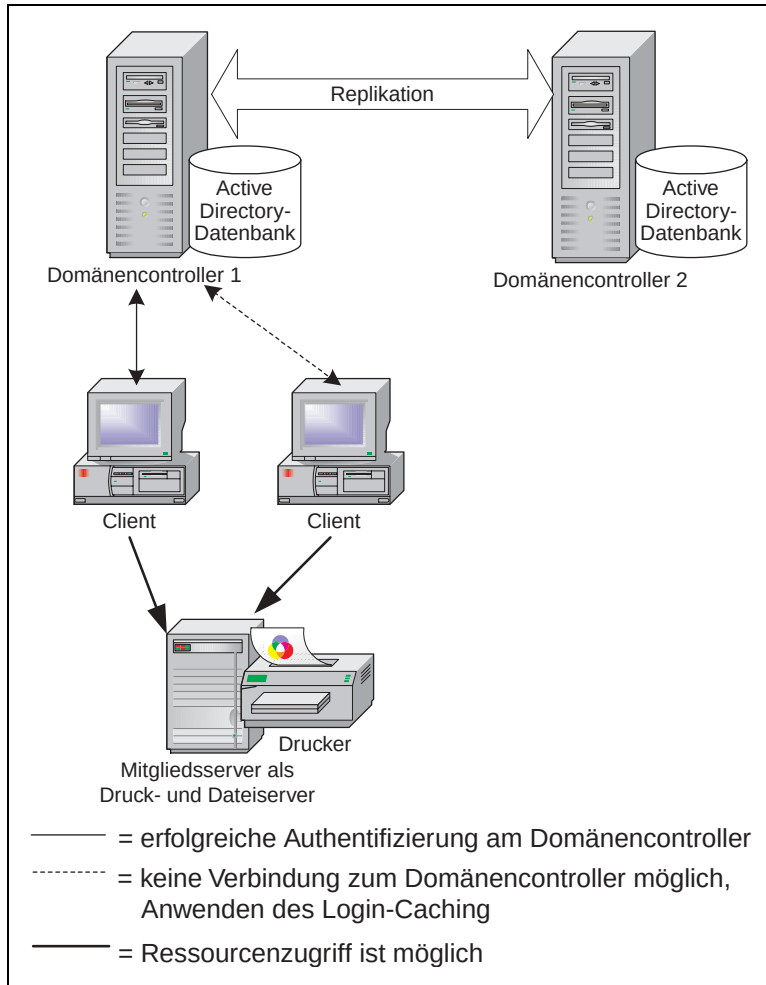


Abbildung 3.1: Computer in einer Active Directory-Domäne

3.2 Strukturen

Strukturen sind eine hierarchische Anordnung von Windows 2000-Domänen. Es gibt übergeordnete und untergeordnete Domänen. Im Rahmen der Strukturen wird zwischen Domänenstruktur (*Tree*) und Gesamtstruktur (*Forest*) unterschieden. Die Domänenstruktur wird manchmal auch nur als Struktur bezeichnet.

3.2.1 Domänenstruktur (Tree)

In einer Domänenstruktur (siehe Abbildung 3.2) haben alle Domänen einen fortlaufenden DNS-Namensraum. Der Namensaufbau ist hierarchisch. Jede Domäne wird durch einen eindeutigen DNS-Namen bezeichnet. Dies soll die folgende Abbildung verdeutlichen.

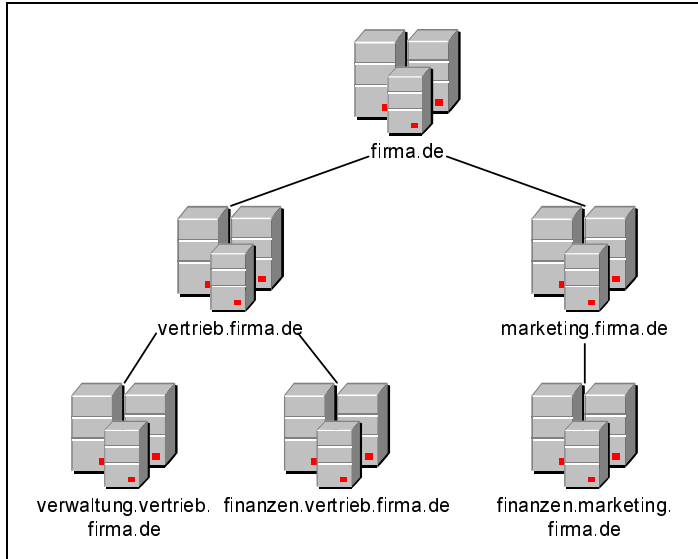


Abbildung 3.2: Eine Domänenstruktur (Tree)

In dieser Domänenstruktur benutzen alle Domänen dasselbe Active Directory-Schema, dieselben Replikationsinformationen und denselben globalen Katalog.

In einer Struktur erbt eine untergeordnete Domäne den Namen der übergeordneten Domäne. Vor diesen wird der relative Name der untergeordneten Domäne gestellt. In unserem Beispiel erbt also die Domäne *vertrieb.firma.de* den Namen der übergeordneten Domäne *firma.de*, und vor diesen wird der relative Name *vertrieb.* gesetzt. Dabei spricht man vom fortlaufenden oder zusammenhängenden Namensraum.

Im Schaubild sehen Sie in zwei verschiedene Hierarchieebenen untergeordnete Domänen. Es wären auch noch weitere Hierarchieebenen möglich, aber Sie sollten dabei auch die Übersichtlichkeit Ihres Directorys im Auge behalten. So erscheint es wenig sinnvoll, etwa eine Domäne mit folgendem DNS-Namen anzulegen: *sekretariat.geschäftsführung.intern.verwaltung.vertrieb.firma.de*. Verwenden Sie stattdessen hierarchische Organisationseinheiten innerhalb der Domänen.

Diese oben abgebildete Domänenstruktur ist gleichzeitig auch eine komplette Gesamtstruktur.

3.2.2 Gesamtstruktur (Forest)

Bei einer Gesamtstruktur handelt es sich um eine hierarchische Anordnung entweder nur einer Domänenstruktur (siehe Abbildung 3.2) oder mehrerer getrennter, unabhängiger Domänenstrukturen (siehe Abbildung 3.3). Selbst eine einzelne Domäne wie *firma.de* ohne weitere untergeordnete Domänen bildet eine in sich geschlossene Gesamtstruktur.

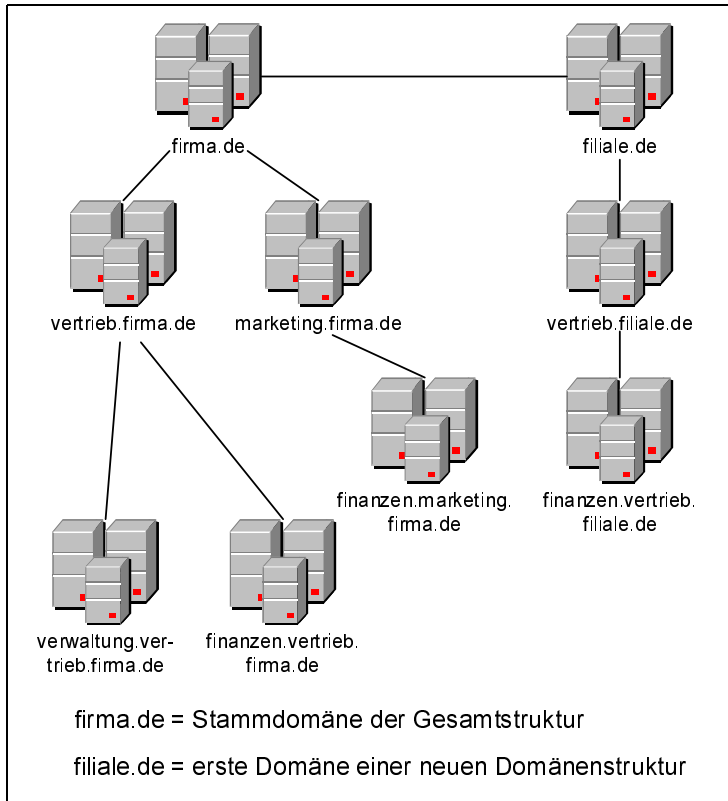


Abbildung 3.3: Eine Gesamtstruktur (Forest) mit getrennten Domänenstrukturen

Innerhalb aller Domänen einer Gesamtstruktur werden dasselbe Active Directory-Schema, dieselben Replikationsinformationen sowie derselbe globale Katalog verwendet. Der Namensraum ist nur innerhalb der Domänenstrukturen zusammenhängend. Die beiden Strukturen *firma.de* und *filiale.de* bilden getrennte Domänenstrukturen innerhalb der Gesamtstruktur. Nur innerhalb der beiden Strukturen ist der Namensraum fortlaufend. Die erste Domäne in einer Gesamtstruktur heißt auch Stammdomäne der Gesamtstruktur, hier also *firma.de*.

Über den Installationsassistenten für Active Directory können Sie bestimmen, an welcher Hierarchieebene in der Gesamtstruktur die neue Domäne erstellt werden soll. Dabei haben Sie folgende Möglichkeiten:

- Erste Domäne in einer Gesamtstruktur, hier also *firma.de*

- Erste Domäne einer neuen Domänenstruktur, hier also *filiale.de*
- Untergeordnete Domäne in bestehender Domänenstruktur, hier alle anderen

Nach dem Einrichten des ersten Domänencontrollers einer der eben genannten Domänenarten können Sie für diese Domäne weitere Domänencontroller installieren.

Weiterhin werden zwischen allen Windows 2000/2003-Domänen innerhalb der Gesamtstruktur automatische gegenseitige Vertrauensstellungen eingerichtet. Dies gilt nur für Windows 2000/2003-Domänen. Wenn Sie noch Windows NT-Domänen innerhalb der Gesamtstruktur verwenden, müssen die Vertrauensstellungen zu diesen manuell konfiguriert werden. Die automatische Einrichtung bezieht sich sowohl auf die Vertrauensstellung zwischen übergeordneten und untergeordneten Domänen als auch zwischen der Stammdomäne der Gesamtstruktur und den ersten Domänen neuer Domänenstrukturen.

3.3 Der globale Katalog

Der globale Katalog ist zuständig für die Suche nach Objekten im Verzeichnis. Er wird automatisch auf dem ersten Domänencontroller der Stammdomäne der Gesamtstruktur erstellt. Damit wird dieser spezielle Domänencontroller auch globaler Katalogserver genannt.

Im globalen Katalog werden zwei verschiedene Replikate der Objektattribute gespeichert. Zum einen enthält der Katalogserver ein vollständiges Replikat aller Objektattribute im gesamten Verzeichnis und zum anderen ein Teilreplikat der Objektattribute, die sich nur im Verzeichnis in jeder Domäne der Gesamtstruktur befinden. Das Teilreplikat enthält zwar alle Objekte, aber nur eine begrenzte Anzahl der Attribute. Über dieses Teilreplikat werden die Suchanfragen zu Objekten im Verzeichnis abgewickelt. Es enthält nur die Attribute der Objekte, die am häufigsten bei Suchanfragen benötigt werden – dazu zählen beispielsweise Benutzernamen – oder die notwendig sind, um das vollständige Replikat des Objektes zu finden. Um die Sicherheit beim Zugriff auf die Objekte über den globalen Katalog zu gewährleisten, erben die Objekte die Zugriffsrechte ihrer Quelldomänen.

Bei einem Objekt sind die Informationen des definierten Namens ausreichend, um den Pfad zum vollständigen Replikat dieses Objektes zu finden. In vielen Fällen ist dem Benutzer aber nicht der vollständige definierte Name bekannt. Über den globalen Katalog wird es ihm ermöglicht, dass er das gewünschte Objekt dennoch findet, wenn er nur einige ihm bekannte Attribute für die Suche angibt. Es ist also nicht erforderlich, dass der Benutzer die genaue Lage des Objekts innerhalb der Gesamtstruktur kennen muss.

Deshalb ist es auch wichtig, bei der Erstellung von Objekten möglichst viele Eigenschaften festzulegen, um die Effektivität des globalen Katalogs optimal nutzen zu können.

Durch die Verwendung des globalen Katalogs wird der Netzwerkverkehr stark minimiert. Da im Katalog Informationen zu allen Objekten in allen Domänen der Gesamtstruktur enthalten sind, kann eine Suchanfrage innerhalb der Domäne bearbeitet werden, in der der Benutzer, der das Objekt sucht, angemeldet ist. Damit entfällt eine Suche und damit auch der Netzwerkverkehr über Domänengrenzen hinweg.

Auch bei der Anmeldung von Benutzern an der Domäne spielt der globale Katalogserver eine wichtige Rolle. Dieser Server stellt dem Domänencontroller Informationen über das Benutzerkonto zur Verfügung. Beim Anmelden des Clients wird eine Liste generiert, die alle Gruppen enthält, in denen der Client Mitglied ist. Dieses Feature wird jedoch nur in Multi-Domänen-Umgebungen genutzt, in denen der Client Mitglied in mehreren Gruppen in mehreren Domänen sein kann. Die globalen Katalogserver enthalten Mitgliedschaftslisten aller universellen Sicherheitsgruppen. Diese Listen werden benutzt, wenn Clients oder Server die Mitgliedschaft in den Sicherheitsgruppen prüfen müssen. Näheres zu universellen Gruppen finden Sie in Kapitel 18.4. Universelle Gruppen können nur im einheitlichen Betriebsmodus oder Windows Server 2003-Betriebsmodus verwendet werden.

Eine weitere Funktion kommt dem globalen Katalogserver zu, wenn Sie in Ihrer Umgebung Microsoft Exchange Server 2000 einsetzen. Die Katalogserver sind zuständig für das Nachschlagen der Adressbucheinträge und das Auflösen von E-Mail-Adressen für Outlook-Clients ab der Version Outlook 98 SP2. Ältere E-Mail-Clients benutzen dafür den Exchange-Server, der dann seinerseits den Zugriff auf einen Katalogserver benötigt.

3.3.1 Standorte von Katalogservern

Aufgrund der eben genannten Aufgaben des Katalogservers können Sie überdenken, wie viele Katalogserver im Netzwerk erforderlich sein können. Dabei sei gleich vorweg eine Warnung ausgesprochen: Zu viele Katalogserver können Ihrer Netzwerk-Performance erheblich schaden. In diesem Zusammenhang sind einige Worte über die Standorte von globalen Katalogservern innerhalb der Gesamtstruktur angebracht.

Standardmäßig befindet sich der globale Katalogserver auf dem Domänencontroller, wenn in einer Domäne nur ein Domänencontroller vorhanden ist. Haben Sie hingegen mehrere Domänencontroller in der Domäne, so muss einer davon als Katalogserver definiert werden. Die praktische Anleitung dazu finden Sie in Kapitel 15.

Versucht sich ein Benutzer an einer Domäne anzumelden, so muss dafür der Zugriff auf einen globalen Katalogserver sichergestellt sein. Andernfalls kann sich der Benutzer nur über das Login-Caching an der Domäne anmelden. Nur die Mitglieder der Gruppe „Domänen-Admins“ können sich auch ohne den globalen Katalogserver stets an der Domäne anmelden. Wenn in Teilen des Netzwerks nur langsame oder nicht immer verfügbare Verbindungen zwischen den Clients und den Katalogservern vorhanden sind, so sollten Sie auf beiden Seiten der langsamen Verbindung einen Katalogserver implementieren. Zusätzlich kann die Replikation mit einem Domänencontroller an einem Standort mit einer langsamen Verbindung so festgelegt werden, dass sie in Zeiträumen mit geringer Netzwerkauslastung, also etwa den Nachtstunden, vollzogen wird.

Richten Sie auch keinen Katalogserver auf dem Domänencontroller ein, der die Betriebsmasterrolle des Infrastrukturmasters (siehe Kapitel 11.1.2) innehat. Der Infrastrukturmaster ist zuständig für die Aktualisierung von Verweisen zwischen Benutzern und Gruppen. Da ein globaler Katalogserver aber keine veralteten, zu aktualisierenden Einträge in seiner Datenbank enthält, kann der Infrastrukturmaster seine Aufgabe nicht wahrnehmen. Ist jeder Domänencontroller gleichzeitig auch ein Katalogserver, brauchen Sie keine Infrastrukturmater einzurichten.

Haben Sie in Ihrer Umgebung nur eine einzelne Domäne und keinen Exchange 2000-Server im Einsatz, so müssen Sie keine zusätzlichen Katalogserver implementieren. Nutzen Sie den Domänencontroller als Katalogserver. Über diesen können die Clients Objekte Ihrer eigenen Domäne suchen.

Setzen Sie den Exchange 2000-Server ein, so richten Sie einen Katalogserver an jedem Standort ein, der über mehr als zehn Benutzer verfügt. In sehr großen Standorten sollten Sie aus Gründen der Lastenverteilung und Fehlertoleranz sogar zwei Katalogserver erstellen.

Idealerweise haben Sie also an jedem physischen Standort je nach Größe mindestens einen Katalogserver und einen oder mehrere Domänencontroller zur Verfügung. Belassen Sie am besten den Katalogserver auf dem Domänencontroller. Haben Sie an einem Standort mehrere Domänencontroller, sollte nicht jeder gleichzeitig auch die Rolle des globalen Katalogservers übernehmen. Dies würde zu einer erhöhten Netzwerkauslastung nur durch den Replikations-Datenverkehr zwischen den Katalogservern führen, da sich alle Katalogserver in der Gesamtstruktur miteinander replizieren. Allerdings wird ein wesentlich größerer Teil des Netzwerkverkehrs durch die Abfragen von Objekten im Active Directory durch Benutzer und Programme verursacht.

An kleineren Standorten können Sie sogar auf einen eigenen Katalogserver verzichten. Allerdings sollte die Netzwerkanbindung mindestens über eine schnelle WAN-Verbindung (Breitbandleitung T1 mit 1,544 Mbit/s oder schneller) zum Standort des nächstgelegenen Katalogservers verfügen.

Der globale Katalog wird automatisch über die Active Directory-Replikation erstellt. Auch die Replikationstopologie wird automatisch eingerichtet. Der Satz von Eigenschaften, der in das Teilreplikat der Objektattribute aufgenommen wird, ist von Microsoft vorgegeben. Allerdings haben Sie als Administrator die Möglichkeit, diesen Satz zu erweitern oder anzupassen.

3.4 Standorte

Standorte strukturieren wie Domänen das Netzwerk. Die Domänen spiegeln dabei die logische Struktur des Unternehmens wider, während Standorte die physische Struktur widerspiegeln. Des Weiteren dienen auch Organisationseinheiten der logischen Strukturierung des Netzwerks.

Ein Standort entspricht einer Gruppe von Computern, die zu einem bestimmten IP-Subnetz gehören. Damit gelten diese Computer untereinander als gut verbunden. Die Computer an einem Standort können auch verschiedenen IP-Subnetzen angehören. Allerdings muss dann auch zwischen diesen eine schnelle Verbindung sichergestellt sein. Diese schnelle Verbindung ist erforderlich, da innerhalb eines Standorts die Replikation sowie Ressourcenabfragen aus dem Active Directory einen nicht unerheblichen Teil der Netzwerkbandbreite in Anspruch nehmen. Deshalb ist es sinnvoller, für WANs mehrere Standorte zu konfigurieren.

Die praktische Anleitung zum Einrichten von Standorten finden Sie in Kapitel 14.1.

Für das Verhältnis zwischen Standorten und Domänen gelten die folgenden Punkte: Eine Domäne kann mehrere Standorte enthalten (siehe Abbildung 3.4), und umgekehrt kann ein Standort auch mehrere Domänen enthalten (siehe Abbildung 3.5). Daraus ergibt sich, dass keine Übereinstimmung zwischen Standortgrenzen und dem Namensraum der Domänen bestehen muss.

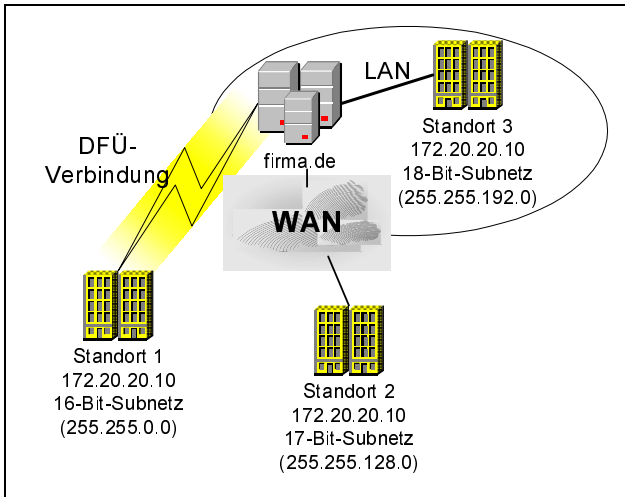


Abbildung 3.4: Eine Domäne mit mehreren Standorten

Im ersten Modell (siehe Abbildung 3.4) verfügt die Domäne *firma.de* über insgesamt drei Standorte. Jeder der drei Standorte hat seinen eigenen Subnetzbereich. Die Computer der Standorte 1 und 2 sind nur über langsame Verbindungen (DFÜ bzw. WAN) mit der Domäne verbunden. Deshalb wurde für sie jeweils ein eigener Standort eingerichtet. Der dritte Standort umfasst die Computer eines Subnetzes, die über eine schnelle LAN-Verbindung mit der Domäne verbunden sind. Die Computer aller Standorte sind Mitglieder der Domäne *firma.de*.

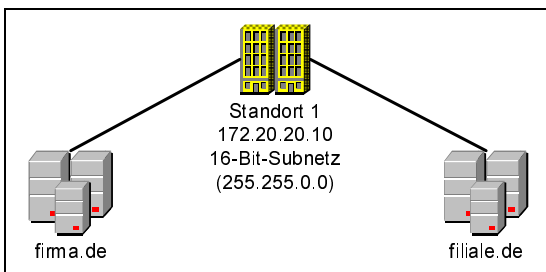


Abbildung 3.5: Ein Standort in mehreren Domänen

Im zweiten Modell (siehe Abbildung 3.5) gibt es nur einen Standort mit einem zusammenhängenden 16-Bit-Subnetz. Zu diesem Standort gehören Computer, die ihrer logischen Struktur nach der Domäne *firma.de* oder der Domäne *filiale.de* angehören. Der Standort sagt also nichts über die logische Zugehörigkeit der Computer aus.

Wenn Sie die mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE öffnen, werden Sie feststellen, dass dort nicht die Computer, die zu einem bestimmten Standort gehören, aufgelistet werden. Das Durchsuchen einer Domäne gibt nur die Computer in ihrer logischen Struktur an. Die einzelnen Computer finden Sie nur unter den Domänen und Organisationseinheiten. Unter ACTIVE DIRECTORY-STANDORTE UND -DIENSTE finden Sie nur die Elemente, die für die Konfiguration der Replikation zwischen den Standorten zuständig sind.

Nun noch einige Worte dazu, inwiefern jeder Standort über einen eigenen Domänencontroller verfügen muss.

Wenn Sie bei bestimmten Rechnern im Netzwerk bemerken, dass die Domänencontroller sehr lange brauchen, um die Clientanforderungen zu bearbeiten, oder die Menge der Benutzer nicht mehr verarbeiten können, so sollten Sie darüber nachdenken, diese Rechner zu einem separaten Standort mit einem eigenen Domänencontroller zusammenzufassen. Bei der Anmeldung sucht ein Client immer zuerst an seinem eigenen Standort nach einem Domänencontroller. Clientsubnetze sollten immer nur den Standorten zugeordnet werden, zu denen eine schnelle Verbindung und damit auch ein effizienter Zugriff auf den Domänencontroller und die Ressourcen besteht.

Wenn sich an einem Standort einer Niederlassung kein Domänencontroller befindet, so werden dorthin auch keine Daten repliziert. Der Client muss also für jede Anmeldung und Ressourcenabfrage eine Netzwerkverbindung zur Hauptstelle oder zu einem Domänencontroller eines anderen Standorts herstellen. Damit dieser Vorgang praktikabel ist, muss eine schnelle Verbindung zum entsprechenden entfernten Domänencontroller vorhanden sein. Nur ein sehr kleiner Standort (bis maximal zehn Clients) muss nicht zwangsläufig über einen eigenen Domänencontroller verfügen. An einem größeren Standort sollen mehrere Domänencontroller eingerichtet werden.

3.5 Organisationseinheiten

Organisationseinheiten sind neben den Domänen die zweite Einheit zur logischen Gruppierung von Netzwerkressourcen. Jede Domäne kann ihre eigene Hierarchie und Gliederung der Organisationseinheiten haben.

Die Mitglieder der Organisationseinheiten sind alle Mitglieder der Domäne, die die Organisationseinheit(en) beinhaltet. Eine Organisationseinheit verfügt im Gegensatz zu einem Standort nicht über eigene Domänencontroller.

Die Organisationseinheiten werden statt der Ressourcendomänen in den Windows NT-Domänenmodellen verwendet. In einer Organisationseinheit werden Objekte in Gruppen gegliedert. Diese Gruppen können die Unternehmensstruktur widerspiegeln. Eine Organisationseinheit kann Objekte wie Computer, Kontakte, Gruppen, weitere Organisationseinheiten, Drucker, Benutzer und freigegebene Ordner enthalten. Durch die Übersichtlichkeit einer geringeren Anzahl von Objekten innerhalb einer Organisationseinheit werden deren Verwaltung und Anzeige erleichtert.

An eine Organisationseinheit können administrative Aufgaben delegiert werden. Die Berechtigungen, die ein Benutzer für die Durchführung seiner administrativen Aufgaben benötigt, können entweder für eine separate Organisationseinheit erteilt werden

oder für eine übergeordnete Organisationseinheit, die die Berechtigungen an die untergeordneten weitervererbt. Damit ist es möglich, die Administration der Domäne an mehrere Administratoren zu verteilen. Sie können so für die Organisationseinheit spezielle Verwaltungsaufgaben erledigen.

Die praktische Anleitung für das Erstellen und Konfigurieren von Organisationseinheiten finden Sie in Kapitel 14.2. Standardmäßig sind keine vorkonfigurierten Organisationseinheiten in der mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER enthalten. Dies würde auch wenig Sinn machen, da ja gerade durch die Individualität der Organisationseinheiten Ihr Unternehmensnetzwerk strukturiert werden soll.

Abbildung 3.6 gibt einen Überblick über Organisationseinheiten innerhalb einer Domäne sowie die verschiedenen Objekte, die in jeder Organisationseinheit enthalten sein können.

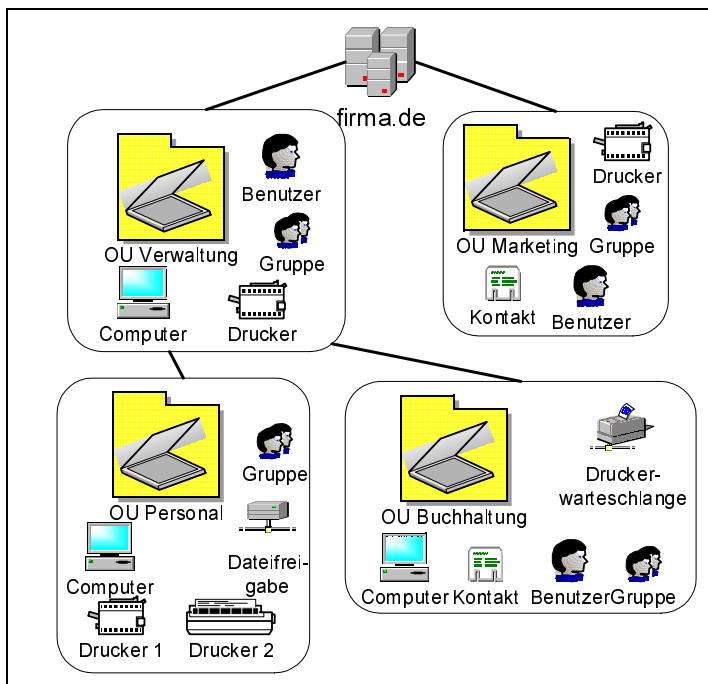


Abbildung 3.6: Die Struktur einer Organisationseinheit

Die Abbildung zeigt eine Domäne mit insgesamt vier Organisationseinheiten. Die beiden Organisationseinheiten Verwaltung und Marketing sind dabei auf einer Hierarchieebene, die Organisationseinheit Verwaltung enthält als untergeordnete Objekte die Organisationseinheiten Personal sowie Buchhaltung.

Jede einzelne Organisationseinheit hat ihre eigene unabhängige Struktur und ihre eigenen Ressourcen. Objekte, die in einer Organisationseinheit vorhanden sind, müssen nicht in allen Organisationseinheiten der Domäne vorkommen, und umgekehrt müssen auch nicht alle Objekte in einer Organisationseinheit eingebunden sein.

3.6 Objekte und Schema

Im Active Directory werden sämtliche Ressourcen als Objekte gespeichert. Objekte können Computer, Konten, Drucker, Kontakte usw. sein. Jedes Objekt besteht aus einem bestimmten Satz von Eigenschaften bzw. Attributen, die für dieses Objekt spezifisch sind. So umfasst z.B. ein Domänencontroller-Objekt die folgenden Attribute unter den allgemeinen Eigenschaften: Computernamen, DNS-Name, Funktion und Beschreibung. Diese Eigenschaften dienen Active Directory als Vorlage für die Objekte. Diese Vorlage muss dem Verzeichnisdienst zum Speichern der Objekte bekannt sein.

Das Active Directory-Schema enthält einen vorgegebenen Satz von Definitionen für die Objekte und Informationen im Active Directory. Es gibt zwei Arten von Definitionen, nämlich Attribute und Klassen. Diese werden auch Schemaobjekte oder Metadaten genannt. Das Active Directory-Schema ist für alle Domänen innerhalb einer Gesamtstruktur verbindlich dasselbe. Die Informationen des Schemas werden automatisch repliziert.

Attribute

Ein Attribut wird nur einmalig im Schema definiert und kann von beliebigen Klassen genutzt werden. So finden Sie z.B. in diversen Objekten wie etwa Computer, Konto usw. das Attribut „Beschreibung“. In jeder dieser Klassen erfüllt das Attribut den allgemeinen Zweck, das entsprechende Objekt näher zu erläutern, aber in jeder Klasse sieht die Beschreibung für das spezielle Objekt verschieden aus.

Klassen

Die Klassen bestimmen, welche Arten von Objekten im Active Directory erstellt werden können, so z.B. Computer, Konten usw. Jede Klasse beinhaltet einen bestimmten Satz aller möglichen Attribute. Wenn Sie ein Objekt neu erstellen, erhalten die Attribute die Werte, die das Objekt konkret beschreiben. Die Klassen werden auch als Objektklassen bezeichnet.

Unter Windows 2000 und 2003 haben Sie die Möglichkeit, das Schema individuell nach Ihren Bedürfnissen anzupassen. Die praktische Anleitung dazu finden Sie in Kapitel 24.3.

Das Active Directory-Schema ist objektorientiert. Es wird im Verzeichnis als ein Satz von Objekt-Instanzen gespeichert. Dies ist der Unterschied zu anderen Verzeichnisdiensten, bei denen das Schema als Textdatei gespeichert wird, die beim Start des Verzeichnisdienstes ausgelesen wird. Aus den gespeicherten Objekten im Active Directory können Applikationen beispielsweise auslesen, welche Objekte und Eigenschaften verfügbar sind.

Das Active Directory-Schema kann dynamisch aktualisiert werden. Beispielsweise kann eine Applikation dem Schema neue Klassen und Attribute hinzufügen und diese neu hinzugefügten Metadaten sofort benutzen. Eine Änderung des Schemas wird durch das Erstellen oder Modifizieren der im Verzeichnis gespeicherten Metadaten erreicht. Auch die Metadaten werden wie jedes andere Objekt im Active Directory durch Zugriffssteuerungslisten (ACLs) geschützt. So wird sichergestellt, dass nur autorisierte Benutzer das Schema ändern können.

3.7 Replikation

Replikation bedeutet das Austauschen von Verzeichnisinformationen zwischen mehreren Domänencontrollern. Sämtliche Domänencontroller einer Domäne müssen immer die aktuellen Verzeichnisinformationen zur Verfügung haben. Wenn Sie an einem beliebigen Domänencontroller der Domäne Änderungen vornehmen, so müssen diese schnellstmöglich auch den anderen Domänencontrollern verfügbar gemacht werden. Bei der Replikation werden die geänderten Verzeichnisinformationen von dem einen Domänencontroller an alle anderen gesendet.

3.7.1 Multimaster-Replikation

In einer Windows NT-Umgebung gibt es einen übergeordneten PDC und untergeordnete BDCs. Unter Windows 2000/2003 sind alle Domänencontroller gleichrangig. Fügen Sie einer Domäne aus Aspekten der Redundanz einen weiteren Domänencontroller hinzu, so bezeichnet man diesen auch als Peer-Domänencontroller. Da Windows 2000/2003 nicht mehr auf einen übergeordneten Master-Domänencontroller beschränkt ist, sondern jeder einzelne als Master agiert, spricht man vom Multimaster-Domänenmodell. Analog dazu verwendet Windows 2000/2003 auch die Multimaster-Replikation. Somit müssen Sie nicht, wie unter Windows NT, alle Änderungen am PDC vornehmen, sondern Sie können die Verwaltung von einem beliebigen Domänencontroller aus vornehmen. Außerdem bietet die Multimaster-Replikation den Vorteil, dass die Replikation auch dann fortgesetzt werden kann, wenn ein Domänencontroller nicht verfügbar ist. Es ist stets eine hohe Verfügbarkeit der Verzeichnisdaten sichergestellt. Durch die Multimaster-Replikation wird weiterhin eine ausgewogenere Lastenverteilung zwischen den Domänencontrollern sowie eine höhere Fehlertoleranz verwirklicht.

Wenn Sie Active Directory im einheitlichen Modus betreiben, so kann keine Replikation mehr mit Windows NT-Domänencontrollern stattfinden. Im gemischten Modus übernimmt der PDC-Emulator-Betriebsmaster (siehe Kapitel 11.1.2) die Replikation mit den Windows NT-BDCs.

Jeder der Domänencontroller besitzt eine beschreibbare Kopie der Verzeichnisdatenbank. Wurden hier Änderungen durchgeführt oder neue Einträge vorgenommen, werden die geänderten bzw. neuen Einträge auf die übrigen Domänencontroller repliziert. Das Active Directory beschränkt sich bei der Replikation ausschließlich auf geänderte oder neue Einträge in der Datenbank. Nicht geänderte Einträge werden nicht zwischen den Domänencontrollern ausgetauscht. Damit ist sichergestellt, dass die durch die Replikation entstehende Netzwerklast auf ein Minimum reduziert wird.

Das Multimaster-Modell könnte nun jedoch auf den ersten Blick auch ein Problem mit sich bringen. Was geschieht nämlich, wenn dieselben Änderungen an einem bestimmten Objekt gleichzeitig an mehreren Domänencontrollern vorgenommen werden?

Jeder Domänencontroller verwendet einen Zähler für die Änderungen, die an seiner eigenen Verzeichnisdatenbank-Kopie durchgeführt wurden (*Originating Write*), sowie einen weiteren Zähler für die Änderungen, die er von seinen Replikationspartnern empfangen hat (*Replicated Write*). Ist nun beispielsweise ein Domänencontroller für eine Weile nicht im Netzwerk verfügbar gewesen, so prüft er bei der Wiederinbetriebnahme

anhand seiner Zähler, ob er alle Änderungen seiner Replikationspartner empfangen hat. Ist dies nicht der Fall, so fordert er nur die aktuellen, bei ihm noch nicht vorhandenen Änderungsinformationen an. Jedes Objekt enthält zwei verschiedene USNs (*Update Sequence Number*). Es gibt einen USN-Wert für das Erstellen (*uSN-Created-Wert*) und einen Wert für das Ändern des Objekts (*uSN-Changed-Wert*).

Angenommen, Sie erstellen über die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER zehn neue Benutzer auf Server 1. Dann wird die USN für Server 1 um den Wert 10 heraufgesetzt, da die Informationen zehnmal aktualisiert worden sind. Bei diesem Schreibvorgang handelt es sich um eine ausgehende Aktualisierung (Originating Update), da der Server selbst die Aktualisierung vorgenommen hat. Auch direkt mit dem Server verbundene Anwendungen führen ausgehende Aktualisierungen durch. Wird hingegen eine Änderung bei der Replikation empfangen, spricht man von replizierter Aktualisierung (Replicated Update). Für beide Aktualisierungen gibt es separate Zähler.

Jede dieser Änderungen enthält eine eindeutige Sequenznummer (USN) sowie einen Zeitstempel. Der höchste USN-Wert ist dabei stets der aktuelle. Die Größe des USN-Wertes beträgt für jedes Objekt 64 Bit. War nun ein Domänencontroller längere Zeit nicht verfügbar, so verfolgt er die zwischenzeitlich vorgenommenen Änderungen nur anhand der Sequenznummer.

Tritt jedoch der kompliziertere Fall auf, dass dieselbe Änderung von verschiedenen Benutzern an zwei Domänencontrollern durchgeführt wurde, während beide im Netzwerk verfügbar waren, so entscheidet zusätzlich der Zeitstempel. Für diesen seltenen Fall ist eine Zeitsynchronisierung der Domänencontroller sinnvoll. Dieses Verfahren wird ausführlich in Kapitel 17.1.5 beschrieben. Auch die Konfliktlösung von weiteren Replikationsproblemen wird in Kapitel 17.3 beschrieben.

Die Replikation der Daten geschieht im Active Directory entweder automatisch oder für standortübergreifende Replikation auch nach einem Zeitplan. Allerdings muss dabei gewährleistet sein, dass eine Änderung nicht vom Quell-Domänencontroller auf andere Domänencontroller und von dort wieder auf die Quelle repliziert wird. Damit würde ein endloser Replikationskreislauf mit hoher Netzwerkbelastung entstehen. Hiergegen verwendet Active Directory jedoch ein systemimmanentes Verfahren, bei dem die Attribute und deren Zähler der ausgehenden Aktualisierungen überwacht werden. Dieser Zähler wird nur bei lokaler Änderung, jedoch nicht bei der Replikation erhöht. Somit ist für den Replikationsprozess erkennbar, dass die Änderung nicht mehr auf den Quellserver repliziert werden muss.

3.7.2 Die Verzeichnispartitionen oder Namenskontexte

Bei der Replikation werden drei Arten von Informationen ausgetauscht. Diese Arten werden auch als Verzeichnispartitionen oder Namenskontexte (NC = Naming Context) bezeichnet. Dabei handelt es sich um

- ▶ Schemainformationen,
- ▶ Konfigurationsinformationen sowie
- ▶ Domänendaten.

Die Schemainformationen geben die Objekte sowie deren Attribute vor, die Sie im Verzeichnis erstellen können. Die Konfigurationsinformationen enthalten alle Angaben zur

Domänenstruktur und Replikationstopologie. Die Domänenendaten enthalten die domänenspezifischen Daten einer Domäne. Ein ausgewählter Teil dieser Daten befindet sich im globalen Katalog aller Domänen einer Gesamtstruktur. Diese Teilmenge wird ausschließlich zwischen globalen Katalogservern repliziert.

Die Konfigurations- und Schemainformationen werden auf sämtliche Domänencontroller der Gesamtstruktur repliziert, die spezifischen Domänenendaten nur auf die Domänencontroller der Domäne und die ausgewählte Teilmenge der Domänenendaten auf alle globalen Katalogserver.

Tabelle 3.1 fasst zusammen, welche Informationen auf einem Domänencontroller und einem globalen Katalogserver vorhanden sind und repliziert werden:

Information	Domänencontroller	Globaler Katalogserver
Schemainformationen	Für die Domänen- oder Gesamtstruktur	Für die Gesamtstruktur
Konfigurationsinformationen	Für alle Domänen der Domänen- oder Gesamtstruktur	Für alle Domänen der Gesamtstruktur
Domänenendaten	Sämtliche Objekte und Eigenschaften der Domäne	Sämtliche Objekte und Eigenschaften der Domäne, der der Katalogserver angehört, sowie die Teilmenge der Objekte und Eigenschaften der Gesamtstruktur

Tabelle 3.1: Replikationsinformationen auf Domänencontrollern und Katalogservern

Unter Windows 2003 ist neben diesen dreien eine zusätzliche Verzeichnispertition verfügbar, die Applikationspartition. Diese Partition kann eine Hierarchie aller Objekttypen (mit Ausnahme der sicherheitsbezogenen Objekte Benutzer, Gruppen und Computer) enthalten und so konfiguriert werden, dass die Replikation mit beliebigen Domänencontrollern innerhalb der Gesamtstruktur und nicht nur derselben Domänenstruktur durchgeführt werden kann. Mit dieser neuen Partition wird es möglich, dynamische Daten im Active Directory zu speichern, wobei Sie die Möglichkeit haben, den Umfang der Replikationsdaten sowie die Platzierung der Repliken zu steuern, ohne dabei die Netzwerklast unnötig steigern zu müssen.

3.7.3 Replikationstopologie

Bei der Replikation wird unterschieden in Replikation innerhalb eines Standortes und standortübergreifende Replikation. Innerhalb eines Standorts erzeugt Active Directory über Replikationstopologie-Verknüpfungen automatisch eine Ringtopologie zur Replikation zwischen den Domänencontrollern. Für die Berechnung der Replikationstopologie ist der Knowledge Consistency Checker (KCC) zuständig. In der Ringtopologie ist immer ein alternativer Replikationspfad vorhanden, falls ein Domänencontroller ausfallen sollte. Damit ist gewährleistet, dass stets alle Domänencontroller, die im Netzwerk verfügbar sind, ihre aktuellen Informationen austauschen können.

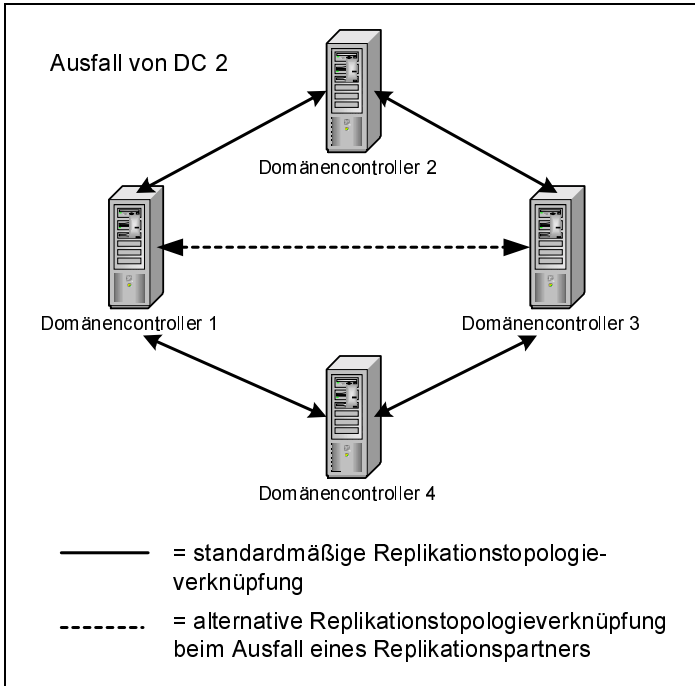


Abbildung 3.7: Replikationstopologie innerhalb eines Standorts

Abbildung 3.7 zeigt den standardmäßigen Replikationspfad zwischen den Domänencontrollern 1 bis 4. Sollte nun der Domänencontroller 2 ausfallen, so bemerkt Domänencontroller 1 den Ausfall und wendet seinen Alternativpfad auf Domänencontroller 3 an, der dann in gewohnter Weise seine Informationen an Domänencontroller 4 repliziert.

Selbst wenn Sie zusätzliche Domänencontroller hinzufügen, gliedert Active Directory diese automatisch in die bestehende Replikationstopologie ein. Auch wenn Sie einen Domänencontroller aus der Domäne entfernen, unternimmt Active Directory automatisch die notwendigen Schritte. Sie sehen also, dass Sie für die standortinterne Replikation keinerlei Einstellungen selber vornehmen müssen.

Die standortübergreifende Replikation müssen Sie hingegen manuell einrichten. Hierbei können Sie Zeiten und Intervalle definieren, Kosten festlegen sowie das Replikationsprotokoll wählen.

Die Replikation findet sowohl automatisch innerhalb eines Standortes als auch benutzerdefiniert zwischen verschiedenen Standorten statt. Bei der standortübergreifenden Replikation werden die Daten zur Entlastung und Beschleunigung des Netzwerkverkehrs zwischen den Standorten komprimiert übermittelt. Für das Entpacken der Daten wird jedoch Prozessorleistung benötigt. Umgekehrt werden die Daten innerhalb eines Standorts nicht komprimiert. Da es sich an einem Standort meistens um eine LAN-Verbindung handelt, ist hier das Komprimieren zur Netzwerkentlastung nicht erforderlich. Dafür entfällt eine höhere Prozessorauslastung durch das Dekomprimieren der Daten.

3.8 Zusammenarbeit mit anderen Betriebssystemen und Verzeichnisdiensten

In diesem Kapitel wird geklärt, mit welchen anderen Betriebssystemen und Verzeichnisdiensten Windows 2000 Active Directory Interoperabilität bietet. Es ist unwahrscheinlich, dass in allen Unternehmen nur eine reine Windows 2000- oder XP-Umgebung vorhanden ist. Gerade der Verzeichnisdienst Novell Directory Service (NDS) von Novell NetWare oder Unix werden oftmals parallel eingesetzt. Zuvor wird beschrieben, inwieweit eine Zusammenarbeit von Active Directory mit älteren Windows-Betriebssystemen gewährleistet ist. Auch die fortschreitende Integration von Microsoft BackOffice-Servern in Active Directory wird in diesem Kapitel besprochen.

3.8.1 ADSI-Clients für Windows 9x und NT

Für die volle Funktionalität aller Active Directory-Features müssen Sie Windows 2000- oder XP-Professional-Clients einsetzen. Dennoch ist es auch möglich, Windows-Clients mit Windows 9x oder NT die Zusammenarbeit mit Active Directory zu ermöglichen. Hierzu werden die Windows 9x / NT Active Directory Services Interface-(ADSI-)Clients eingesetzt. Diese ermöglichen immerhin wichtige Grundfunktionalitäten von Active Directory für die älteren Windows-Clients. Die Windows-Versionen 3.x und Windows for Workgroups werden nicht von ADSI unterstützt. Die ADSI-Clients werden wie ein zusätzlicher Netzwerk-Client, etwa der Client für Microsoft-Netzwerk oder Client Service für NetWare, installiert.

Über die ADSI-Services werden Ihnen wie gesagt nur die Kernfeatures von Sicherheit und Benutzerzugriff bereitgestellt. Die folgenden Features werden geboten:

- ▶ Der ADSI-Client beinhaltet die NTLM-(NT LAN-Manager-)Authentifizierung in der Version 2.0. Mit der neuen Version werden viele Sicherheitslücken gegenüber der von Windows 9x und NT verwendeten Version 1.0 geschlossen.
- ▶ Der ADSI-Client unterstützt die Kenntnis über seinen aktuellen Standort. Damit wird es ermöglicht, dass Sie sich bei dem Domänencontroller anmelden, der Ihrem Standort am nächsten ist. Standardmäßig melden sich die 9x / NT-Clients zufällig an einem beliebigen Domänencontroller an. Dabei ist es den Clients auch gleichgültig, falls sich der ausgesuchte Domänencontroller am anderen Ende eines WANs befinden sollte.
- ▶ Ein weiteres Handicap des Windows 9x-Clients besteht darin, dass er in einer Windows 2000-Domäne zur Passwortänderung zwingend Zugriff auf den PDC-Emulator-Betriebsmaster benötigt. Auch dieses Problem wird durch den ADSI-Client behoben.
- ▶ Die ADSI-Clients unterstützen eine Skripting-Schnittstelle für ADSI-basierte Skripte. Über diese Skripte, die z.B. in Form von Login-Skripten erstellt werden können, kann direkt auf das Active Directory zugegriffen werden.
- ▶ Standardmäßig können Windows 9x- und NT-Client nur auf allein stehende Wurzelverzeichnisse von DFS (Distributed File System) zugreifen. Mit dem ADSI-Client wird ihnen jedoch der Zugriff auf die fehlertoleranteren verteilten Verzeichnisse ermöglicht, durch die eine höhere Zuverlässigkeit und Fehlertoleranz der DFS-Struktur ermöglicht wird.

- ▶ Als letztes Feature haben die ADSI-Clients Zugriff auf die Eigenschaften des Windows-Adressbuches (Funktion: Suchen nach Personen) im Active Directory. Mit den entsprechenden Zugriffsrechten können Sie dort sogar Eigenschaften wie die Telefonnummer ändern.

Wie gesagt, der Einsatz von ADSI ermöglicht Ihnen nicht die komplette Funktionspalette von Active Directory. Deshalb werden Ihnen nun auch einige Features aufgelistet, die trotz ADSI nicht von Windows 9x- und NT-Clients unterstützt werden können.

- ▶ Die Unterstützung der Gruppenrichtlinie sowie der IntelliMirror-Funktionen wie etwa der Softwareverteilung fehlen völlig. Dies ist eindeutig der größte Mangel. Eine Anpassung der beiden ADSI-Clients hätte einen enormen Arbeitsaufwand für Microsoft bedeutet, da diese Technologien eine der größten Änderungen ab der Windows-Version 2000 darstellen.
- ▶ Auch das Kerberos V5-Protokoll (siehe Kapitel 2.2.3) wird nicht unterstützt. Die fehlende Unterstützung des speziellen Speicherbereichs zum Cachen der Kerberos-Tickets versagt den Windows 9x- und NT-Clients dieses Feature.

Sie sehen also, dass der ADSI-Client eine gute Zwischenlösung sein kann, bis sämtliche Client-Computer auf Windows 2000 oder XP Professional migriert sind. Aufgrund der fehlenden wichtigen Funktionalitäten ist der ADSI-Client keine Alternative zu einem echten Windows 2000- oder XP-Client. Deswegen sollte sein Einsatz auch nur bis zu dem Zeitpunkt einer Migration beschränkt bleiben.

Um sich die Arbeit der ADSI-Clientinstallation möglicherweise zu sparen, überlegen Sie, ob Sie in Ihrem Netzwerk die durch den ADSI-Client bereitgestellten Funktionalitäten des Active Directory überhaupt nutzen. Werden Sie überhaupt ein verteiltes fehlertolerantes DFS einsetzen? Oder verfügt Ihr Unternehmen überhaupt über mehrere Standorte, sodass es wichtig wird, welcher Domänencontroller zur Authentifizierung herangezogen wird? Dies wird in einem kleinen Unternehmen nicht der Fall sein. Können Sie diese Fragen mit Nein beantworten, müssen Sie den ADSI-Client als Zwischenlösung nicht unbedingt installieren.

Den ADSI-Client für Windows 9x finden Sie auf der Windows 2000 Server-CD unter \CLIENTS\DSCLIENT.EXE. Den ADSI-Client für Windows NT können Sie direkt von der Microsoft-Webseite downloaden. Die Verteilung der Clients können Sie beispielsweise über Login-Skripte oder ein beliebiges Softwareverteilungsprogramm vornehmen. Die Clients unterstützen beide die Silent Installation.

Die ADSI-Schnittstellen umfassen ein Verzeichnisdienstmodell und eine Gruppe von COM-Schnittstellen. Über diese Schnittstellen können Anwendungen für Windows 95, Windows 98, Windows NT, Windows 2000 und XP Professional auf verschiedene Verzeichnisdienste zugreifen, beispielsweise auf Active Directory. Sie können als SDK (Software Development Kit) bezogen werden. Die Schnittstellen unterstützen die als Internetstandard (siehe dazu RFC 1823) festgelegten LDAP-Anwendungsprogrammierschnittstellen in der Programmiersprache C. Hierdurch können auch andere Verzeichnisdienstapplikationen so modifiziert werden, dass sie über Active Directory-Schnittstellen und LDAP auf Informationen im Active Directory zugreifen können.

3.8.2 Unix und Linux

Die Zusammenarbeit zwischen Windows und Unix erfolgt über die Services for Unix (SFU). Diese werden von Windows 2000 ab der Version 2.0 unterstützt. Aktuell ist die Version 3.0 der Unix-Services. Für Windows NT gab es die Unix-Services in der Version 1.0. Diese Unix-Services bestehen aus einigen Microsoft-eigenen Programmen sowie auch weiteren Dienstprogrammen und Verfahren von Drittanbietern zur Zusammenarbeit zwischen den beiden Betriebssystemen. In SFU 3.0 sind über 300 Tools sowie ein SDK für die Unterstützung von über 1900 Unix-APIs enthalten. Folgende Funktionalitäten werden über die Unix-Services für Windows ermöglicht:

- ▶ Die Unterstützung für das Network File System (NFS) ist integriert. NFS ist ein Dienst, der verteilten Computersystemen ein verteiltes Dateisystem bereitstellt. Hierbei handelt es sich um das Unix-Pendant zum DFS (Distributed File System) unter Windows 2000.
- ▶ Weiterhin wird unter Windows eine Unix-Befehlsshell, genauer gesagt die Korn Shell-Umgebung (ksh), zur Verfügung gestellt.
- ▶ Die für die Remote-Verwaltung und den Remote-Zugriff erforderlichen Telnet-Dienste werden bereits standardmäßig von Windows 2000/2003 geliefert. Sie sind aber auch in den Unix-Services enthalten.
- ▶ Auch die Kennwortsynchronisierung zwischen Unix und Windows wird über die Unix-Services unterstützt. Es ist eine gemeinsame Verwaltung von Passwörtern möglich, da die Windows-SAM und die Unix-Kontendatenbank *passwd/shadow passwd* synchronisiert werden können. Wenn die Namen der Benutzerkonten auf beiden Systemen gleich sind, übermittelt Windows 2000 Änderungen an den Kennwörtern automatisch an die Unix-Computer.
- ▶ Auch die Network Information Services (NIS) werden unterstützt. NIS ist der von der Firma SUN vertriebene Verzeichnisdienst.

Eines der neuen Features unter Windows 2000 ist die Authentifizierung über Kerberos-Tickets. Diese Methode ist unter Unix schon lange verbreitet und damit auch sehr ausgereift und stabil. Sie haben die Möglichkeit, bestehende Kerberos-Server unter Unix ins Active Directory zu integrieren. Andererseits kann auch Windows 2000 für die Ausgabe der Kerberos-Tickets verantwortlich sein, die von Unix durch Implementierung von Kerberos verwendet werden können.

Der Hauptunterschied zwischen SFU 2.0 und 3.0 liegt darin, dass nun Microsoft Interix vollständig in die Services integriert ist. Die Subsystem-Technologie von Interix beschert eine universelle Umgebung, in der Windows- und Unix-Applikationen auf einem System laufen können. Das Unix-Environment läuft auf dem Windows-Kernel. Somit ist es Applikationen und Skripten unter Unix möglich, zusammen mit Windows-Applikationen nativ unter dem Windows-Betriebssystem zu laufen.

Eine ausführlichere Beschreibung der Koexistenz zwischen Unix/Linux und dem Active Directory finden Sie in Kapitel 29.

3.8.3 Microsoft BackOffice-Server und Active Directory

Microsoft wird auch die stärkere Integration seiner BackOffice-Programme ins Active Directory vorantreiben. Diese Anwendungen sollen Active Directory als ihren primären Speicher verwenden. Bei Microsoft Exchange 2000/2003 ist dieser Schritt bereits vollzogen. Es gibt kein separates Exchange-Verzeichnis mehr. Alle Informationen werden direkt im Active Directory gespeichert.

Vergleichbar mit den eben beschriebenen ADSI-Clients für Windows 9x und NT gibt es auch für die – zumindest vorübergehend – weitere Nutzung von Exchange 5.5 eine Lösung. Diese heißt Active Directory-Connector (ADC). Hierbei handelt es sich um einen Dienst, der die Daten zwischen dem alten Exchange-Verzeichnis und Active Directory austauscht. Damit ist sichergestellt, dass beide Datenspeicher immer auf demselben Stand sind und somit die Exchange 2000- wie auch 4.0- oder 5.x-Clients in ihrer jeweiligen Datenbank dieselben Informationen vorfinden. Deshalb wird auch das von den Exchange-Clients der Versionen 4.0 und 5.x verwendete NSPI-Protokoll von Active Directory unterstützt.

3.8.4 Grundlagen der Verzeichnisdienstzusammenarbeit

Bevor im nächsten Kapitel auf die Zusammenarbeit zwischen Active Directory und Novells NDS eingegangen wird, sollen Sie zunächst als Grundlage wissen, welche Schwierigkeiten bei der Zusammenarbeit mit anderen Verzeichnisdiensten auftreten können und welche Lösungen von Active Directory dafür bereitgestellt werden.

In vielen Unternehmen werden Daten in verschiedenen Verzeichnissen gepflegt. Mit der Entwicklung von Active Directory wurde versucht, alle Objekte in einem einzigen Verzeichnis zu speichern. Damit wird ein geringerer Verwaltungsaufwand nötig und der Zugriff auf die Daten verbessert. Dafür wurden aber auch Anforderungen an den neuen Verzeichnisdienst gestellt. So muss Active Directory erweiterbar sein, um die Daten beliebiger Anwendungen aufnehmen zu können. Zusätzlich muss sowohl die Migration alter Daten als auch die Zusammenarbeit mit neuen Verzeichnissen möglich sein.

Ein Problem liegt vor, wenn die Daten in zwei verschiedenen Verzeichnissen zwar dieselben sind, aber in beiden Verzeichnissen in einer verschiedenen Struktur angelegt und gespeichert sind. Sie müssen sich in diesem Fall überlegen, welche Hierarchie Sie für die Zuordnungen benutzen möchten. Auch auf die Integrität der Daten muss ein Blick geworfen werden. Wird ein Objekt aus dem Verzeichnis gelöscht, muss es komplett aus dem Verzeichnisdienst entfernt werden. Weiterhin muss auch die referenzielle Integrität zwischen Objekten und deren zugehörigen Attributen gewährleistet sein. Wenn Sie ein Attribut ändern, muss das dazugehörige Objekt auch in anderen Verzeichnissen aktualisiert werden. In diesem Zusammenhang muss auch der Besitz von Objekten angesprochen werden. Wenn sich ein Objekt in zwei Verzeichnissen befindet und beide Verzeichnisse meinen, der Besitzer des Objekts zu sein, und dies ändern, sind Konflikte vorprogrammiert. Auch wenn Objektattribute ausschließlich von der besitzenden Applikation geändert werden sollen, darf nicht zusätzlich noch das Verzeichnis, in dem sich das Objekt befindet, Änderungen durchführen.

Durch die Standardisierung der Verzeichnisdienste kann über ADSI (Active Directory Service Interfaces) oder COM-(Component Object Model-)Komponenten die Verwaltung von Objekten in mehreren verschiedenen Verzeichnissen vereinfacht werden. ADSI kann als Schnittstelle zwischen Active Directory, Novell Directory Service (NDS), anderen LDAP-konformen Verzeichnisdiensten und Windows NT eingesetzt werden. Über die gemeinsam genutzten APIs können Sie selbst Programme oder Skripte schreiben, mit denen Sie mehrere Verzeichnisdienste parallel administrieren können.

Zur Synchronisation des Active Directory wird die Multimaster-Replikation durchgeführt. Dabei wird eine Verbindung zwischen dem Quell- und Zielsystem aufgebaut, ermittelt, welche geänderten Daten übertragen werden müssen, und diese werden schließlich auf den Zielsystem kopiert. Dieser komplette Prozess wird auch als Verbinder (Connector) bezeichnet. Ein Verbinder kann auch verzeichnisübergreifend Daten austauschen. Er ist in der Lage, zeitgesteuert zu arbeiten. Sollen die Daten an einen anderen Verzeichnisdienst übertragen werden, so weiß er auch, wie dort die Objektklassen hierarchisch angeordnet sind und wie er demnach die Objekte in das andere Verzeichnis einpflegen muss. Das Senden der Replikationsdaten geschieht immer nur in eine Richtung. Somit arbeitet ein Verbinder unidirektional. Es gibt aber auch bidirektionale Verbindungen. Ein bidirektionaler Verbinder ist eine Kombination aus zwei unidirektionalen Verbindungen. Dieser doppelte Verbinder wird benutzt, wenn Sie noch zwei Verzeichnisse im Einsatz haben, wobei ausschließlich am aktuellen Änderungen vorgenommen werden und das alte Verzeichnis nach Abschluss der Migration endgültig gelöscht werden kann. Dabei ist das neue Verzeichnis die Quelle, in der Sie beispielsweise neue Attribute anlegen. Aus dem alten Verzeichnis, dem Ziel, werden bestehende Einstellungen und Informationen in das neue Verzeichnis übertragen, und gleichzeitig werden die Änderungen am neuen Verzeichnis an das alte übertragen, damit die Clients des alten Verzeichnisses ebenfalls auf aktuelle Informationen zugreifen können. Ein Datentransfer findet also in beide Richtungen statt.

Diese Verbindertechnologien wurden von Microsoft als ein allgemeiner DirSync-Connector und ein spezieller bidirektionaler NDS DirSync-Connector für NDS entwickelt. Weitere Informationen zu NDS finden Sie im folgenden Kapitel.

Microsoft verfolgt selbstverständlich das Ziel, Active Directory als den Verzeichnisstandard zu etablieren. Da Active Directory als erster Verzeichnisdienst völlig konform mit LDAP in der Version 3.0 ist und zahlreiche Verbindungen zu anderen Verzeichnisdiensten entwickelt wurden und weiterentwickelt werden, stehen die Chancen nicht schlecht. Ein schlagendes Argument für den Einsatz nur eines Verzeichnisses ist, dass die Synchronisation zweier Verzeichnisse und alle damit verbundenen Schwierigkeiten und Probleme entfallen.

3.8.5 Novell Directory Services (NDS)

Wichtig für Active Directory ist die Interoperabilität mit Novells NDS. Da Novell als erster Hersteller einen Verzeichnisdienst herausbrachte, ist dieser entsprechend weit verbreitet. Deshalb sollte auch die Synchronisierung zwischen Active Directory und NDS möglich sein, damit beide Verzeichnisdienste parallel eingesetzt werden können.

In den „Services for NetWare 5“ von Microsoft befinden sich die Microsoft Directory Synchronization Services (MSDSS). Diese ermöglichen eine bidirektionale Synchronisierung zwischen Active Directory und NDS. Damit wird der Verwaltungsaufwand gesenkt, da Sie nur noch ein Verzeichnis zu verwalten haben. Haben Sie bereits ein umfangreiches NDS implementiert, so kann Active Directory die bestehende Umgebung nutzen. MSDSS unterstützt alle NDS-Versionen (NDS auf NetWare 4.0, 4.1, 4.11, 4.2, 5.0 und 5.1) sowie zahlreiche Bindery-Versionen (NetWare 3.1, 3.11, 3.12, 3.2 sowie im Bindery-Emulationsmodus konfiguriertes NetWare 4.x). Dabei ist es auch gleichgültig, ob Sie als Standardprotokoll TCP/IP oder IPX/SPX einsetzen. Der Zugriff auf die MSDSS ist zunächst auf die lokale Sicherheitsgruppe „MSDSS-Admins“ beschränkt. Damit wird unautorisierter Zugriff verhindert.

Mit MSDSS können beide Verzeichnisse von einem zentralen Verwaltungspunkt aus administriert werden. Sämtliche Änderungen, die Sie am Active Directory vornehmen, werden an NDS übertragen. Über beide Verzeichnisse hin ist durch die Synchronisierung die Integrität der Daten sichergestellt. Wenn Sie an einem der beiden Verzeichnisse beispielsweise das Passwort eines Benutzers ändern, wird diese Änderung fast in Echtzeit an das andere Verzeichnis repliziert. Zur Kontrolle stehen Überwachungs- und Eventlog-Programme zur Verfügung. Ebenfalls werden nun Passwörter synchronisiert, was einen entscheidenden Schritt auf dem Weg zum Single Sign-on-Verfahren darstellt. Wenn Sie die Passwörter zentral im Active Directory festlegen, werden diese Passwörter an NDS übergeben. Ein Benutzer kann sich also mit demselben Benutzernamen und Passwort sowohl an Active Directory als auch an NDS anmelden.

Wenn Sie bereits eine NDS-Umgebung implementiert haben, müssen Sie diese meistens nicht ändern, da MSDSS auch die Schemaerweiterungen (sofern sie ein Äquivalent in Active Directory haben) in NDS an Active Directory übertragen kann. Die NDS-Struktur kann komplett repliziert und in Windows 2000 importiert werden. Damit ist eine enorme Zeiteinsparung sichergestellt, da Sie nicht alle Informationen manuell neu unter Windows 2000 erstellen müssen. Sie haben ferner die Möglichkeit, Ihr bestehendes NDS komplett in Active Directory zu migrieren. Damit besteht nicht mehr die Notwendigkeit, zwei Verzeichnisse parallel zu betreiben. Hierzu bietet Ihnen MSDSS einen eigenen Migrations-Wizard an. Auch die Unterstützung verschiedener Hierarchiestrukturen ist gewährleistet. Jedes Objekt mit einem anderen Namensraum in jedem Verzeichnis kann synchronisiert werden, indem die Objektklassen und Attributtypen in statischen Zuweisungstabellen gespeichert werden. Die Synchronisierung zwischen beiden Verzeichnissen vollzieht sich also auf dem Objekt-Level.

MSDSS bietet eine simple Handhabung. Sie benötigen einen Windows 2000-Domänencontroller mit einem Client für NetWare. Die Synchronisationseinstellungen können Sie in einem fünfstufigen Wizard einstellen. Nach maximal einer Viertelstunde können Sie die erste Synchronisierung durchführen. Ein einzelner Windows 2000-Domänencontroller kann 50 gleichzeitige Synchronisationssitzungen verarbeiten. Für die Verwaltungsaufgaben wird eine neue Microsoft Management Console installiert. Damit können Sie gleichzeitig das Active Directory und NDS betrachten.

Auch das Replikationsintervall zwischen beiden Verzeichnissen kann vom Administrator frei festgelegt werden. Die Replikation kann automatisch und manuell erfolgen.

Da Novell NetWare auch Clients für beispielsweise Mac OS-Betriebssysteme anbietet, wird es ermöglicht, auch diese ins Windows Active Directory zu integrieren. Diese Lösung erfordert zwar einigen Aufwand an Konfiguration, es ist aber die einzige Möglichkeit, Mac OS-Clients in einer Windows 2000 Active Directory-Domäne zu betreiben.

3.8.6 Features von ADSI

Dieses Kapitel zeigt Ihnen kurz einige der wichtigsten Features von ADSI (Active Directory Services Interface). ADSI bietet Ihnen eine Schnittstelle für eigene Anwendungen in zahlreichen Betriebssystemen zum Zugriff auf verschiedene Verzeichnisdienste.

- ▶ ADSI ermöglicht Ihnen einen leichten Zugang zu Verzeichnisdiensten über das Component Object Model (COM). Die Applikationen sind an keine bestimmte Programmiersprache gebunden und können z.B. in Visual Basic, C/C++ oder Java geschrieben werden.
- ▶ ADSI arbeitet verzeichnisdienstunabhängig. Sie können Applikationen entwickeln, ohne die verschiedenen anbieterspezifischen Verzeichnis-APIs kennen zu müssen. Gerade administrative Applikationen sind nicht fest an einen bestimmten Verzeichnisdienst gebunden.
- ▶ Sie können jede beliebige automatisierungskompatible Skriptsprache (z.B. VBScript, REXX oder Perl) benutzen, um Applikationen für den Verzeichnisdienst zu entwickeln.
- ▶ ADSI kann von Verzeichnisdienst Anbietern, Softwareentwicklern und Administratoren durch das Hinzufügen neuer Objekte und Funktionen erweitert werden. Dies ist wichtig, wenn Ihr Verzeichnis sehr spezielle Bedingungen erfüllen muss.
- ▶ ADSI bietet ein OLE-Datenbank-Interface, sodass auch Datenbankprogrammierer rasch über dieses Interface produktiv arbeiten können.

Ausführlich wird das Thema ADSI und ADSI-Skripte in Kapitel 32 abgehandelt.

Teil B – Konzeption

Über diesen Teil

Dieser Teil des Buches betrachtet die Thematik Active Directory aus dem Winkel des Projektmanagements. Eine gründliche Planung der Active Directory-Implementierung ist die Grundlage für einen später reibungslosen Betrieb. Es werden Ihnen hier Methoden und Verfahren vorgestellt, die für die Planungs-, Implementierungs- und Testphase eines Active Directory notwendig sind. Auch selbst dann, wenn in Ihrem Unternehmen bereits Active Directory eingesetzt wird, können Sie hier Anhaltspunkte finden, wie Sie durch Anpassungen oder kleine Veränderungen eine höhere Effizienz und Leistung erzielen können.

In diesem Teil erhalten Sie umfangreiche Anleitungen in Form von Checklisten und Fragestellungen. Diese erstrecken sich von der Gliederung des Gesamtprojekts und vom Festlegen der einzelnen Projektschritte über die Zieldefinition des Projekts bis hin zum Design der Umgebung, dem Aufbau einer Testumgebung sowie dem abschließenden Rollout.

Dieser Teil setzt nur in geringem Maße ein technisches Verständnis von Active Directory und den Windows-Betriebssystemen an sich voraus, da der Schwerpunkt auf den Bereich Projektmanagement sowie die betriebswirtschaftliche Sicht ausgerichtet ist. An den Stellen, an denen es nötig erscheint, wird auf geeignete Quellen verwiesen, aus denen das notwendige technische Wissen bezogen werden kann.

4 Planung der Active Directory-Migration

Die Einführung von Active Directory in einem Unternehmen ist nicht nur eine simple Erweiterung des bestehenden Netzwerks, sondern ein tief greifender Einschnitt in die vorhandene IT-Infrastruktur. Die Gründe für einen solchen Eingriff wie die Einführung von Active Directory müssen der Geschäftsleitung deshalb zunächst plausibel erklärt werden, da das Projekt anfänglich einen großen Zeit- und höchstwahrscheinlich auch Kostenaufwand erfordert. Die Vision des Projektziels könnte lauten: Die Verwaltung aller Benutzer, Computer, Programme und Daten geschieht zentral, wobei die Desktops der internen und externen Benutzer mit einer Mixtur aus selbst geschriebener und gekaufter Software versorgt werden. Die Minimierung von Verwaltungskosten und dafür gleichzeitig eine bessere und effektivere Nutzbarkeit und Konsistenz der Unternehmensinformationen sind erste gute Argumente, um Vorstände für das Thema Active Directory-Implementierung zu sensibilisieren.

Eine weitere Effektivitätssteigerung liegt darin, dass es bisher oftmals doppelte Arbeit für die Administratoren gegeben hat, die identische Daten an mehreren Orten pflegen müssen, z.B. im E-Mail-Verzeichnis, in der Personaldatenbank usw. Außerdem werfen Sie einmal einen kritischen Blick in Ihr Unternehmen: Für wie viele Daten werden noch Zettel und Listen geführt: Telefonlisten für die Mitarbeiter, Hardware- und Softwareinventarlisten für die Administratoren usw. Diese Papiere aktualisieren sich nicht von selbst, sondern müssen bei jeder Änderung neu geschrieben und ausgeteilt werden. Im Active Directory genügt ein Blick in eine einzige Verzeichnisdatenbank, und Sie finden immer die aktuelle Information.

Vor Beginn der Migrationsplanung müssen Sie sich selbstverständlich umfassende Kenntnisse über Windows 2000/2003 und Active Directory angeeignet haben, um entscheiden zu können, ob und wie Ihre Ziele im Active Directory umgesetzt werden können. Wenn Sie erst während der Planung Ihre Kenntnisse erwerben, wird die Planungsphase nur unnötig in die Länge gezogen, Sie können nicht erkennen, ob Ihre Planung korrekt ist, und bei Umsetzung der mangelhaften Planung werden Sie später so einige negative, mit weiteren Kosten verbundene Auswirkungen feststellen. Nutzen Sie die Zeit, um sich in Schulungen über Active Directory zu informieren. Je mehr Detailinformationen Sie besitzen, umso einfacher dürfte es werden, Überzeugungsarbeit für die Implementierung von Active Directory zu leisten.

4.1 Die Phasen der Migration und deren Milestones

Die Migration einer bestehenden Umgebung auf Windows 2000 Active Directory ist ein tiefer Schnitt und verlangt daher eine gründliche Vorlaufphase, bevor Sie endgültig Active Directory in Ihrem Unternehmen einsetzen. Der gesamte Migrationsprozess lässt sich in vier große Abschnitte einteilen. Diese Abschnitte sind:

- ▶ Planungsphase
- ▶ Designphase
- ▶ Testphase
- ▶ Rollout

Die bedeutendste dieser Phasen ist die Designphase. In ihr wird das Active Directory entworfen, wobei die während der Planungsphase gewonnenen Erkenntnisse eingebracht werden. Dieser Entwurf muss später bei der Implementierung den Anforderungen des Unternehmens entsprechen. Andernfalls kann das Projekt als fehlerhaft, wenn nicht sogar gescheitert betrachtet werden. Ebenso wichtig ist auch der Migrations- und Implementierungsplan, der ebenfalls in dieser Phase ausgearbeitet wird. Selbst ein noch so gut entworfenes Active Directory nützt Ihrem Unternehmen gar nichts, wenn es nur betriebsstörend oder terminverzögert implementiert werden kann.

In diesem Kapitel werden Ihnen allgemeine Aufgaben dieser vier Migrationsphasen vorgestellt. In den folgenden vier Kapiteln werden die spezifischen Planungsphasen aufgegriffen und anhand von Checkpunkten und To-do-Listen präzisiert.

Für die Planungs-, Design- und Testphase vor der eigentlichen Migration sollte nicht am Faktor Zeit gespart werden. Je gründlicher Sie Planung, Design und Tests betreiben, desto mehr Zeit haben Sie, um auf unvorhergesehene Probleme oder Fehler aufmerksam zu werden und diese zu beseitigen, bevor Sie später in der produktiven Umgebung akut werden können. Das Sparen von Zeit – und damit auch Kosten – in Planung, Design und Test kann sich später rächen, wenn Sie in der produktiven Umgebung durch die Investition von möglicherweise noch mehr Zeit und Kosten die Fehler ausmerzen müssen.

Das folgende Schaubild gibt Ihnen einen Überblick über die verschiedenen Arbeitsschritte, die in jeder dieser Phasen zu erledigen sind, sowie die Abschnitte, die parallel oder Phasen übergreifend ablaufen können bzw. die zunächst abgeschlossen sein müssen, bevor mit dem nächsten Schritt begonnen werden darf. Jeder aufgezeichnete Arbeitsschritt entspricht einem Milestone im Projektfortschritt.

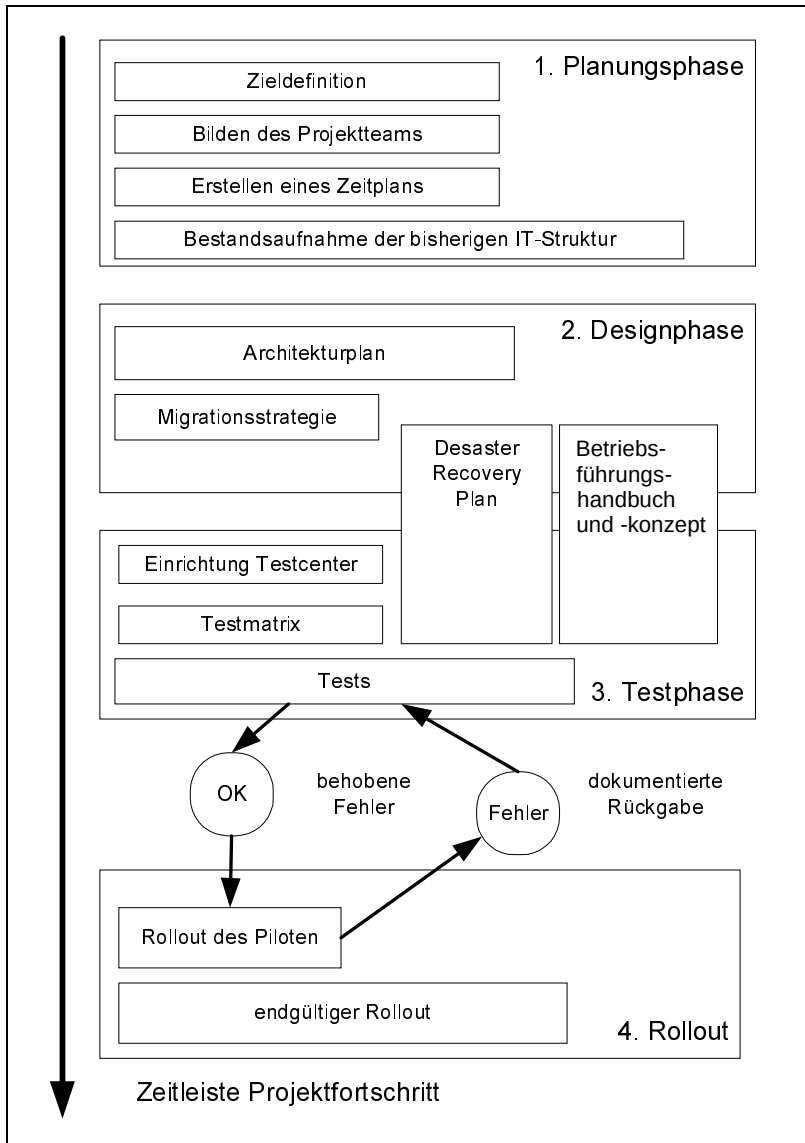


Abbildung 4.1: Die Migrationsphasen im Überblick

4.1.1 Die Planungsphase

In der Planungsphase werden zunächst die Ziele definiert, die mit dem Migrationsprojekt Active Directory in Ihrem Unternehmen erreicht werden sollen. Diese Ziele können je nach Unternehmen auch sehr spezifischer Natur sein. Für jedes dieser Ziele muss anfänglich geklärt werden, ob es sich durch die Implementierung von Active Directory verwirklichen lässt oder nicht.

Nachdem die Ziele definiert worden sind, müssen Sie das Projektteam benennen. Von der Implementierung von Active Directory sind viele Einzeldisziplinen betroffen, wie z.B. das Netzwerk, DNS, Clients, Server usw. Die für diese Bereiche verantwortlichen Personen sind bei der Migration für die Durchsetzung ihrer Interessen in ihren Teilbereichen verantwortlich. Ermitteln Sie auch, inwieweit Schulungen für die Mitglieder des Projektteams erforderlich sind, um die Neuerungen von Windows 2000/2003/XP kennen zu lernen.

Sobald das Projektteam benannt ist, muss ein Zeitplan für die Migration erstellt werden. Definieren Sie Eckpunkte und deren Erfüllungskriterien, anhand derer ein Projektpunkt als erledigt gilt. Sollte in Ihrem Unternehmen noch kein standardisiertes Verfahren für die Umsetzung von Projekten vorhanden sein, so sollten Sie nun ein allgemein gültiges Verfahren eines Projektmanagement-Plans einführen. In diesem Plan werden alle weiteren Schritte der folgenden Phasen festgehalten.

Als Letztes müssen Sie in der Planungsphase eine Bestandsaufnahme Ihrer bisherigen IT-Struktur im Unternehmen durchführen. Zur Bestandsaufnahme gehören beispielsweise die Standorte der Organisation, die bisherige Hardware-Landschaft, Netzwerktechnisches, Benutzerbezogenes und Applikationsbezogenes.

4.1.2 Die Designphase

In der Designphase wird zunächst ein Architekturplan für die Active Directory-Implementierung entworfen. In diesem Plan werden die Konzepte für alle Bereiche festgelegt, die von Active Directory tangiert werden. Hierzu zählen etwa die Struktur der Domänen, Standorte, OUs und der DNS-Namensraum usw.

Nach der Entwicklung eines Architekturplans ist als Nächstes eine Migrationsstrategie zu empfehlen und zu dokumentieren. Da in vielen Unternehmen nicht die gesamte Migration mit einem Schlag durchgeführt werden kann und wird, müssen Sie Pläne für die Koexistenz von verschiedenen Betriebssystemen erstellen. Möglicherweise wird auch das Endziel eine Koexistenz von beispielsweise Active Directory und Novells NDS oder Unix sein. Auch in einer reinen Windows-Umgebung kann eine vorübergehende oder auch dauerhafte Zusammenarbeit von Windows 2000/2003/XP und Windows NT erforderlich sein. Auch für diesen Fall müssen Sie entscheiden, ob und wann welche Domänencontroller aktualisiert werden. Auch die Entscheidung, ob zuerst die Clients oder die Server aktualisiert werden sollen, ist nun zu fällen.

Weiterhin müssen Sie einen Disaster Recovery-Plan erstellen. Bei einem so komplexen Vorgang wie der Migration auf Active Directory müssen Sie immer damit rechnen, dass unvorhergesehene Probleme auftreten. Für diesen Fall müssen Sie jedoch eine Strategie entwickelt haben, um möglichst rasch den Status quo wiederherzustellen, damit der laufende Betrieb nicht durch Fehler beeinträchtigt oder sogar völlig unmöglich wird. Dieser Disaster Recovery-Plan muss spätestens dann fertig gestellt sein, wenn es an den Rollout am Piloten geht. Während der Testphase können noch Erkenntnisse in diesen Plan einfließen. Beim endgültigen Rollout muss der Disaster Recovery-Plan feststehen und idealerweise in der Testumgebung bereits erprobt sein.

Zusätzlich sollten in jedem Unternehmen zwei Dokumentationen erstellt werden. Dabei handelt es sich um das Betriebsführungskonzept und -handbuch. Im Konzept werden die Erfordernisse für die Implementierung sowie die endgültige Architektur des Active Directory dokumentiert. Das Betriebsführungshandbuch ist eine praktische Anleitung mit allen Arbeitsschritten, die für den täglichen Betrieb des Active Directory notwendig sind. Diese Dokumentation dient als Nachschlagewerk für die Administratoren. Die beiden Dokumentationen müssen fertig gestellt sein, bevor der Rollout am Piloten beginnt. Die Implementierung und der tägliche Betrieb werden anhand der beiden Dokumentationen durchgeführt. Nur wenn sich dabei die Dokumentation als unzureichend erweist, ist eine Überarbeitung notwendig.

4.1.3 Die Testphase

Als Grundlage für die Testphase müssen Sie zunächst ein Testcenter einrichten. Das Design des Testcenters ergibt sich aus dem Hardwarebestand und der vorhandenen Netzwerkumgebung des Unternehmens. Diese Umgebung muss möglichst detailgetreu abgebildet werden, um eine große Anzahl an verschiedenen Szenarien testen zu können.

Während das Testcenter eingerichtet wird, müssen Sie parallel festlegen, welche Prozesse, Vorgänge und Arbeitsschritte dort getestet werden sollen.

Zur Durchführung der Tests sollten Sie sich dann eine Testmatrix erstellen. Hier legen Sie die Kriterien fest, die geprüft werden müssen, die Erfüllungskriterien für einen Test, das Ergebnis des Tests und eine Bewertung. Bewertungen können in mehrere Kategorien eingeteilt werden, je nachdem, wie weit Ihr Testergebnis von den Erfüllungskriterien entfernt ist oder diese erfüllt. Sämtliche Testergebnisse sind dort zu dokumentieren, sodass auch wechselseitige Beziehungen und Auswirkungen von Anpassungen leichter nachzuvollziehen sind. Erst wenn alle Testergebnisse den Erfüllungskriterien entsprechen, können Sie die Testphase abschließen und zum Rollout des Piloten übergehen.

Die Testphase ist mit dem Rollout des Piloten noch relativ eng verzahnt. Sobald dort Probleme auftreten, werden diese an das Testcenter zurückgegeben und dort ausgewertet. Erst wenn schwerwiegende Fehler dort vollständig behoben sind, können die Modifikationen an den Piloten weitergereicht werden.

Das eingerichtete Testcenter bleibt auch nach der endgültigen Implementierung von Active Directory bestehen. Wenn später entscheidende Änderungen am Active Directory erforderlich werden, müssen auch dann erst alle geplanten Schritte hier ausführlich getestet werden.

4.1.4 Der Rollout

Die Rolloutphase gliedert sich in zwei Abschnitte: den Rollout eines Piloten und den endgültigen Rollout auf alle Bereiche, in denen Active Directory implementiert werden soll. Der Rollout des Piloten ist im Prinzip nichts weiter als eine verlängerte Testphase, in der einerseits grobe Probleme ausgemerzt sein sollten, sich andererseits aber die Chance bietet, unter realeren Bedingungen als im Testcenter auf Schwierigkeiten zu stoßen. Am Piloten lassen sich auch Erkenntnisse darüber gewinnen, inwieweit der Architekturplan fürs Active Directory sich in einer realen Umgebung umsetzen lässt. Möglicherweise

werden auch noch Verbesserungen, die an der Migrationsstrategie vorzunehmen sind, offenkundig, sodass die Verteilung im gesamten Unternehmen noch effizienter und besser ablaufen kann.

Die am Pilotprojekt mitwirkenden Personen werden deshalb eng mit dem Team des Testcenters zusammenarbeiten. Jeder Fehler, der beim Piloten auftritt, sollte im Testcenter nachgestellt und behoben werden. Dies gilt auch für konzeptionelle Nachbesserungen.

Zusätzlich können in der Pilotphase auch Erkenntnisse über nicht unmittelbar mit Active Directory zusammenhängende Vorgänge gewonnen werden. Dazu zählen etwa Systematiken und Informationen für den technischen Support oder auch den Bereich Netzwerk.

Die Pilotphase kann als abgeschlossen betrachtet werden, wenn dort für einen vorher bestimmten Zeitraum Active Directory problemlos funktioniert. Dabei ist es gleichgültig, ob das Projektziel die Koexistenz mit einem anderen Netzwerkbetriebssystem oder ein reines Active Directory lautet. Nach Abschluss der Pilotphase kann dann der endgültige Rollout beginnen. Dieser gleicht prinzipiell dem Rollout des Piloten, nur mit dem Unterschied, dass die Implementierung nun im breiteren Rahmen durchgeführt wird. Damit zeigt sich dann, ob der Architektur- und Implementierungsplan erfolgreich umgesetzt werden konnten. Mit der erfolgreichen Implementierung ist das Migrationsprojekt beendet.

Während des endgültigen Rollouts oder auch im produktiven Betrieb werden sich sicherlich immer noch kleinere Nachkorrekturen ergeben, die sich erst dann als Problem erwiesen haben, aber nicht unternehmenskritisch sind. Weiterhin sollte sich das Active Directory als so flexibel erweisen, dass es auf eine Vergrößerung oder andere betriebswirtschaftliche Veränderungen im Unternehmen reagieren kann.

4.2 Ausblicke und Möglichkeiten

Die Implementierung von Active Directory bietet neben der Vereinfachung der Administration, höheren Verfügbarkeit und besseren Handhabung für die Benutzer auch weitere Ausblicke und Möglichkeiten. Hierzu zählen die Verwirklichung einer Single Sign-on- und Single Point of Access-Strategie oder die Einführung eines Asset-Managements, auch die Übernahme bestehender Datenbestände der Windows NT-Domänen sowie auch weiterer Informationen wie z.B. Personalstammdaten aus SQL-Datenbanken.

4.2.1 Single Sign-on- und Single Point of Access-Strategie

Active Directory ist idealerweise der zentrale und einzige Anmeldepunkt für alle Ressourcen des Netzwerks. Hierzu zählen beispielsweise Drucker oder freigegebene Verzeichnisse, aber auch Applikationen im Client-Server-Umfeld. Neben der zentralen Anmeldestelle für Ressourcen kann Active Directory also auch der zentrale Zugriffspunkt für sämtliche Anwendungen sein. Ein einziges Kennwort kann applikations- und plattformübergreifend eingesetzt werden (Single Sign-on). Meldet man sich darüber hinaus an einem Server in seinem LAN an, kann man je nach Definition der Zugriffsrechte auch auf Ressourcen außerhalb dieses lokalen Umfeldes (z.B. Datenbanken) zugreifen (Single Point of Access).

So kann es mit einer einzigen Anmeldung am Active Directory möglich werden, auch auf andere Anwendungen oder Datenbanken usw. zuzugreifen, für die bisher eine gesonderte Authentifizierung nötig ist. Wahrscheinlich verwendet jeder Benutzer separate Kennwörter zur lokalen Anwendung, für das Versenden von E-Mails oder für den Zugriff auf Druck- und Dateiserver. Wahrscheinlich erfordern die verschiedenen Server auch eine regelmäßige Änderung des Kennworts. So ist der Benutzer gezwungen, sich stets eine Reihe von Passwörtern merken zu müssen. Höchstwahrscheinlich wird dabei ein Teil der Benutzer zur Bequemlichkeit neigen und seine Passwörter sauberlich auf einem Zettel oder in einer Datei notieren. Damit ist der Zugriff auf das Netzwerk durch unbefugte Personen jederzeit möglich. Es ist also für den Benutzer wesentlich komfortabler, sich nur ein einziges Kennwort merken zu müssen, mit dem er Zugriff auf alle benötigten Programme und Ressourcen gemäß seiner Rollendefinition erhält. Weiterhin wird durch die Benutzung nur eines Kennwortes auch der Helpdesk entscheidend entlastet. Bei bis zu 2/3 aller Anfragen handelt es sich um vergessene Passwörter, die dann vom Helpdesk zurückgesetzt werden müssen. Auch die effektive Arbeitszeit der Mitarbeiter kann erhöht werden. Ein Benutzer, der nur drei verschiedene Anwendungen mit unterschiedlichen Passwörtern startet, benötigt im Jahr bis zu 33 Stunden nur für die Logins. Diese Zeit ist aber für das Unternehmen unproduktiv.

Die eingesetzten Anwendungen können so modifiziert werden, dass keine separate Authentifizierung für die Applikation notwendig ist. Selbstverständlich ist diese Modifikation nicht bei allen Applikationen möglich. Aber im Rahmen Ihrer Bestandsaufnahme zu vorhandener Software sollten Sie ermitteln, welche Applikationen ins Active Directory integrierbar sind oder welche möglicherweise durch andere Produkte ersetzt werden könnten.

Ein Active Directory, auf das von den Applikationen direkt zugegriffen werden kann, ist ein wichtiger Bestandteil in der Verzeichnis-Infrastruktur. Das Verzeichnis bietet eine einzelne logische, transparente Übersicht über Benutzer, Ressourcen und alle weiteren Objekte. Damit ist das Active Directory ein Ganzes, in das verschiedene Bestandteile integriert sind. Es ist nicht mehr eine Ansammlung von diversen unabhängigen Teilen. In dieses Ganze können neben den Objekten auch Applikationen integriert werden. Diese Directory-enabled Applikationen verbessern so seine Funktionalität und Administration und erleichtern zugleich die Benutzung. Nehmen Sie dazu den folgenden Fall an: Es soll ein Meeting in einem Raum einberufen werden, der von Größe und Ausstattung her bestimmte Anforderungen erfüllen muss. Außerdem müssen die Teilnehmer dieses Meetings über Ort und Zeit informiert werden. In den meisten Fällen werden Sie in einer separaten Applikation – wenn nicht sogar nur in einer Liste oder über eine telefonische Auskunft – erfragen müssen, welcher Raum den Anforderungen entspricht und ob dieser Raum zum gewünschten Zeitpunkt verfügbar ist. Sobald Sie den Raum bestimmt haben, müssen Sie über eine E-Mail-Applikation den Teilnehmern die Einladung für das Meeting verschicken. Bei der Integration geeigneter Anwendungen oder bei selbst entwickelten Applikationen würden Sie einen Blick ins Directory werfen und daraus die benötigten Informationen über den Konferenzraum wie Größe, Ausstattung oder Lage erfahren. Zusätzlich kann die Funktion erweitert werden, indem für die Räume angegeben wird, wann diese belegt oder frei sind. Der Benutzer kann also eine Liste aller Räume erhalten, die seinen Anforderungen entsprechen. Mit wenigen weiteren Mausklicks

wählen Sie dann die Personen aus, die eine Einladung zum Meeting erhalten sollen. Für jede Person haben Sie auf einen Blick die persönlichen Daten wie E-Mail-Adresse, Telefonnummer oder Handynummer.

In diversen Unternehmen werden als Ansatz der Verzeichnisdiensteinführung mehrere parallele Directories betrieben, so etwa ein Verzeichnis für das E-Mail-System, ein zweites für Datenbanken und weitere für andere Groupware-Applikationen. Durch die Einführung eines zentralen Directorys verbessern Sie die Benutzerfreundlichkeit, senken Entwicklungs- und Supportkosten und verbessern die Datenkonsistenz. Mit ADSI-Skripten (Active Directory Service Interfaces) steht den Administratoren unter Active Directory ein mächtiges Werkzeug zur Automatisierung von Verwaltungsaufgaben zur Verfügung. Auch die Software von Drittanbietern verwendet verstärkt ADSI, um diese für Verzeichnisdienste nutzbar zu machen. Da ADSI nicht an einen bestimmten Verzeichnisdienst gebunden ist, können diese Applikationen in verschiedenen Netzwerk- und Verzeichnisdienstumgebungen eingesetzt werden.

Active Directory beruht auf standardisierten Ansätzen wie Erweiterbarkeit auf verschiedene Typen von Daten, Skalierbarkeit, geringem Ressourcenverbrauch, hohe Sicherheit und Zugriff über eine Standard-API. Alle diese Funktionalitäten werden mit dem Standardzugriffsprotokoll LDAP bereitgestellt. Somit ist LDAP neben HTTP und FTP ein unverzichtbarer Bestandteil der Internetprotokoll-Suite.

4.2.2 Datenübernahme aus Datenbanken und Verzeichnissen – Metadirectories

Ein Ziel sollte darin bestehen, bereits vorhandene Unternehmens-Stammdaten aus den Windows NT-Kontendatenbanken ins Active Directory zu übernehmen. In kaum einem Unternehmen ist es möglich, diese Daten alle nach der Migration neu zu erstellen. Das selbe gilt auch für weitere Ressourcen wie Drucker oder freigegebene Ordner. Ein sehr hilfreiches Werkzeug dazu ist das Active Directory Migration Tool (ADMT) von Microsoft. Mit ADMT haben Sie die Möglichkeit, bestehende Windows NT-Domänenendaten ins Active Directory zu integrieren. Das Programm besteht aus diversen Wizards, mit denen Sie z.B. folgende Aufgaben durchführen können:

- ▶ Migration von Kontendomänen zwischen Gesamtstrukturen
- ▶ Migration von Ressourcendomänen zwischen Gesamtstrukturen
- ▶ Migration von Kontendomänen innerhalb einer Gesamtstruktur
- ▶ Migration von Ressourcendomänen innerhalb einer Gesamtstruktur
- ▶ Konsolidierung der Ressourcendomänen in Organisationseinheiten und Delegierung der Administration an OU-Administratoren
- ▶ Redesign der Domänenstruktur. Die Gesamtzahl der Domänen kann verringert oder auf eine einzelne reduziert werden.
- ▶ Sie können Optionen festlegen, wie Benutzer, Gruppen, Gruppenmitgliedschaften, Sicherheitseinstellungen und Passwörter während der Migration gehandelt werden sollen.

Für alle diese Vorgänge können Berichte erstellt werden, die Auskunft über den Erfolg der jeweiligen Aktion geben. Die verschiedenen Wizards des ADMT sind übersichtlich in eine einzige mmc eingebunden.

Ein weiterer zentraler Punkt ist die Übernahme/Synchronisation von Personalstammdaten aus SQL-Datenbanken wie DB2, Oracle etc. Das LDAP-Protokoll bietet die Möglichkeit, Metadirectories zu definieren. Es wird eine übergeordnete Datenbankstruktur zur Synchronisation der beteiligten Datenbankinhalte angelegt. Inhalte können einmalig übernommen oder zur Laufzeit aktualisiert werden. Doppelte Datenpflege entfällt somit. Ein Beispiel: Ein User wird in die Personalstammdatenbank eingepflegt, und das Active Directory übernimmt diese Informationen, dabei kann das Active Directory auch als Metadirectory fungieren und die Information anderen Datenbanken zur Verfügung stellen. Ein neu aufgestelltes Gerät (z.B. Netzwerk-Drucker) wird in das Active Directory eingepflegt, und eine Inventar-Datenbank übernimmt bestimmte Informationen zur Kostenabrechnung und Wartung aus der Active Directory-Information zu diesem Objekt. Es müssen also im Active Directory-Schema nur die geeigneten Objektinformationen als Felddefinitionen eingepflegt werden, damit Wartungsinformationen in einer Unternehmens-Datenbank aktualisiert werden können. Diese Datenbank muss natürlich über eine LDAP-Schnittstelle auf das Active Directory zugreifen können. Ein mögliches Programm zur Synchronisierung von Datenbeständen in SQL-Datenbanken mit Active Directory ist das weiter unten erwähnte MMS 2.2 und dessen Nachfolger MIIS 2003 (siehe Kapitel 30.2).

Durch die Anbindung von BackOffice-Servern wie Exchange 2000 an das Active Directory wird die Handhabung der entsprechenden Daten vereinfacht. Die Daten werden direkt im Active Directory abgelegt. Benutzer und Applikationen können direkt darauf zugreifen. Auch mit weiteren BackOffice-Server-Produkten plant Microsoft die Anbindung an Active Directory. In diesem Fall werden die Daten innerhalb der Versionen der einzelnen Serverprodukte übernommen und dann dem Directory zur Verfügung gestellt.

Auch die Verwendung von Daten älterer BackOffice-Server-Versionen ist gewährleistet. Für Exchange 5.5 ist die Datenanbindung über den Active Directory Connector (ADC) gewährleistet. Der ADC läuft als Dienst und verändert einmalig das Active Directory-Schema, um den Active Directory-Objekten Attribute hinzuzufügen, die für Exchange relevant sind. Damit können Exchange Attribute durch die bidirektionale Replikation abgeglichen und dann im Active Directory gespeichert werden. Der ADC kann neben der bidirektionalen Verbindung, bei der wechselseitig Änderungen am Active Directory und unter Exchange repliziert werden, auch in jeweils nur eine Richtung betrieben werden. So werden entweder nur die Änderungen am Active Directory aufgezeichnet und an Exchange übertragen oder umgekehrt. Diese Änderungen beziehen sich auf Erstellen, Modifizieren und Löschen von Benutzern und Gruppen, Verteilergruppen sowie Kontakten. Bei den beiden unidirektionalen Varianten können Sie die Änderungen selbstverständlich nur am Quellverzeichnis durchführen. Änderungen am Zielverzeichnis werden nicht an die Quelle repliziert und könnten sogar bei einer Replikation durch andere Werte überschrieben werden.

Auch eine Anbindung an andere Directory Services via LDAP wird sichergestellt. Für den Network Directory Service (NDS) von Novell NetWare wird DirSync von Microsoft verwendet.

Ein weiterer Hersteller zur Verzeichnissynchronisierung ist NetVision mit Synchronicity 3.5. Dieses Programm bietet Unterstützung für die folgenden Plattformen und Anwendungen: MS Windows NT, Active Directory, Exchange, Lotus Notes, Novell NetWare sowie GroupWise. Weitere Informationen zu diesem Programm finden Sie unter folgender Adresse:

<http://netvision.com/products/synchronicity.html>

Ein anderes wichtiges Tool sind die Microsoft Metadirectory Services (MMS) 2.2. Dieses Programm basiert auf den Technologien der Firma Zoomit, die von Microsoft aufgekauft wurde. Über MMS können Informationen und Daten verschiedener Betriebssysteme und Applikationen ins Directory integriert werden. Dazu zählen: MS Windows NT, MS Active Directory, MS Exchange 5.x, Novell NDS, Novell Bindery, GroupWise, Lotus Notes, Lotus Domino, iPlanet Directory / Metadirectory Server und verschiedene SQL-Datenbanken. Weitere Informationen zu MMS 2.2 finden Sie auf folgender Webseite:

<http://www.microsoft.com/windows2000/technologies/directory/mms/default.asp>

Kurz nach der Fertigstellung des Windows Server 2003 wurde eine neue Version der MMS herausgebracht. Dabei handelt es sich um die Version MIIS 2003.

4.2.3 Erstellen eines Asset-Managements im Active Directory

Eine weitere Möglichkeit des Active Directory bietet sich im Bereitstellen eines Asset-Managements. An zentraler Stelle würde ein Blick genügen, um gebündelte Informationen über sämtliche vorhandene Hard- und Software des Unternehmens zu bekommen. In der Regel werden solche Daten bislang in Tabellen oder separaten Datenbanken gepflegt. Für deren Pflege sind zusätzliche Personen erforderlich. Es wäre doch wesentlich praktischer, durch Aufrufen eines bestimmten Rechners im Active Directory über diesen sämtliche Informationen, angefangen bei seinem konkreten Standort über Anschaffungsdaten, Ausstattung, verwendete Lizenzen bis hin zu IP- und MAC-Adresse, auf einen Blick zu haben. Diese zentrale Übersicht wäre besonders sinnvoll z.B. bei Revision, Steuerprüfung oder Reparaturen: Auf einen Blick hätte man folgende Informationen: Das gesuchte Gerät befindet sich in Abteilung A, in der zweiten Etage, Seitenflügel rechts, Raum 25. Der Computer wurde am 01.07.2001 angeschafft. Es handelt sich um einen PIII 800, 384 MB RAM, 32 GB Harddisk, er verwendet Lizenzen für Windows 2000 Professional sowie Office 2000 Professional, die IP-Adresse lautet 172.20.20.106 und die MAC-Adresse 00-50-BA-7C-1D-BA.

Normalerweise kennt diese präzisen Informationen nur ein lokaler Administrator. Es ist unter Umständen ein langer Kommunikationsweg, bis der zentrale Verwalter des Active Directory über mehrere Autoritätsebenen vom lokalen Administrator erfahren hat, wo der genaue Standort oder wie die Rechnerspezifikationen lauten. Dieses breite Informationsspektrum lässt sich selbstverständlich nicht nur für Computer, sondern auch für andere Netzwerkressourcen wie Drucker, Plotter, Router usw. bereitstellen.

Ermöglicht wird diese Bereitstellung zusätzlicher Daten, die standardmäßig nicht im Active Directory vorhanden sind, durch das Hinzufügen von Datenfeldern in LDAP, wodurch das Active Directory-Schema erweitert wird. Dabei werden Active Directory-Objekte um selbst definierbare Attribute erweitert. Im oben genannten Beispiel würden Attribute wie Kaufdatum oder verwendete Lizenzen zu den standardmäßigen Attributen hinzugefügt werden.

Zu bedenken ist, wann die Erweiterung des Schemas für die Funktionen des Asset-Managements vorgenommen werden sollte, genauer gesagt, im Zuge der Migration oder erst zu einem späteren Zeitpunkt. Für einen späteren Zeitpunkt spricht zunächst, dass die Schemaerweiterung bei der Implementierung von Active Directory einen enormen Mehraufwand bedeutet. Hierfür werden Personen benötigt, die sich sehr umfassend in LDAP und Active Directory auskennen müssen. Auch die Zeiten, die für den Test des geänderten Schemas aufgewendet werden müssen, dürfen nicht unterschätzt werden. Falsche Einstellungen am Active Directory-Schema können im schlimmsten Fall den gesamten Netzwerkbetrieb stören. Andererseits muss für eine Migration ohnehin Zeit investiert werden. Bedenken Sie auch, wie viel Zeit Ihnen ein von Anfang an funktionierendes Asset-Management später einsparen kann. Außerdem können somit auch Kosten gespart werden, da später keine Asset-Management-Tools von Drittanbietern gekauft und lizenziert werden müssen, da Sie durch die Erweiterung des Active Directory-Schemas sozusagen mit Bordmitteln, die in der Windows 2000/2003-Serverlizenz inbegriffen sind, die Kosten für Zusatztools sparen.

5 Die Planungsphase

In der Planungsphase geht es zunächst darum, alle nötigen Erkenntnisse über Active Directory zu sammeln, um dann zu entscheiden, wie es im Unternehmen eingesetzt und welche Ziele durch die Implementierung erreicht werden sollen.

Die Planungsphase ist die Grundlage für ein später zufrieden stellendes Gesamtergebnis der Implementierung und Migration. Die Planungsphase an sich lässt sich in mehrere Unterphasen gliedern, die aber zum Teil zeitlich parallel ablaufen und von verschiedenen Verantwortlichen durchgeführt werden können. Grob gesagt besteht die Planung aus der Definition von Zielen, die mittels Active Directory im Unternehmen erreicht werden sollen, dem Aufstellen eines Zeitplans für das Migrationsprojekt, dem Bilden eines Projektteams und Festlegen von Verantwortlichkeiten sowie einer Bestandsaufnahme der Istsituation der IT-Struktur im Unternehmen.

Diese detaillierte Planungsphase kann in einem großen Unternehmen mehrere Monate in Anspruch nehmen. Eine sorgfältige Planungs- und Testphase, die nun einmal viel Zeit in Anspruch nimmt, kann sich später auszahlen, wenn während des Tests bisher ungeahnte Probleme auftauchen und diese noch behoben werden können, bevor Sie mit dem Rollout beginnen. Haben Sie diese Probleme später im laufenden Betrieb, nützt es Ihnen nichts mehr, dass die Planungsphase keine allzu lange Zeit in Anspruch genommen hat. Sie werden dann womöglich mehr Zeit und auch Kosten investieren müssen, um die Probleme oder sogar Schäden wieder zu beheben.

5.1 Zieldefinition

Als Erstes müssen das Ziel oder die Ziele definiert werden, die mit der Migration auf Active Directory im Unternehmen erreicht werden sollen. Die Zieldefinitionen werden dabei sehr vielschichtig sein. So kann auf rein technischer Ebene etwa die Migration sämtlicher Computer auf eine homogene Active Directory-Umgebung oder eine Koexistenz mit einem anderen Netzwerkbetriebssystem definiert werden. Aus Sicht der Administratoren wird als Ziel eine Vereinfachung der Verwaltung propagiert. Ihnen bietet sich mit Active Directory ein konsistenter Mechanismus zum Verwalten der überall im Netzwerk verteilten Ressourcen. Diese Vereinfachung der Verwaltung und Zentralisierung zieht wiederum eine Einsparung von Kosten nach sich – auch dies dürfte ein nicht zu unterschätzendes Ziel sein. Die Erhöhung von Sicherheit, Verfügbarkeit und Konsistenz des Verzeichnisses ist ein weiteres Ziel, das mit der Implementierung erreicht werden kann. Weiterhin kann auch die Umstrukturierung der bisherigen NT-Domänenlandschaft als Ziel definiert werden. Im Active Directory bietet sich mit der Einrichtung von Organisationseinheiten die Chance, das Unternehmen in seiner funktionellen Gliederung genau abzubilden, während die NT-Domänen oftmals nur einer willkürlichen Zweckgemeinschaft von Konten und Ressourcen glichen.

Ein weiteres Ziel, das eher in die Kategorie „Prestige“ einzuordnen ist, könnte es sein, mit der Implementierung im eigenen Unternehmen anderen Firmen – idealerweise der Konkurrenz – zu zeigen, dass eine gut durchdachte Planung und Architektur in einer komplikationsfreien Implementierung sowie einer funktionierenden Active Directory-Umgebung endet. Und welches Unternehmen hätte nicht gern bereits das Migrationsprojekt bei sich erfolgreich abgeschlossen, während die Konkurrenz noch in der Beratungsphase steckt!

Die Grundlage einer reibungslosen Durchführung dieses Projekts muss die Akzeptanz im Unternehmen sein. Interne Querelen, machtpolitische Spielchen, Kompetenzgerangel oder andere Organisationsprobleme können den Fortschritt und damit die Effizienz des Projekts stören oder sogar gefährden. Bei sämtlichen projektbezogenen Entscheidungen muss dafür gesorgt werden, dass die Pläne durchgesetzt werden, die für das Unternehmen im Ganzen eine optimale Wirkung erzielen, und dass nicht auf individuellen Wünschen einiger Gruppen beharrt wird. Eine solche Disharmonie in der Planung und Umsetzung beruht oftmals auf der Angst, dass die Interessen bestimmter Unternehmensbereiche nicht gewahrt sein könnten, während anderen Bereichen quasi jeder Wunsch von den Augen abgelesen wird. Um diese Querelen bereits im Keim zu ersticken, ist ein starker, neutraler Projektleiter erforderlich.

Während des gesamten Migrationsprozesses, insbesondere während des Rollouts und in der Anfangsphase des täglichen Betriebs, muss das Minimieren negativer Nebenaspekte für die Endbenutzer ebenfalls ein wichtiges Ziel sein.

5.2 Das Bilden des Projektteams

Während der Planungsarbeit am Projekt Active Directory müssen viele Gruppen ihr Wissen mit einbringen, um durch ihre speziellen Kenntnisse in Einzelgebieten dem gesamten Vorhaben zum Erfolg zu verhelfen. Definieren Sie zunächst alle Bereiche, die in das Projekt mit einbezogen werden müssen. Für jeden dieser Bereiche sollte es bereits einen oder mehrere Verantwortliche im Unternehmen geben. Sie können an dieser Stelle auch neue Verantwortlichkeiten festlegen.

Die folgenden verschiedenen Punkte sind für das Gesamtprojekt Active Directory zu berücksichtigen. Für jeden dieser Bereiche sollten Sie nach Möglichkeit ein eigenes Projektteam bilden. Dabei kann ein Mitarbeiter auch für mehrere Bereiche zuständig sein und diese dann zu einem Bereich zusammenfassen, wenn sich seine Kompetenzbereiche mit anderen überschneiden:

- ▶ die Funktionsweise und Möglichkeiten des Verzeichnisdienstes an sich
- ▶ das Netzwerk
- ▶ die Betriebssysteme Windows NT, 2000, XP, 2003
- ▶ DNS, DHCP, WINS
- ▶ die Server
- ▶ die Clients
- ▶ die Sicherheit
- ▶ die Kompatibilität der Applikationen mit Active Directory, insbesondere Datenbanken, Client-Server-Applikationen

- ▶ die Tests
- ▶ die Qualitätssicherung (QA)
- ▶ die Logistik (z.B. das Bestellen neuer Hardware und Rollout)
- ▶ die Ausbildung und das Training der Mitarbeiter
- ▶ die Planung der Durchführung an sich, das Projektmanagement

Alle verantwortlichen Personen dieser Bereiche werden in das Gesamtprojektteam berufen und arbeiten dort in einem kleinen Team an ihrem Spezialbereich. Aber dabei darf keineswegs der Blick über den Tellerrand vergessen werden. Es darf nicht eine Gruppe vor sich hinarbeiten, ohne zu berücksichtigen, was eine andere macht. Der Kommunikationsfaktor ist sehr hoch anzusetzen. Dafür kann es auch sinnvoll sein, wenn die verantwortlichen Personen Mitglieder in zwei verschiedenen Teams sind. Neben den verschiedenen technischen Skills kommt die zentrale Rolle dem Projektleiter und den Verantwortlichen des Bereichs Projektmanagement zu. In einem derartig komplexen Projekt sind Konflikte und Meinungsverschiedenheiten zwischen den verschiedenen Interessengruppen nahezu vorprogrammiert. Als Projektleiter ist also weniger eine Person gefordert, die die Teammitglieder nur mit netten Grafiken und Präsentationen zu begeistern versucht, als vielmehr eine Persönlichkeit mit Menschenführungskompetenz, die Konfliktpotenzial bereits im Keim ersticken kann, Kritiker zu überzeugen und umzustimmen vermag sowie dem ganzen Projekt deutlich seine Handschrift verleiht.

Für die Bildung der einzelnen Projektgruppen sollten Sie auch auf Skills in weiteren Bereichen berücksichtigen. Dazu zählen Erfahrungen mit anderen Verzeichnisdiensten. Wer bereits beispielsweise mit NDS gearbeitet hat, für den ist die Verständnisgrundlage für Active Directory wesentlich höher. Auch Erfahrungen im Bereich heterogener Betriebssystemumgebungen sind von Vorteil. Dabei kann es sich um NT-Unix-, NT-OS/2- oder auch NT-2000-Erfahrungen handeln. Weiterhin sollte auch Spezialwissen über Windows 2000-Sicherheitstechnologien wie Kerberos oder PKI in das Projektteam mit eingebracht werden. Auch Kenntnisse in Anwendungen zur Softwareverteilung sowie Systems Management-Prozessen können sich fruchtbar im Projektteam auswirken.

Sollten Sie bei der Zusammenstellung des Projektteams feststellen, dass Ihnen in entscheidenden Bereichen nicht die erforderlichen Kompetenzen zur Verfügung stehen, müssen Sie entscheiden, ob diese Kompetenzen von betriebsinternen Mitarbeitern in Schulungen erworben werden oder ob Sie für diese Bereiche auf externe Ressourcen zurückgreifen wollen. Sie sollten von unabhängigen Personen den Status der vorhandenen Ressourcen (Wissen etc.) und den gewünschten Stand bewerten lassen und danach entscheiden, wie die Teams gebildet werden.

Wenn Sie sich entscheiden, für die Mitglieder des Projektteams Schulungen zu planen, müssen Sie dieses möglichst zeitnah durchführen. Zunächst müssen Manager und andere Entscheidungsträger über die Vorteile von Active Directory aufgeklärt werden. Bereits hierfür sollte ein gutes Verständnis über Active Directory vorhanden sein, um einen Manager mit Argumenten zu überzeugen und gleichzeitig seine Einwände und Befürchtungen zu zerstreuen. Ein noch tieferes Wissen sollte erworben sein, wenn es in der Designphase an die Planung der Active Directory-Architektur geht. Weiterhin müssen Sie verschiedene Schulungen für die Administratoren und Endbenutzer planen. Der Schulungsplan für die Endbenutzer wird in der Pilotphase getestet.

Die Arbeit als Administrator eines kompletten Active Directory ist wesentlich anspruchsvoller als die Arbeit eines Administrators, der nur für bestimmte Teilbereiche im Unternehmensnetzwerk zuständig ist. Da die Grundtechnologien einem Windows NT-Administrator bekannt sein müssen, muss er in den neuen und geänderten Features von Windows 2000/XP/2003 geschult werden, um seine technischen Skills und seine Kompetenz auf der Höhe der Zeit zu halten. Scheuen Sie weder während noch später nach der Implementierungsphase Investitionen in die Ausbildung Ihrer Mitarbeiter.

Später im laufenden Betrieb muss sich der Administrator um die Pflege sowie Wiederherstellung von Daten kümmern. Auch für die Qualitätssicherung und die Planung bestimmter Standards für unternehmensweite Anwendungen ist er zuständig. In einem großen Unternehmen sollten Sie ein Team bilden für die administrativen und Pflegeentscheidungen bezüglich Active Directory, das mit Mitgliedern aus jeder größeren Unter-
einheit der Firma besetzt ist.

5.3 Erstellen eines Zeitplans

Für das gesamte Projekt muss ein zeitlicher Rahmen definiert werden. An dieser Stelle kann sicherlich kein allgemein gültiger Rat abgegeben werden, wie lange die Gesamtimplementierung in Anspruch nehmen wird. Dies hängt von einer Reihe verschiedener Faktoren ab, so z.B. der Größe und Komplexität des Unternehmens, den definierten Zielen und nicht zuletzt auch von der Qualifikation der Mitarbeiter. So ist es in einem großen Unternehmen durchaus möglich, dass von den ersten Planungen bis zur Fertigstellung der Implementierung weit über ein Jahr an Zeit aufgewendet werden muss. Bei allen Planungsphasen sollten Sie lieber zunächst zu viel als zu wenig Zeit einkalkulieren. So bleiben immer noch genügend Reserven, falls sich ein bestimmter Teil des Projekts länger hinzieht als erwartet. Nur im ungünstigsten Fall, wenn Sie feststellen, dass sich der anfänglich definierte Zeitplan unter keinen Umständen einhalten lässt, sollte dieser überarbeitet werden – jedoch nicht bei kleinen Verzögerungen, die mit Sicherheit an einigen Stellen des Projekts auftreten werden.

Die Mitglieder des Projektteams können für ihre speziellen Fachbereiche präzise Angaben machen, wie lange bestimmte Schritte dauern könnten. Aus diesen Einzelinformationen muss ein Zeitplan als Einheit geformt werden.

Das gesamte Projekt wird zunächst in grobe Phasen eingeteilt, die dann ihrerseits mit groben und feinen Arbeitsschritten gefüllt werden. Eine Zeitlinie ist einzurichten, an der sich die Detailplanungen orientieren müssen. Für jede der Phasen und deren einzelne Arbeitspakete müssen Erfüllungskriterien benannt werden, wann eine Phase oder ein Arbeitsschritt als abgeschlossen gilt. Es müssen aber auch für jeden Planungsschritt Eckpunkte definiert werden, an denen eine Entscheidung in eine bestimmte Richtung fallen muss. Andernfalls würde das gesamte Projekt ins Stocken geraten. Wenn bestimmte Punkte bis zu einem festen Datum nicht gelöst sind, müssen diese zunächst außen vor gelassen oder vorher definierte, alternative Vorgehensweisen abgearbeitet werden. Die Problemlösung muss dann im Laufe des weiteren Projekts stattfinden. Da aber diese späteren Entscheidungen möglicherweise inkompatibel mit Ihren weiteren Planungen sind, sollten Sie immer für jeden Punkt des Projekts genügend Zeit einplanen. Wenn Sie mehrere Punkte unterhalb des Zeitlimits abarbeiten, haben Sie für schwierigere Probleme dadurch ein Zeitpolster geschaffen.

Für sämtliche Planungsschritte gilt, nicht abzuschweifen und zu vergessen, was das Ziel des Projekts ist. Dabei darf sich nicht in Kleinigkeiten verzettelt werden. Ein wichtiges Ziel muss immer sein, die Veränderungen so gering wie möglich zu halten. Die neue Architektur soll für mehrere Jahre im Unternehmen Bestand haben. Deshalb muss die Architektur auch für Wachstum und Expansion des Unternehmens erweiterungsfähig und auf andere neue Unternehmensbereiche anwendbar sein.

Da es sich bei der Migration um einen lange dauernden komplexen Prozess in vielen Schritten handelt, sollten Sie auch entscheiden, welche Hilfsmittel für die Projektplanung und Durchführung eingesetzt werden sollen, damit die Planungen für die Unternehmensarchitektur verkürzt und vereinfacht werden können, indem die Planung in einzelne Meilensteine geteilt wird. Führend auf diesem Gebiet ist die Software Microsoft Solutions Framework (MSF). MSF unterstützt die Planungen z.B. bezüglich Architektur, Team, Design, Risk Management usw.

5.4 Bestandsaufnahme

Bevor Sie das Design Ihrer neuen Active Directory-Umgebung weiter planen können, müssen Sie zunächst eine Bestandsaufnahme der bisherigen IT-Infrastruktur des Unternehmens vornehmen. Auf den in dieser Phase gewonnenen Erkenntnissen basiert der gesamte Architekturplan. Je gründlicher Sie die bestehende Struktur analysieren und dokumentieren, desto geringer wird der Aufwand in der Architekturplanung, wenn Sie auf gesicherte Erkenntnisse zurückgreifen können. Diese Bestandsaufnahme ist auch wichtig für die Einrichtung des Testcenters, da dort die produktive Umgebung so weit wie möglich nachgestellt werden soll.

Während der Bestandsaufnahme sind die folgenden Punkte zu analysieren und dokumentieren:

- ▶ Standorte der Organisation
- ▶ Bisherige Hardware-Landschaft
- ▶ Netzwerktechnisches
- ▶ Applikationsbezogenes
- ▶ Benutzerbezogenes

Die speziellen Aufnahmekriterien für die einzelnen Punkte werden Ihnen im Folgenden vorgestellt.

5.4.1 Standorte der Organisation

Wichtig für eine gelungene Umsetzung des Active Directory ist die Abstimmung auf die vorhandenen Standorte eines Unternehmens. Dieser Punkt erübrigt sich zwar in einer Firma, die nur an einem Standort residiert, ist aber für weit verzweigte Unternehmen umso wichtiger.

Bezüglich der Standorte gibt es drei wichtige Bereiche. Dabei handelt es sich zum einen um die Administration, zum anderen um die Gliederung und um die Netzwerkstruktur der Standorte.

Administration der Standorte

Hier ist zu ermitteln, wie die bisherige Administration der Standorte aussieht. Dabei sollten folgende Daten ermittelt werden:

- ▶ Verfügt bislang jeder Standort über eine eigene Domäne? Besitzen bestimmte Standorte mehrere Domänen? Wenn ja, hat dieses funktionelle Gründe, oder wurde lediglich die Datenbankobergrenze erreicht, sodass eine zweite Domäne notwendig wurde?
- ▶ Ist momentan jede Außenstelle selbst für die Verwaltung der Domäne zuständig, oder geschieht dies zentral?
- ▶ Über welche Berechtigungen verfügen die Administratoren der einzelnen Standorte?
- ▶ Wie hoch sind die Qualifikationen der lokalen Administratoren? Welche Kompetenzen sollen ihnen im Active Directory zugestanden werden?

Struktur und Gliederung der Standorte

Zur Bestimmung der Struktur der einzelnen Standorte müssen folgende Punkte ermittelt werden:

- ▶ Wie viele Standorte gehören insgesamt zum Unternehmen?
- ▶ Wie viele Benutzer gibt es an jedem Standort? Bestimmen Sie weiterhin die Anzahl anderer Ressourcen wie Computer, Drucker usw. Diese Angaben benötigen Sie für die einzelnen Standorte, wenn Sie den serverseitigen Hardwarebedarf für die Domänen ermitteln wollen.
- ▶ Gibt es an jedem Standort mehrere funktionelle Abteilungen?
- ▶ Ist die Verteilung der Abteilungen an jedem Standort identisch?
- ▶ Sind verschiedene Unternehmensbereiche nur auf einen Standort beschränkt?
- ▶ Ist bereits jetzt absehbar, dass es neue Standorte des Unternehmens geben wird? Wenn ja, wie groß werden diese sein?

Netzwerkstruktur der Standorte

Die Bestandsaufnahme zum Thema Standorte geht in einigen Bereichen auch in die Zuständigkeit des Bereichs Netzwerk über. Hierzu zählen beispielsweise Fragestellungen über Netzwerkkapazitäten und Verbindungen zwischen den einzelnen Standorten. Explizite Fragestellungen dazu finden Sie im übernächsten Kapitel „Netzwerktechnisches“.

5.4.2 Hardware-Landschaft

Im nächsten Schritt müssen Sie nun eine Bestandsaufnahme der vorhandenen Hardware durchführen. Sollten die Ergebnisse dazu führen, dass der Kauf neuer Hardware erforderlich wird, so sollte zeitnah das Bestellungs- und Logistikteam darüber informiert werden.

Ermitteln Sie zunächst, welche Windows-basierte Hardware client- und serverseitig eingesetzt wird. In den meisten Unternehmen dürfte standardisierte Hardware eines Herstellers im Einsatz sein. Ist dies nicht der Fall, so wird die Bestandsaufnahme zeitaufwändiger.

Es ist zu klären, ob die bisher eingesetzten Rechner überhaupt die Hardwareanforderungen für die Installation von Windows 2000 oder XP erfüllen. Ist dies sichergestellt, so müssen Sie weiterhin herausfinden, ob die eingesetzten Komponenten in der Hardware Compatibility List (HCL) aufgeführt sind oder nicht. Erfüllt ein Rechner zwar die Mindestanforderungen, ist jedoch eine Komponente nicht die HCL, so muss entschieden werden, ob lediglich der Austausch der Komponente oder des gesamten Geräts erfolgen soll. Sie müssen zwar nicht auf jedem Client Windows 2000 installieren, jedoch werden Sie die volle Leistungsfähigkeit des Active Directory erst in reinem Windows 2000- oder höherem Netzwerk ausnutzen können. Es sollte also sichergestellt sein, dass ein Budget vorhanden ist, um sämtliche Computer zu einem bestimmten Zeitpunkt erneuern zu können. Es ist wenig sinnvoll, das Budget so aufzuteilen, dass zum Stichtag 1 x% der Rechner erneuert werden können, zum Stichtag 2 weitere y% usw., bis eines Tages 100% erreicht sind. Verfahren Sie lieber so, auf allen Rechnern, die knapp die Systemanforderungen erfüllen, Windows 2000 zu installieren, anstatt einen Teil sofort für die Migration zu erneuern und einen Teil unter Windows NT 4.0 zu belassen. Die weniger leistungsfähigen Computer können sukzessive erneuert werden.

Ermitteln Sie auch, wie viele PDCs und BDCs bisher in der Unternehmensstruktur vorhanden sind. Ist bei diesen die Kapazität ausreichend, um als Domänencontroller im Active Directory zu fungieren? Sind außerdem die alten Datei- und Druckserver noch von ausreichender Kapazität?

Neue Serverrollen sind zu definieren, z.B. für globale Katalogserver. Sofern der Einsatz globaler Katalogserver notwendig wird, muss für diese neue Rolle ebenfalls Hardware bereitgestellt werden.

Im Zusammenhang mit Domänencontrollern und globalen Katalogservern spielt neben der Prozessorleistung auch der für die Active Directory-Datenbank verfügbare Festplattenplatz eine wichtige Rolle. Um einen ersten Überblick über die benötigten Kapazitäten (in Byte) zu bekommen, kann nach folgender Faustregel gerechnet werden:

Anzahl der Benutzer * (3600 + Anzahl der zusätzlichen Attribute pro Benutzer * 100)

Nach dieser Formel erreichen Sie zumindest für mittlere bis große Unternehmen einen relativ präzisen Wert. In kleineren Unternehmen hat sich der errechnete Wert eher als zu gering erwiesen. Von Microsoft wird ohnehin empfohlen, den doppelten Platz als den mit dieser Formel errechneten einzuplanen. So bleiben immer noch genügend Reserven für zusätzliche Attribute und Objekte. Setzen Sie zusätzlich noch Applikationen ein, die ihre Informationen im Active Directory ablegen, so müssen Sie mit entsprechend mehr Speicherplatz kalkulieren. Wenn eine große Anzahl von Objekten gelöscht wurde, sollte die Datenbank immer defragmentiert werden. Auch das Tombstoning-Verfahren spielt dabei eine wichtige Rolle. Alle gelöschten Objekte werden dabei erst 60 Tage nach dem Löschvorgang physikalisch von der Festplatte entfernt. Der so gewonnene Platz kann dann für neue Objekte benutzt werden.

5.4.3 Netzwerktechnisches

Eine weitere Bestandsaufnahme muss im netzwerktechnischen Bereich durchgeführt werden. Als Grundlage listen Sie zunächst sämtliche Netzwerkverbindungen auf, die in Ihrem Unternehmen vorhanden sind. Dazu zählen LANs, WANs oder auch Verbindungen zum Internet-Provider. Dokumentieren Sie die Bandbreite und Redundanz der einzelnen Netzwerkverbindungen.

- ▶ Welche Netzwerkverbindungen gibt es zwischen den Standorten bzw. am Standort? Gibt es redundante Verbindungen zwischen diesen?
- ▶ Wie hoch ist die Geschwindigkeit dieser Netzwerkverbindungen?
- ▶ Bei wie viel Prozent liegt die Auslastung der einzelnen Verbindungen?
- ▶ Welche Netzwerkprotokolle werden verwendet? Werden außer TCP/IP noch IPX/SPX, AppleTalk oder andere Protokolle verwendet?
- ▶ Wie sind bisher die Subnetze strukturiert? Ist das Einteilen des Unternehmens in neue Subnetzbereiche erforderlich?

Auch das Sammeln von Netzwerkstatistiken ist sehr sinnvoll. Zu diesem Zweck können Sie entweder den Microsoft-eigenen Netzwerkmonitor verwenden oder ein Programm eines Drittanbieters. So können Sie frühzeitig mögliche Engpässe in der LAN- oder WAN-Bandbreite, z.B. dem Backbone zur Zentrale, erkennen. Berücksichtigen Sie für die Bewertung der Bandbreite auch die Replikationslast innerhalb der Domänen sowie die Netzwerkaktivitäten in Zusammenhang mit IntelliMirror oder ein generelles Wachstum der Netzwerkinformationen. Dies gilt auch, wenn beispielsweise im Netzwerk das Senden von Audio- oder Videoinformationen in Echtzeit erfolgen soll. Damit eventuell die Bandbreite verbessert werden kann, ist eine frühzeitige Planung notwendig. Der Zukauf von Netzwerkbandbreite einer Standleitung muss beantragt werden. Auch die Verbesserung des LANs kann durch Verlegung zusätzlicher Kabel oder Austausch der bisher verwendeten verbessert werden. Dies alles nimmt jedoch auch Zeit in Anspruch. Diese Umstrukturierungen sollten bereits parallel zur Design- und Testphase durchgeführt werden.

Auch serverseitig müssen Sie Ihre bisherige Netzwerkstruktur dokumentieren. Dazu zählt die Beantwortung der folgenden Fragen:

- ▶ Wo sind die DNS-, WINS- und DHCP-Server verteilt, und wie viele werden eingesetzt?
- ▶ Für welche Adressbereiche sind die DHCP-Server konfiguriert?
- ▶ Welche statischen IP-Adressen werden verwendet? Welchen Servern, Clients oder sonstigen Netzwerkgeräten sind diese zugeordnet?

Gerade der Einsatz von DHCP sollte unter Windows 2000 in Erwägung gezogen werden. Mit der Einführung des dynamischen DNS (DDNS) benutzt Windows 2000 die Informationen der DHCP-Server, um diese in die automatische Erstellung der DNS-Einträge einfließen zu lassen.

Auch die verwendeten Router müssen einer Bestandsaufnahme unterzogen werden. Analysieren Sie dazu alle statischen Routing-Tabellen. Ermitteln Sie auch die Firmware-Version sowie die Version des Betriebssystems. In einigen Fällen kann eine Aktualisierung der Router erforderlich werden. Weitere Hinweise dazu entnehmen Sie RFC 1542.

Auch die Sicherheitsaspekte im Netzwerk müssen berücksichtigt werden. Hierzu zählen die Konfigurationseinstellungen der Firewall und des RAS-Zugriffs. Weiterhin gehört in diese Kategorie auch eine Dokumentation der Zugriffsbeschränkungen auf die vorhandenen Netzwerkressourcen.

5.4.4 Applikationsbezogenes

Die applikationsspezifische Standortbestimmung des Unternehmens ist in die Bereiche Betriebssysteme und Applikationen zu gliedern.

Betriebssysteme

Als Erstes sollten Sie einen Blick auf die eingesetzten Betriebssysteme und deren Servicepacks werfen. Um ein voll funktionsfähiges Active Directory betreiben zu können, muss aufseiten der Clients und Server auf Windows 2000/2003 oder XP migriert werden. Aufgrund der preislichen Differenz zwischen Update- und Vollversionen sind insbesondere die Update-Versionen interessant. Deshalb werden im Folgenden die Update-Pfade der beiden Betriebssysteme angegeben.

- ▶ Ein Update auf Windows 2000 Professional ist von folgenden Betriebssystemen aus möglich: Windows 9x und ME, NT Workstation 3.51 und 4.0.
- ▶ Das Update auf Windows XP Professional ist von Windows 98, 98SE, ME, NT 4.0 Workstation, 2000 Professional sowie XP Home möglich.

Serverseitig können Sie folgendermaßen updaten:

- ▶ auf Windows 2000 Server von Windows NT 3.51- und 4.0-Server
- ▶ auf Windows 2000 Advanced Server von Windows NT 3.51 sowie 4.0 Server, Windows NT 4.0 Enterprise Server sowie Windows 2000 Server
- ▶ auf Windows 2003-Standard-Server von Windows 2000 und NT 4.0 Server
- ▶ auf Windows 2003-Enterprise-Server von Windows 2000 Advanced Server, Windows NT 4.0 Enterprise Server sowie Windows 2003-Standard-Server

Unterstützt Active Directory die Betriebssysteme des Desktops (Windows 9x, NT 4.0), ist für einige Clients möglicherweise der Einsatz von ADSI-Clients ausreichend. Dies wäre eine Zwischen- oder auch endgültige Lösung, wenn Sie aus Kostengründen nicht das komplette Unternehmen mit Windows 2000- oder XP-Professional-Client-Lizenzen versorgen können.

In diesem Zusammenhang sollten auch die Versionen der eingesetzten BackOffice-Server-Produkte analysiert werden. Wird in Ihrem Unternehmen beispielsweise noch Exchange 5.5 eingesetzt, so wäre es zumindest eine Überlegung wert, auf die Version Exchange 2000 oder 2003 zu migrieren, die Active Directory beide nativ unterstützt. Weitere BackOffice-Server werden folgen, die in der nächsten Version ebenfalls nativ das Active Directory nutzen.

Applikationen

Die Bestandsaufnahme der Applikation wird stark erleichtert, wenn Sie in Ihrem Unternehmen bereits standardisierte Arbeitsplatztypen mit vordefinierter Software verwenden. Ist dies nicht der Fall, muss der erste Schritt der Bestandsaufnahme darin bestehen zu analysieren, welche Software in welchen Versionen an welchen Stellen des Unternehmens von wie vielen Personen benutzt wird. Sobald Sie die Erkenntnisse darüber gewonnen haben, beginnen Sie mit der Analyse dieser Applikationen.

- ▶ Handelt es sich bei den Applikationen um gekaufte Software, oder sind es Eigenentwicklungen?
- ▶ Welche Applikationen werden unternehmensweit eingesetzt, welche nur in einigen Bereichen oder von einzelnen Personen?
- ▶ Sind die Versionen der verwendeten Software noch up to –date, oder sollten sie im Zuge der Migration auch aktualisiert werden?
- ▶ Werden z.B. in einer Außenstelle und der Zentrale verschiedene Applikationen für eine bestimmte Aufgabe eingesetzt? Ein klassisches Beispiel ist der parallele Einsatz von Microsoft Exchange und Lotus Notes als Mailsystem.
- ▶ Welche der eingesetzten Applikationen nutzen das Active Directory als Datenspeicher?
- ▶ Gibt es Applikationen, bei denen absehbar wird, dass bei der Implementierung Änderungen am Active Directory-Schema vorgenommen werden müssen?
- ▶ Sind die vorhandenen Versionen oder die zur Anschaffung geplanten unter Active Directory lauffähig oder nicht? Diese Frage bezieht sich jedoch nur auf den nativen Modus vom Active Directory. Im mixed Mode ist mit keiner Beeinträchtigung zu rechnen, solange das Programm unter Windows 2000 oder XP ausgeführt werden kann.

Wie schon gesagt, bezieht sich die Funktionalität auf den nativen Betriebsmodus von Active Directory. Im Klartext heißt dieses, dass die Software ohne NetBIOS arbeiten muss. Auch mit der Ablösung von WINS durch DNS muss die Applikation zurechtkommen. Gerade dieser Punkt wird häufig von vielen Personen nicht bedacht. Dieser Support wird auch nicht von allen Softwareanbietern gewährleistet.

Stellt sich nun heraus, dass bestimmte Software nicht im nativen Modus funktionieren wird, so sind folgende Punkte zu klären:

- ▶ Wie groß ist der Wert der eingesetzten Applikationen für das Unternehmen? Daraus ist abzuleiten, ob es sich überhaupt lohnt, diese zu upgraden oder sogar umzuschreiben. Der Kosten-Nutzen-Faktor muss hierbei in erster Linie beachtet werden.
- ▶ Wenn Sie sich entschließen, nicht lauffähige Applikationen durch Update oder Redesign für Active Directory kompatibel zu machen, so müssen Sie bestimmen, welche Programme dafür benötigt werden.
- ▶ Wie viel Zeit wird benötigt, um selbst geschriebene Applikationen 2000-kompatibel zu machen? Ist möglicherweise eine Neuentwicklung weniger zeitintensiv?

Wenn Sie bei der Bestandsanalyse feststellen, dass eine große Anzahl der Applikationen überarbeitet werden muss, so müssen Sie eine Priorisierung der Anpassungsarbeiten vornehmen. Vorzugsweise sollten Sie mit solchen Anwendungen bis zum Schluss warten, die unter Active Directory zwar lauffähig sind, aber nur nicht ihre Daten im

Verzeichnis ablegen oder bei denen absolut sicher absehbar ist, dass ihre Modifikation nur einen geringen Zeitaufwand erfordert. Auch Applikationen, die nur von einer beschränkten Anzahl von Mitarbeitern genutzt werden, können zunächst zurückgestellt werden, da nur eine kleine Gruppe davon betroffen ist.

5.4.5 Arbeitsplatz- und Benutzerbezogenes

Im Rahmen der Softwarebestandsaufnahme haben Sie bereits die auf den Desktops der Benutzer vorhandenen Programme ermittelt. Gehen Sie nun einen Schritt weiter, und definieren Sie daraus für jeden Bereich und jede Abteilung des Unternehmens die Standardkomponenten des Arbeitsplatzes. Nach der Definition der standardmäßigen Softwareausstattung sollten Sie nochmals prüfen, ob auch die Hardware für die Anforderungen der Applikationen ausreichend ist.

Überprüfen Sie auch durch Erstellen von Statistiken, wie viel Speicherplatz die Benutzer belegen. Gibt es dabei große prozentuale Unterschiede zwischen bestimmten Benutzergruppen? Auf Grundlage dieser Daten sollten Sie später Kontingentgrenzen für die Benutzer durchsetzen. Darauf aufbauend kann auch ein verteiltes fehlertolerantes DFS (Distributed File System) implementiert werden.

Für die spätere Einrichtung von Benutzergruppen und Gruppenrichtlinien ist zu evaluieren, wo die Benutzer hauptsächlich tätig sein werden.

- ▶ Verfügen Sie nur über Inhouse-Mitarbeiter innerhalb einer Hauptstelle?
- ▶ Sind die Benutzer über viele Filialen verteilt?
- ▶ Sind viele Mitarbeiter in Außeneinsätzen bei Kunden vor Ort?
- ▶ Ist für die Außendienstler RAS-Zugriff für die Domäne konfiguriert?

Auch die Aspekte der Datensicherheit vor bestimmten Benutzern müssen geregelt werden. Klären Sie dazu die folgenden Punkte:

- ▶ Gibt es Benutzer bestimmter Filialen, deren Domänenrechte restriktiv gehandhabt werden, z.B. nur Zugriff auf bestimmte Bereiche?
- ▶ Sind höchst sensitive Daten besonders zu schützen: Die Zugriffsberechtigungen müssen auf den Rollen und nicht auf dem augenblicklichen Standort des Benutzers beruhen.

Bereits zu diesem Zeitpunkt sollten Sie analysieren, ob sich aufgrund bestimmter Bedürfnisse der Benutzer Änderungen an der Struktur der Administration, am Helpdesk oder weiteren Support ergeben sollen

6 Die Designphase

Nachdem Sie in der Planungsphase die Ziele definiert, eine Bestandsaufnahme der Ist-Situation durchgeführt und ein Projektteam gebildet haben, können die Verantwortlichen nun darangehen, in ihren Bereichen mit dem Design zu beginnen. Die Designphase darf erst nach Abschluss der Planungsphase und der Bestandsaufnahme begonnen werden.

Die Designphase beginnt mit dem Erstellen eines Architekturplans für alle Bereiche der IT-Struktur, die von den verschiedenen Mitgliedern des Projektteams ausgearbeitet werden müssen. Im Architekturplan wird der komplette Aufbau des zu implementierenden Active Directory beschrieben. Dies beginnt bei der Planung der Domänenstruktur, geht weiter über die DNS-Anforderungen bis hin zu Details in der Replikationsplanung.

Bereits während der Architekturplanung sollte die Planung der Migrationsstrategie empfohlen und dokumentiert werden. Hierbei ist festzulegen, ob in einer homogenen Windows-Umgebung alle Rechner auf einen Schlag migriert werden sollen, ob eine heterogene Umgebung das Teil- oder Endziel ist, wie die Zusammenarbeit mit anderen Betriebssystemen sicherzustellen ist, ob alle Unternehmenszweige und Standorte gleichzeitig migrieren usw. In diese Planung können aber jederzeit Erkenntnisse einfließen, die bei der Planung der Architektur gewonnen wurden.

Sind die Migrationsstrategie und der Architekturplan erstellt, muss als Nächstes darauf beruhend ein Disaster Recovery-Plan erstellt werden. Bei einem so komplexen und einschneidenden Eingriff in die IT-Struktur des Unternehmens muss immer damit gerechnet werden, dass nicht alles nach Plan verlaufen wird – auch wenn ein umfangreicher Test in einer nicht zu knappen Testphase durchgeführt wurde.

Sobald dieser Plan ausgearbeitet ist, kann mit der Erstellung eines Betriebsführungskonzeptes und eines Betriebsführungshandbuchs begonnen werden. In das Konzept fließen alle Erkenntnisse des Ist-Zustandes und des Architekturplans ein. Dieses Konzept bildet die dokumentierte Grundlage für den Beginn der Migration. Im Betriebsführungshandbuch werden dezidiert alle technischen Schritte aufgelistet, die für die Aufrechterhaltung und den täglichen Betrieb des Active Directory notwendig sind. In beide Dokumentationen können noch die Änderungen einfließen, die in der Testphase als notwendig erkannt werden. Nach der Testphase aber müssen beide Dokumentationen abgeschlossen sein, da mit ihrer Hilfe die endgültige Migration durchgeführt wird. Die Pilotphase wird zeigen, ob anhand der beiden Dokumentationen der tägliche Betrieb reibungslos ablaufen kann. In einem Unternehmen sollte keineswegs jemand auf die Idee kommen, diese beiden Dokumentationen erst nach Abschluss des Migrationsprojekts anhand der erzielten Ergebnisse zu erstellen. Zu viele Informationen können hierbei auf der Strecke bleiben.

Als wichtigste Frage für den Architekturplan stellt sich: Wann ist das Design abgeschlossen? Der richtige Zeitpunkt muss gefunden werden. Dabei liegt die Kunst darin, den idealen Punkt zu finden, damit die Planung nicht zu früh produktiv umgesetzt wird, aber auch nicht unnötig lange herausgezögert wird.

6.1 Der Architekturplan

Der Architekturplan besteht aus einer detaillierten Funktionsübersicht und basiert auf den groben Umrissen der bisherigen Erkenntnisse der Bestandsaufnahme. Dabei werden einige weniger komplexe Bereiche schneller abgearbeitet sein als andere aufwändigere Bereiche. Die im Architekturplan festgelegten Kriterien und Entscheidungen zur Implementierung dienen dem Erstellen und Dokumentieren eines Testprozesses. Dieser kann zur Validierung von Verfahrens- und Implementierungsmethoden führen. Die Ergebnisse des Architekturplans werden später in das Betriebsführungskonzept aufgenommen.

In den ersten Architektur-Meetings wird der Schwerpunkt auf der groben Struktur des internen Domänendesigns und dem Projektmanagement an sich liegen. Von Anfang an sollten Sie auf eine Vereinheitlichung und Vereinfachung im Design Wert legen. Bis zur Erstellung des endgültigen Architekturplans sind viele Einzelschritte und damit auch spezielle Meetings im kleineren Kreis von einer oder mehreren Projektgruppen erforderlich.

Die folgenden Kapitel liefern eine Übersicht über die verschiedenen Punkte und Konzepte, die beim Design des Active Directory bedacht und geplant werden müssen.

6.1.1 Domänen und Strukturen

Dieses Kapitel zeigt Ihnen die Überlegungen, die bei der Planung der Domänen und Domänenstrukturen zu bedenken sind.

Anzahl der Domänen

Erstellen Sie für die Domänenstruktur zunächst nur grobe Schemata, in denen Sie festlegen, welches die übergeordnete Domäne des Unternehmens werden wird. Da eine einzelne Domäne am einfachsten zu verwalten ist, sollten Sie in Ihrer Planung nicht von Anfang an eine komplizierte Domänenstruktur entwerfen. Bedenken Sie, dass Sie im Gegensatz zu einer Domäne unter Windows NT nicht mehr der empfohlenen Datenbankgröße von maximal 40 MB unterworfen sind, sondern eine Domäne nun Millionen Objekte und verschiedene Standorte umfassen kann. Sie müssen also nur unter speziellen Bedingungen mehrere Domänen erstellen. Dazu zählen folgende Punkte:

- ▶ Sie verfügen über mehrere Millionen Objekte, sodass auch die Höchstgrenze für eine Windows 2000-Domäne erreicht ist.
- ▶ Betriebsspezifische Anforderungen verschiedener Standorte sind nicht miteinander vereinbar, z.B. können Sicherheits- oder Passwortanforderungen in verschiedenen Bereichen unterschiedlich sein.
- ▶ Verschiedene Geschäftsbereiche haben bereits Domänennamen registriert und wollen diese auch als interne DNS-Namen beibehalten. Dies gilt auch, wenn Sie Standorte in verschiedenen Staaten haben, die als Domäne erster Ordnung ihre regionale Kennung verwenden.
- ▶ Zwischen bestimmten Standorten oder Geschäftsbereichen darf der Replikationsverkehr nur zeitgesteuert stattfinden, da sonst eine Behinderung der normalen, ohnehin schon hohen Netzwerklast stattfinden würde.

In einem kleinen Unternehmen mit einem oder nur wenigen Standorten sind die eben genannten Punkte wahrscheinlich nicht von großer Bedeutung, und es kann das Einzel-domänenmodell verwendet werden. In einem großen Konzern mit weltweit verzweigten Filialen und einer großen Bandbreite an verschiedenen Geschäftsbereichen müssen Sie jedoch festlegen, nach welchem Prinzip die Domänen gegliedert werden sollen.

Domänen nach geografischen oder funktionellen Aspekten gliedern?

Sie müssen sich zu Beginn der Planung Ihrer Domänenstruktur entscheiden, ob diese eher geografischen oder eher funktionalen Aspekten oder einer Kombination beider Möglichkeiten folgen soll. So können Sie entweder für jeden Standort eine separate Domäne anlegen, in der sich alle funktionalen Bereiche wie beispielsweise Marketing, Vertrieb oder Personal als Organisationseinheit wiederfinden. Andererseits können Sie auch die Domänen anhand der Funktionen im Unternehmen erstellen. Errichten Sie also eine Domäne Marketing, der die Mitglieder aller Standorte angehören, die eine Marketingabteilung besitzen. Die Entscheidung darüber ist beispielsweise abhängig von der Netzwerkverbindung der einzelnen Standorte untereinander. Gliedern Sie Ihre Domänen nach funktionellen Aspekten, sollten alle Mitgliedsstandorte über eine schnelle Verbindung untereinander verfügen.

Um die Domänenstruktur der aktuellen Situation und einer Expandierung des Unternehmens anzupassen, sollten Sie die folgenden Daten im Unternehmen ermitteln:

- ▶ Wie viele Mitarbeiter gibt es insgesamt momentan?
- ▶ Wie sind diese auf die einzelnen Standorte und auf die verschiedenen Funktionsbereiche verteilt?
- ▶ Wie sah bislang die Statistik der Wachstumsrate der Standorte und Geschäftsbereiche aus?
- ▶ Um wie viele Benutzer kann das Unternehmen maximal anwachsen?
- ▶ Wie viele Geschäftsbereiche könnten neu dazukommen?

Auch im Bereich Netzwerk sollten Sie folgende Punkte in Ihre Überlegungen einbeziehen:

- ▶ Welche Netzwerkverbindungen gibt es zwischen den Standorten? Gibt es redundante Verbindungen?
- ▶ Wie hoch ist die Geschwindigkeit dieser Netzwerkverbindungen?
- ▶ Bei wie viel Prozent liegt die Auslastung der einzelnen Verbindungen?

Bei einer ausgedehnten Unternehmensstruktur stellt sich weiterhin die Frage, ob Sie einen Forest (Gesamtstruktur) oder nur einen Tree (Single Forest/Domänenstruktur) verwenden möchten. In beiden Fällen ist aufgrund automatisch eingerichteter Vertrauensstellungen der Austausch von Daten innerhalb der Domäne gewährleistet, wobei alle Geschäftseinheiten eine autonome Sicherheitsstruktur behalten können. Der Unterschied liegt lediglich darin, wie Sie den DNS-Namensraum konfigurieren. Bei einem fortlaufenden Namensraum beinhalten alle untergeordneten Domänen der Domänenstruktur den Namen der übergeordneten Domäne, also beispielsweise *marketing.firma.de*. Wenn Sie jedoch mehrere Geschäftsbereiche mit verschiedenen Namen in Ihrem Domänenmodell unterbringen müssen, verwenden Sie eine Gesamtstruktur mit getrenntem Namensraum, z.B. *marketing.firmenbereich1.de* und *marketing.firmenbereich2.de*. Bedenken

Sie bei der Planung auch, ob in Zukunft die Möglichkeit besteht, dass weitere Firmenteile oder Geschäftsbereiche mit eigenem Namen zum Unternehmen hinzustoßen könnten. Weitere Hinweise zum DNS-Namensraum finden Sie im nächsten Kapitel.

Verwaltungsmodelle

Nachdem Sie sich für eine bestimmte Domänenstruktur entschlossen haben, müssen Sie bestimmen, wie diese administriert werden soll. Sie haben die Möglichkeit einer zentralen, dezentralen oder benutzerdefinierten Verwaltung. Für ein kleineres Unternehmen werden Sie die zentrale Verwaltung verwenden. Sie haben ein Administratorenteam am Hauptstandort des Unternehmens. Von dort aus wird die Verwaltung zentral gesteuert. An kleinen Standorten müssen Sie kein eigenes Administratorenteam bereitstellen.

In einem großen Unternehmen mit regional weit verteilten Standorten sollten Sie an jedem Ort ein Administratorenteam bereitstellen. Die Administratoren können aber auch alle an einem Standort residieren und ihre Aufgaben für die verschiedenen Geschäftsbereiche vornehmen. Die Einteilung ist auch davon abhängig, ob Sie Ihre Domänen anhand regionaler oder funktionaler Aspekte gegliedert haben.

Als dritte Möglichkeit können Sie die Verwaltung benutzerdefiniert – etwa nach bestimmten Verwaltungsvorgaben des Unternehmens – vornehmen. So können bestimmte Bereiche und Objekte zentral verwaltet werden, z.B. DNS-Vorgaben, während andere dezentral administriert werden, so z.B. die Benutzer an den jeweiligen Standorten.

6.1.2 DNS und Active Directory-Objektnamen

Dieses Kapitel gibt Ihnen einen Überblick über die Schritte, die vor der Implementierung des DNS-Namensraumes Ihrer Domänenstruktur zu überlegen sind. Das Planen des DNS-Namespaces mit Hierarchie und Verzeichnisbaum erfordert ein Grundverständnis über Domänenstrukturen und Gesamtstrukturen. Deshalb kann mit der DNS-Planung erst begonnen werden, wenn die Domänenstruktur feste Gestalt angenommen hat. Sämtliche Domänen in einer Active Directory-Struktur verwenden DNS-Namen im Format *firma.de*. Bei der Planung des DNS-Namensraums sind folgende Punkte zu klären und festzulegen:

- ▶ Wie wird der Namensraum angelegt?
- ▶ Verfügt Ihr Unternehmen bereits über Domännennamen im Internet, die über die DENIC/InterNIC registriert sind?
- ▶ Falls Sie bereits einen Domännennamen registriert haben, soll dieser externe Internet-Namespace derselbe werden wie der interne Ihres Intranets?
- ▶ Welche Namenskonventionen und -anforderungen für die Domänen soll es geben? Müssen Sie dabei spezielle Anforderungen für Namenskonventionen bei der Vergabe des DNS-Namens berücksichtigen? Bestehen bereits Namenskonventionen?
- ▶ Können die bisher verwendeten NetBIOS-Namen als DNS-Namen verwendet werden oder nicht?

Diese Fragen werden in den folgenden Kapiteln diskutiert und verschiedene Entscheidungsansätze gegeneinander abgewogen.

Interne oder externe Namensräume der Domäne?

Die Frage, ob Sie für Ihre interne Domänenstruktur dieselben DNS-Namen verwenden wollen wie für die externen Domänen, stellt sich selbstverständlich nur, wenn Ihr Unternehmen bereits Domännennamen im Internet über die DENIC/InterNIC registriert hat. Sollte dies nicht der Fall sein, so sind Sie bei der Wahl des internen Domännennamens freier. Überlegen Sie sich jedoch, ob es nicht an der Zeit wäre, sich den gewünschten Namen auch über die DENIC/InterNIC reservieren zu lassen, oder ob Sie generell keine Domäne mit dem Firmennamen registrieren lassen wollen. Die Fragestellung interner und externer Domännennamen hat sich nicht unter Windows NT-Domänen gestellt, da diese nicht auf dem Internet-Namenskonzept beruhen.

Gleiche interne und externe Namensräume

Möglicherweise haben Sie einen NT-Domännennamen wie *FIRMA* benutzt und gleichzeitig auch eine Domäne unter dem Namen *firma.de* im Internet registrieren lassen. Wenn Sie denselben internen und externen Namensraum verwenden, können Sie eine in sich geschlossene Namensstruktur verwenden. Zusätzlich zur übersichtlichen Namensstruktur benötigen die Mitarbeiter nur einen Anmeldennamen für interne und externe Ressourcen. So kann beispielsweise die E-Mail-Kennung *p.mustermann@firma.de* auch als Anmeldename für die Domäne gelten. Allerdings müssen Sie sicherstellen, dass die Mitarbeiter auf die internen und externen Server Zugriff haben, zwischen denen sich in den meisten Fällen eine Firewall befinden dürfte. Es müssen dazu zwei verschiedene DNS-Zonen eingerichtet werden. Eine DNS-Zone befindet sich außerhalb der Firewall auf dem DNS-Server Ihres Internet-Providers und ist lediglich für die Namensauflösung externer Internetressourcen eingerichtet. Würden hier auch die internen Namen aufgelöst, so hätten externe Clients gleichzeitig auch Zugriff auf die internen Ressourcen – und dies wird das Unternehmen sicherlich nicht wünschen. Umgekehrt müssen jedoch die internen Clients auf die externen Ressourcen zugreifen können. Richten Sie in Ihrem Intranet DNS-Server ein, die als autorisierend für den Domännennamen gelten. Diese erhalten damit den SOA-Ressourceneintrag. Danach müssen die internen DNS-Server so konfiguriert werden, dass sie die Anfragen an die DNS-Server des Internet-Providers weiterleiten. Damit ist sichergestellt, dass die internen Clients auch weiterhin auf Internetressourcen zugreifen können. Allerdings werden Ihre internen DNS-Server keine Anfragen für den Domännennamen an die DNS-Server des Internet-Providers weiterleiten. Somit könnten die internen Clients vor dem Problem stehen, dass sie nicht auf die Internetseite des Unternehmens zugreifen können. Für diesen Fall müssen Sie eine Liste der Host-Datensätze von den DNS-Servern des Internet-Providers anfordern und für jeden dieser Hosts einen statischen Eintrag bei den internen DNS-Servern vornehmen. Der Zugriff von außen kann nur auf die Ressourcen erfolgen, die in den Host-Listen der DNS-Server des Internet-Providers eingetragen sind. Sofern Sie Ihre eigenen DNS-Server statt die eines Internet-Providers für beide Arten der Ressourcen verwenden, steigt das Sicherheitsrisiko, dass sämtliche Hostnamen und IP-Adressen der internen Clients für das Internet verfügbar wären. Über *NSLOOKUP* könnten so alle Hostnamen des DNS-Servers aufgelistet werden. Dies bietet einen idealen Angriffspunkt für Hacker. Wenn Sie einen Proxyserver einsetzen, muss dieser den externen DNS-Namen als interne Ressource behandeln. Auch wenn bei dieser Methode die Konfiguration von DNS- und Proxyeinstellungen aufwändiger wird, so sollten Sie sich nach Möglichkeit doch immer für diese Variante entscheiden.

Unterschiedliche interne und externe Namensräume

Für die Verwendung unterschiedlicher Domänennamen wird meistens der Faktor Sicherheit angeführt. Jedoch sollte die eben genannte Konfiguration der DNS-Server gezeigt haben, dass diese Zweifel unberechtigt sind. In diesem Fall würde beispielsweise folgende Konfiguration verwendet werden: Als interner Name wird *firma.de* verwendet, als externer Name jenseits der Firewall *firmenname.de*. Um sicherzugehen, dass der interne DNS-Name nur von Ihrem Intranet und nicht von einem anderen öffentlichen Netzwerk verwendet wird, sollten Sie auch den internen Namen registrieren lassen, oder aber Sie verwenden eine Domäne erster Ordnung (Top-Level-Domain, TLD), die im Internet nicht verwendet wird, so z.B. .local. Andernfalls wäre der intern verwendete und gleichzeitig von einem anderen Netzwerk öffentlich verwendete Name für die internen Clients nicht zu unterscheiden. Der Domänenname an sich kann beliebig lauten, solange er auf .local endet. Für den Benutzer bringt dies zwar den Vorteil, dass er eindeutig zwischen internen und externen Ressourcen unterscheiden kann, allerdings muss er dafür auch zwei verschiedene Anmeldenamen benutzen. Und die Verwendung verschiedener Anmeldenamen ist genau das, was durch die Single Sign-on-Strategie des Active Directory nicht mehr notwendig sein muss. Um die Anmeldenamen für interne und externe Ressourcen zu vereinheitlichen, müssten die UPNs (User Principal Name) sämtlicher Anmeldenamen für die Domäne auf den der E-Mail-Anmeldung geändert werden. Dies wäre ein zusätzlicher unnötiger Faktor an Verwaltungsaufwand. Die Verwendung verschiedener Namen bringt Ihnen nur zunächst Vorteile in der Konfiguration von DNS- und Proxy-Einstellungen. Allerdings wird den Benutzern die Vereinfachung der Anmeldung genommen.

Nach dieser grundsätzlichen Entscheidung über die Namensvergabe wird der DNS-Namespace nun detaillierter strukturiert. Dazu zählen Namenskonventionen, Architektur der Domänen und Standorte sowie die Sicherheitsarchitektur.

Namenskonventionen und Anforderungen für Domänen und Active Directory-Objekte

Bei der Namensvergabe und Strukturierung Ihrer Domänen sollten Sie die folgenden Punkte bedenken:

- ▶ Überlegen Sie sich zuvor genau, wie die Stammdomäne Ihrer Struktur heißen soll. Das spätere Umbenennen von Domänen ist unter Windows 2000 nicht möglich. Erst in einer 2003-Domänenstruktur haben Sie die Möglichkeit, mit dem Support-Tool *DOMAINRENAME* bestehende Domänen umzubenennen.
- ▶ Ein einzelner Domänenname darf nicht mehr als 63 Zeichen umfassen, die Gesamtlänge inklusive der Trennpunkte nicht mehr als 255 Zeichen. Als Zeichen sind alle DNS-Standardzeichen möglich. Dies sind A–Z, a–z, 0–9 sowie -. Weitere Informationen zur Benutzung von Unicode-Zeichen finden Sie in RFC 2044.
- ▶ Bedenken Sie auch, dass die Domänenstruktur nicht unübersichtlich werden darf. Sie sollten maximal fünf Ebenen der DNS-Hosteinträge verwenden. Empfohlen sind sogar nur drei bis vier.

Sämtliche Objekte im Active Directory werden über ihren Namen identifiziert. Hierzu verwendet Windows verschiedene Kategorien von Namen. Dazu zählen:

- ▶ definierte Namen
- ▶ relativ definierte Namen
- ▶ User Principal Names
- ▶ Global Unique Identifiers

Als allgemein gültige Regel zur Festlegung aller dieser Namen gilt, dass Sie kurze, einprägsame Namen verwenden, die die Benutzer leicht behalten können.

Definierte Namen (DN)

Mit dem definierten Namen, der auch als Distinguished Name bezeichnet wird, wird jedes Objekt im Active Directory eindeutig identifiziert. Deshalb darf der definierte Name nur einmal im gesamten Verzeichnis vorhanden sein. Der Name enthält den kompletten Pfad zu der Stelle, an der sich das Objekt in der Domäne befindet. Dieser Pfad wird in der LDAP-konformen Schreibweise angegeben. Der definierte Name eines Computers mit dem Namen Archimedes in der OU Marketing der Domäne *firma.de* würde folgendermaßen aussehen: *CN=Archimedes,CN=Marketing,DC=Firma,DC=de*. Dabei haben die Attribute des definierten Namens folgende Bedeutung:

- ▶ DC = Namen der Domänenkomponenten, hier der TLD *.de* und der Domäne zweiter Ordnung *firma*.
- ▶ CN = Common Name, allgemeiner Name, hier der Name der Organisationseinheit, hier *Marketing* und Computernamen *Archimedes*.

Dem definierten Namen entspricht funktionell gesehen der kanonische Name. Allerdings verwendet dieser statt der LDAP-konformen Schreibweise die Form *firma.de/Marketing/Archimedes*.

Relativ definierte Namen (RDN)

Der relativ definierte Name ähnelt dem definierten Namen, allerdings wird mit dem RDN das Objekt nur im übergeordneten Container eindeutig identifiziert. In unserem eben angeführten Beispiel lautet der RDN des Computers *CN=Archimedes*. Dieser Computernamen muss nur innerhalb der übergeordneten Organisationseinheit eindeutig sein, in einer anderen OU kann es durchaus einen gleichnamigen Computer geben. Über die RDNs werden innerhalb des Active Directory Suchanfragen von Objekten gestartet, deren vollständiger definierter Name nicht bekannt ist. Wenn Sie eine Suche nach *CN=Archimedes* starten und dieser Rechnername mehrmals innerhalb des Verzeichnisses vorkommt, werden alle Ergebnisse aufgelistet.

Der definierte sowie relativ definierte Name werden automatisch vom Active Directory erstellt und nicht manuell geändert.

User Principal Name (UPN)

Über den UPN verfügen nur die Benutzerobjekte im Active Directory. Dieser Name wird vom Administrator vergeben und nicht vom Active Directory. Der UPN ist der Anmelde-name eines Benutzerkontos. Er setzt sich aus dem Vor- und Nachnamen des Benutzers

sowie der Domäne innerhalb der Domänenstruktur zusammen, in der sich das Benutzerobjekt befindet. Sie müssen von Anfang an eine Namenskonvention festlegen, nach der die UPNs gebildet werden. Möglichkeiten wären z.B. erster Buchstabe des Vornamens und Nachname, kompletter Vor- und Nachname oder Vor- und Nachname durch einen Punkt getrennt. Es wären also folgende UPNs möglich:

- ▶ *pmustermann@firma.de*
- ▶ *PeterMustermann@firma.de*
- ▶ *P.Mustermann@firma.de*

Den Benutzeranmeldenamen finden Sie in der mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER auf der Registerkarte KONTO in den Benutzereigenschaften.

Global Unique Identifiers (GUID)

Beim GUID handelt es sich um einen Wert, der eine Weiterentwicklung der aus den Windows NT-Domänen bekannten SIDs (Security Identifiers) darstellt. Der GUID hat einen Wert von 128 Bit Länge und wird jedem Objekt beim Erstellen automatisch hinzugefügt. Der SID war nur innerhalb einer Domäne gültig, der GUID hingegen bleibt auch dann erhalten, wenn Sie ein Objekt zwischen Domänen verschieben, bearbeiten oder umbenennen. Dabei ändern sich lediglich der DN, RDN sowie kanonische Name. Der GUID ist in allen Domänen gültig. Dieser Wert wird erst gelöscht, wenn Sie auch das Objekt löschen. Selbst wenn dann ein gleichnamiges Objekt neu erstellt wird, erhält dieses nicht den alten GUID. So können beispielsweise Anwendungen, die den GUID eines Objekts gespeichert haben, nach dessen Löschung nicht mehr auf das Objekt zugreifen, auch wenn wieder ein gleichnamiges existiert.

Benennungskonventionen

Bei der Benennung von Computer- und Benutzerkonten sowie Gruppen müssen Sie einige Punkte bezüglich der maximalen Länge und Zeichenverwendung bedenken. Es dürfen alle Unicode-Zeichen verwendet werden, Ausnahmen bilden die Sonderzeichen `< > # + \ , ; " .` Weiterhin darf kein Name mit einem Leerzeichen beginnen oder aufhören. Die standardmäßig maximale Zeichenanzahl beträgt für Computerkonten 15 Zeichen, für Benutzerkonten 20 und für Gruppenkonten 63 Zeichen.

6.1.3 Organisationseinheiten

Nach der Planung der Domänen- und DNS-Struktur steht nun die Planung der Organisationseinheiten (OUs) an. Organisationseinheiten gehören zur logischen Struktur des Active Directory. Beim Einrichten einer Architektur für die OUs stellt sich natürlich zuerst die Frage, nach welchem Prinzip sie gegliedert werden sollen. Mit Organisationseinheiten können Sie dynamisch und flexibel Ihr Unternehmen abbilden. OUs können verschiedene Unternehmensbereiche, funktionelle, geografische oder räumliche Aspekte widerspiegeln. Auch eine Kombination verschiedener Strukturierungsansätze kann vorgenommen werden. Die Einrichtung der OUs kann auch entsprechend der Helpdesk-Organisation oder gemäß der alten NT 4-Ressourcendomänen erfolgen.

Zusätzlich kann eine Organisationseinheit weitere Organisationseinheiten umfassen. Die Tiefe der Hierarchie der einzelnen Organisationseinheiten ist zwar nicht eingeschränkt, aber aus Gründen der Übersichtlichkeit gilt auch hier das für die Domänenstruktur Gesagte, nämlich dass maximal fünf Ebenen verwendet werden sollten.

Weiterhin kann in jeder einzelnen Domäne eine unabhängige OU-Hierarchie implementiert werden. Die Verwendung von Organisationseinheiten bietet vor allem bei Änderungen eine größere Flexibilität als das Erstellen verschiedener Unterdomänen. Objekte können einfacher zwischen OUs als zwischen Domänen verschoben werden. Dennoch sollten Sie beim Einrichten der Organisationseinheiten darauf achten, dass Sie die Unternehmensstrukturen abbilden, die nicht permanenten Änderungen unterworfen sind.

Ohne die Implementierung von Organisationseinheiten würden sämtliche Benutzer-, Gruppen- und Computerobjekte einer Domäne in je einem Container dargestellt werden. Dabei wird jedoch nichts über ihre funktionale oder räumliche Zugehörigkeit ausgesagt. Es wäre lediglich eine unübersichtliche Liste mit einer großen Ansammlung von Objekten.

Durch die Zusammenfassung von Objekten in Organisationseinheiten wird auch der Aspekt der einfacheren Verwaltung berücksichtigt. Die Administration einzelner OUs kann an bestimmte Personen, beispielsweise an lokale Administratoren, delegiert werden.

Auch die Sicherheit kann mit der Bereitstellung von OUs verbessert werden. Auf OU-Ebene können Sie beispielsweise Benutzer zusammenfassen, die nur vorübergehend dem Unternehmen angehören (z.B. externe Berater etc.).

6.1.4 Standorte

Die Standorte beziehen sich nur auf die physische Struktur des Netzwerks und nicht wie Domänen und OUs auf die logische Struktur. Somit ist es möglich, dass eine Domäne mehrere Standorte umfasst und umgekehrt ein Standort auch mehrere Domänen oder Teile von Domänen umfassen kann. Ein Standort ist ein Verbund von Rechnern, die sich innerhalb eines Subnetzes befinden und über eine schnelle Verbindung untereinander verfügen. Die Einrichtung von Standorten ist ein kritischer Schritt, da über die Standorte bestimmt wird, wie die Replikation die Informationen im Verzeichnis weiterleitet und wie die Anmeldeinformationen an der Domäne verarbeitet werden. Standorte sollten Sie immer gemäß der vorhandenen Netzwerkbandbreite erstellen. Vorher müssen also alle Details über die WAN-Verbindungen zwischen den Standorten bekannt sein.

Standorte, Replikation und Anmeldung

Bei der Konfiguration von mehreren physikalischen Standorten können Sie den Replikationspfad und -intervall für die standortübergreifende Replikation festlegen. Diese funktioniert im Gegensatz zur standortinternen Replikation nicht automatisch. Auch bei der Domänenanmeldung spielt der Standort eines Clients eine wichtige Rolle. Jeder Domänenclient versucht immer zuerst einen Domänencontroller für die Anmeldung an seinem Standort zu finden, damit diese möglichst rasch vollzogen werden kann. Sollte Ihr Unternehmen nur ein einzelnes LAN (Local Area Network) an einem Standort umfassen, ist die Planung einer Standortstruktur denkbar einfach. Sie müssen nämlich in diesem Fall keinen Standort anlegen und konfigurieren, da die Faktoren Replikation und Anmeldung nicht betroffen sind.

Standorte und Netzwerktopologie

Verfügt Ihr Unternehmen hingegen über verteilte Netzwerke an mehreren physischen Standorten, so sollte die Planung der Standorte gut durchdacht werden. Anhand der in der Planungsphase ermittelten Daten zu vorhandenen Subnetzen, Netzwerkverbindungen und Kapazitäten, redundanten Verbindungen und zur Netzwerkauslastung legen Sie fest, wie eine Standortstruktur innerhalb der Domäne aussehen könnte. Ermitteln Sie dabei auch, welche Standorte zu welcher Domäne gehören sollen oder ob ein Standort möglicherweise zu verschiedenen Domänen gehören soll. Dies ist in erster Linie davon abhängig, für welche Methode der Domänenstrukturierung Sie sich entschieden haben. Beruhen die Domänen auf funktionellen Aspekten, ist es durchaus möglich, dass jeder Standort mit entsprechenden Geschäftsbereichen einer anderen Domäne angehört.

Selbst wenn Ihr Unternehmen nur über einen einzigen Standort verfügt, kann die Einrichtung eines Pseudo-Standorts sinnvoll sein. Soll für bestimmte Clients die Anmeldezeit herabgesetzt oder sollen für einen Teil des Netzwerks andere Replikationsansprüche erfüllt werden als die standortinternen, so können Sie für einen bestimmten Bereich von Clients einen eigenen Standort einrichten.

Sollte sich eine Geschäftseinheit an einem Standort für einen anderen Verzeichnisdienst als Active Directory entscheiden, muss immer noch die Interoperabilität gewährleistet sein. Da Active Directory auf standardmäßigen Verzeichnisdienst-Zugriffsprotokollen basiert, ist die Zusammenarbeit mit anderen LDAP-konformen Verzeichnisdiensten gewährleistet.

6.1.5 Replikation

Wenn in diesem Kapitel vom Planen des Replikationsschemas die Rede ist, so bezieht sich die Replikation hier ausschließlich auf die standortübergreifende Replikation. Für jeden eingerichteten Standort wird ein Standortverknüpfungsobjekt erstellt. Jedes dieser Objekte enthält wiederum Verknüpfungsattribute, die den Replikationszeitplan und die Replikationskosten regeln. Für den effizienten Einsatz von Active Directory im WAN sprechen Features, wie dass nur die benötigten Änderungen bei der Replikation übertragen werden und die Replikation zudem zeitgesteuert erfolgen kann. Damit wird die Netzwerkbelastung stark minimiert, und Kosten werden gesenkt.

Replikationszeitplan

Für die Durchführung der Replikation sollten Sie sich überlegen, zu welchen Zeiten unbedingt stets aktuelle Verzeichnisdaten übertragen werden müssen. Dies wird normalerweise nur während der Arbeitszeiten der Fall sein. Idealerweise legen Sie die Replikationsverfügbarkeit so fest, dass die Replikation eine Stunde vor Beginn der Hauptarbeitszeit beginnt und bis zu einer Stunde danach noch durchgeführt wird. In den Nachtstunden sowie am Wochenende müssen Sie keine standortübergreifende Replikation durchführen, da zu diesen Zeiten niemand am Standort arbeitet, der die neuen Daten benötigt.

Replikationskosten

Zusätzlich zur Festlegung des Replikationszeitplans können auch die Replikationskosten konfiguriert werden. Hierzu ermitteln Sie alle vorhandenen Netzwerkverbindungen zwischen den Standorten und versehen die Standardverbindung mit einem bestimmten Wert. Alle Verbindungen, die kostengünstiger sind, werden mit einem niedrigeren Wert, die kostenintensiveren Verbindungen mit einem höheren Wert versehen. Es wird dann für die Replikation automatisch grundsätzlich die kostengünstigste verfügbare Verbindung benutzt.

Komplett geroutetes Netzwerk

Weiterhin müssen Sie analysieren, ob das Unternehmensnetzwerk komplett zwischen allen Standorten geroutet ist oder nicht. Verfügen Sie über ein komplett geroutetes Netzwerk, werden automatisch Standortverknüpfungsbrücken eingerichtet. Ansonsten müssen diese manuell konfiguriert werden. Standortverknüpfungsbrücken dienen der Redundanz der Netzwerkverbindungen. Wenn die Verbindung einer Standortverknüpfung ausfällt, kann nur über die in der Standortverknüpfungsbrücke konfigurierte alternative Route der Replikationsverkehr stattfinden. Die Standortverknüpfungsbrücken erhöhen somit die Fehlertoleranz zwischen Standorten.

Bridgehead-Server

Wenn Sie an einem Standort mehrere Domänencontroller verwenden, würden diese alle an der Replikation teilnehmen. Dieses Verhalten können Sie jedoch durch die Einrichtung eines Bridgehead-Servers umgehen. Dieser Server erhält primär sämtliche Replikationsdaten über die standortübergreifende Replikation und kann diese Daten dann standortintern an die übrigen Domänencontroller weitergeben. Bevor Sie einen Bridgehead-Server einrichten, müssen Sie klären, ob ein Domänencontroller am Standort eine ausreichende Bandbreite und Kapazität besitzt, um in dieser Rolle zu fungieren.

Sind die Standorte von einer Firewall umgeben, so muss in diesem Fall der Firewall-Proxy der bevorzugte Bridgehead-Server werden.

6.1.6 Gruppen und Gruppenrichtlinien

Bevor mit der Einrichtung von Gruppenrichtlinien begonnen wird, müssen Sie zuvor die Benutzer in logische Benutzergruppen strukturieren. Höchstwahrscheinlich sind die Benutzer bereits in der bestehenden Umgebung in Gruppen eingeteilt, sodass ein planerischer Neuaufbau hier wahrscheinlich entfällt.

Nach dem Implementieren von Benutzergruppen sind im nächsten Schritt für diese Gruppenrichtlinien festzulegen. Ein Vorteil bei der Implementierung von Gruppenrichtlinien ist gegeben, wenn bereits unter Windows NT mit Systemrichtlinien gearbeitet wurde. Die Gruppenrichtlinien unter Windows 2000/2003/XP sind zwar wesentlich komplexer als die NT-Systemrichtlinien, jedoch ist das logische Grundkonzept dasselbe.

Als Erstes ist zu bestimmen, auf welcher Ebene die Gruppenrichtlinien eingesetzt werden sollen: auf lokaler Ebene oder auf Ebene der Organisationseinheiten, Domänen bzw. Standorte. Die Richtlinien werden in dieser Reihenfolge abgearbeitet. Sollten sich dabei

Einstellungen widersprechen, so überschreibt die hierarchiehöhere jeweils die unteren. Ergeben sich keine Widersprüche, werden die Einstellungen addiert.

Für jede Ebene der Gruppenrichtlinien sollte weiter festgelegt werden, für welche Bereiche sie verwendet werden sollen. Sollen diese benutzer- und/oder computerbezogen eingesetzt werden? Werden auch Gruppenrichtlinien für Software- und/oder Windows-Einstellungen benutzt?

Fertigen Sie zur Veranschaulichung eine schematische Aufstellung aller zu implementierenden Richtlinien an und vermerken dabei folgende Punkte:

- ▶ Zweck der jeweiligen Richtlinie
- ▶ Wie weit reicht die Vererbung der Richtlinie? An welcher Stelle wird die Vererbung aus welchem Grund unterbrochen?
- ▶ Werden durch die Gruppenrichtlinien andere Richtlinien unterschrieben?
- ▶ Sind bestimmte Richtlinien zu deaktivieren? Wenn ja, aus welchem Grund?

Wenn Sie sich für den Einsatz von IntelliMirror entschlossen haben, müssen auch dafür die Zielgruppen definiert werden.

- ▶ Welche Benutzer und Benutzergruppen sollen welche Applikationen und Profile über die Softwareverteilungsfunktion von IntelliMirror erhalten?
- ▶ Auf welchen Servern sollen diese Applikationen bereitgestellt werden?
- ▶ Wie oft ist mit einer Softwareinstallation von neuen Applikationen bzw. bei der Systemwiederherstellung zu rechnen?

6.1.7 Sicherheit

Auch das Thema Sicherheit darf bei der Implementierung nicht außer Acht gelassen werden. Bevor Sie mit der Implementierung eines bestimmten Sicherheitskonzeptes beginnen, müssen Sie die Anforderungen an die Sicherheit festlegen. Sollen dazu die bisherigen Sicherheitsnormen beibehalten oder noch weiter verstärkt werden?

Prinzipiell können Sie zwei verschiedene Wege der Sicherheitsimplementierung beschreiten. In einer homogenen Windows 2000/XP/2003-Umgebung werden Sie die betriebssystemimmanenten Kerberos-Mechanismen verwenden. Über Kerberos können Sie die Benutzerauthentifizierung sowie den Zugriff auf die Ressourcen steuern.

Wollen Sie auch weitere Betriebssysteme wie etwa Novell oder Unix mit Windows 2000/2003 so kombinieren, dass allein über Active Directory die Anmeldung stattfindet und sämtliche Informationen nur aus dieser Verzeichnisdatenbank bezogen werden, müssen Sie auch mit den Sicherheitsprinzipien und -modellen der anderen Betriebssysteme vertraut sein, damit diese untereinander abgeglichen werden können. In diesem Fall werden Sie natürlich einen größeren Aufwand treiben müssen.

Gehören zu Ihrem Unternehmen einige Geschäftsbereiche oder Außenstellen, die zunächst oder auch gar nicht die Migration auf Active Directory planen, aber dennoch von ihrer NT-Domäne aus auf die internen Daten zugreifen müssen, können Sie etwa eine Vertrauensstellung zur NT-Domäne einrichten. An der Konfiguration und Aufrechterhaltung müssen jedoch die Administratoren beider Domänen immer zusammen-

arbeiten. Ein weiterer Ansatz wäre die Erstellung von Zertifizierungsstellen und die Verteilung von Zertifikaten an alle Personen, die auf die internen Daten und Ressourcen zugreifen müssen. Der Aufwand dafür ist davon abhängig, wie vielen Personen dieser Zugriff gewährt werden sollte.

Auch über eine Firewall können Sie die internen und externen Benutzer voneinander trennen. Hierzu können Sie zwei Domänen in einem getrennten Namensraum erstellen, z.B. *firma.de* für das interne und *firma.net* für das externe Netzwerk. Zwischen diesen beiden Domänen wird eine Firewall eingerichtet. So können Sie in jeder der beiden Domänen separate Berechtigungen setzen, es existieren keine automatischen Vertrauensstellungen und jede der Domänen kann ein eigenes Active Directory-Schema verwenden. Sollten es jedoch Anwendungen erfordern, auf Ressourcen jenseits der Firewall zugreifen zu müssen, muss sichergestellt sein, dass Ihnen nur diese Daten, aber keine anderen verfügbar gemacht werden. Auch hierfür liegt die Stärke in einem Verzeichnisdienst.

Die Windows 2000/2003-Sicherheit bezieht sich auf zwei verschiedene Bereiche. Zum einen wird über die Sicherheit festgelegt, wie der Benutzerzugriff auf das Netzwerk und die Daten und Ressourcen erfolgt. Der zweite Sicherheitsbereich beschreibt die Sicherheit der Daten, die zwischen den Clients und Servern durch das Netzwerk geschickt werden. Zur Durchsetzung dieser beiden Sicherheitsaspekte verfügt Windows 2000 und neuer über drei verschiedene Typen der Sicherheit. Dies sind:

- ▶ Kerberos
- ▶ PKI (Public Key Infrastructure)
- ▶ IPSec (IP Security)

Kerberos und PKI beziehen sich auf die Authentifizierung für den Ressourcenzugriff, während IPSec die Verschlüsselung der im Netzwerk gesendeten Daten gewährleistet.

Kerberos

Das Kerberos V5-Protokoll ist die Standardauthentifizierungsmethode unter Windows 2000/2003. Die Authentifizierung geschieht unter Kerberos durch den Austausch von Schlüsseln zwischen Client und Server oder zwei Servern. Für jede Sitzung wird ein symmetrisches geheimes Schlüsselpaar verwendet. Im Gegensatz zur NTLM-Authentifizierung unter Windows NT ist nun eine gegenseitige Authentifizierung zwischen Client und Server möglich. Vorher war der Client nicht in der Lage, den Server zu authentifizieren, an dem er sich angemeldet hat. Außerdem konnte die Authentifizierung unter NTLM nur über den Domänencontroller erfolgen. Kerberos bietet auch die Möglichkeit an, dass sich die Clients über Dateiserver oder Applikationen authentifizieren können. Ein weiterer Vorteil besteht darin, dass eine Kerberos-authentifizierte Sitzung auch zwischen einem Client und Server stattfinden kann, die verschiedenen Domänen angehören. Mit NTLM war dies nur möglich, wenn zwischen den beiden Domänen eine explizite Vertrauensstellung eingerichtet worden war. Innerhalb einer Windows 2000/2003-Gesamtstruktur wird dafür der so genannte Interdomänenschlüssel verwendet, da zwischen diesen Domänen automatisch eine Vertrauensstellung besteht. Auch weitere Domänen, zu denen Sie manuell eine explizite Vertrauensstellung eingerichtet haben, können Sie in das Kerberos-Modell mit einbeziehen.

PKI

Auch PKI (Public Key Infrastructure) ist zuständig für die Verschlüsselung von Daten und Authentifizierungen. PKI steht jedoch nicht in Konkurrenz zu Kerberos, sondern kann als Erweiterung der Kerberos-Dienste betrachtet werden. Im Gegensatz zu Kerberos arbeitet PKI jedoch mit nicht symmetrischen Schlüsseln. Jeder Authentifizierungspartner besitzt einen öffentlichen und einen privaten Schlüssel, die gemeinsam ein Schlüsselpaar bilden. Wenn zwei Computer Daten austauschen wollen, stellt der Sender dem Empfänger seinen öffentlichen Schlüssel bereit. Die Entschlüsselung erfolgt über den privaten Schlüssel. Der Vorteil gegenüber Kerberos besteht darin, dass nicht zuvor geheime Schlüssel ausgetauscht werden müssen und außerdem über die öffentlichen Schlüssel digitale Signaturen möglich sind. Diese Signatur ist mit dem privaten Schlüssel des Schlüsselpaars eines bestimmten Benutzers verschlüsselt. Der öffentliche Schlüssel kann ermitteln, ob die Signatur tatsächlich mit dem privaten Schlüssel erstellt wurde.

Der Austausch der Schlüssel kann auf verschiedene Arten erfolgen. So besteht erstens die traditionelle Möglichkeit, die Schlüssel von Hand beispielsweise auf Disketten auszutauschen. Zweitens haben Sie die Möglichkeit, die PKI-Schlüssel über das Windows-interne Kerberos-Verfahren auszutauschen. Die dritte Möglichkeit besteht darin, die Schlüssel über eine PKI-Struktur zu beziehen. Dies setzt jedoch eine bereits im Einsatz befindliche, ausgebaute PKI-Infrastruktur voraus. Alternativ dazu können die Schlüssel auch von einer unabhängigen öffentlichen Struktur bezogen werden. Ein Beispiel hierfür wäre Verisign. Weitere Informationen dazu finden Sie unter www.verisign.com.

Unter Kerberos fungiert das KDC (Key Distribution Center) als Instanz, der beide Seiten vertrauen, dass das gelieferte Dienstticket ordnungsgemäß ist. Da PKI öffentliche Schlüssel verwendet, muss als vertrauende Instanz analog zum KDC eine CA (Zertifizierungsstelle/Certificate Authority) eingerichtet werden. Diese CA liefert ein Zertifikat, mit dem die Authentizität des öffentlichen Schlüssels bescheinigt wird. Diese Prüfung und Ausgabe der Zertifikate geschieht über die Windows 2000/2003-Zertifikatsdienste. Die CAs können in verschiedenen Hierarchieebenen angelegt werden. Zwischen den einzelnen Zertifizierungsstellen gibt es übergeordnete und untergeordnete Beziehungen. Jeder Zertifizierungsstelle, die ein Zertifikat ausgibt, wird von der Stammzertifizierungsstelle vertraut. Somit kann jede andere Zertifizierungsstelle das Zertifikat prüfen, indem nur bei der Stammzertifizierungsstelle nachgefragt wird und nicht bei den möglicherweise zwischen den beiden liegenden Zertifizierungsstellen.

Zertifizierungsstellen können nach verschiedenen Aspekten im Unternehmen implementiert werden. So können diese Stellen analog zur Einteilung der Domänen auch nach funktionellen oder regionalen Aspekten eingerichtet werden. Besonders im letzten Fall kann die Implementierung von standorteigenen Zertifikatsstellen wichtig sein, wenn die Standorte über langsame Verbindungen miteinander verbunden sind. Sie haben eine Stammzertifizierungsstelle, die allen regional oder funktionell untergeordneten Stellen vertraut. Außerdem können Sie auch für verschiedene Aufgaben Zertifikatsstellen einrichten. So ist eine Stelle nur für Zertifikate innerhalb des Intranets zuständig, während eine andere nur für E-Mail-Zertifikate benutzt wird. Auch diese einzelnen Stellen vertrauen alle einer Stammzertifizierungsstelle.

IPSec

Die dritte Windows 2000 / 2003-Sicherheitskomponente ist IPSec (IP Security). Über IPSec werden die im Netzwerk versendeten Daten verschlüsselt. Dazu enthält jedes Paket einen Authentifizierungs-Header, mit dem der Sender vom Empfänger als der rechtmäßige Sender identifiziert werden kann, sowie eine kryptografische Checksumme, in der auch der Verschlüsselungsschlüssel integriert ist. Anhand dieser Checksumme kann der Empfänger erkennen, ob das Paket auf seinem Weg geändert worden ist. Das IPSec-Sicherheitsprotokoll ist unterhalb der Transportschicht im OSI-Referenzmodell angesiedelt. Damit wird es automatisch von den Anwendungen in den darüber liegenden Schichten übernommen. IPSec wird über die erweiterten Eigenschaften der LAN-Verbindung aktiviert oder deaktiviert. Standardmäßig ist IPSec deaktiviert. Für die Implementierung von IPSec-Richtlinien muss zunächst analysiert werden, für welchen Datenverkehr besondere Sicherheitsvorschriften zu implementieren sind. Beispielsweise können sämtliche Daten, die von Benutzern der Finanzabteilung gesendet werden, mit einer bestimmten Sicherheitsrichtlinie versehen werden. Diese Einstellungen werden über die entsprechende Sicherheits-mm in der Windows-Verwaltung vorgenommen.

In einer reinen Windows 2000-Umgebung ist Kerberos leicht zu implementieren. Auch andere Kerberos-Implementierungen in der Version 5, z.B. unter Unix, können mit Kerberos unter Windows 2000 kombiniert werden. Innerhalb einer Kerberos-Domäne kann sich sowohl ein Windows-Client an einem Nicht-Windows-KDC authentifizieren als auch ein Nicht-Windows-Client gegenüber einem Windows-KDC.

Verfügen Sie jedoch über mehrere Kerberos-Domänen, die nicht alle unter Windows 2000 agieren, wird die Implementierung wesentlich schwieriger. Die Sicherheitsprincipals wie Benutzer, Gruppen und Computer ohne Windows 2000 besitzen nicht die Daten zur Authentifizierung, die von Windows 2000 benötigt werden – auch dann nicht, wenn Sie explizite Vertrauensstellungen zwischen den Domänen eingerichtet haben. Sie müssten also jedem Windows 2000-externen Sicherheitsprincipal ein derartiges Principal im Active Directory zuweisen. Sollte es sich dabei aber um einige hundert oder noch mehr Objekte handeln, werden Sie von dieser Methode schnell ablassen. Sie sollten stattdessen in diesem Fall PKI implementieren. Auch für die Zugriffe externer Anwender sollten Sie eine Zertifizierungsstelle implementieren, die der Stammzertifizierungsstelle vertraut. Wenn Sie digitale Zertifikate für den E-Mail-Verkehr einsetzen möchten, müssen Sie ohnehin auf PKI zurückgreifen.

IPSec sollte nur für den Datenaustausch zwischen Computern verwendet werden, bei denen es wirklich notwendig ist, da die Implementierung von IPSec zusätzliche Netzwerklast verursacht. Sinnvoll ist die Implementierung meist nur beim Datenverkehr zwischen Computern verschiedener Subnetze sowie bei VPN-Verbindungen. Als Alternative zu IPSec sollten Sie aber auf jeden Fall den Einsatz einer Firewall in Betracht ziehen.

Generelles

Für die Implementierung der oben genannten Sicherheitstechnologien sind einige allgemein gültige Punkte zu überdenken:

Wenn Kerberos oder PKI eingesetzt werden sollen, muss sichergestellt sein, dass im gesamten Unternehmen flächendeckend eine Struktur vorhanden ist, über die die Anfor-

derungen durchgesetzt werden können. Dazu zählen beispielsweise Zertifizierungsstellen oder KDCs. Die Wahl der zu verwendenden Sicherheit kann, aber muss nicht auf der bereits vorhandenen Struktur basieren. Ist noch keine derartige Struktur implementiert, müssen die Standorte von Zertifikatsservern bestimmt sowie deren Sicherheit konfiguriert werden. In den Gruppenrichtlinien müssen neue Richtlinien für den clientseitigen Umgang mit den digitalen Zertifikaten sowie für die Bereitstellung und Erneuerung erstellt werden.

Auch durch die Vererbung von Sicherheitseinstellungen und -richtlinien können die Sicherheitsaspekte flexibel angewendet werden. Auf Zugriffsebene wird nun eine wesentlich feinere Vergabe von Berechtigungen ermöglicht. Durch die frei steuerbare Vererbung und Beschränkung der Vererbung der einzelnen Berechtigungen können Sie ein komplexes Sicherheitsmodell für Ressourcen entwickeln. Zusätzlich können über die umfangreichen Gruppenrichtlinien weitere Konfigurationen bezüglich der Sicherheit vorgenommen werden.

Ein weiterer Aspekt zum Thema Sicherheit ist der Einsatz des Encrypting File System (EFS). Der Implementierungsaufwand hierfür entfällt, da diese Komponente automatisch ins Betriebssystem eingebunden ist. Der Einsatz von EFS ist sowohl für hochsensible Daten auf lokalen Rechnern als auch bei Daten, die mobil über Laptops ausgetauscht werden, äußerst sinnvoll.

6.1.8 Hardware- und Netzwerkanforderungen

Als Nächstes müssen Sie die Hardwareanforderungen für den aktuellen Stand der Netzwerkkumgebung definieren. Für die Bestimmung der Hardwareanforderungen steht Ihnen bereits vor der Implementierung ein nützliches Active Directory-Support-Tool zur Verfügung, nämlich der Active Directory-Sizer (*ADSIZER*, siehe Kapitel 23.1.3). Mit diesem Programm ist es möglich zu bestimmen, wie viele Domänencontroller, globale Katalogserver und Bridgehead-Server in einem Netzwerk benötigt werden. Auch die Größe der Active Directory-Datenbank wird angegeben. Damit diese Daten berechnet werden können, müssen Sie einige Angaben machen z.B. über die Anzahl der Objekte, Anzahl der zusätzlichen Benutzerattribute, Anzahl der Windows 2000/XP- und übrigen Windows-Computer usw. Auch der mögliche Einsatz von Exchange 2000 wird berücksichtigt. Weiterhin können Sie hier Ihre Standortstruktur einfließen lassen. Zur Berechnung müssen Sie lediglich Angaben zur Prozessorleistung und -anzahl der gewünschten Domänencontroller vornehmen.

Um auch für künftige Expansionen gerüstet zu sein, können Sie mit dem *ADSIZER* auch höhere Werte angeben und überprüfen, ob die Hardwareausstattung der Server immer noch ausreichend ist.

Neben den Anforderungen an die Hardware müssen auch die Anforderungen für den Netzwerkverkehr festgelegt werden. Basierend auf den Informationen, die Sie bei der netzwerktechnischen Bestandsaufnahme gesammelt haben, muss nun entschieden werden, ob die vorhandenen Netzwerkressourcen ausreichend sind oder nicht. Auch hierbei muss stets an die mögliche Vergrößerung des Unternehmens gedacht werden, inwieweit die Ressourcen dann immer noch ausreichend sind.

Wichtig für die Einschätzung der Netzwerkkapazitäten ist selbstverständlich auch, welche Technologien von IntelliMirror genutzt werden sollen. Je mehr der IntelliMirror-Komponenten (Gruppenrichtlinien, Betriebssysteminstallation, Softwareverteilung sowie wandernde Benutzerprofile; Multi-Roaming und Multi-User-Konzepte) zum Einsatz kommen sollen, desto höher wird selbstverständlich die Belastung für das Netzwerk und für die Server. Dies gilt auch für den Einsatz von Applikationen, die serverbasiert arbeiten. Um die Auslastung abschätzen zu können, sollten Sie ermitteln, wie oft pro Client durchschnittlich eine Neuinstallation des Betriebssystems und der Applikationen erfolgt. Auch wenn Sie keine Softwareinstallationen über IntelliMirror, sondern über ein anderes Softwareverteilungstool vornehmen, so müssen Sie dessen benötigte Bandbreite ebenfalls in Ihre Berechnungen mit einbeziehen. Dies gilt selbstverständlich auch für die grundsätzliche Netzwerkauslastung durch DHCP- und DNS-Verkehr. Die größten Kapazitäten müssen jedoch für die Bereitstellung wandernder Benutzerprofile einkalkuliert werden, auch wenn nur geänderte Dateien zwischen Client und Server hin- und herkopiert werden, was bereits eine leichte Entlastung mit sich bringt.

6.1.9 Definition von Standards

Die Definition von Standards ist zwar nicht Inhalt eines Migrationsplans für Active Directory, sondern allgemein gültiger Natur. Die Schaffung einheitlicher Rahmenbedingungen und Standards trägt jedoch auch wesentlich zur Qualitätssicherung des Migrationsverfahrens bei. Sie helfen, sowohl unnötigen Ressourcenverbrauch, Administration und Entwicklung zu vermeiden, als auch bei einer einfacheren Handhabung der benutzten Komponenten. Dies bringt als Resultat weniger Fehlerquellen durch den Einsatz gleicher Methoden zum Administrieren unterschiedlicher Ressourcen.

Standards können im Rahmen der Migration für diverse Punkte definiert werden. Dies hat bereits in der Planungsphase mit dem Einsatz eines standardisierten Verfahrens zur Projektdurchführung begonnen. Neben diesen organisatorischen Standards sind natürlich auch auf technischer Ebene Standards definierbar. Die Standardisierung beginnt bei den Namenskonzepten für Domänen, Computer- und Benutzernamen. Sie geht weiter über die Schaffung von standardisierten Arbeitsplätzen bezüglich Hard- und Softwareausstattung für bestimmte Benutzer und Gruppen. Auch Testabläufe und deren Dokumentation werden durch die Testmatrix in einer bestimmten einzuhaltenden Form vorgegeben. Standardverfahren und -vorgehensweisen für den täglichen Betrieb können im Betriebsführungshandbuch vorgegeben werden. Selbst die Vorgehensweisen für den Support und das Helpdesk können nach einem festen Prinzip durchgeführt werden.

Konsequent durchgesetzte Standards erhöhen die Produktivität und Leistungsfähigkeit, während parallel dazu Kosten und Arbeitsaufwand reduziert werden.

6.1.10 Spätere Planungen

Im Rahmen des Architekturplans werden die wichtigsten zentralen Punkte für die Implementierung geklärt. Sicherlich ist diese Planung nicht unbedingt bindend und kann auch erweitert werden. Von einer Reduzierung der festzulegenden Punkte ist eher abzuraten. Der Bezug zum Gesamtprojekt darf bei zusätzlichen Planungen nicht aus dem Blickfeld geraten. Nur zu schnell kann das gesamte Vorhaben unnötig verschleppt

werden, wenn sich die Beteiligten in Kleinigkeiten verzetteln oder zu viele Änderungen auf einmal in das Projekt mit einbringen wollen.

Welche Planungen nun genau in die Kategorie gehören, die zusätzlich in den Architekturplan aufgenommen werden könnten, ist abhängig von den Bedürfnissen des Unternehmens. Dazu könnten beispielsweise Änderungen oder Erweiterungen des Active Directory-Schemas zählen. Auch das Implementieren einer Asset-Management-Funktion oder die sofortige Integration und Anpassung von Datenbanken oder anderen Applikationen für die Nutzung des Active Directory ist kein Standardfaktor beim Erstellen des Architekturplans. Sollte eine homogene Umgebung nicht sofort durchsetzbar sein (die Gründe dafür können vielfältig sein, z.B. Lizenzkosten, Portierungsschwierigkeiten von Applikationen auf Windows 2000/2003/XP), muss auch dieses Vorhaben zunächst zurückgestellt werden. Eine heterogene Umgebung kann jedoch auch das Endziel des Projekts bedeuten.

Sie sollten jedoch immer überlegen, wann die noch nicht berücksichtigten Punkte geplant werden sollten. Einerseits spricht für die Integration in den Architekturplan in der Designphase, dass auf einen Schlag sämtliche Planungen innerhalb des Gesamtkontextes abgeschlossen sind. Allerdings kann sich durch zusätzliche Planungen auch die Dauer der Designphase in die Länge ziehen. Zusätzlich wird auch die Testphase verlängert, da natürlich auch mehr Komponenten und Szenarien zu analysieren sind.

Andererseits spricht für spätere Planungen nach dem Abschluss des Migrationsprojekts, dass alle Beteiligten dann besser mit der Materie vertraut sind. Dies gilt sowohl in technischer Sicht als auch in der Projekterfahrung. Auch aus planerischen Fehlern und Schwächen des Gesamtprojekts haben die Beteiligten ihre Konsequenzen und Lehren gezogen. Weitere Planungen können aufgrund dieser Tatsachen zu einem späteren Zeitpunkt schneller und effektiver durchgeführt werden.

Ein weiterer Faktor für Aufgaben, die erst nach der Migration durchgeführt werden sollen, können auch zu hohe Kosten sein. Ist beispielsweise das jährliche Budget für den IT-Bereich durch den Erwerb neuer Client- und Serverlizenzen sowie möglicherweise auch Hardware ausgeschöpft, so müssen zwangsläufig weitere kostenträchtige Investitionen in das nächste Jahr verlagert werden. Ein gutes Beispiel wäre eine bereits vorhandene Datenbank, deren Daten mit dem Active Directory synchronisiert werden sollen, für die jedoch zunächst ein kostspieliges Update zur Active Directory-Kompatibilität zu erwerben oder zu entwickeln ist. Hier bietet sich die Alternative an, zunächst nur die gewünschten Datenbankfelder ins Active Directory einzupflegen, die Daten an sich aber erst nach dem Update der Datenbank einzufügen.

6.2 Die Migrations- und Koexistenzstrategie

Nachdem Sie nun im Architekturplan Konzepte entworfen haben, müssen Sie eine Migrationsstrategie auf Betriebssystemebene entwickeln. Nur in den seltensten Fällen, z.B. in einem kleinen Unternehmen, werden Sie zu einem bestimmten Zeitpunkt gleichzeitig sämtliche Clients und Server auf Windows 2000 oder XP migrieren.

In den meisten Fällen werden Sie in großen Unternehmen – zumindest vorübergehend – eine gemischte Umgebung aus Windows 2000 und Windows NT, Unix oder Novell betreiben. Diese heterogene Umgebung kann je nach Anforderungen des Unternehmens ein Teilziel oder möglicherweise auch das endgültige Ziel der Migration sein. Wenn beispielsweise in einem Windows NT-Umfeld die meisten Applikationen nicht im Active Directory lauffähig sind, so ist zuerst ein Plan für die Koexistenz und erst später ein Plan für die Migration der bestehenden Umgebung zu erstellen. Da sich der Migrationsprozess auch über einen längeren Zeitraum – in einem großen Unternehmen über Monate, wenn nicht noch länger – erstrecken kann, ist der Betrieb in einer heterogenen Umgebung denkbar, wenn Sie sukzessive Domänen von Windows NT ins Active Directory integrieren oder nach und nach alle Standorte auf Active Directory umstellen. Auch beim bisherigen Einsatz von Novells Verzeichnisdienst NDS oder dem Einsatz von Unix wird eine heterogene Umgebung meistens das Endziel sein. Auch wenn Microsoft mit Active Directory den alleinigen Standard für Verzeichnisdienste etablieren möchte, muss diese Vorherrschaft nicht zwangsläufig umgesetzt werden. Auch wenn das Unternehmen über eine Reihe von Unter-Geschäftseinheiten oder Filialen verfügt, ist zu entscheiden, ob diese alle gleichzeitig migrieren wollen oder erst die Durchführung der Migration im übergeordneten Unternehmen abgewartet werden soll. Wenn nicht alle Bereiche des Unternehmens zu einem bestimmten Zeitpunkt migrieren, muss für die noch nicht migrierten Bereiche ebenfalls eine Koexistenzstrategie erarbeitet werden, damit diesen auch weiterhin die Zusammenarbeit mit den bereits migrierten Unternehmensteilen möglich ist.

Neben der Entwicklung der Migrations- und / oder Koexistenzstrategie müssen auch die Werkzeuge und Programme ermittelt werden, die zur Durchsetzung dieses Ziels notwendig sind. Verschiedene Programme sind dabei in ihren Vor- und Nachteilen gegeneinander abzuwägen.

Bevor mit der detaillierten Planung der Migration begonnen wird, sind zuerst die Daten zu ermitteln, die in der zu migrierenden Umgebung vorhanden sind und die auch ins Active Directory übernommen und synchronisiert werden sollen. Dokumentieren Sie das bestehende Verzeichnis bezüglich Aufbau, Hierarchie und vorhandener Daten.

Im folgenden Kapitel wird auf die Koexistenzstrategien von Active Directory mit NetWare und Unix eingegangen. Die Koexistenz- und Migrationsstrategien für Windows NT werden in den beiden folgenden Kapiteln dargelegt.

6.2.1 Die Koexistenz mit Novell NetWare und Unix

Beim Einsatz einer heterogenen Umgebung sollten Sie bei der Auswahl der Standorte für die Server eine sorgfältige Planung vornehmen. Der bereits vorhandene Verzeichnisserver des NDS sowie der neue Server mit der Active Directory-Datenbank sollten möglichst so platziert werden, dass bei der ständigen Synchronisation der beiden Verzeichnisse keine unnötige Datenlast im Netzwerk entsteht.

Novell NetWare

Für die Koexistenz zwischen Active Directory und NDS ist die Richtung der Synchronisierung der beiden Verzeichnisse zu bestimmen. Ein Verzeichnis wird zum Besitzer der Daten, während das andere daraus die Daten bezieht. Soll langfristig Active Directory in einer homogenen Umgebung bestehen, so wird es von Anfang an das Stammverzeichnis, und die Synchronisierung findet nur unidirektional statt. Soll hingegen NDS längerfristig beibehalten oder von einem Geschäftsbereich dauerhaft eingesetzt werden, muss die Administration der NDS-Objekte geregelt werden. Der NDS-Administrator muss seine Objekte des NDS-Baums nun über die entsprechende Organisationseinheit im Active Directory pflegen. Dazu muss er für den entsprechenden Bereich Administrationsrechte erhalten.

Um eine bidirektionale Synchronisierung von NDS und Active Directory zu betreiben, ist der Einsatz eines Zusatzprogramms erforderlich. Microsoft bietet hierfür als Bestandteil der Services für Netware 5 die Microsoft Directory Synchronization Services (MSDSS) an. Auch Novell bietet ein Programm zur Synchronisierung der Verzeichnisse an. Dabei handelt es sich um DirXML. DirXML bietet Treiber für z.B. folgende Datenbanken, Applikationen und Verzeichnisse: Active Directory, NT-Domänen, Exchange 5.5, LDAP, NDS, GroupWise, Lotus Notes oder SAP HR. Weitere Hinweise zu diesem Programm finden Sie unter <http://www.novell.com/products/edirectory/dirxml/>.

In den meisten Unternehmen wird folgendes Windows NT- und NDS-Modell vorhanden sein: Windows NT wird ausschließlich als Anwendungsserver eingesetzt, während statt NT-Domänen die Verwaltung über NDS durchgeführt wird. Windows NT wird möglicherweise auch noch als Print-Server eingesetzt und ist als Clientbetriebssystem mit aufgesetztem NetWare-Client anzutreffen. Ab Windows 2000 bietet sich nun die Möglichkeit, statt des NDS alternativ das Active Directory einzusetzen. Für diese Konstellation bietet sich das Modell an, dass keine Migration der NDS-Server, sondern evtl. nur der Anwendungsserver erfolgt.

Wenn in Ihrem Unternehmen bereits der Novell Directory Service (NDS) erfolgreich und stabil ausgeführt wird, besteht an und für sich keine Notwendigkeit, von NDS auf Active Directory umzustellen. Eine Umstellung ist nur dann zwingend erforderlich, wenn Sie die Active Directory-Features wie Gruppenrichtlinien, IntelliMirror oder dynamisches DNS (DDNS) benutzen möchten. Eine Alternative zur zentralen Verwaltung und Softwareverteilung, wie sie über die Gruppenrichtlinien und IntelliMirror unter Windows 2000 erfolgen kann, bietet Novells Z.E.N. Works – wenn auch in eingeschränkterem Umfang. In NDS können Sie auch ohne Active Directory einen Windows 2000 Server als Anwendungsserver integrieren. Als Druck- und Dateiserver kann sowohl ein Windows 2000 Server als auch ein NetWare-Server betrieben werden. Bedenken Sie aber auch, dass Applikationen aus dem Microsoft BackOffice-Bereich verstärkt in Active Directory integriert werden und deshalb ein Active Directory voraussetzen und nicht unbedingt nativ mit NDS kompatibel sein werden. Hierzu zählt beispielsweise der Exchange Server 2000 und 2003. Eine Lösung hierfür wäre, die beiden Verzeichnisdienste Active Directory und NDS durch Synchronisierung parallel zu betreiben. Aufseiten der Clients können Sie einen NetWare-Client für Windows 9x, NT, 2000 und XP für die Zusammenarbeit mit NDS einsetzen.

Eine ausführliche englischsprachige Erklärung und Planungsanleitung zu NDS-Spezifikationen finden Sie im „NetWare to Windows 2000 Server Planning Migration Guide“ unter folgender Adresse:

<http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/netmigr.asp>

Unix

Auch wenn in Ihrem Unternehmen bereits serverseitig Unix eingesetzt wird, werden diese Server wohl in den wenigsten Fällen durch Windows ersetzt werden. Über die Windows Services for Unix (SFU) können Sie die beiden Betriebssysteme in einer heterogenen Umgebung betreiben.

Über SFU haben Sie die Möglichkeit, unidirektional Active Directory und NIS miteinander zu synchronisieren. Die im Active Directory erstellten Passwörter überschreiben dabei einseitig die Passwörter des NIS-Verzeichnisses. Um auch den NIS-Verzeichnis-Benutzern Änderungen des Passworts zu gestatten, muss die Applikation „yppaswd“ ausgeführt werden. Um Konten zu synchronisieren, muss auf dem Windows-Domänencontroller, auf dem SFU ausgeführt werden, die spezielle Gruppe „PasswordPropAllow“ eingerichtet werden.

6.2.2 Die Migrationsreihenfolge der Clients und Server

Im Zusammenhang mit der Migration aus einem Windows NT-Umfeld heraus stellt sich zunächst die Frage, ob erst die Clients oder erst die Server auf Windows 2000 oder XP migriert werden sollen. Prinzipiell sind beide Optionen technisch möglich.

Wenn Sie zunächst sämtliche Clients auf Windows 2000 oder XP migrieren und die Server unter Windows NT belassen, bieten die neuen Clients zunächst nur die Funktionalität der alten NT-Clients in einer Windows NT-Domäne. Erst mit der Migration der Server können die Clients ihren vollen Funktionsumfang ausspielen. Der vorübergehend eingeschränkte Funktionsumfang beeinträchtigt jedoch nicht die Arbeit an den Clients. Die Benutzer können sich so zunächst an ihr neues Betriebssystem an sich gewöhnen, z.B. die Bedienoberfläche, und werden erst später die Features ihrer neuen Clients wie z.B. die verbesserten Suchfunktionen kennen lernen. Bei einigen Clients kann es erforderlich sein, dass sie auch nach der Migration der Domänencontroller weiterhin unter Windows NT betrieben werden müssen. Dies kann der Fall sein, wenn z.B. unternehmenswichtige Anwendungen auf dem Client nicht unter Windows 2000 laufen oder einen nicht gerechtfertigten Anpassungs- und Kostenaufwand des Redesigns für die Funktion unter Windows 2000 oder XP erfordern würden. Nachdem Sie alle Clients auf Windows 2000 oder XP migriert haben, kann es jedoch zu Inkonsistenzen dieser Clients bezüglich der Gruppenrichtlinien kommen, wenn während der Servermigration ein Teil der Domänencontroller bereits unter Windows 2000 oder XP läuft, der andere Teil aber noch aus BDCs unter Windows NT besteht.

Eine Migration der Clients auf Windows 2000 ist von folgenden Betriebssystemen aus möglich: Windows 95, 98, 98SE, ME und NT Workstation 3.51 und 4.0. Eine direkte Migration von Windows 3.x oder Windows for Workgroups ist nicht möglich. In diesem Fall müssen Sie eine Neuinstallation durchführen. Auch bei Clients mit einem Unix/Linux- oder OS/2-Betriebssystem müssen Sie den Client komplett neu installieren.

Bei der Migration auf Windows 2000 oder XP können Sie ebenso gut zunächst auch die Server updaten, da Windows NT- oder 9x-Clients mit den aktualisierten Servern ohne Probleme zusammenarbeiten können. Allerdings sind die alten Clients nicht in der Lage, mit dem Multimaster-Domänenmodell von Active Directory zusammenzuarbeiten. Die Clients benutzen lediglich einen Domänencontroller wie ihren alten PDC z.B. zur Änderung von Kennwörtern. Sie haben die Möglichkeit, entweder einen neuen Server als Windows 2000/2003-Domänencontroller einzurichten oder den bestehenden NT-PDC auf Windows 2000/2003 zu migrieren. Verschiedene Modelle zur Migration der Server finden Sie im nächsten Kapitel. Für die Anmeldung können die alten Clients jeden beliebigen Windows 2000-Domänencontroller benutzen, ebenso wie im Windows NT-Domänenmodell jeder BDC zur Anmeldung benutzt werden konnte. Wenn Sie also zunächst die Server migrieren, zeigen die NT-Clients dasselbe Verhalten, das sie auch unter der Windows NT-Domäne gezeigt haben. Dies sollte damit für die Übergangszeit kein großes Problem darstellen. Für Windows 9x-Clients steht (wie auch für Windows NT) für die Übergangszeit der ADSI-Client bereit. Mit diesem speziellen Client können einige, aber nicht alle der Active Directory-Features auch für die alten Clients bereitgestellt werden. Es ist auch zu erwägen, ob die über den ADSI-Client bereitgestellten Active Directory-Features für Ihr Unternehmen nicht völlig ausreichend sind. In diesem Fall könnte ein beträchtlicher Teil der Kosten für die Client-Lizenzen für Windows 2000 oder XP eingespart werden. Lediglich die Lizenzkosten für die neuen Server-Betriebssysteme würden bei diesem Modell fällig werden.

Ein Update der Server können Sie ausführen, wenn Sie Windows NT 3.51 oder 4.0 Server einsetzen. Die Update-Möglichkeit gilt jedoch nur für einen Windows 2000/2003-Standard-Server. Das Update auf einen Advanced oder Datacenter Server ist nicht möglich. Ältere Serverversionen wie Windows NT 3.1 müssen komplett neu installiert werden.

6.2.3 Möglichkeiten einer heterogenen Windows-Umgebung

Nachdem Sie im vergangenen Kapitel erfahren haben, dass es prinzipiell egal ist, ob Sie zunächst die Server- oder die Clientseite aktualisieren, haben Sie aufseiten der Server verschiedene Optionen, wie und ob Sie die bestehenden Server mit Active Directory versorgen, und wenn ja, welche Server und in welcher Reihenfolge aktualisiert werden. Sie sehen verschiedene Szenarien, in denen Windows NT-PDCs und -BDCs und Anwendungsserver vorhanden sind.

Im Gegensatz zum unidirektionalen Synchronisationsmodell mit Unix werden Windows 2000/2003-DCs und NT-PDCs innerhalb derselben Domäne ihre Informationen bidirektional austauschen – solange sich die Domäne im gemischten Betriebsmodus befindet. Im einheitlichen Modus besteht kein Zugriff mehr für die NT-PDCs.

Modell 1: Erst Migration der Anwendungsserver, dann der Domänencontroller

Sie setzen Windows 2000/2003 zunächst nur als Anwendungsserver ein, während die Domänencontroller noch unter Windows NT betrieben werden. Die Anwendungsserver agieren als Stand-alone-Server unter Windows 2000/2003 ohne Active Directory. Sie sind performanter als die NT-Anwendungsserver. In der Zwischenzeit werden die bestehenden NT-Clients auf Windows 2000 oder XP aktualisiert, falls Sie dieses wünschen. So können Sie später jederzeit serverseitig Active Directory implementieren, da aufseiten der Clients alle Voraussetzungen erfüllt sind. Bis zu diesem Zeitpunkt können Sie die 2000- und XP-Clients in die Windows NT-Domänen platzieren, ebenso auch die Windows 2000/2003-Anwendungsserver. Nach der Migration der Server steht Ihnen dann der volle Funktionsumfang von Active Directory für die Clients und Anwendungsserver zur Verfügung.

Sind Sie dann an dem Punkt angekommen, an dem die Migration der Domänencontroller durchgeführt werden kann, müssen Sie zunächst den ursprünglichen NT-PDC migrieren. Sollten Sie in der Planungsphase bereits festgestellt haben, dass die Hardware des PDCs nicht mehr ausreichend ist, so muss ein leistungsfähigerer Server zum neuen ersten Domänencontroller des Active Directory werden. Außerdem haben Sie beim Einsatz eines neuen Rechners immer die Möglichkeit eines schnellen Fallbacks, falls sich mit dem neuen Windows-Server Probleme ergeben sollten. Sie können in diesem Fall immer noch auf den ehemaligen PDC zurückgreifen, der unter Windows NT einwandfrei gearbeitet hat. Sofern Sie den alten PDC migrieren, bleiben jedoch alle Vertrauensstellungen erhalten, die ursprünglich zwischen den NT-Domänen bestanden haben. Bei der Neuinstallation des Domänencontrollers müssen Sie diese Vertrauensstellungen alle manuell wieder herstellen.

Nachdem Sie nun den ersten Domänencontroller auf Windows 2000/2003 aktualisiert oder diesen Server neu eingerichtet haben, wird dieser zunächst im gemischten Modus betrieben. Sie haben also nun einen Domänencontroller unter Windows 2000/2003, die BDCs unter Windows NT sowie den Anwendungsserver und die Clients unter Windows 2000 oder XP. Im gemischten Modus bietet der Domänencontroller Abwärtskompatibilität mit früheren Windows-Versionen als Windows 2000. Er kann mit den NT-BDCs kommunizieren und auch mit Clients, die möglicherweise immer noch unter Windows NT betrieben werden. Selbst wenn einige Clients auch später unter NT oder 9x betrieben werden müssen oder lediglich über den ADSI-Client mit Grundfunktionen des Active Directory versehen werden, können Sie diese ins Active Directory integrieren, solange das Active Directory im gemischten Modus betrieben wird. Solange die Domäne im gemischten Modus betrieben wird, wird weiterhin das NetBIOS-Protokoll verwendet, die Authentifizierung erfolgt auch weiterhin über die NTLM-Authentifizierung anstatt über das Kerberos V5-Authentifizierungsprotokoll, das nur von Windows 2000/XP unterstützt wird, und es wird bei der Replikation der SAM der migrierte Windows 2000/2003-Domänencontroller als PDC angesehen oder ein anderer Domänencontroller unter Windows 2000/2003, der die Betriebsmasterrolle des PDC-Emulators ausführt.

Modell 2: Nur Migration der Domänencontroller, nicht der Anwendungsserver

Umgekehrt zu unserem ersten Beispiel kann auch Windows NT weiterhin als Anwendungsserver dienen, während die Clients auf Windows 2000 oder XP aktualisiert werden und danach auch die ursprünglichen PDCs und BDCs im Active Directory aufgehen. Zwar ist ein Windows 2000-Server als Anwendungsserver performanter als ein NT-Server, aber was nützt die bessere Performance, wenn die Anwendungen des Servers nicht unter Windows 2000 Server funktionieren? Klassische Beispiele sind der Systems Management Server bis zur Version 1.2 sowie auch der Vorgänger von Citrix MetaFrame, nämlich der Citrix WinFrame-Server. Hier würde das Update der entsprechenden Serverversionen einerseits einen hohen Kostenfaktor durch die neuen Lizenzen verursachen, andererseits auch sehr viel Zeit in Anspruch nehmen, um die bestehenden Server mit allen Einstellungen und Konfigurationen auf die neue Version zu migrieren. Sollten Sie sich entschließen, alte Anwendungen auf den Servern zu behalten, so müssen Sie lediglich die Domänencontroller auf Windows 2000 oder 2003 migrieren. Der Windows NT-Anwendungsserver kann aufgrund der Abwärtskompatibilität der neuen Domänencontroller im gemischten Modus in der Domäne betrieben werden. Auf ihn können gleichermaßen Windows NT-Clients wie auch Windows 2000/XP-Clients zugreifen.

6.3 Der Disaster Recovery-Plan

Während der Planung der Migration müssen Sie jedoch stets bedenken, dass dieser komplexe Prozess an einer beliebigen Stelle fehlschlagen kann. Dies kann sowohl bei der Aktualisierung der Clients als auch bei der Aktualisierung der Server oder im Zusammenspiel von bereits aktualisierten und noch nicht aktualisierten Rechnern geschehen. Für diesen Fall müssen Sie einen Disaster—Recovery-Planbereiten haben, damit Sie so schnell wie möglich den Fehler beheben können, bevor durch den Systemausfall oder mangelnde Funktionalitäten dem Unternehmen Ausfallkosten durch Unproduktivität entstehen.

Der Disaster Recovery-Plan muss spätestens beim Rollout des Piloten abgeschlossen sein. Sollte es in der Abteilung oder dem Standort des Piloten zu Problemen kommen, muss hier in jedem Fall möglichst rasch die Produktionsumgebung auf dem Level des Status quo wieder hergestellt werden.

Bei der Migration der Server ist es eine sinnvolle Möglichkeit, parallel zum bestehenden NT-PDC einen neuen Rechner als Windows 2000/2003-Domänencontroller einzurichten. Idealerweise hat dieser dieselbe IP-Adresse und denselben Hostnamen wie der alte PDC. So haben Sie die Möglichkeit, den neuen Domänencontroller anstelle des alten einzusetzen, wobei er von sämtlichen Clients wie der alte PDC gefunden wird. Treten nun mit dem neuen Domänencontroller Probleme auf, so können Sie wieder auf den alten PDC zurückgreifen und diesen weiter einsetzen, bis die Probleme an dem neuen Domänencontroller behoben sind. Würden Sie hingegen den alten PDC migrieren und während der Migration Probleme auftreten, so müssten Sie einen der NT-BDCs zum PDC heraufstufen, damit sich die Clients an der Domäne anmelden können. Während des Zeitraums der Heraufstufung ist für die Clients jedoch kein Domänencontroller verfügbar. Ein fliegender Wechsel zwischen dem alten und neuen Domänencontroller nimmt auf jeden Fall

weniger Zeit in Anspruch. Und außerdem stehen Sie weniger unter dem Zeitdruck, ein Problem auf die Schnelle lösen zu müssen, da Sie ja immer noch den alten PDC verwenden können.

Unabhängig davon, ob Sie nun einen neuen oder migrierten Domänencontroller einsetzen, so sollte dieser testweise zu Zeiten online geschaltet werden, zu denen nicht viele oder idealerweise keine Benutzer auf die Domäne zugreifen. Es wäre wenig sinnvoll, zur Hauptanmeldezeit am Morgen Experimente mit dem Domänencontroller durchzuführen.

Auch aufseiten der Clients müssen Sie Methoden definieren, wie diese möglichst schnell wieder auf den alten, noch funktionierenden Stand gebracht werden können. Wenn Sie bereits vor der Migration ein Verfahren zur Scratch-Installation und Softwareverteilung im Einsatz hatten, können die nach der Migration nicht funktionierenden Clients rasch wieder hergestellt werden. Dies gilt jedoch nur, wenn auch sichergestellt ist, dass die alten Clients mit dem neuen Domänencontroller zusammenarbeiten können. Verfügt Ihr Unternehmen über kein standardisiertes Verfahren zur Clientinstallation, müssen diese manuell wieder hergestellt werden. Bevor Sie jedoch darangehen, aufseiten des Clients wieder den Status quo herzustellen, muss ausgeschlossen sein, dass das Problem serverseitig zu suchen ist.

6.4 Betriebsführungskonzept und -handbuch

Eine weitere Aufgabe im Migrationsplan ist die Erstellung eines Betriebsführungskonzeptes und -handbuches. Das Konzept beschreibt den architektonischen Aufbau, die dafür benötigten Ressourcen (Personen, Hardware, Software usw.) und Verantwortlichkeiten. Das Handbuch wird im täglichen Betrieb eingesetzt und kann als Nachschlagewerk für die Administratoren betrachtet werden. Im Handbuch werden alle Schritte beschrieben, die in irgendeiner Form in der produktiven Umgebung notwendig werden können. Beide Dokumentationen müssen vor dem endgültigen Rollout fertig gestellt sein. Das Betriebsführungskonzept muss bei der Implementierung am Standort des Piloten seine Funktionstüchtigkeit beweisen. Dasselbe gilt auch für das Konzept. In beide Dokumentationen sollen jedoch alle Änderungen einfließen, die sich im Rahmen der Test- oder Pilotphase ergeben. Kein Unternehmen darf den Fehler begehen, diese Dokumentationen erst dann anzufertigen, wenn die Umgebung bereits produktiv eingesetzt wird. Aus den Implementierungsergebnissen darf nicht der Weg dazu hergeleitet werden.

Das Ziel der Dokumentationen besteht darin, die tägliche Arbeit am Active Directory zu optimieren und die Funktion aufrechtzuerhalten. Auch die Kosten können durch eine saubere Dokumentation der Active Directory-Unternehmensstruktur minimiert werden. Je detaillierter und präziser die Strukturen und Anweisungen zu einzelnen Arbeitsschritten beschrieben werden, desto effektiver können die Aufgaben im laufenden Betrieb durchgeführt werden.

6.4.1 Betriebsführungskonzept

Im Betriebsführungskonzept wird zunächst die Zieldefinition beschrieben. Weiterhin ist die Architektur des Active Directory zu dokumentieren. Darin spiegeln sich die Erfordernisse des Unternehmens für die Implementierung des Active Directory wider.

In einem nächsten Schritt sind die benötigten Ressourcen aufzuzählen. Dazu gehören Personen, Skill, Hardware, Software, Netzwerk, Räumlichkeiten, Disaster Recovery usw.

Auch die verantwortlichen Personen der verschiedenen Bereiche des Active Directory werden benannt und sollten bei Problemen zur Verfügung stehen. Eine Möglichkeit, dies übersichtlich zu gestalten, könnte z.B. das Erstellen einer Verantwortlichkeitsmatrix sein. Diese sollte die Implementierungsschritte bzw. Entscheidungen oder Events enthalten und sollte auf verschiedene Personen oder Funktionsgruppen verweisen. Etwa vorstellen könnte man sich zu einer bestimmten Entscheidung: *WER* ist verantwortlich auslösend, *WER* ist betroffen von diesem Punkt, *WER* muss informiert werden, weil es seinen Teilbereich betrifft, *WER* entscheidet über das weitere Vorgehen (wer also ist handlungsanweisend und befugt), *WER* ist für die Ausführung verantwortlich. Eine übersichtliche Tabelle der Beteiligten mit Ansprechpartnern und Erreichbarkeit ist sinnvoll.

6.4.2 Betriebsführungshandbuch

Das Betriebsführungshandbuch enthält alle technischen Details, die für die tägliche Arbeit am Active Directory benötigt werden. Angefangen von speziellen Einstellungen bei der Installation über die exakte Beschreibung von Backup-Routinen bis hin zu Automatisierungen, wie etwa dem Einsatz von Skripten, werden hier alle Schritte dokumentiert. Somit ist gewährleistet, dass der Betrieb z.B. auch beim Ausfall der eigentlich verantwortlichen Personen aufrechterhalten werden kann. Auch bei der Expansion des Unternehmens können die Administratoren bei der Implementierung auf das Gerüst der erforderlichen Aufgaben zurückgreifen. Die vollständige Transparenz der System- und Anwendungskonfiguration bildet die Grundlage für ein effektives Management des Systems und der darauf verfügbaren Anwendungen. Diese Transparenz muss durch die Dokumentationen im Betriebsführungshandbuch gewährleistet sein.

Das Betriebsführungshandbuch wird dabei für verschiedene Bereiche des Unternehmens unterschiedlich aussehen. So werden Sie für die Administratoren von Filialen, denen nur die eigene Organisationseinheit zur Verwaltung delegiert wurde, nicht eine Anleitung zur Implementierung von Domänen oder Standorten erhalten. Es müssen also mehrere angepasste Dokumentationen mit den jeweils relevanten Inhalten erstellt werden.

7 Die Testphase

Auch zwischen der Design- und Testphase muss eine klare Trennung vollzogen werden. Es kann nicht an einer Stelle bereits getestet werden, während man an anderer Stelle feststellt, dass der bereits im Test befindliche oder möglicherweise bereits fertig getestete Plan auf Probleme stößt und so nicht realisiert werden kann. Durch die klare Trennung sparen Sie sich Zeit und Kosten. Außerdem können Sie in Ihrem Testcenter praktische Vorführungen Ihres Projektfortschritts geben.

7.1 Design des Testcenters und Auswahl der Mitglieder des Testteams

Das Testcenter sollte – zumindest in großen Teilen – die produktive Umgebung Ihres Unternehmens widerspiegeln. Dies gilt für die Hard- und Software, Netzwerktechnisches sowie weitere Daten, wie z.B. Benutzerdatenbanken usw. Sie testen hier auf einer beschränkten Anzahl von Rechnern exemplarisch die Vorgehensweise der Implementierung von Active Directory. Dabei ist jedoch unbedingt darauf zu achten, dass das Testcenter entweder über ein physikalisch separates Netzwerk verfügt oder zumindest in einem vom produktiven Netzwerk separaten IP-Adressbereich betrieben wird.

Die Einrichtung des Testcenters beginnt mit der Bereitstellung einer geeigneten Räumlichkeit. Um dort exakt die Hardwarevoraussetzungen des Unternehmens abbilden zu können, sollten Sie für die Testserver und -clients identische bzw. vergleichbare (niedriger skalierte) Hardware bereitstellen. Sofern Sie standardisierte Hardware eines Herstellers einsetzen, minimiert sich der Aufwand für die zu testende Hardware. Verfügt Ihr Unternehmen über ein Konglomerat verschiedenster PC-Typen, ist zu entscheiden, welche für das Testcenter ausgewählt werden. Weiterhin müssen Sie analysieren, welche Rechner der speziellen Hardware für die Testzwecke benutzt werden sollen. Entweder bringen Sie Rechner ins Testcenter, die momentan im Unternehmen nicht benutzt werden, oder aber Sie müssen einige neue Geräte anschaffen.

In das Testcenter gehören alle Typen von Rechnern, die auch produktiv eingesetzt werden. Dazu zählen

- ▶ die Domänencontroller (unter NT der PDC und ein BDC),
- ▶ weitere Server wie Exchange-Server, Anwendungsserver usw., die ebenfalls migriert werden sollen,
- ▶ die Clients; werden Clients verschiedener Betriebssysteme eingesetzt, müssen Sie für jedes Client-Betriebssystem mindestens einen Testrechner bereitstellen;
- ▶ möglicherweise auch Server, die unter Novell Netware oder anderen Betriebssystemen betrieben werden, die in Koexistenz mit Active Directory betrieben werden sollen.

Sie sehen also, dass die Größe des Testcenters davon abhängig ist, wie viele verschiedene von der Migration betroffene Komponenten verwendet werden.

Um den Datenbestand Ihrer produktiven Umgebung ins Testcenter zu transferieren, richten Sie den Server, der im Testcenter als PDC dienen soll, in der produktiven Umgebung als zusätzlichen BDC ein. Sobald dieser die Daten als Replikat erhalten hat, wird er im Testcenter zum PDC heraufgestuft. Damit verfügen Sie über die realen Domänendaten des Unternehmens.

Weiterhin müssen auf allen Testrechnern die Applikationen installiert werden, die entweder auch migriert werden sollen oder deren Migrationsfähigkeit oder Active Directory-Kompatibilität geprüft werden soll.

Schwieriger als die Abbildung der vorhandenen Hard- und Software sowie der Datenbestände wird die Abbildung der Netzwerkstruktur. Die Netzwerktests sind auf den LAN-Bereich des Testcenters beschränkt. Aber weitere Komponenten wie Standleitungen oder RAS-Zugriffe können im Testcenter nicht analysiert werden. Diese Komponenten können erst in der realen Umgebung der Pilotphase mit einbezogen werden. Sie sollten im Testcenter jedoch nach Möglichkeit auch Router mit einbinden, um die Netzwerkbandbreite zu testen.

Neben der Bereitstellung von Hardware-Ressourcen müssen Sie auch die Zusammenstellung des Teams für das Testcenter überdenken. Die Größe des Teams variiert je nach Größe des Unternehmens. In jedem Fall müssen Sie eine Person benennen, die für die technische Durchführung zuständig ist. Von ihr wird zunächst die Testmatrix festgelegt und dann mit der Durchführung dieser Tests begonnen. Dieser Testverantwortliche muss eng mit dem Projektleiter zusammenarbeiten, wenn es um die Einhaltung von Zeitplänen oder anderen Vorgaben geht. In einem großen Unternehmen kann die Durchführung der Tests auch von mehreren Personen in speziellen Bereichen durchgeführt werden. So ist eine Person zuständig für netzwerkbezogene Tests, eine andere für applikationsbezogene usw. In jedem Fall muss bei den Mitgliedern des Testteams ein hoher technischer Skill vorhanden sein.

Wie Sie sehen, erfordert die Einrichtung des Testcenters zunächst ein hohes Maß an Zeit und Arbeitsaufwand. Dieser Aufwand ist aber gerechtfertigt, wenn Sie bedenken, wie viele technische und konzeptionelle Fehler in dieser ersten praktischen Phase der Migration noch aufgedeckt werden können, bevor diese ansonsten ohne Tests in die Produktionsumgebung übertragen werden würden.

7.2 Was wird getestet?

Im Testcenter wird das Testverfahren nach der Methode „deep and small“ durchgeführt: Dabei wird bei einer kleinen Anzahl von Testrechnern ein tief gehender Test diverser Funktionalitäten durchgeführt. Es geht beim Test mehr in die Tiefe als in die Breite. Das dazu gegenteilige Verfahren heißt „flat and wide“. Bei diesem Verfahren erfolgt ein Test gleich auf einer größeren Anzahl an Clients, bei diesen werden aber nur oberflächliche Tests durchgeführt. Dieses zweite Verfahren eignet sich für die Pilotphase, sobald im Testcenter kritische Einzeltests erfolgreich durchgeführt worden sind.

Die Tests beziehen sich auf unterschiedliche Bereiche. Zum einen müssen die Grundfunktionalitäten von Active Directory wie die Replikation, Verfügbarkeit oder Redundanz getestet werden. Zum anderen müssen auch applikationsspezifische Tests durchgeführt werden. Dazu zählt die Untersuchung der als Standard definierten Applikation dahingehend, ob diese problemlos unter Active Directory arbeiten, wie aufwändig ein Redesign dieser Applikation ist oder ob Konflikte zwischen einzelnen Applikationen vorliegen. Alle kritischen Unternehmensapplikationen und Daten müssen in der Testumgebung einwandfrei repliziert werden und arbeiten. Die einzelnen Applikationen müssen auf Softwarekonflikte, Versionskonflikte und Softwareabhängigkeiten hin untersucht werden.

Weiterhin sollten Sie auch die Applikationen testen, die Änderungen am Active Directory-Schema vornehmen. Sollten hierbei Probleme auftreten, muss das gesamte Active Directory neu installiert werden, da die Schemaänderungen nicht mehr rückgängig zu machen sind. Gerade derartige Problematiken, die eine Neuinstallation des Active Directory nach sich ziehen, sollten ausführlich untersucht werden, da weder in der Pilotphase noch nach dem endgültigen Rollout die Neuinstallation nicht erwünscht sein kann.

Nach der Implementierung von Active Directory sollten Sie zunächst normale administrative Aufgaben durchführen. Beginnen Sie zunächst mit simplen Vorgängen wie dem Hinzufügen oder Editieren von Objekten. Gehen Sie später dazu über, verschiedene Fehler zu provozieren. So sollten Sie die Redundanz der Active Directory-Informationen durch mutwilliges Zerstören von Elementen testen. Wie reagieren Clients auf Ausfälle der Domänencontroller? Auch die Einstellungen, Ergebnisse und Zeitpläne für die Replikation sind zu testen. Zusätzlich sollten Sie auch das Backup und Wiederherstellen von Active Directory testen. Machen Sie sich bereits zu diesem Zeitpunkt mit den Möglichkeiten der zahlreichen Active Directory-Support-Tools vertraut. Je besser Sie diese kennen gelernt haben, desto effektiver können diese später eingesetzt werden. Dasselbe gilt auch für den Einsatz von Skripten.

Nach Abschluss einer Testreihe kann mit einer genauen Dokumentation der Spezifizierungen dieser Erkenntnisse begonnen werden. Dabei werden die aufgetretenen Probleme und Lösungen beschrieben. Die verwendeten Methoden und Verfahren werden als Standardempfehlungen in das Betriebsführungshandbuch und -konzept aufgenommen.

7.3 Die Testmatrix

Bevor Sie Ihre Tests durchführen, sollten Sie eine Testmatrix entwerfen. In diese Matrix können Sie sämtliche Tests und deren Ergebnisse übersichtlich eintragen. Außerdem wird so auch schnell deutlich, wie sich z.B. Änderungen an einer Einstellung auf eine andere positiv oder negativ auswirken. In einer Testmatrix wird definiert, welche Kriterien oder Funktionalitäten und deren Parameter getestet werden, wie die minimalen und maximalen Grenzwerte für die Erfüllung des Kriteriums aussehen, wie das tatsächliche Testergebnis aussieht und wie dieses Ergebnis zu bewerten ist. Sie können so schnell sehen, welche Kriterien eindeutig erfüllt sind, welche verbesserungsbedürftig und welche eindeutig nicht erfüllt sind. Für die Erfüllung der Kriterien sollten Sie sich jeweils zwei Schwellwerte überlegen. Der erste Wert wird so gewählt, dass Sie einen Wert fest-

legen, bei dessen Erreichen das Kriterium als gerade eben erfüllt, aber noch nicht perfekt gilt. Ein zweiter Schwellenwert legt einen Wert fest, bei dessen Überschreiten das Kriterium als eindeutig erfüllt gilt. Diese Werte müssen Sie für jedes einzelne Kriterium festlegen, das Sie in Ihrem Testcenter analysieren möchten.

Die folgende Tabelle gibt Ihnen einen exemplarischen Vorschlag, wie eine Testmatrix aussehen könnte. Selbstverständlich müssen in ihr alle zu testenden Aspekte aufgenommen werden.

Zu testende Funktion	Oberer und unterer Grenzwert	Ist-Wert	Bewertung
Dauer der Client-anmeldung am Domänencontroller	Minimal fünf Sekunden, maximal zehn Sekunden	5,9 Sekunden	Bestanden
Auffinden eines Druckers in 10.000 AD-Objekten	Minimal drei Sekunden, maximal acht Sekunden	zehn Sekunden	Nicht bestanden

Tabelle 7.1: Vorschlag einer Testmatrix

Sie können auch noch zusätzliche Angaben wie das Datum oder eine Kurzbeschreibung des Tests hinzufügen. Je mehr Werte Sie in die Matrix aufnehmen, desto aussagekräftiger werden diese im Gesamtzusammenhang.

Die Kriterien, die eindeutig Ihre Anforderungen erfüllen, können Sie in Ihrer Matrix getrost abhaken und als erledigt ansehen. Wird eine Anforderung zum Teil erfüllt oder bleibt nur wenig hinter den Erfüllungskriterien zurück, so sollten Sie diese Punkte gesondert markieren. Oftmals kann schon eine kleine Konfigurationsänderung das Problem so weit beheben, dass das Kriterium als erfüllt angesehen werden kann. Mit Glück haben Sie durch die Änderungen an diesen Einstellungen im Zusammenspiel mit anderen bereits einige der bei weitem nicht erfüllten Anforderungen verbessert. Sollte sich die Lösung des Problems jedoch längerfristig verzögern, muss geklärt werden, ob sich durch die Überschreitung eines festen Termins eine Verzögerung im gesamten Projekt ergeben kann. Ist dies der Fall, sind alternative Maßnahmen zu ergreifen, wie das Problem behoben werden kann. Für die Planung alternativer Schritte sollten Sie ein (Krisen-)Meeting sämtlicher Teammitglieder einberufen. Bevor Sie jedoch nicht alle Ergebnisse, die als inakzeptabel gelten, zumindest auf einen akzeptablen, wenn nicht idealerweise sogar auf einen Level der 100%igen Anforderungserfüllung gehoben haben, darf die Testphase nicht abgeschlossen werden.

Eigentlich sollte es überflüssig zu erwähnen sein, aber dennoch sollte nicht der Fehler begangen werden, dass aus Mangel an Zeit, wegen Kosten oder aus Bequemlichkeit die Erfüllungskriterien den Testergebnissen angepasst werden. Es darf nur dann ein Erfüllungskriterium herabgesetzt werden, wenn sich keine Probleme im Zusammenspiel mit anderen Tests ergeben oder Sie fälschlicherweise ein Kriterium anfangs als zu hoch angesetzt haben, das in dieser Form niemals erfüllt werden kann. Ansonsten müssen Sie so lange Änderungen vornehmen oder Verbesserungen an Hardware oder Netzwerk vornehmen, bis alle Anforderungen erfüllt sind.

8 Rollout und Migrationsabschluss

Nach Abschluss aller Tests kann der Rollout beginnen. Zunächst wird der Rollout an einem Piloten getestet. Die Pilotphase entspricht einer weiter ausgedehnten Testphase, in der bereits grundlegende Probleme behoben sein sollten, aber noch nicht solche der Implementierung an sich. Oberstes Ziel muss es sein, den laufenden Betrieb des Piloten durch die Einführung von Active Directory nicht zu beeinflussen. Dennoch muss den Pilotbenutzern klar gemacht werden, dass dies nicht 100%ig auszuschließen ist. Bei dem Rollout spielt es keine Rolle, ob Sie als Ziel die Einführung eines reinen Active Directory oder eine temporäre bzw. dauerhafte Koexistenz von Active Directory mit einem anderen Netzwerkbetriebssystem definiert haben. Die Rollout-Phase ist damit in zwei Schritte geteilt: den Rollout des Piloten und den endgültigen Rollout im gesamten Unternehmen.

8.1 Der Rollout des Piloten

In der Pilotphase wird an einem Standort oder einer Abteilung die Implementierung von Active Directory vorgenommen. Der Pilot für den Rollout muss bereits in der Testphase bestimmt werden. Wählen Sie idealerweise einen Standort oder eine Abteilung als Piloten aus, der die folgenden Kriterien erfüllt:

- ▶ Technisch versiertes Personal, das für Änderungen offen ist.
- ▶ Gute Erreichbarkeit, falls Fragen vor Ort geklärt werden müssen.
- ▶ Der Standort oder die Abteilung sollte nicht zu klein, aber auch nicht zu groß sein.

Nach der Implementierung von Active Directory am Piloten müssen dort alle Arbeiten und Aufgaben wie gewohnt durchgeführt werden. Bei der täglichen Arbeit werden mögliche Probleme schneller offenkundig werden als bei willkürlichen Tests und Versuchen. Bedenken Sie: Für das ausgiebige Testen steht Ihnen das Testcenter zur Verfügung.

Treten in der produktiven Umgebung zahlreiche schwerwiegende Fehler und Probleme auf, sollten Sie diese dokumentieren und in Ihrer Testumgebung nachstellen. Sie müssen einschätzen, wie lange es dauern wird, bis das Problem behoben ist. Sollte die Lösung des Problems einen längeren Zeitraum in Anspruch nehmen, müssen Sie für den Piloten auf den allgemeinen Disaster Recovery Plan zurückgreifen können, um den alten Zustand schnellstmöglich wiederherzustellen und den Angestellten ein störungsfreies Arbeiten zu ermöglichen.

Jeder Fehler – auch ein zunächst unbedeutend erscheinender – muss nochmals im Testcenter überprüft werden, sofern sich die Lösung nicht im laufenden Betrieb verwirklichen lässt.

Die Pilotphase wird von den Personen begleitet, die bereits in der Testphase praktische Erfahrungen mit der Arbeit am Active Directory gesammelt haben. Außerdem besteht auch ein enger Kontakt mit dem Testcenter, da dort jederzeit am Piloten auftretende Fehler analysiert werden müssen. Den Benutzern muss klar gemacht werden, dass ihnen dieses Team für die Lösung von Problemen zur Seite steht. Während der Pilotphase muss der für die Endbenutzer und die Administratoren erarbeitete Schulungsplan an diesen Gruppen getestet werden. Zum Abschluss der Pilotphase muss ferner ein Verfahren für die Anforderungen an den technischen Support erarbeitet sein.

Die Migration und die Anweisungen für den täglichen Betrieb des Active Directory basieren auf den Erkenntnissen des Betriebsführungshandbuchs, das während der Testphase erstellt wurde. Hier muss diese Dokumentation die erste praktische Probe bestehen. Sollten sich hierbei Probleme ergeben, so muss das Betriebsführungshandbuch entsprechend angepasst werden. Die in der Pilotphase ermittelten Erkenntnisse sind allgemein gültig für den späteren kompletten Rollout.

Die definierte Dauer der Pilotphase ist abhängig vom Umfang und der Komplexität des architektonischen Entwurfs. Im Idealfall ist innerhalb des Zeitrahmens die Implementierung erfolgt und sind alle Fehler behoben. Sollte dies nicht der Fall sein und können die Probleme auch nicht im Testcenter behoben werden, so muss der Architektur- und Implementierungsplan geändert werden. Dies verzögert zwar mit Sicherheit den festgelegten Zeitplan, kann aber unter Umständen die einzige Möglichkeit sein, dass das Gesamtprojekt erfolgreich durchgeführt werden kann.

Nach Ablauf der Testphase am Piloten beginnt der endgültige Rollout auf alle übrigen Abteilungen und Standorte des Unternehmens.

8.2 Der endgültige Rollout

Der endgültige Rollout gleicht der Arbeitsweise am Piloten. Der einzige Unterschied besteht darin, dass die Implementierung nun in einem größeren Rahmen stattfindet. Hier zeigt sich, wie gut Sie in der Planung vorgesorgt haben und alle erforderlichen Ressourcen bereitgestellt worden sind. Dazu zählen neue Hardware, geänderte oder verbesserte Netzwerke sowie die Schulungspläne für die Administratoren und Endbenutzer. Gegebenenfalls werden hier nun auch die Änderungen am Architekturplan umgesetzt, die sich während der Implementierung des Piloten ergeben haben. Auf den erstellten Disaster Recovery-Plan sollte dabei hoffentlich nicht zurückgegriffen werden müssen.

Ein weiterer Unterschied und gleichzeitig eine neue Herausforderung liegt nun darin, dass Probleme überall gestreut auftreten können. Dies stellt hohe Ansprüche an den technischen Support und die Administratoren. Weiterhin muss klargestellt sein, dass bei Problemen nun nicht mehr ein ständiger Austausch mit dem Testcenter stattfinden wird.

Je nach Implementierungsplan werden entweder alle Standorte aktualisiert, oder aber einzelne Unternehmensbereiche nehmen noch nicht sofort an der Migration teil. Hierbei ist zu testen, ob die noch nicht migrierten Standorte auch weiterhin die Möglichkeit haben, fehlerfrei mit den bereits aktualisierten zusammenzuarbeiten.

Mit dem endgültigen Rollout ist die Implementierung abgeschlossen. Damit ist auch das Gesamtprojekt Active Directory zu einem hoffentlich erfolgreichen Abschluss gekommen. Nach der erfolgreichen Migration liegt die Hauptaufgabe nun in der Aufrechterhaltung und Optimierung des laufenden Betriebs.

8.3 Der Migrationsabschluss

Nach der Migration sollten Sie eine Verzeichnisstruktur implementiert haben, die für die nächsten Jahre Bestand hat und keinen großen Änderungen unterworfen wird. Dennoch werden Sie nicht umhinkommen, im laufenden Betrieb immer wieder kleinere Änderungen durchzuführen. Die Flexibilität muss gegeben sein, sodass Ihre IT-Infrastruktur auf ein Wachstum des Unternehmens reagieren kann, z.B. durch die Einbindung weiterer Standorte und neuer Domänen oder Organisationseinheiten. Diese Aufgaben nach der Implementierung von Active Directory werden von verschiedenen Personen oder Personengruppen durchgeführt.

Eine zentrale Aufgabe ist die Stabilitätspflege des Active Directory. Dazu zählen Aufgaben wie das Hinzufügen, Bearbeiten und Löschen von Objekten, die Durchführung von Sicherungen, die Leistungsprüfung sowie das Umsetzen von Änderungen am Active Directory. Als Faustregel kann man empfehlen, dass pro 1500 Benutzer ein Administrator mit den eben genannten Verwaltungsaufgaben betraut werden sollte.

Eine weitere Person muss für die Gliederung und Struktur des Active Directory zuständig sein. Bei der Expansion des Unternehmens oder anderen betriebswirtschaftlich bedingten Änderungen muss die Struktur erweitert oder in anderer Weise geändert werden. Für die Planung dieser Änderungen sollte nur eine Person oder eine kleine Gruppe zuständig sein. Die Änderungen, die vom Strukturverantwortlichen festgelegt worden sind, werden nach dessen Vorgabe von den Administratoren umgesetzt.

Eine zusätzliche Aufgabe besteht in der Anwendungsentwicklung unter Active Directory. Ein Anwendungsentwickler hat die Aufgabe, die Informationen des Active Directory, die für die Administratoren oder Endbenutzer relevant sind, in Form von einer Anwendung bereitzustellen. Damit wird sichergestellt, dass die Verzeichnisdatenbank auch als die zentrale Informationsquelle genutzt wird. Auch beim parallelen Einsatz von verschiedenen Verzeichnisdiensten ist er gefragt, um die Informationen für entsprechende Benutzergruppen zusammenzustellen. Wichtige Anforderungen könnten z.B. ein beschränkter Zugriff auf bestimmte Bereiche der Datenbank oder eine Suche nach Informationen anhand beliebiger Datenbankfelder sein. Die Anzahl der Anwendungsentwickler ist weitgehend abhängig davon, wie viele selbst geschriebene Anwendungen benötigt werden, nicht jedoch unbedingt von der Größe des Unternehmens.

Das Betriebsführungshandbuch steht zum Nachlesen für wichtige Routinen der täglichen Arbeit den Administratoren zur Verfügung. Je präziser die Angaben dort sind, desto besser kann der Administrator eigenständig seine ihm zugeteilten Aufgaben durchführen.

Teil C – Praxis

Über diesen Teil

Dieser praxisorientierte Teil ist das Kernstück des Buches. Er wendet sich in erster Linie an Administratoren, die täglich am Active Directory arbeiten. Grundlage für das Verständnis dieses Teils ist Teil A dieses Buches. Hier werden technische Anleitungen und Hintergründe sowie praktische Beispiele geliefert. Die Thematik ist breit gefächert und beginnt bei der Installation, reicht über komplexe Themen wie die Beschreibung von DNS, der Funktionsweise von Gruppenrichtlinien oder des Replikationsablaufs bis hin zu Spezialthemen wie die Implementierung von Active Directory und Unix, der Einsatz von Metadirectory Services, der Konfiguration von Firewalls im Zusammenspiel mit Active Directory, der Sicherheit im Active Directory oder ADSI-Skripten.

Von besonderem Wert ist auch das separate umfangreiche Kapitel über die Windows 2000/2003-Support-Tools. Diese oftmals unbeachteten Programme bieten zahlreiche Möglichkeiten für die Konfiguration, Administration und Fehleranalyse im Zusammenhang mit Active Directory. Diese kostenlosen „Bordmittel“ sollten immer zuerst eingesetzt werden, wenn Probleme auftreten.

Hilfreich sind in diesem Zusammenhang auch die Checklisten und Fehlerszenarien, die zu verschiedenen Thematiken wie DNS, Gruppenrichtlinien oder Replikation direkte Hinweise auf die Probleme sowie deren Lösungsansätze liefern. Dasselbe gilt für zahlreiche Tipps und Tricks, mit denen ein Administrator sich die tägliche Arbeit erleichtern kann. Anhand expliziter und leicht verständlicher Anleitungen und Beispiele gewinnt der Leser schnell Sicherheit in den komplexen Thematiken und kann die gewonnenen Kenntnisse schnell in seinem eigenen Umfeld einsetzen.

Der Leser findet in diesem Teil an vielen Stellen auch Hinweise zu weiteren Informationen oder Artikeln aus der Microsoft Knowledge Base oder der MSDN-Datenbank, um sein Wissen noch weiter zu vertiefen. Dasselbe gilt für einige Programme und Applikationen – sowohl von Microsoft als auch von Drittanbietern –, die für die Administration des Active Directory empfehlenswert sind oder die sogar den Funktionsumfang erweitern.

9 Installation

In diesem Kapitel lernen Sie zunächst exemplarisch Schritt für Schritt die Installation von Active Directory auf einem Windows 2000 und 2003 Server kennen. Auch die Deinstallation von Active Directory einschließlich der damit verbundenen Konsequenzen wird beschrieben. Zum Schluss erhalten Sie eine Checkliste, die bei der Installation zusätzlicher Domänencontroller in einer Domäne zu prüfen ist, sowie eine Anleitung zur Vorbereitung der Domäne, wenn in diese Windows Server 2003 integriert werden sollen.



Vor der Installation des Active Directory müssen Sie sicherstellen, dass der Domänencontroller über eine aktive LAN-Verbindung verfügt. Andernfalls erhalten Sie die Fehlermeldung „Das Netzlaufwerk ist nicht erreichbar. Weitere Informationen über die Behebung von Netzwerkproblemen finden Sie in der Windows-Hilfe“. Soll der Domänencontroller zum Zeitpunkt der Installation nicht in ein Netzwerk integriert sein, so müssen Sie den Microsoft Loopback-Adapter als NIC installieren.

9.1 Starten des Installationsassistenten

Sie starten den Installationsassistenten unter Windows Server 2003 über VERWALTUNG / SERVERKONFIGURATIONS-ASSISTENT und dort über die Schaltfläche WEITER oder über die SERVERVERWALTUNG und dort über den Link FUNKTION HINZUFÜGEN ODER ENTFERNEN. Unter Windows 2000 Server können Sie PROGRAMME / VERWALTUNG / KONFIGURATION DES SERVERS auswählen. Wählen Sie dort in der linken Fensterhälfte den Eintrag ACTIVE DIRECTORY und klicken auf den Link STARTEN DES ASSISTENTEN FÜR ACTIVE DIRECTORY. Alternativ dazu können Sie auch unter beiden Windows-Versionen an der Eingabeaufforderung DCPROMO aufrufen.

Vorbereitungen unter Windows Server 2003

Nach dem Start des Serverkonfigurations-Assistenten erhalten Sie als Erstes das Fenster ACTIVE DIRECTORY-DOMÄNENNAME. Hier legen Sie den DNS-Namen für die neue Domänen- bzw. Gesamtstruktur fest. Standardmäßig wird die Top-Level-Domain (TLD) .local vorgeschlagen. Da es sich hierbei um einen internen Namensraum handelt, besteht kein Konfliktpotenzial mit im Internet registrierten identischen Namensräumen. Sie können diese TLD beibehalten oder eine anders lautende Domäne anlegen, z.B. .de.

Im nächsten Fenster wird der NetBIOS-Name angegeben. Dieser wird automatisch aus der DNS-Namensgebung hergeleitet, in unserem Fall also FIRMA. Dieser Name kann jedoch auch geändert werden.

Sie sehen nun eine Zusammenfassung der durchzuführenden Schritte. Klicken Sie auf WEITER, und bestätigen Sie mit OK, dass der Server während des Installationsvorgangs neu gestartet wird.

Sofern der Server vorher noch nicht als DNS- und DHCP-Server eingerichtet war, erfolgt jetzt auch die Installation und Konfiguration dieser Komponenten. Nach dem automatischen Neustart klicken Sie im Serverkonfigurations-Assistenten auf FERTIG STELLEN. Sie können nun den Installationsassistenten DCPROMO aufrufen.

9.2 Die Active Directory-Installation

Im Folgenden werden die verschiedenen Optionen und Auswahlmöglichkeiten beschrieben, die Sie bei der Active Directory-Installation treffen können.

9.2.1 Die Installation einer neuen Domäne

In unserem Beispiel wird ein neuer Domänencontroller für die Domäne *firma.de* in einer neuen Struktur eingerichtet. Es wird dabei der Installationsassistent unter Windows Server 2003 beschrieben. Unter Windows 2000 sind ähnliche Schritte erforderlich.

1. Als Erstes starten Sie den Installationsassistenten über DCPROMO. Nach dem Begrüßungsbildschirm des Installationsassistenten erhalten Sie einen Hinweis, dass ein Domänencontroller unter Windows Server 2003 mit Sicherheitseinstellungen arbeitet, die eine Kommunikation mit Clients unter Windows 95 und NT 4.0 vor Servicepack 4 unmöglich machen. (siehe Abbildung 9.1). Klicken Sie dann auf WEITER.



Abbildung 9.1: Hinweis zur Betriebssystemkompatibilität bei der Active Directory-Installation

2. Sie werden nun aufgefordert, den Typ des zu installierenden Domänencontrollers zu bestimmen. Sie müssen entscheiden, ob es sich um den Domänencontroller für eine neu einzurichtende Domäne handelt oder ob Sie für eine bereits bestehende Domäne einen zusätzlichen Domänencontroller einrichten möchten (siehe Abbildung 9.2). Beim Hinzufügen eines weiteren Domänencontrollers zu einer bestehenden Domäne spricht man auch vom Peer-Domänencontroller. Die Peer-Domänencontroller dienen der Redundanz im Netzwerk und können die Auslastung des bereits bestehenden Domänencontrollers minimieren. Dieser Vorgang wird in Kapitel 9.2.4 beschrieben. Klicken Sie dann auf WEITER.



Abbildung 9.2: Auswahl des Domänencontroller-Typs

3. Im Fenster NEUE DOMÄNENSTRUKTUR ERSTELLEN (siehe Abbildung 9.3) müssen Sie festlegen, ob Sie eine Domäne in einer neuen Gesamtstruktur, eine neue untergeordnete Domäne in einer bereits vorhandenen Domänenstruktur oder vorhandenen Gesamtstruktur erstellen möchten. Zur Installation des ersten Domänencontrollers einer neuen Gesamtstruktur wählen Sie die erste Option. Wenn Sie bereits über eine Domänenstruktur verfügen und einer bestehenden Domänen- oder Gesamtstruktur eine neue untergeordnete Domäne hinzufügen möchten, wählen Sie die zweite bzw. dritte Option. Dies wäre erforderlich, wenn Sie beispielsweise der bereits vorhandenen Domäne *firma.de* eine untergeordnete Domäne *vertrieb.firma.de* hinzufügen möchten. Die Option UNTERGEORDNETE DOMÄNE IN EINER BESTEHENDEN DOMÄNENSTRUKTUR wird in Kapitel 9.2.2 beschrieben, die Option DOMÄNENSTRUKTUR IN EINER BESTEHENDEN GESAMTSTRUKTUR in Kapitel 9.2.3. Klicken Sie dann auf WEITER.

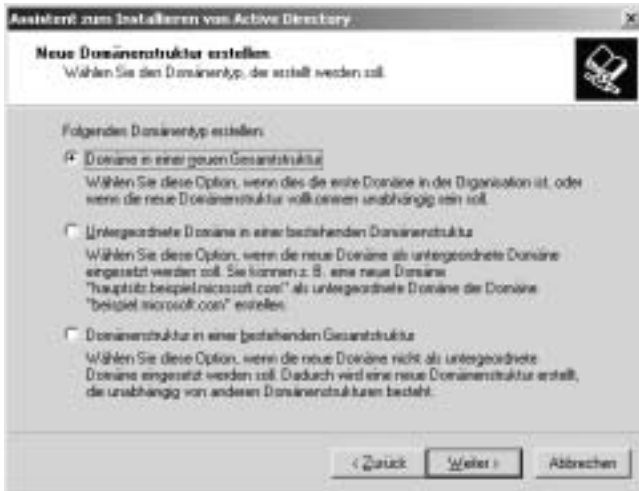


Abbildung 9.3: Auswahl des zu installierenden Domänentyps

4. Im Feld VOLLSTÄNDIGER DNS-NAMEN FÜR DIE NEUE DOMÄNE geben Sie den DNS-Namen für die neue Domäne an (siehe Abbildung 9.4). Der Name muss in dem Format (DC).DC.DC angegeben werden, in unserem Beispiel also *firma.de*. Für den DNS-Namen können nur die folgenden Zeichen benutzt werden: A bis Z, a bis z, 0 bis 9 sowie - (Bindestrich). Geben Sie in das Textfeld hingegen nur den NetBIOS-Namen (hier also FIRMA) ein, erhalten Sie einen Hinweis, dass die Namenskonvention nicht eingehalten wurde. Andernfalls würde der Name der Domäne *firma.* lauten. Sofern es sich um die erste Domäne einer neuen Gesamtstruktur handelt, wird diese automatisch zur Stammdomäne der Gesamtstruktur. Klicken Sie dann auf WEITER.

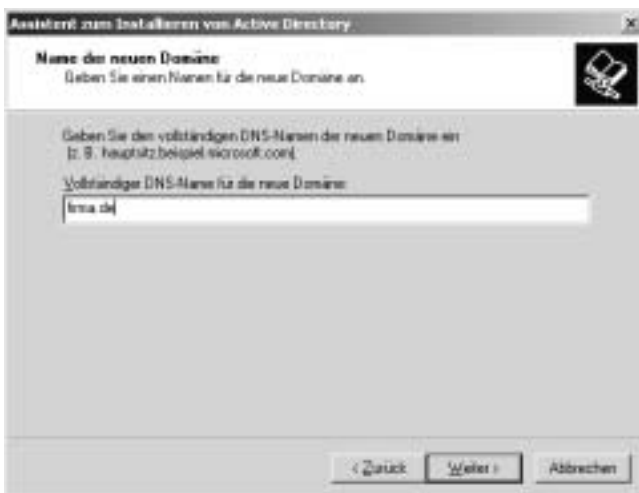


Abbildung 9.4: Den DNS-Namen für die neue Domäne bestimmen

5. Im Fenster NetBIOS-Domänenname geben Sie den NetBIOS-Namen an (siehe Abbildung 9.5). Dieser ist für die Kommunikation sämtlicher nicht-DNS-fähiger Clients notwendig. Klicken Sie dann auf WEITER.

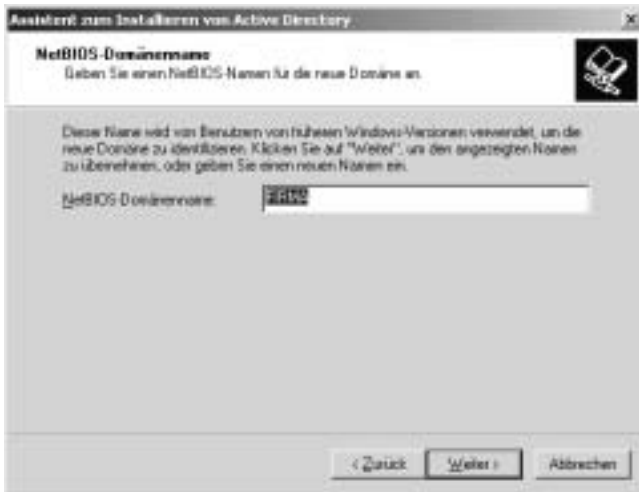


Abbildung 9.5: Den NetBIOS-Namen für die neue Domäne bestimmen

6. Im Fenster DATENBANK UND PROTOKOLLORDNER sind die Pfadangaben für die Active Directory-Datenbank *NTDS.DIT* sowie die Protokolldatei festzulegen (siehe Abbildung 9.6). Der vorgeschlagene Pfad lautet %SYSTEMROOT%\NTDS. Die beiden Pfade können jedoch beliebig geändert werden.

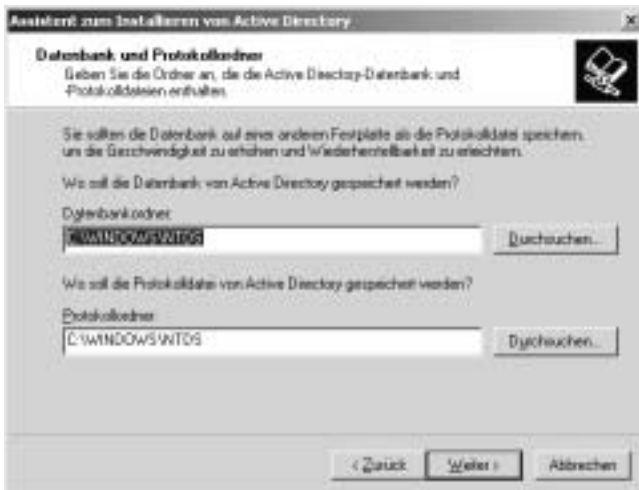


Abbildung 9.6: Festlegen des Speicherorts für die Datenbankdatei *NTDS.DIT*

Eine bessere Leistung wird erzielt, wenn Sie die Datenbank und die Protokolldateien auf zwei verschiedenen Festplatten speichern. Die Datenbank selbst sollte sich nicht auf demselben Laufwerk befinden wie das Betriebssystem selbst. Die Datenbank muss

sich auf einem NTFS-Laufwerk befinden, die Installation auf einem FAT-Laufwerk ist nicht möglich. Die Datenbank stellt das Verzeichnis für die neue Domäne dar. Für die Installation der Active Directory-Datenbank wird ca. 40 MB Speicherplatz benötigt. Dieser Wert wird später je nach Komplexität der Datenbank entsprechend zunehmen. Um hier den Lesefluss der Installationsanleitung nicht zu unterbrechen, findet sich eine detaillierte Beschreibung der NTDS-Datenbankdatei in Kapitel 13.1.1. Klicken Sie dann auf WEITER.

7. Im nächsten Fenster müssen Sie den Pfad zum freigegebenen Systemdatenträger SYSVOL festlegen (siehe Abbildung 9.7). Der vorgeschlagene Pfad lautet %SYSTEM-ROOT%\SYSVOL. Auch dieser kann beliebig geändert werden. Allerdings muss es sich zwingend um einen NTFS-Datenträger handeln. Dieser freigegebene Systemdatenträger umfasst eine Ordnerstruktur, die Skripte und Gruppenrichtlinienobjekte für die Domäne enthält. Diese Struktur wird auf alle Domänencontroller repliziert. Die Funktion von SYSVOL wird ausführlicher in Kapitel 13.1.2 erläutert. Klicken Sie dann auf WEITER.

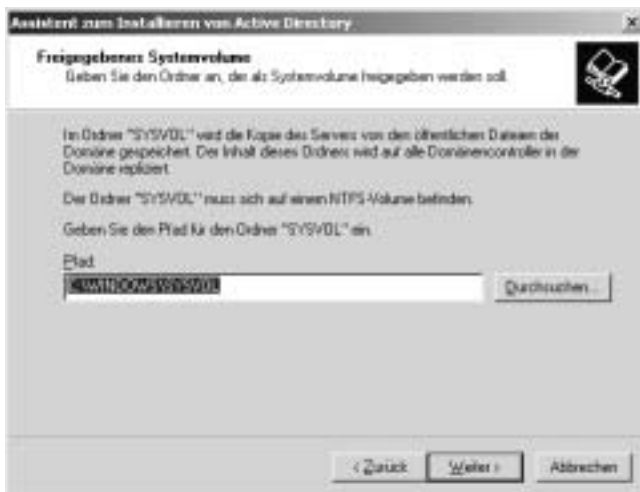


Abbildung 9.7: Festlegen des Speicherorts für den Ordner SYSVOL

8. Sie erhalten nun das Fenster DNS-REGISTRIERUNGSDIAGNOSE (siehe Abbildung 9.8). Dabei wird untersucht, ob eine Verbindung zu einem DNS-Server hergestellt werden konnte. Dabei werden die statisch auf dem Server eingetragenen oder per DHCP-Server zugewiesenen DNS-Server dahingehend überprüft, ob diese für die Namensauflösung im Active Directory verwendet werden können. Sie sehen im oberen Teil die Diagnoseergebnisse. Ist es dabei zu Fehlern gekommen, haben Sie die Möglichkeit, die DNS-Konfiguration zu ändern und die Diagnose erneut durchzuführen (DER FEHLER WURDE BEHOBEN, DNS-DIAGNOSETEST ERNEUT AUSFÜHREN). Alternativ können Sie auch die Option DER FEHLER WIRD SPÄTER DURCH MANUELLE DNS-KONFIGURATION BEHOBEN wählen. Sofern der Server noch nicht als DNS-Server konfiguriert wurde, können Sie auch den DNS-Server auf dem Server installieren und als bevorzugten DNS-Server verwenden. Dabei wird automatisch eine neue primäre DNS-Zone für die Domäne angelegt. Klicken Sie dann auf WEITER.

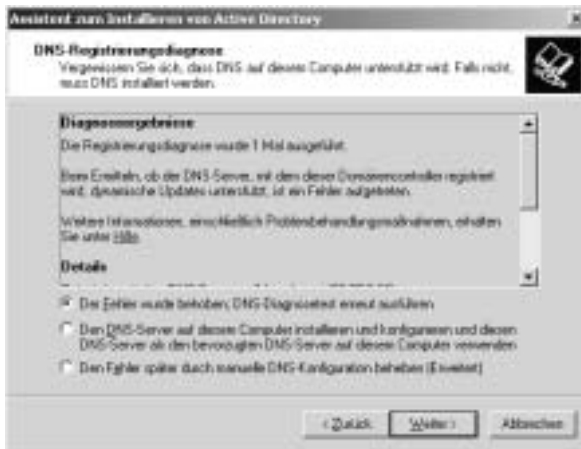


Abbildung 9.8: Die automatische Durchführung des DNS-Diagnosetests und dessen Ergebnis

9. Im Fenster **BERECHTIGUNGEN** müssen Sie die Zugriffsrechte für die Gruppe „Jeder“ festlegen (siehe Abbildung 9.9). Wichtig ist dieses z.B. bei RAS-Servern, da einige Applikationen und Dienste unter Windows NT 4.0 voraussetzen, dass die Gruppe „Jeder“ auch Zugriffe anonymer Benutzer beinhaltet. Im Active Directory hingegen gehören nur an der Domäne authentifizierte Mitglieder zur Gruppe „Jeder“. Verwenden Sie noch Applikationen und Serverdienste in NT-Domänen, so aktivieren Sie die Option **MIT PRÄ-WINDOWS 2000-SERVERBETRIEBSSYSTEMEN KOMPATIBLE BERECHTIGUNGEN**. Bedenken Sie aber, dass damit der anonyme Zugriff auf die Domänendaten möglich ist. Ältere Serveranwendungen sind noch sehr weit verbreitet. Außerdem ist zu überprüfen, ob selbst geschriebene oder eigenentwickelte Anwendungen mit der Active Directory-Anmeldung zurechtkommen oder nicht. Für diese Applikationen ist über eine Portierung nachzudenken, sodass sie zu Active Directory kompatibel werden. Klicken Sie dann auf **WEITER**.



Abbildung 9.9: Festlegen der Optionen für den Umgang mit zu Prä-Windows 2000 kompatiblen Berechtigungen

10. Als Nächstes wird das Passwort zur Verzeichnisdienstwiederherstellung festgelegt (siehe Abbildung 9.10). Bei diesem Passwort spricht man auch vom DSRM-Passwort (Directory Service Restore Mode). Dieses Passwort wird verwendet, um in den erweiterten Startoptionen die Option VERZEICHNISDIENSTE WIEDERHERSTELLEN auszuführen. Aus Sicherheitsgründen sollten Sie in jedem Fall ein Passwort für das Administratorkonto vergeben, und dieses sollte sich von dem Administratorpasswort unterscheiden. Unter Windows Server 2003 besteht die Möglichkeit, das hier gesetzte Passwort zu einem späteren Zeitpunkt über das Kommandozeilenprogramm *NTDSUTIL* zu ändern (siehe Kapitel 23.1.18). Klicken Sie dann auf WEITER.



Abbildung 9.10: Festlegen des Kennworts für die Verzeichnisdienstwiederherstellung

11. Sie erhalten nun eine Zusammenfassung aller Ihrer Einstellungen (siehe Abbildung 9.11). Sie sollten diese nochmals sorgfältig durchlesen. Haben Sie dabei festgestellt, dass eine Eingabe falsch war, können Sie über ZURÜCK bis zu dem gewünschten Fenster zurückgehen und dort Ihre Eingabe korrigieren. Klicken Sie dann auf WEITER.

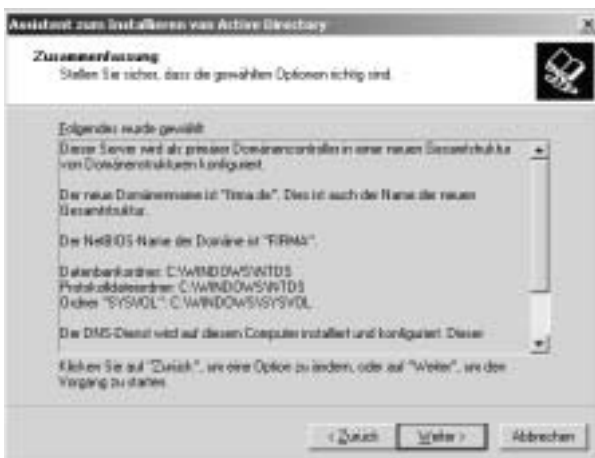


Abbildung 9.11: Zusammenfassung der Einstellungen für die Installation des Active Directory

12. Damit wird die Installation gestartet. Während der Installation haben Sie noch die Möglichkeit, den Installationsvorgang abzubrechen, ohne dass das Active Directory installiert wird. Nach Abschluss der Installation klicken Sie auf FERTIG STELLEN. Danach muss der Server neu gestartet werden.

Während des Neustarts erfolgt die Registrierung des Domänencontrollers an seinem DNS-Server, sodass die Clients diesen als Domänencontroller erkennen. Sobald der neue Domänencontroller seine Netzwerkverbindung herstellt, erhält er die SYSVOL-Informationen von bereits vorhandenen Replikationspartnern. Solange dieser Vorgang nicht abgeschlossen wurde, werden auf dem Domänencontroller nicht die Ordner SYSVOL und NETLOGON angelegt. Ist dieser Vorgang erfolgreich abgeschlossen, findet sich in der Ereignisanzeige des Dateireplikationsdienstes ein Ereignis mit der ID 13516. Danach wird der Netlogon-Dienst gestartet, und der Domänencontroller ist in der Domäne verfügbar. Dieser Vorgang kann, abhängig von der Verbindungsgeschwindigkeit zwischen dem Domänencontroller und seinen Replikationspartnern, eine Viertelstunde oder länger dauern.

Beim Neustart des Rechners werden Sie im Anmeldefenster feststellen, dass Sie jetzt unter ANMELDEN AN nur noch die eben erstellte Domäne angeben können. Eine lokale Anmeldung am Domänencontroller ist nicht mehr möglich.

Im Verzeichnis %SYSTEMROOT%\DEBUG finden Sie die Protokolldateien des Installationsprozesses. Die Datei *DCPROMO.LOG* enthält sämtliche Einträge über die Vorgänge, die bei der Installation des Active Directory durchgeführt worden sind. Bei Problemen sollten Sie diese Datei zunächst zur Fehleranalyse heranziehen.

Nach der Installation des Active Directory befinden sich auf dem Domänencontroller einige neue Management-Konsolen (mmcs) zur Verwaltung des Active Directory. Dabei handelt es sich um die mmcs ACTIVE DIRECTORY-BENUTZER UND -COMPUTER, ACTIVE DIRECTORY-DOMÄNEN UND VERTRAUENSSTELLUNGEN, ACTIVE DIRECTORY-STANDORTE UND -DIENSTE sowie SICHERHEITSRICHTLINIE FÜR DOMÄNEN UND SICHERHEITSRICHTLINIE FÜR DOMÄNENCONTROLLER. Unter Windows Server 2003 gibt es zusätzlich die mmc ACTIVE DIRECTORY-VERWALTUNG. In dieser mmc sind die Inhalte der mmcs ACTIVE DIRECTORY-BENUTZER UND -COMPUTER, -STANDORTE UND DIENSTE, -DOMÄNEN UND VERTRAUENSSTELLUNGEN sowie zusätzlich die mmc DNS zusammengefasst.

9.2.2 Eine neue untergeordnete Domäne in einer Domänenstruktur einrichten

Dieser Vorgang ist auszuführen, wenn Sie einer bestehenden Domänenstruktur eine neue Domäne hinzufügen möchten. Angenommen, es ist bereits eine Domänenstruktur *firma.de* eingerichtet, und Sie möchten nun die untergeordnete Domäne *vertrieb.firma.de* hinzufügen. Auch in diesem Fall rufen Sie den Active Directory-Installationsassistenten über DCPROMO auf.

1. Im Fenster TYP DES DOMÄNENCONTROLLERS (siehe Abbildung 9.2) müssen Sie in diesem Fall die Option DOMÄNENCONTROLLER FÜR EINE NEUE DOMÄNE wählen. Klicken Sie dann auf WEITER.
2. In dem dann folgenden Fenster NEUE DOMÄNENSTRUKTUR ERSTELLEN (siehe Abbildung 9.3) wählen Sie die Option UNTERGEORDNETE DOMÄNE IN EINER BESTEHENDEN DOMÄNENSTRUKTUR. Klicken Sie dann auf WEITER.

3. Im Fenster SICHERHEITSINFORMATIONEN FÜR DAS NETZWERK (siehe Abbildung 9.12) müssen Sie ein gültiges Benutzerkonto mit Kennwort in der übergeordneten Domäne angeben. Dieses Konto muss über die Berechtigung verfügen, neue untergeordnete Domänen zu erstellen. Klicken Sie dann auf WEITER.

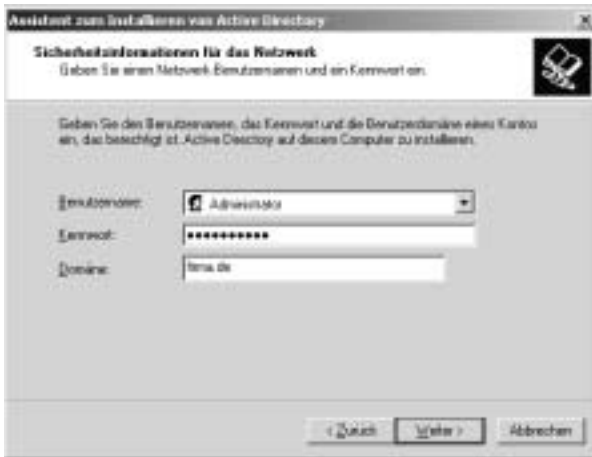


Abbildung 9.12: Angabe eines Benutzerkontos für das Erstellen einer neuen untergeordneten Domäne

4. Als Nächstes müssen Sie den DNS-Namen der übergeordneten Domäne sowie der neu zu erstellenden untergeordneten Domäne angeben (siehe Abbildung 9.13). In unserem Beispiel geben Sie in das Feld ÜBERGEORDNETE DOMÄNE den Namen *firma.de* ein, in das Feld UNTERGEORDNETE DOMÄNE den Namen *vertrieb*. Im Feld VOLLSTÄNDIGER DNS-NAME DER NEUEN DOMÄNE wird aus diesen beiden Angaben automatisch der neue DNS-Name zusammengefügt. Klicken Sie dann auf WEITER.

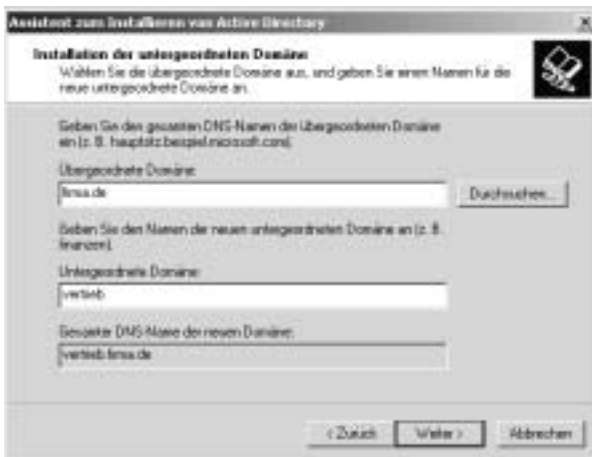


Abbildung 9.13: Hinzufügen einer neuen untergeordneten Domäne zu einer bestehenden Domänenstruktur

5. Die folgenden Installationsschritte entsprechen denen der Installation eines Domänencontrollers einer neuen Domäne (siehe Kapitel 9.2.1, Schritt 6 bis 12).

9.2.3 Erstellen einer neuen Domänenstruktur in einer vorhandenen Gesamtstruktur

Diese Situation ergibt sich, wenn zu einer bestehenden Gesamtstruktur eine neue Domänenstruktur mit einem anderen Namensraum hinzugefügt werden soll. Dies ist beispielsweise der Fall, wenn die beiden Strukturen *firma.de* und *filiale.de* zusammengeführt werden sollen. Auch in diesem Fall rufen Sie den Active Directory-Installationsassistenten über DCPROMO auf.

1. Im Fenster TYP DES DOMÄNENCONTROLLERS (siehe Abbildung 9.2) müssen Sie in diesem Fall die Option DOMÄNENCONTROLLER FÜR EINE NEUE DOMÄNE wählen. Klicken Sie dann auf WEITER.
2. In diesem Fall wählen Sie in dem Fenster NEUE DOMÄNENSTRUKTUR ERSTELLEN die dritte Option DOMÄNENSTRUKTUR IN EINER BESTEHENDEN GESAMTSTRUKTUR (siehe Abbildung 9.3). Klicken Sie dann auf WEITER.
3. Als Nächstes geben Sie die Benutzerinformationen für ein Konto aus der Stammdomäne der Gesamtstruktur an (siehe Abbildung 9.12). Dieses Benutzerkonto muss berechtigt sein, in einer Gesamtstruktur eine neue Domänenstruktur zu erstellen. Klicken Sie dann auf WEITER.
4. Danach wird die TCP/IP-Konfiguration des künftigen Domänencontrollers geprüft. Dieser muss in der Lage sein, den DNS-Namen der Stammdomäne aufzulösen. Ist die Stammdomäne nicht erreichbar, erhalten Sie eine Fehlermeldung.
5. Als Nächstes müssen Sie einen DNS-Namen für die neue Domänenstruktur angeben (siehe Abbildung 9.14). In unserem Beispiel wäre dies *filiale.de*. Klicken Sie dann auf WEITER.

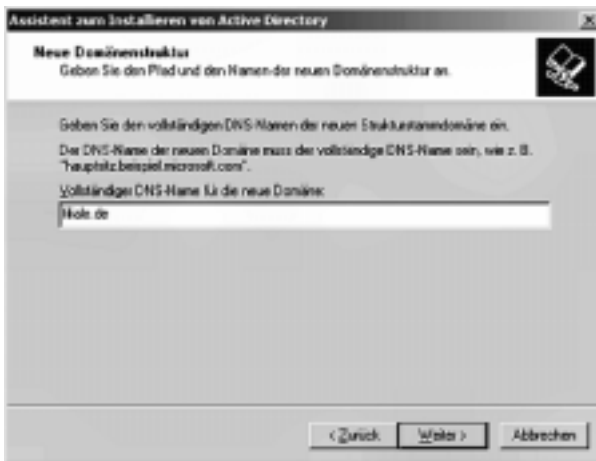


Abbildung 9.14: Hinzufügen einer neuen Domäne in eine bestehende Gesamtstruktur

6. Danach geben Sie den NetBIOS-Namen der Domäne an, in unserem Beispiel also *FILIALE*. Klicken Sie dann auf WEITER.
7. Die folgenden Installationsschritte entsprechen denen der Installation eines Domänencontrollers einer neuen Domäne (siehe Kapitel 9.2.1, Schritt 6 bis 12).

9.2.4 Die Installation zusätzlicher Domänencontroller



Wenn Sie einen neuen Domänencontroller einrichten, werden vom Server alle bestehenden lokalen Benutzer- und Computerkonten gelöscht. Ferner werden alle kryptografischen Schlüssel gelöscht und sollten zuvor gesichert werden. Außerdem sollten alle mit EFS (Encrypting File System) verschlüsselten Dateien zuvor entschlüsselt werden. Ansonsten können Sie nach der Umwandlung des Servers nicht mehr auf die Daten zugreifen. Nur der Wiederherstellungsagent, der Ersteller einer Datei und evtl. weitere designierte Konten sind berechtigt, mit EFS verschlüsselte Dateien wieder zu entschlüsseln und damit den Zugriff auf die Datei zu ermöglichen. Da aber sämtliche lokalen Konten gelöscht wurden, ist kein Zugriff mehr möglich.

1. Um einen zusätzlichen Domänencontroller hinzuzufügen, wählen Sie im Fenster **TYP DES DOMÄNENCONTROLLERS** die Option **ZUSÄTZLICHER DOMÄNENCONTROLLER FÜR EINE BESTEHENDE DOMÄNE** (siehe Abbildung 9.2). Klicken Sie dann auf **WEITER**.
2. Im Fenster **SICHERHEITSINFORMATIONEN FÜR DAS NETZWERK** (siehe Abbildung 9.12) müssen Sie einen gültigen Benutzernamen, Kennwort und die Domäne dieses Netzwerkkontos angeben. Das Benutzerkonto, das hier für den Prozess des Hinzufügens angegeben wird, muss in derselben Gesamtstruktur liegen wie die bestehende Domäne. Ansonsten erhalten Sie eine Fehlermeldung. Klicken Sie dann auf **WEITER**.
3. Als Nächstes wählen Sie die Domäne aus, für die Sie den zusätzlichen Domänencontroller einrichten möchten (siehe Abbildung 9.15). Geben Sie entweder den Domänennamen in das Textfeld ein, oder wählen Sie über **DURCHSUCHEN** die gewünschte Domäne aus. Klicken Sie dann auf **WEITER**.

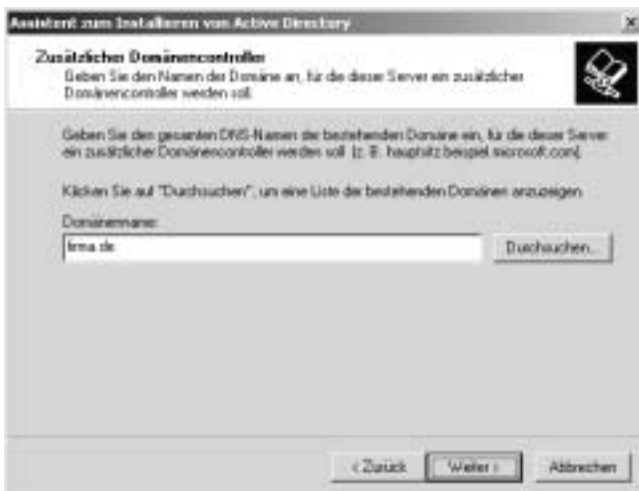


Abbildung 9.15: Auswahl der Domäne, der ein neuer Domänencontroller hinzugefügt werden soll

4. Es werden dann nur noch die in Kapitel 9.2.1 beschriebenen Schritte 6 (Pfadangabe für Datenbank- und Protokolldatei sowie SYSVOL angeben) und 9 (Kennwort zur Wiederherstellung des Verzeichnisdienstes) durchgeführt. Die übrigen Schritte sind nicht notwendig, da die Einstellungen nur einmalig bei der Installation des ersten Domänencontrollers der Domäne getroffen werden.

Fügen Sie einen zusätzlichen Domänencontroller zu einer Domäne hinzu, wird eine Verbindung zum ersten Domänencontroller hergestellt. Treten dabei DNS-bedingte Fehler auf, wird ein Report mit Hinweisen zur Fehlerbehebung ausgegeben. Auf jedem bereits bestehenden Domänencontroller wird überprüft, ob dieser in der Lage ist, die Domain Controller Locator DNS-Ressourceneinträge (siehe Kapitel 16.2.5) dynamisch aufzuzeichnen.

Weitere Hinweise zur Installation zusätzlicher Domänencontroller finden Sie in Kapitel 9.4.

9.3 Deinstallation des Active Directory

Sämtliche installierten Programme sollten sich auch wieder deinstallieren lassen. Dies trifft auch für Active Directory zu. Allerdings sind für eine ordnungsgemäße Deinstallation einige Punkte zu bedenken: Wenn Sie das Active Directory von einem Domänencontroller deinstallieren, wird er zum Mitgliedsserver der Domäne. Entfernen Sie das Active Directory vom letzten verbliebenen Domänencontroller in der Domäne, so wird dieser zum Stand-alone-Server. Hierbei wird die Verzeichnisdatenbank und somit die gesamte Domäne gelöscht. Das Entfernen des letzten Domänencontrollers zieht also die folgenden Konsequenzen nach sich:

- ▶ Da die Verzeichnisdatenbank und somit die komplette Domäne gelöscht werden, können sich die Clients nicht mehr an der Domäne anmelden. Ihnen bleibt nur noch die lokale Anmeldung am Clientrechner.
- ▶ Sämtliche kryptografischen Schlüssel werden gelöscht. Deshalb müssen sie vorher exportiert werden.
- ▶ Auch die Verschlüsselung der per EFS (Encrypting File System) verschlüsselten Dateien sollte vorher aufgehoben werden. Da sämtliche Domänenbenutzerkonten vom Computer entfernt werden, sind somit auch die Konten des Wiederherstellungsagenten und des Besitzers der Datei gelöscht. Allein diesen beiden Gruppen wäre jedoch das Entschlüsseln der Datei möglich.
- ▶ Überprüfen Sie vor der Deinstallation, welche Betriebsmasterrollen der Domänencontroller innehat. Diese Rollen müssen manuell an andere Domänencontroller übertragen werden.
- ▶ Prüfen Sie auch, ob der Domänencontroller als DNS-Server für die Domäne konfiguriert ist. In diesem Fall muss ein anderer Domänencontroller diese Rolle übernehmen. Überprüfen Sie dann die DNS-Funktionalität mit dem Kommandozeilenprogramm *Netdiag*. Verwenden Sie den Befehl `netdiag /test:dns` . Zusätzliche Informationen erhalten Sie, wenn Sie den ausführlichen Modus mit dem Parameter `/v` benutzen. Sie sollten das Ergebnis `DNS Test: Passed` erhalten.

Im folgenden Beispiel wird Active Directory vom letzten Domänencontroller der Domäne firma.de deinstalliert. Damit wird die Domäne gelöscht. Um Active Directory zu deinstallieren, führen Sie folgende Schritte durch:

1. Rufen Sie DCPROMO auf. Es erscheint der bereits bekannte Installationsassistent. Er weist Sie darauf hin, dass Sie im Begriff sind, das Active Directory zu installieren und welche Konsequenzen dies hat (siehe Abbildung 9.16). Klicken Sie auf **WEITER**.



Abbildung 9.16: Der Assistent für die Deinstallation des Active Directory

2. Sie erhalten einen Hinweis, wenn dieser Domänencontroller zugleich Server für den globalen Katalog ist (siehe Abbildung 9.17). In diesem Fall müssen Sie sicherstellen, dass der globale Katalog auf einem anderen Domänencontroller der Domäne vorhanden ist. Ansonsten können Benutzeranmeldungen der Clients nicht mehr verarbeitet werden. Klicken Sie dann auf **OK**. Um den globalen Katalog auf einem anderen Domänencontroller einzurichten, öffnen Sie auf dem DC die mmc **ACTIVE DIRECTORY-STANDORTE UND -DIENSTE**. Wählen Sie unter dem Standort aus den Eigenschaften der NTDS-SETTINGS des gewünschten Servers die Registerkarte **ALLGEMEIN** und aktivieren die Checkbox **GLOBALER KATALOG**.



Abbildung 9.17: Hinweis des Deinstallations-Assistenten, wenn der Domänencontroller gleichzeitig globaler Katalogserver ist

3. Sie müssen nun angeben, ob es sich um den letzten Domänencontroller in der Domäne handelt, von dem Active Directory entfernt werden soll (siehe Abbildung 9.18). Ist dies der Fall, aktivieren Sie die Checkbox **DIESER SERVER IST DER LETZTE DOMÄNENCONTROLLER IN DER DOMÄNE**. Klicken Sie dann auf **WEITER**.



Abbildung 9.18: Bestätigung, ob es sich um den letzten Domänencontroller in einer Domäne handelt

4. Dieses sowie das folgende Fenster erhalten Sie nur, wenn Sie das Active Directory von einem Windows Server 2003-basierten Domänencontroller entfernen möchten. Es sind dort Einstellungen zum Löschen der Anwendungspartitionen erforderlich. Ein Domänencontroller unter Windows Server 2000 kennt noch keine Anwendungspartitionen. Im Fenster **ANWENDUNGSVERZEICHNISPARTITIONEN** (siehe Abbildung 9.19) sehen Sie eine Liste der Anwendungspartitionen, deren letztes Replikat der Server enthält. Klicken Sie dann auf **WEITER**.

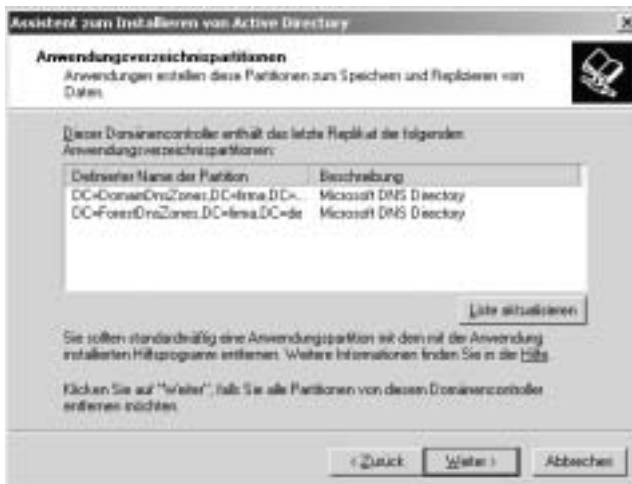


Abbildung 9.19: Auswahl der Partitionen, die vom Domänencontroller entfernt werden sollen

5. Im Fenster LÖSCHEN BESTÄTIGEN (siehe Abbildung 9.20) müssen Sie die Checkbox ALLE ANWENDUNGSVERZEICHNISPARTITIONEN AUF DIESEM DOMÄNENCONTROLLER LÖSCHEN aktivieren. Damit werden alle im letzten Fenster gezeigten Partitionen sowie die darin enthaltenen Daten gelöscht. Klicken Sie dann auf WEITER.

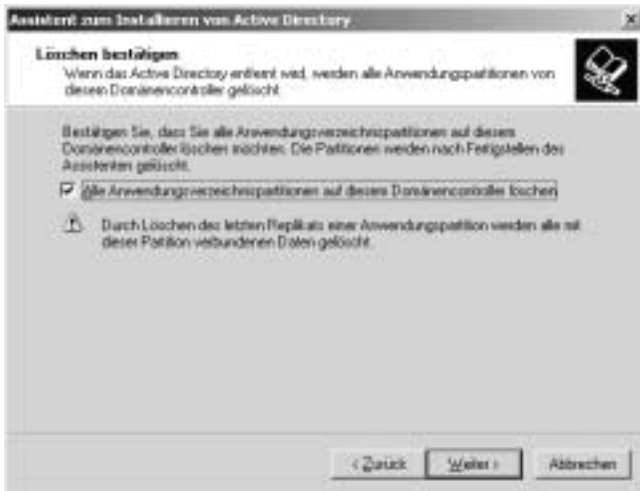


Abbildung 9.20: Das Löschen der Anwendungspartitionen bestätigen

6. Im Fenster ADMINISTRATORKENNWORT geben Sie im Feld NEUES ADMINISTRATORKENNWORT ein Kennwort ein, das dem Administratorkonto zugewiesen werden soll, und bestätigen dieses (siehe Abbildung 9.21). Klicken Sie dann auf WEITER.

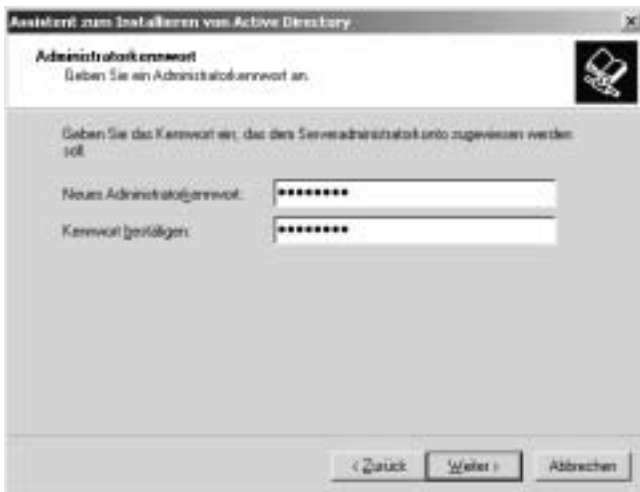


Abbildung 9.21: Zuweisen eines Kennworts für das Administratorkonto

7. In der Zusammenfassung sehen Sie dann eine Auflistung der Vorgänge, die bei der Deinstallation stattfinden werden, und welche Konsequenzen das Deinstallieren des Active Directory hat. Klicken Sie dann auf WEITER.
8. Klicken Sie im Abschlussfenster auf FERTIG STELLEN. Damit wird der Deinstallationsprozess eingeleitet.
9. Abschließend öffnen Sie die mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE. Öffnen Sie hier den Container des Standorts und dort den Container SERVERS. Markieren Sie den Server und löschen diesen über das Kontextmenü. Für diesen Vorgang müssen Sie über die Berechtigung des Domänenadministrators verfügen.



Wenn Sie das Serverobjekt löschen, dürfen sich unter diesem keine untergeordneten Objekte mehr befinden. Befindet sich jedoch noch ein NTDS-Objekt oder ein anderes Objekt unterhalb des Servers, so ist entweder die neue Information noch nicht auf den Server repliziert worden, von dem aus Sie die mmc betrachten, oder aber der Deinstallationsprozess auf dem Domänencontroller ist fehlgeschlagen. Im ersten Fall sollten die untergeordneten Objekte nach einem Replikationsintervall nicht mehr sichtbar sein, sodass nun das Serverobjekt gelöscht werden kann. Andernfalls müssen Sie den Domänencontroller, auf dem das Active Directory nicht erfolgreich deinstalliert werden konnte, manuell mit dem Kommandozeilenprogramm *NTDSUTIL* zum Mitgliedsserver herabstufen.

9.3.1 Die Deinstallation des Active Directory erzwingen

Neben der eben beschriebenen Methode zum Herabstufen eines Domänencontrollers zum Mitgliedsserver und der damit verbundenen Deinstallation des Active Directory können Sie die Herabstufung auch erzwingen.



Sie sollten diese Methode jedoch nur dann anwenden, wenn das eben beschriebene Verfahren fehlschlägt. Keinesfalls sollten Sie dieses Verfahren als Standardmethode für das Herabstufen von Domänencontrollern verwenden.

Um die Deinstallation zu erzwingen, verwenden Sie den Befehl `DCPROMO /FORCE REMOVAL`. Hierdurch wird der Domänencontroller sofort aus dem Active Directory entfernt. Während bei der Deinstallation über DCPROMO noch eine Replikation mit den übrigen Domänencontrollern stattfindet und die Verweise auf diesen Domänencontroller aus dem Active Directory entfernt werden, findet bei `DCPROMO /FORCEREMOVAL` keine Replikation mehr statt. Dies bedeutet, dass Sie die nicht mehr gültigen Verweise manuell von den übrigen Domänencontrollern entfernen müssen. Hierzu verwenden Sie das Kommandozeilenprogramm *NTDSUTIL* (siehe Kapitel 23.1.18).

9.3.2 Herunterstufen eines Domänencontrollers über die Registry

Alternativ können Sie den Server auch über eine Änderung an der Registry wieder zum Mitgliedsserver herabstufen.



Dieses Verfahren wird jedoch offiziell weder für Windows Server 2000 noch für Windows Server 2003 von Microsoft empfohlen.

Benutzen Sie hierzu unter Windows 2000 *regedt32*, unter 2003 *regedit*. Der Windows Server 2003 verwendet lediglich den Registrierungseditor *regedit*. Dieser ist erweitert worden, sodass Sie mit diesem auch *REG_MULTI_SZ*-Werte usw. zuweisen können. Er vereint den Funktionsumfang der beiden Windows 2000-Registrierungsedatoren *regedit* und *regedt32*.

Navigieren Sie zum Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl\Product Options`. Ändern Sie dort den Wert des Schlüssels von `LanmanNT` auf `ServerNT`. Achten Sie auf die exakte Schreibweise. Danach muss der Server neu gestartet werden. Entfernen Sie dann den NTDS-Ordner.

9.4 Die Installation zusätzlicher Domänencontroller

Nachdem Sie den ersten Domänencontroller Ihrer neuen Domäne erfolgreich aufgesetzt haben, sollten Sie nicht auf den Gedanken verfallen, jetzt mit Leichtigkeit zusätzliche Domänencontroller dieser Domäne hinzufügen zu können. Gerade bei der Installation weiterer Domänencontroller kann es oftmals zu Problemen kommen, weil simple Punkte übersehen oder falsch konfiguriert werden. Die folgende Checkliste soll Ihnen bei der Installation weiterer Domänencontroller helfen. Dieser Schritt sollte immer geprüft werden, egal ob Sie einen Windows 2000- oder 2003-Domänencontroller hinzufügen möchten.

Prüfen Sie am bereits vorhandenen Domänencontroller mit installiertem und konfiguriertem DNS-Dienst die folgenden Punkte:

- ▶ Ist die korrekte DNS-Zone für die Active Directory-Domäne eingetragen?
- ▶ Handelt es sich bei der Forward Lookup-DNS-Zone um eine primäre oder Active Directory-integrierte Zone? Eine sekundäre Zone ist schreibgeschützt und kann nur als Kopie auf einem weiteren DNS-Server vorhanden sein.
- ▶ Ist auch bereits eine Reverse Lookup-Zone für das Subnetz konfiguriert?
- ▶ Sind in der DNS-Zone dynamische Updates aktiviert?
- ▶ Ist in der TCP/IP-Konfiguration des Domänencontrollers als DNS-Server der local-host angegeben? Nur so trägt er sich selbst im DNS ein.

- ▶ Sehen Sie in der DNS-mmc nach, ob die Dienstinträge (`_msdcs`) vorhanden sind. Sind diese nicht korrekt vorhanden, so ist sein eigener Eintrag fehlgeschlagen, und er kann nicht von anderen Computern gefunden werden. Versuchen Sie, den Netzwerkanmeldedienst zu beenden und wieder neu zu starten (`net stop netlogon`, `net start netlogon`). Erzielen Sie hiermit keine Wirkung, verwenden Sie `ipconfig /registerdns`.
- ▶ Ist der Domänencontroller als globaler Katalogserver eingerichtet (siehe Active Directory-Standorte und -Dienste, NTDS-Settings des Servers)?
- ▶ Wird der Name des Domänencontrollers korrekt als FQDN angezeigt? In den Eigenschaften des Arbeitsplatzes sollte der Name in der Form "server.domäne.de" angegeben sein und nicht in der Form "Server". Ändern Sie im zweiten Fall das DNS-Suffix über die Registry. Fügen Sie unter dem Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters` die Reg-SZ-Werte `Domain` und `NVDomain` hinzu. Beide erhalten als Wert das entsprechende DNS-Suffix. Danach muss der Server neu gestartet werden, und die TCP/IP-Konfiguration sollte überprüft werden, ob die Änderungen korrekt übernommen worden sind.

Auf dem Mitgliedsserver, der als neuer Domänencontroller konfiguriert werden soll, sollten Sie die folgenden Punkte überprüfen:

- ▶ Stellen Sie sicher, dass der Domänencontroller und der neu aufzusetzende Domänencontroller dasselbe Windows-Servicepack verwenden. Abweichende Servicepack-Versionen können zu unvorhersehbaren Problemen führen.
- ▶ Ist in der TCP/IP-Konfiguration die IP-Adresse des ersten Domänencontrollers als bevorzugter DNS-Server eingetragen? Andernfalls wird die Domäne nicht gefunden.
- ▶ Ist in den Eigenschaften des Arbeitsplatzes auf der Registerkarte NETZWERKIDENTIFIKATION das DNS-Suffix der Domäne eingetragen? Ist dies nicht der Fall, können Sie das Suffix über die Schaltfläche EIGENSCHAFTEN hinzufügen.
- ▶ Wenn Sie beim Ausführen von `DCPROMO` nach dem Benutzerkonto gefragt werden, dürfen Sie nicht das lokale Administratorkonto des Noch-Mitgliedsservers angeben, sondern müssen das Konto des Domänenadministrators oder eines Organisations-Admins angeben.

9.4.1 Installation eines Active Directory-Replikats

Eine weitere Möglichkeit zur Installation eines neuen Domänencontrollers bietet unter Windows Server 2003 die Option *Install from Media* des Active Directory-Installationsassistenten. Hierzu muss zunächst von einem beliebigen Domänencontroller, der sich in derselben Domäne befinden muss, zu der der neue hinzugefügt werden soll, ein Backup durchgeführt werden (siehe Kapitel 21.6), bei dem auch sein Replikat der Verzeichnisdatenbank `NTDS.DIT` gesichert ist. Diese gesicherten Daten müssen in ein Verzeichnis auf dem zukünftigen Domänencontroller kopiert werden. Der Installationsassistent ist danach in der Lage, das Replikat der Verzeichnisdatenbank zu finden.



Es darf nur eine Sicherungsdatei zurückgespielt werden, die nicht älter als 60 Tage ist. Dieser Zeitraum ist die standardmäßige Einstellung für das Tombstoning (siehe Kapitel 21.4). Haben Sie diesen Zeitraum geändert, gilt selbstverständlich das von Ihnen bestimmte Intervall. Im Active Directory werden alle Daten endgültig gelöscht, wenn das Tombstoning-Intervall überschritten worden ist. Sofern Sie Daten zurückspielen, die älter sind als das Tombstoning-Intervall, so sind diese in den übrigen Replikaten der Domänencontroller bereits gelöscht. Wird eine solche Datei auf einem anderen Domänencontroller wieder eingespielt, so kann es zu unvorhergesehenen Fehlern kommen.

Der Vorteil dieser Installationsmethode besteht darin, dass der neue Domänencontroller keine vollständige Replikation mit den anderen Domänencontrollern der Domäne mehr durchführen muss, sondern lediglich die Änderungen bezogen werden müssen, die nach dem Einspielen des Replikats an den übrigen Domänencontrollern vorgenommen worden sind. Dieses Verfahren bietet sich besonders für Domänencontroller an, die an ihrem Standort lediglich über eine langsame Verbindung mit anderen Domänencontrollern verbunden sind.

Sofern der Domänencontroller, dessen Sicherung eingespielt werden soll, auch als globaler Katalogserver (siehe Kapitel 15) eingerichtet ist, können die Daten des globalen Katalogs ebenfalls gesichert und auf dem neuen Domänencontroller eingespielt werden. Damit ist es möglich, dem neuen Domänencontroller auch die Rolle eines globalen Katalogservers zuzuweisen. Auch hier besteht der Vorteil darin, dass lediglich die Daten des globalen Katalogs mit den übrigen Katalogservern abgeglichen werden müssen, die sich seit dem Einspielen des Replikats geändert haben.

Um die Option `INSTALL FROM MEDIA` ausführen zu können, führen Sie die folgenden Schritte durch:

1. Führen Sie zunächst auf dem Quelldomänencontroller eine Sicherung der Systemstatusdaten durch. Dieses Verfahren wird ausführlich in Kapitel 21.6 beschrieben. Als Zielmedium verwenden Sie eine Freigabe im Netzwerk, eine CD oder DVD.
2. Die gesicherten Daten müssen Sie nun in ein beliebiges Verzeichnis auf dem Zieldomänencontroller kopieren. Dieses Verzeichnis müssen Sie zuerst erstellen. Starten Sie dann das Sicherungsprogramm über `STARTMENÜ / AUSFÜHREN / NTBACKUP` oder über `STARTMENÜ / PROGRAMME / ZUBEHÖR / SYSTEMPROGRAMME / SICHERUNG`.
3. Wählen Sie dort den Link `ERWEITERTER MODUS` und danach die Registerkarte `MEDIEN WIEDERHERSTELLEN UND VERWALTEN`. Wählen Sie aus dem Kontextmenü von `DATEI` den Eintrag `DATEI KATALOGISIEREN`.
4. Im folgenden Fenster `SICHERUNGSDATEI ÖFFNEN` geben Sie den Pfad zur gesicherten Datei an. Es ist also der Pfad zum CD / DVD-Laufwerk oder zu der Netzwerkfreigabe anzugeben. Klicken Sie dann auf `OK`.
5. Sie sehen nun auf der rechten Seite den Katalogeintrag für die gewählte Sicherungsdatei. Öffnen Sie den Strukturbereich und markieren die Checkbox `SYSTEM STATE`. Unter `DATEIEN WIEDERHERSTELLEN` wählen Sie den Eintrag `ALTERNATIVER BEREICH`. Geben Sie nun den Pfad zu dem in Schritt 2 erstellten Verzeichnis an.

6. Klicken Sie abschließend auf die Schaltfläche **WIEDERHERSTELLUNG STARTEN**. Damit werden die Systemstatusdaten im angegebenen Verzeichnis wiederhergestellt.
7. Rufen Sie nun den Active Directory-Installationsassistenten auf. Damit die Option **INSTALL FROM MEDIA** verfügbar ist, muss unter **STARTMENÜ / AUSFÜHREN** der Befehl **DCPROMO /ADV** eingegeben werden.
8. Markieren Sie zunächst die Checkbox **ZUSÄTZLICHER DOMÄNENCONTROLLER FÜR EINE BESTEHENDE DOMÄNE** und klicken dann auf **WEITER**.
9. Im Fenster **DOMÄNENINFORMATIONEN WERDEN KOPIERT** geben Sie zunächst unter **VON FOLGENDEN WIEDERHERGESTELLTEN SICHERUNGSDATEIEN KOPIIEREN** den Pfad zum Ordner mit den wiederhergestellten Systemstatusdaten an (siehe Abbildung 9.22). Klicken Sie dann auf **WEITER**.

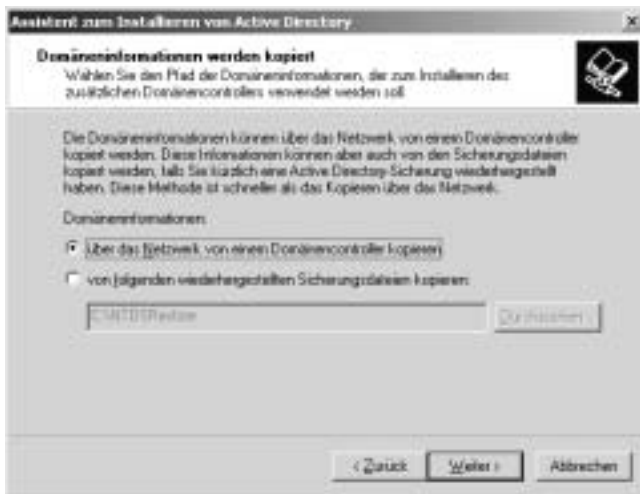


Abbildung 9.22: Die Installation des Active Directory über ein Replikat durchführen

10. Sofern die Systemstatusdaten von einem globalen Katalogserver gesichert worden sind, erhalten Sie das Fenster **GLOBALER KATALOG**. Dort müssen Sie entscheiden, ob die Daten des globalen Katalogs ebenfalls auf den neuen Domänencontroller kopiert werden sollen. Klicken Sie dann auf **WEITER**.
11. Die folgenden Schritte entsprechen denen einer herkömmlichen Active Directory-Installation, bei der der Server zum Domänencontroller heraufgestuft wird (siehe Kapitel 9.2.1).
12. Nach Abschluss der Active Directory-Installation muss ein Neustart durchgeführt werden.
13. Nach dem Neustart des Domänencontrollers erfolgt die Anmeldung an der neuen Domäne. Sie müssen sich mit einem gültigen Benutzerkonto für diese Domäne anmelden.
14. Nachdem der neue Domänencontroller eingerichtet worden ist, können Sie das in Schritt 2 angelegte Verzeichnis mit den darin wiederhergestellten Systemstatusdaten wieder löschen.

9.4.2 Die netzwerkbasierte Active Directory-Installation

Neben dem eben beschriebenen Verfahren der Active Directory-Installation, die auf einem gesicherten Replikat der Datenbank von einem Server beruht, kann auch eine netzwerkbasierte Installation durchgeführt werden. Dabei wird bei der Installation nicht auf das gesicherte Replikat zurückgegriffen, das sich in einem lokalen Verzeichnis des zukünftigen Domänencontrollers befindet, sondern die Informationen werden über das Netzwerk aus der Datenbank eines aktiven Domänencontrollers ausgelesen. Diese Option sollten Sie nur nutzen, wenn die Domänencontroller über eine schnelle Netzwerkverbindung untereinander verfügen. Der Vorteil gegenüber der auf dem Replikat basierenden Installation besteht darin, dass Sie nicht erst eine Sicherung der Systemstatusdateien auf einem Domänencontroller durchführen und diese Daten auf den zukünftigen Domänencontroller kopieren müssen. Auch diese Option ist nur unter Windows Server 2003 verfügbar.

1. Um diese Art der Installation zu nutzen, geben Sie ebenfalls unter STARTMENÜ / AUSFÜHREN den Befehl `DCPROMO /ADV` ein.
2. Markieren Sie zunächst die Checkbox **ZUSÄTZLICHER DOMÄNENCONTROLLER FÜR EINE BESTEHENDE DOMÄNE** und klicken dann auf **WEITER**.
3. Im Fenster **DOMÄNENINFORMATIONEN WERDEN KOPIERT** markieren Sie die Checkbox **ÜBER DAS NETZWERK VON EINEM DOMÄNENCONTROLLER KOPIEREN** (siehe Abbildung 9.22). Klicken Sie dann auf **WEITER**.
4. Als Nächstes geben Sie den Namen der Domäne ein oder wählen diese über **DURCHSUCHEN** aus. Der Server wird zu einem zusätzlichen Domänencontroller der ausgewählten Domäne. Klicken Sie dann auf **WEITER**.
5. Ab hier sind die restlichen Schritte mit denen in Kapitel 9.2.1 beschrieben für die Installation des ersten Domänencontrollers identisch. Nach der Installation muss der Server neu gestartet werden.
6. Nach dem Neustart des Domänencontrollers erfolgt die Anmeldung an der neuen Domäne. Sie müssen sich mit einem gültigen Benutzerkonto für diese Domäne anmelden.

9.5 Domänenvorbereitung für Windows 2003-Domänencontroller mit ADPREP

Wenn eine bestehende Windows 2000 Active Directory-Gesamtstruktur oder -Domäne auf Windows 2003 aktualisiert oder ein zusätzlicher Domänencontroller mit 2003 in eine bestehende Windows 2000-Domäne aufgenommen werden soll, muss diese Domäne sowie die Gesamtstruktur, in der sie enthalten ist, entsprechend vorbereitet werden. Hierzu wird das Tool **ADPREP** benutzt. Dieses Kommandozeilenprogramm befindet sich im /i386-Verzeichnis des Windows Server 2003-Installationsmediums. Bevor Sie auf einem Domänencontroller den Windows 2003-Server installieren, sollten Sie zusätzlich überprüfen, inwieweit die Hardware und Software mit dem Betriebssystem kompatibel ist. Legen Sie die Windows Server 2003-CD ein, und führen Sie für diesen Test den folgenden Befehl aus: `<CD-ROM-Laufwerk>:\i386\winnt32 /checkupgradeonly`.

Bereits in der Domäne vorhandene Domänencontroller sollten unter Windows 2000 mindestens das Servicepack 2 installiert haben. Befinden sich zusätzlich noch Domänencontroller mit Windows NT 4.0 in der Domäne, so sollten Sie diese möglichst zeitnah auf Windows 2000 oder ebenfalls 2003 aktualisieren. Für ein Update muss mindestens das NT Servicepack 5 installiert sein.

Wird die Domäne nicht mit *ADPREP* vorbereitet und Sie führen auf dem ersten Domänencontroller das Update auf 2003 durch oder versuchen den ersten 2003-Domänencontroller hinzuzufügen, so wird der Setup-Prozess bzw. der Active Directory-Installationsassistent entsprechende Fehlermeldungen verursachen.

Zur Vorbereitung der Domäne sind mehrere Schritte erforderlich.

1. Zunächst müssen Sie herausfinden, welche Domänencontroller in der Domäne die Betriebsmasterrollen des Infrastruktur-Masters und des Schemamasters innehaben (siehe Kapitel 11.1.4).
2. Führen Sie ein Backup des Schema-Masters durch und trennen diesen danach physikalisch vom Netzwerk.
3. Legen Sie in den Schema-Master die Server-CD ein, wechseln an der Kommandozeile ins i386-Verzeichnis und geben folgenden Befehl ein: `adprep /forestprep`. Überprüfen Sie, ob der Befehl erfolgreich ausgeführt wurde. Sehen Sie dazu nach, ob in der Ereignisanzeige Fehler aufgelistet sind und ob das Support-Tool *DCDIAG* (siehe Kapitel 23.1.4) Fehlermeldungen liefert.
4. Wurde dieser Befehl erfolgreich ausgeführt, verbinden Sie den Schemamaster wieder mit dem Netzwerk, sodass der Schema-Master sich mit dem Infrastruktur-Master replizieren kann.
5. Legen Sie in den Infrastruktur-Master die Server-CD ein, wechseln an der Kommandozeile ins i386-Verzeichnis und geben folgenden Befehl ein: `adprep /domainprep`. Überprüfen Sie, wie in Schritt 3 beschrieben, ob der Befehl korrekt ausgeführt wurde.
6. Warten Sie nun ab, bis der Infrastruktur-Master seine Änderungen an die übrigen Domänencontroller repliziert hat.

Damit ist die Domänenvorbereitung abgeschlossen. Sie können nun die vorhandenen Windows 2000-Server updaten oder zusätzliche Windows 2003-Domänencontroller zur Domäne hinzufügen.

9.5.1 ADPREP im Zusammenspiel mit weiteren Diensten

Bei der Domänenvorbereitung mit *ADPREP* müssen Sie einige Punkte bedenken, wenn weitere Dienste wie Exchange 2000 oder die Services for Unix (SFU) 2.0 in der Gesamtstruktur ausgeführt werden.

Exchange 2000

Durch die Installation eines Exchange 2000-Servers werden ebenfalls Änderungen am Active Directory-Schema vorgenommen. Diese Änderungen sind jedoch nicht kompatibel mit den Modifikationen, die bei der Domänenvorbereitung via *ADPREP* durchgeführt werden. Wollen Sie in einer Domäne, in der Exchange 2000 ausgeführt wird,

ADPREP durchführen, so müssen zuerst die von Exchange 2000 vorgenommenen Schemaänderungen modifiziert werden. Hierzu führen Sie folgende Schritte aus:



Verwenden Sie ausschließlich Exchange 2003 auf Windows 2003-Domänencontrollern, sind die folgend beschriebenen Schritte nicht erforderlich.

1. Im Verzeichnis `SUPPORT\TOOLS` des Windows Server 2003-Installationsmediums befindet sich die Datei *Support.cab*. Aus dieser Datei entpacken Sie die Datei *inetorgpersonfix.ldf* in ein beliebiges Verzeichnis.
2. Wechseln Sie an der Eingabeaufforderung zu dem Verzeichnis, in das Sie die Datei *inetorgpersonfix.ldf* entpackt haben.
3. Geben Sie dort den Befehl `ldifde -i -f inetorgpersonfix.ldf -c -v „DC=X“ <Name der Stammdomäne der Gesamtstruktur> ↵` ein.

Weitere Hinweise zur Verwendung des Programms *LDIFDE* und zu dessen Parametern finden Sie in Kapitel 25.2.

Services for Unix 2.0

Werden die Services for Unix in der Version 2.0 (siehe Kapitel 29.2) eingesetzt, müssen Sie zunächst einen Patch einspielen, bevor Sie *ADPREP* ausführen können. Hierbei handelt es sich um den Patch Q293783. Weiterführende Hinweise dazu finden Sie unter dem Link <http://support.microsoft.com/default.aspx?scid=kb;EN-US;293783>.



Verwenden Sie die Services for Unix in der Version 3.0, muss dieser Patch nicht eingespielt werden.

10 Die Betriebsmodi des Active Directory

Active Directory kann unter Windows Server 2000 in zwei, unter dem Windows Server 2003 sogar in drei verschiedenen Betriebsmodi ausgeführt werden.

10.1 Die Betriebsmodi im Überblick

Nach der Installation von Active Directory sowie einem Upgrade eines Windows NT-Servers auf Windows 2000/2003 wird dieser standardmäßig im gemischten Modus betrieben. Der gemischte Modus wird auch als *mixed mode* bezeichnet. In diesem Modus kann der Domänencontroller mit anderen Domänencontrollern zusammenarbeiten, auf denen noch Windows NT 3.5x- oder 4.0-Versionen ausgeführt werden. Damit die in der Domäne vorhandenen NT-BDCs mit den Windows 2000-Domänencontrollern kommunizieren können, muss mindestens einer von ihnen die Rolle des PDC-Emulators übernehmen.

Wenn in einer Domäne keine Windows NT-BDCs mehr vorhanden sind, kann der Domänencontroller in den einheitlichen Modus gebracht werden. Dieser Modus wird auch als *native mode* bezeichnet. In diesem Modus ist keine Kommunikation mehr mit Windows NT-Servern möglich. Es können auch keine NT-BDCs mehr zu der Domäne hinzugefügt werden.

Im Windows 2003 Active Directory können Sie wahlweise für die Domänen- oder die Gesamtstruktur den zusätzlichen Betriebsmodus Windows Server 2003 aktivieren. In diesem Modus sind erweiterte Features wie z.B. das Umbenennen von Domänen möglich. Dieser Modus kann nur ausgeführt werden, wenn sich keine Windows NT-BDCs oder Windows 2000-Domänencontroller mehr in der Domänen- bzw. Gesamtstruktur befinden.

10.1.1 Der gemischte Modus

Im gemischten Modus können die Windows 2000-Domänencontroller mit noch vorhandenen Windows NT-BDCs sowie auch mit Windows NT- und 9x- sowie 3.x-Clients zusammenarbeiten. Für diese Clients verhält sich der Domänencontroller wie ein NT-PDC. Die Kommunikation mit den NT-BDCs geschieht über den PDC-Emulator-Betriebsmaster. Im gemischten Modus sind nicht alle Features von Windows 2000 oder 2003 anwendbar, z.B. die Eliminierung des NetBIOS-Protokolls. Da Windows NT auch keine universellen Gruppen (siehe Kapitel 18.4) kennt, haben Sie nicht die Möglichkeit, im gemischten Modus eine Benutzergruppe zu einer anderen hinzuzufügen. Sie müssen alle Benutzerobjekte der ersten Gruppe einzeln zur neuen Gruppe hinzufügen.

Windows 2000 bzw. 2003 wird im gemischten Modus auf den Funktionsumfang von Windows NT reduziert. Besonders wichtig ist dieses Verhalten für die Einschränkungen der NT 4 SAM-Datenbank. Da der Windows 2000-Domänencontroller, der die PDC-Emulatorrolle innehat, seine Informationen mit den NT-BDCs replizieren muss, darf die Datenbank das alte NT-Limit von 40.000 Objekten nicht überschreiten.

10.1.2 Der einheitliche Modus

Nach der Umstellung auf den einheitlichen Modus gibt es in der Domäne keinen primären Domänencontroller mehr. Dies war für die NT-BDCs sowie die alten Windows-Clients der Server in der Domäne, auf dem der PDC-Emulator eingerichtet worden war. Im einheitlichen Modus gibt es nur noch gleichberechtigte Peer-Domänencontroller. Die Bezeichnungen PDC und BDC werden für eine reine Windows 2000-Domäne nicht mehr benutzt.

Da die Rolle des PDC-Emulators entfällt, können keine Replikationsinformationen mehr mit NT-BDCs ausgetauscht werden. Es existiert nur noch die Multimaster-Replikation der Windows 2000-Domänencontroller untereinander. Weiterhin können auch keine NT-Server mehr zur Domäne hinzugefügt werden. Sollen in der Domäne noch Windows NT- bzw. 9x-Clients eingesetzt werden, so müssen Sie auf diesen den jeweiligen ADSI-Client installieren (siehe Kapitel 3.8.1), damit diese auf die Windows 2000/2003-Serverressourcen zugreifen können.

Weiterhin sind nun alle Features von Windows 2000 verfügbar. So ist im einheitlichen Modus auch die Einrichtung universeller Gruppen möglich. Im gemischten Modus gab es nur globale sowie domänenübergreifende lokale Gruppen. Ferner entfällt auch die Limitierung der Datenbank auf maximal 40.000 Objekte.

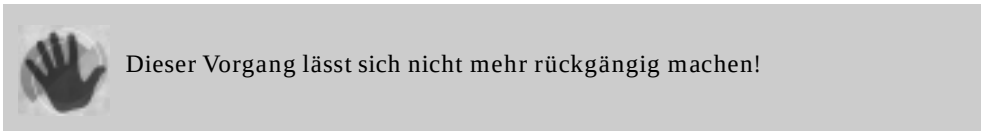
Außerdem wird auch die Netzwerksicherheit verbessert. Im gemischten Modus wurde ausschließlich die NTLM-(NT-LAN-Manager-)Authentifizierung von den Domänen-Clients benutzt. Im einheitlichen Modus steht auch das wesentlich sicherere Kerberos-Protokoll (siehe Kapitel 2.2.3) zur Verfügung.

Ferner ist das NetBIOS-Protokoll nun abschaltbar. Im gemischten Modus war es für die Kommunikation mit noch vorhandenen NT- und 9x-Computern zwingend erforderlich. Sobald Sie aus der Domäne alle Computer auf Windows 2000 oder höher aktualisiert haben, können Sie NetBIOS über TCP/IP abschalten. Allerdings müssen Sie zuvor sicherstellen, dass keine verwendeten Applikationen auf dieses Protokoll angewiesen sind.

Weiterhin wird die Rolle des RID-(Relativer ID-)Masters verändert (siehe Kapitel 11.1.3). Im gemischten Modus konnte lediglich auf einem Rechner zentral die Verwaltung der relativen IDs durchgeführt werden. Jetzt ist eine verteilte Verwaltung der relativen IDs möglich.

10.1.3 Wechsel des Betriebsmodus unter Windows 2000

Um die Domäne vom gemischten in den einheitlichen Modus zu bringen, führen Sie folgende Schritte durch. Vorweg jedoch ein wichtiger Hinweis: Überlegen Sie gut, wann Sie mit der Domäne in den einheitlichen Modus wechseln möchten.



1. Öffnen Sie in der Verwaltung das Snap-In ACTIVE DIRECTORY BENUTZER UND COMPUTER.
2. Klicken Sie mit der rechten Maustaste die Domäne an und wählen aus dem Kontextmenü den Eintrag EIGENSCHAFTEN. Auf der Registerkarte ALLGEMEIN klicken Sie auf die Schaltfläche MODUS WECHSELN (siehe Abbildung 10.1).



Abbildung 10.1: Wechsel des Betriebsmodus

3. Sie erhalten dann nochmals den Hinweis darauf, dass dieser Vorgang nicht wieder rückgängig zu machen ist. Klicken Sie hier zum Bestätigen auf JA. Danach muss der Computer neu gestartet werden.

10.1.4 Der Domänenfunktionsmodus Windows Server 2003

Standardmäßig befindet sich der Domänenfunktionsmodus im gemischten Modus. In diesem Modus können Sie Domänencontroller unter Windows NT, 2000 und 2003 einsetzen. Sobald Sie den Domänenfunktionsmodus auf Windows Server 2003 heraufsetzen, werden die zusätzlichen 2003-Features aktiviert, die lediglich die einzelne Domäne betreffen. Sie können nun die Domänencontroller dieser Domäne umbenennen, Versionsnummern des Kerberos KDC verwenden sowie ein Passwort für das InetOrg-Person-Objekt vergeben. Wurde der Modus heraufgestuft, können Sie keine Windows 2000-Domänencontroller mehr zu dieser Domäne hinzufügen.

Um den Domänenfunktionsmodus vom gemischten oder einheitlichen Modus auf den Windows Server 2003-Modus heraufzustufen, führen Sie die folgenden Schritte aus:



Dieser Vorgang lässt sich nicht mehr rückgängig machen!

1. Öffnen Sie die mmc ACTIVE DIRECTORY DOMÄNEN- UND VERTRAUENSSTELLUNGEN.
2. Wählen Sie aus dem Kontextmenü der Domäne DOMÄNENFUNKTIONSEBENE HERAUFSTUFEN.
3. Im Fenster DOMÄNENFUNKTIONSEBENE HERAUFSTUFEN (siehe Abbildung 10.2) wählen Sie aus der Listbox den Eintrag WINDOWS SERVER 2003 und klicken dann auf HERAUFSTUFEN. Sie erhalten eine Warnmeldung, dass dieser Vorgang nicht mehr rückgängig gemacht werden kann.

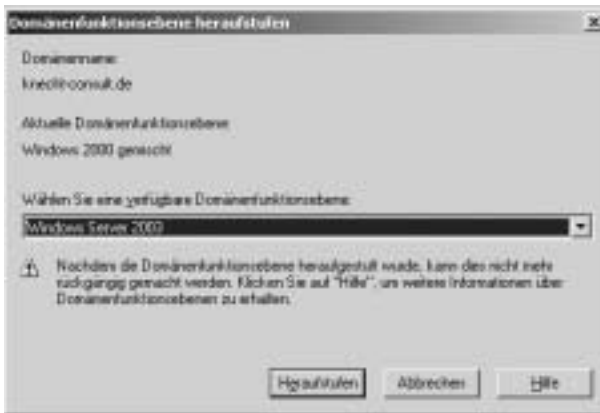


Abbildung 10.2: Die Domänenfunktionsebene auf Windows Server 2003 heraufstufen

Nachdem dieser Vorgang erfolgreich abgeschlossen wurde, erhalten Sie die Statusmeldung, dass die Änderung der Domänenfunktionsebene jetzt an alle übrigen Domänencontroller der Domäne repliziert wird.

Die Domänenfunktionsebene kann auch heraufgesetzt werden, indem Sie in der mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER aus dem Kontextmenü der gewünschten Domäne den Eintrag DOMÄNENFUNKTIONSEBENE HERAUFSTUFEN wählen.

10.1.5 Der Gesamtstrukturfunktionsmodus Windows Server 2003

Wird der Gesamtstrukturfunktionsmodus auf Windows Server 2003 heraufgestuft, werden die erweiterten Features in sämtlichen Domänen der Gesamtstruktur aktiviert. In diesem Modus können Sie u.a. Domänen umbenennen, Vertrauensstellungen zwischen Gesamtstrukturen einrichten, die Replikation des globalen Katalogs anpassen sowie von den verbesserten Replikationsalgorithmen profitieren.

Standardmäßig ist jedoch der Windows 2000-Funktionsmodus aktiviert. In diesem können Windows NT, 2000 und 2003 Server betrieben werden. Zusätzlich ist auch der Windows Server 2003-Interimsmodus verfügbar, wenn der PDC einer NT-Domäne von Windows NT 4.0 auf 2003 heraufgestuft worden ist. Dieser Level erscheint in der GUI nur bei einem von Windows NT upgedateten Domänencontroller. Dieser Domänencontroller kann nach dem Update manuell konfiguriert werden. In dieser Funktionsebene werden keine Windows 2000-Domänencontroller unterstützt. Diese können auch keiner Domäne hinzugefügt werden, die im InterimsModus betrieben wird.

Um den Funktionsmodus der Gesamtstruktur auf den Windows Server 2003-Modus heraufzustufen, führen Sie die folgenden Schritte aus. Voraussetzung ist, dass alle Domänencontroller unter Windows Server 2003 ausgeführt werden und die Domänenfunktionsebene entweder im einheitlichen Windows 2000-Modus oder Windows Server 2003-Modus ist. Außerdem müssen Sie mit der Berechtigung eines Domänen-Administrators angemeldet sein.



Dieser Vorgang lässt sich nicht mehr rückgängig machen!

1. Öffnen Sie die mmc ACTIVE DIRECTORY DOMÄNEN- UND VERTRAUENSSTELLUNGEN.
2. Wählen Sie aus dem Kontextmenü von ACTIVE DIRECTORY-DOMÄNEN- UND VERTRAUENSSTELLUNGEN den Eintrag GESAMTSTRUKTUR-FUNKTIONSEBENE HERAUFSTUFEN.



Befindet sich die Domänenfunktionsebene noch im gemischten Windows 2000-Modus, so ist der Eintrag im Kontextmenü nicht vorhanden. Stufen Sie in diesem Fall zunächst die Domänenfunktionsebene auf Windows 2000 im einheitlichen Modus oder Windows Server 2003 hoch.

3. Im Fenster GESAMTSTRUKTUR-FUNKTIONSEBENE HERAUFSTUFEN wählen Sie aus der Listbox den Eintrag WINDOWS SERVER 2003 und klicken dann auf HERAUFSTUFEN. Sind noch nicht alle Domänencontroller in der Gesamtstruktur auf Windows Server 2003 upgedatet, erhalten Sie eine entsprechende Fehlermeldung. Sie können über die Schaltfläche SPEICHERN UNTER die Logdatei speichern, die Informationen darüber enthält, welche Domänencontroller upgedatet werden müssen. Sie erhalten eine Warnmeldung, dass dieser Vorgang nicht mehr rückgängig gemacht werden kann.

Nachdem dieser Vorgang erfolgreich abgeschlossen wurde, erhalten Sie die Statusmeldung, dass die Änderung der Gesamtstruktur-Funktionsebene jetzt an alle übrigen Domänencontroller der Gesamtstruktur repliziert wird.

11

Die Betriebsmasterrollen

Jetzt lernen Sie die verschiedenen Rollen und Funktionen von Betriebsmastern kennen, die Sie nach der Installation den Domänencontrollern zuweisen können. Sie lernen, wie diese Rollen überprüft und geändert werden können. Auch die Schritte, die nach dem Ausfall eines Betriebsmasters nötig sind, werden detailliert beschrieben.

11.1 Die Betriebsmaster im Überblick

Bei Betriebsmasterrollen handelt es sich um spezielle Rollen von Domänencontrollern in der Gesamtstruktur und Domäne. Active Directory unterstützt die Multimaster-Replikation. Es gibt jedoch einige Vorgänge, die nicht gleichzeitig an mehreren Stellen im Netzwerk, also im Multimasterbetrieb, durchgeführt werden dürfen. Diese Aufgaben werden von einem bestimmten Domänencontroller als Einzelmaster durchgeführt. Die Computer, die Aufgaben als Einzelmaster durchführen, erhalten eine oder mehrere der Betriebsmasterrollen.

Insgesamt gibt es in einer Gesamtstruktur fünf verschiedene Betriebsmaster. Einige dieser Rollen müssen in jeder Domäne der Gesamtstruktur ausgeführt werden, andere dürfen nur einmalig in der Gesamtstruktur vorkommen. Die bei der Active Directory-Installation automatisch an einen Domänencontroller zugewiesenen Betriebsmasterrollen können später jederzeit auf einen anderen Domänencontroller übertragen werden. Deswegen werden die Betriebsmasterfunktionen zuweilen auch *FSMOs (Flexible Single Master Operations)* genannt. Im Active Directory werden die Besitzer der Betriebsmasterrollen an verschiedenen Stellen gespeichert. Für alle Objekte, die auf eine oder mehrere der Betriebsmasterrollen zugreifen, wird der definierte Name (DN) des Servers als FSMORoleOwner-Attribut gespeichert. Das Attribut speichert den Pfad zu der Stelle im Active Directory, die den jeweiligen Server angibt.

Die Betriebsmasterrollen werden unterschieden in Betriebsmaster der Gesamtstruktur sowie Betriebsmaster der Domäne.

11.1.1 Die Betriebsmaster der Gesamtstruktur

In jeder Gesamtstruktur des Active Directory müssen die beiden Rollen Schemamaster und DNS-Master einmalig vorhanden sein. In der Gesamtstruktur darf es also nur einen Schemamaster und einen DNS-Master geben.

Der Schemamaster

Der Schemamaster steuert und überwacht alle Änderungen am Active Directory-Schema. Änderungen des Schemas in der Gesamtstruktur können nur vom Schemamaster selbst

aus vorgenommen werden. Das heißt also, dass Sie über Zugriffsrechte für diesen Computer verfügen müssen, um das Schema zu ändern.

Der DNS-Master

Der DNS-Master wird auch Domänennamenmaster genannt. Über diesen Domänencontroller wird das Hinzufügen und Entfernen von Domänen in der Gesamtstruktur gesteuert.

11.1.2 Die Betriebsmaster der Domänenstruktur

In jeder einzelnen Domäne der Gesamtstruktur müssen die drei folgenden Betriebsmasterrollen ausgeführt werden: RID-Master, PDC-Emulator und Infrastrukturmater. Diese drei Rollen dürfen in jeder Domäne nur einmal ausgeführt werden.

Der RID-Master

Der RID-(Relativer ID-)Master ist für die Zuordnung von Sequenzen relativer IDs an die Domänencontroller seiner Domäne zuständig. Wenn von einem Domänencontroller ein Objekt, z.B. eine Benutzer oder ein Computer, erstellt wird, erhält das Objekt eine eindeutige Sicherheitskennung (SID). Diese Sicherheitskennung setzt sich aus zwei Teilen zusammen: einer globalen Domänensicherheitskennung, die für alle Objekte in der Domäne identisch ist, sowie einer relativen ID, die für jede in der Domäne erstellte Sicherheitskennung eindeutig ist. Diese relative ID bezieht der Domänencontroller von seinem RID-Master. Wenn Sie über das Active Directory-Support-Tool *MOVETREE* Objekte zwischen Domänen verschieben wollen, so muss der Vorgang vom RID-Master aus inszeniert werden. *MOVETREE* wird ausführlich im Rahmen der Active Directory-Support-Tools in Kapitel 23.1.15 beschrieben.

Der PDC-Emulator

Der PDC-Emulator ist erforderlich, wenn in einer Domäne im gemischten Modus noch BDCs unter Windows NT oder Nicht-Active Directory-Clients vorhanden sind. Für diese Rechner übernimmt er die Rolle eines NT-PDCs. Der PDC-Emulator ist zuständig für Kennwortänderungen der Nicht-Active Directory-Clients und führt die Replikation dieser Änderungen an die BDCs in der Domäne durch. Auch im einheitlichen Modus empfängt der PDC-Emulator zuerst die Replikation von Kennwortänderungen, die von anderen Domänencontrollern ausgeführt wurden. Da die Replikation der Kennwortänderungen auf alle Domänencontroller abhängig vom eingestellten Replikationsintervall einige Zeit in Anspruch nehmen kann, wird bei einer misslungenen Authentifizierung an einem Domänencontroller zunächst von diesem eine Anfrage an den PDC-Emulator gestellt, da dieser die aktuellsten Einträge besitzt. Erst wenn auch am PDC-Emulator die Authentifizierung des Clients scheitert, wird die Anmeldung des Clients endgültig abgebrochen.

Der Infrastrukturmater

Der Infrastrukturmater aktualisiert die Verweise zwischen Benutzern und Gruppen, wenn Mitglieder einer Gruppe umbenannt oder verschoben wurden. Nachdem Sie ein Mitglied einer Gruppe, das einer anderen Domäne angehört als die Gruppe, umbenannt oder verschoben haben, ist dieses Gruppenmitglied scheinbar zeitweise nicht in der Gruppe als Mitglied enthalten. Deshalb sollte die Gruppe nach der Änderung eines Mit-

glieds vom Infrastrukturmater der Domäne aktualisiert werden, damit dann der neue Name oder Standort des Mitglieds angezeigt werden kann. Die Aktualisierung des Mitglieds wird dann über die Multimaster-Replikation an die übrigen Domänencontroller übermittelt.

Abbildung 11.1 soll abschließend nochmals einen Überblick über die Verteilung der Betriebsmasterrollen innerhalb einer Gesamtstruktur geben.

Nur auf dem Domänencontroller der übergeordneten Domäne firma.de der Gesamtstruktur werden alle fünf Betriebsmasterrollen ausgeführt. Die beiden Betriebsmasterrollen Schemamaster und DNS-Master der Gesamtstruktur dürfen nur ein einziges Mal in der Gesamtstruktur vorhanden sein.

Auf allen anderen Domänencontrollern werden nur die Betriebsmaster der Domäne ausgeführt. Dies gilt sowohl für die untergeordneten Domänen von firma.de, nämlich vertrieb.firma.de, marketing.firma.de sowie verwaltung.vertrieb.firma.de, als auch für die Stammdomäne filiale.de in der neuen Domänenstruktur sowie deren untergeordneter Domäne vertrieb.filiale.de.

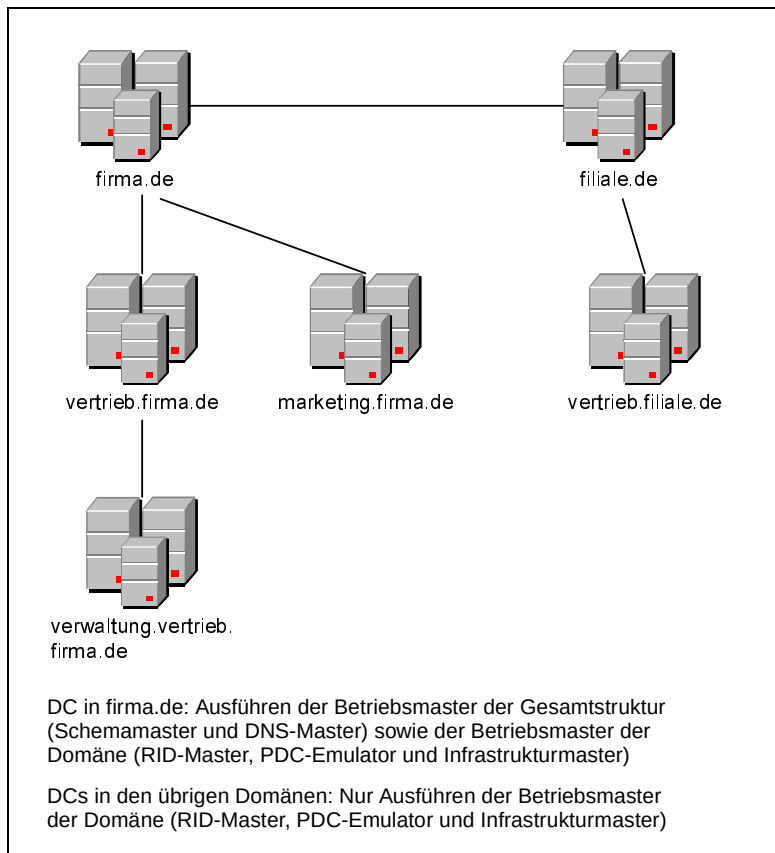


Abbildung 11.1: Die Anordnung der Betriebsmaster in einer Gesamtstruktur

11.1.3 Verteilen von Betriebsmasterrollen

Das obere Schaubild gibt die standardmäßige Installation der jeweiligen Betriebsmaster auf dem ersten Domänencontroller einer Domäne wider. Sie können jedoch die Betriebsmasterrollen auch auf andere Domänencontroller der Domäne verlegen. Dabei sollten Sie jedoch die folgenden Regeln und Empfehlungen beachten, um administrativen Overhead zu vermeiden und gleichzeitig eine optimale Performance zu erzielen.

In einer komplexen Struktur sollten die beiden gesamtstrukturweiten Betriebsmaster Schemamaster und DNS-Master auf einem Domänencontroller der Root-Domäne liegen. Zusätzlich sollte der Domänencontroller, der diese beiden Rollen innehat, auch als globaler Katalogserver konfiguriert sein. Die drei domänenstrukturweiten Betriebsmaster RID-Master, PDC-Emulator und Infrastrukturmaster sollten auf einem Domänencontroller liegen. Dieser Domänencontroller sollte jedoch nicht als globaler Katalogserver eingerichtet sein. Wählen Sie je einen Domänencontroller, der als Standby-Betriebsmaster für die beiden gesamtstrukturweiten und die drei domänenstrukturweiten Betriebsmaster dient. Dieser greift beim Ausfall des eigentlichen Betriebsmaster-Domänencontrollers und führt die entsprechenden Rollen aus.

Der Schemamaster und DNS-Master

Die beiden Betriebsmaster der Gesamtstruktur, der Schemamaster und DNS-Master, werden standardmäßig dem ersten Domänencontroller der Root-Domäne zugewiesen. Diese beiden Rollen sollten Sie auf diesem Server belassen. Das Separieren der beiden Rollen bringt keinen Gewinn an Performance, sondern erschwert nur die Administration beim Backup oder Wiederherstellen sowie dem Einrichten von Standby-Betriebsmastern. Auf dem ersten Domänencontroller der Root-Domäne befindet sich neben diesen beiden Betriebsmastern auch der globale Katalog. Der DNS-Master muss sich dabei auf jeden Fall auf demselben Domänencontroller befinden, der den globalen Katalog besitzt. Dieses ist erforderlich, weil der DNS-Master beim Anlegen eines neuen Domänenobjekts auf den globalen Katalog zurückgreift, um sicherzustellen, dass der Name des neuen Domänenobjekts bislang noch nicht vergeben ist. Da der globale Katalog ein Teilreplikat jedes Objekts der Gesamtstruktur enthält, ist die Konsistenz bei der Namensgebung gewährleistet.

Der Infrastrukturmaster, RID-Master und PDC-Emulator

Die drei domänenweiten Betriebsmaster werden automatisch auf dem ersten Domänencontroller einer neuen Domäne eingerichtet. Diese drei Rollen sollten Sie so lange gemeinsam auf diesem Domänencontroller belassen, bis dieser mit der gleichzeitigen Ausführung der drei Rollen überlastet ist. Da die Root-Domäne der Gesamtstruktur gleichzeitig auch eine neue Domäne ist, befinden sich auf dem ersten Domänencontroller dieser Domäne neben den beiden gesamtstrukturweiten Betriebsmastern auch die drei domänenweiten sowie der globale Katalog. Aus Gründen der Performance sollten Sie in der Root-Domäne die drei domänenweiten Betriebsmaster auf einen anderen Domänencontroller verlegen.

Der PDC-Emulator und der RID-Master sollten nach Möglichkeit immer auf demselben Domänencontroller bleiben. Sämtliche Nicht-Active Directory-Clients senden ihre Updates allein an den PDC-Emulator. Da der Domänencontroller mit dem PDC-Emulator deshalb eine große Anzahl relativer IDs benötigt, sollte sich der RID-Master auf demselben Domänencontroller befinden. Wenn Sie in Ihrer Domäne noch zahlreiche Nicht-Active Directory-Clients verwenden, steigt dadurch auch die Auslastung des PDC-Emulators. Deshalb sollten Sie darüber nachdenken, den PDC-Emulator und einen Standby-PDC-Emulator auf separate Domänencontroller zu legen, die sich direkt mit dem Standby-Betriebsmaster-Domänencontroller replizieren. Der PDC-Emulator ist von allen Betriebsmastern derjenige, der den größten Overhead verursacht. Deshalb sollte der PDC-Emulator auf einem leistungsstarken Server eingerichtet sein.

Weiterhin sollte der Infrastrukturmater nicht auf dem Domänencontroller liegen, auf dem der globale Katalog verwaltet wird. Jedoch sollte der Infrastrukturmater über eine gute Netzwerkverbindung zum Domänencontroller mit dem globalen Katalog am Standort haben. Diese Trennung ist jedoch nicht erforderlich, wenn mit keiner übermäßigen Belastung des Infrastrukturmasters zu rechnen ist. Wenn keine physische Trennung zwischen Infrastrukturmater und Domänencontroller mit globalem Katalog vollzogen ist, kann und muss der Infrastrukturmater seine Funktion nicht ausführen. Es gibt auf dem Domänencontroller mit dem globalen Katalog keine zu aktualisierenden Benutzerdaten. Wenn in einer Domäne auf allen Domänencontrollern der globale Katalog ausgeführt wird, ist es gleichgültig, auf welchem Domänencontroller der Infrastrukturmater liegt. Er findet nirgendwo veraltete Daten, um seiner Aufgabe nachkommen zu können.

11.1.4 Überprüfen und Ändern der Betriebsmasterrollen

Damit Sie die eben vorgeschlagenen Änderungen an der Verteilung der Betriebsmasterrollen vornehmen können, müssen Sie zunächst überprüfen, welcher Domänencontroller in der Domäne welche Betriebsmasterrollen ausführt. Das Überprüfen und anschließende Ändern geschieht bei allen fünf Betriebsmastern über die Konsole. Dieses Kapitel zeigt Ihnen, wie Sie sämtliche Betriebsmaster überprüfen und ändern können.

Überprüfen und Ändern des DNS-Masters

Um die Rolle des DNS-Masters zu überprüfen und anschließend zu ändern, führen Sie folgende Schritte durch:

1. Öffnen Sie die Konsole **ACTIVE DIRECTORY-DOMÄNEN UND -VERTRAUENSSTELLUNGEN**.
2. Klicken Sie mit der rechten Maus auf **ACTIVE DIRECTORY-DOMÄNEN UND -VERTRAUENSSTELLUNGEN** und wählen aus dem Kontextmenü **BETRIEBSMASTER** (siehe Abbildung 11.2). Es wird der aktuelle Betriebsmaster angezeigt.

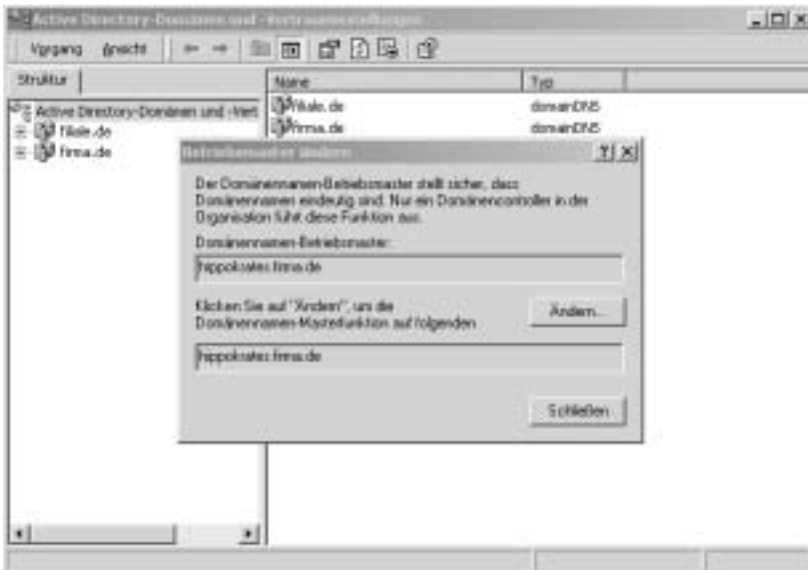


Abbildung 11.2: Überprüfen des DNS-Masters

3. Um den DNS-Master zu ändern, klicken Sie in der Baumstruktur auf den Domänencontroller, der neuer DNS-Master werden soll. Wählen Sie aus dem Kontextmenü den Eintrag VERBINDUNG MIT DOMÄNE HERSTELLEN.
4. Geben Sie nun im Feld DOMÄNE (siehe Abbildung 11.3) den Namen der gewünschten Domäne an, oder klicken Sie auf die Schaltfläche DURCHSUCHEN. Unten werden die in der Domäne verfügbaren Domänencontroller aufgelistet. Wählen Sie den gewünschten Domänencontroller aus und klicken auf OK.

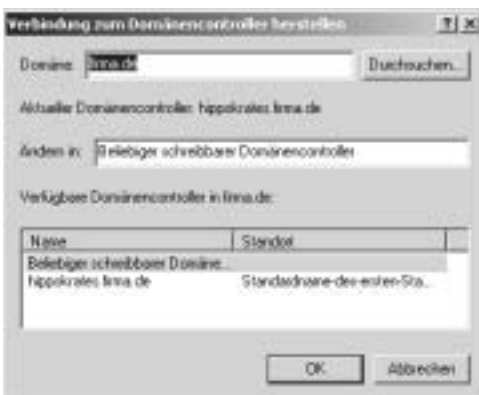


Abbildung 11.3: Ändern des DNS-Masters

5. Wählen Sie nun wieder den Eintrag BETRIEBSMAS-TER aus dem Kontextmenü, wie in Schritt 2 beschrieben. Klicken Sie auf ÄNDERN. Wenn Sie den neuen DNS-Master ausgewählt haben, klicken Sie auf OK.

Überprüfen und Ändern des Schemamasters

Um die Rolle des Schemamasters zu überprüfen und anschließend zu ändern, führen Sie folgende Schritte durch:

1. Öffnen Sie die Konsole ACTIVE DIRECTORY SCHEMA. Diese Konsole befindet sich standardmäßig nicht in der Windows-Verwaltung. Wie Sie diese Konsole verfügbar machen, wird in Kapitel 2.3.4 beschrieben.
2. Klicken Sie mit der rechten Maus auf ACTIVE DIRECTORY SCHEMA und wählen aus dem Kontextmenü BETRIEBSMASTER. Es wird der aktuelle Betriebsmaster angezeigt (siehe Abbildung 11.4).

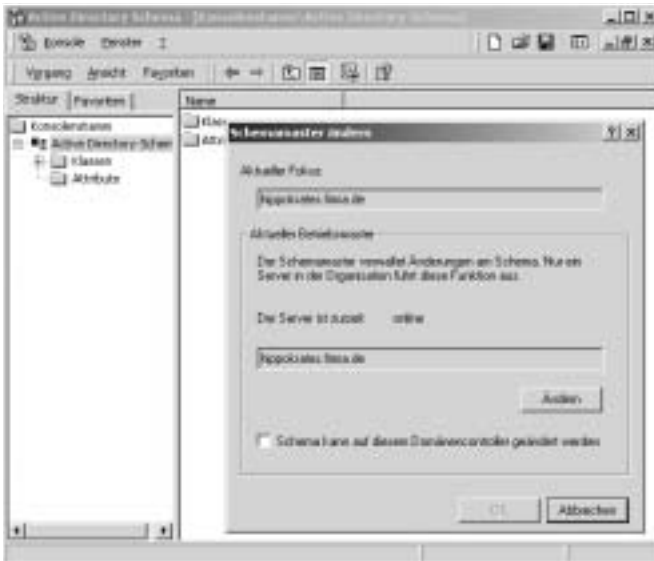


Abbildung 11.4: Überprüfen des Schemamasters

3. Um den Schemamaster zu ändern, klicken Sie mit der rechten Maus auf ACTIVE DIRECTORY SCHEMA und wählen aus dem Kontextmenü DOMÄNENCONTROLLER ÄNDERN.
4. Sie können nun entweder das Active Directory selbst einen beliebigen Domänencontroller auswählen lassen oder einen bestimmten Namen für den Schemamaster angeben (siehe Abbildung 11.5). Klicken Sie dann auf OK.



Abbildung 11.5: Ändern des Schemamasters

- Wählen Sie nun wieder BETRIEBSMASTER aus dem Kontextmenü, wie in Schritt 2 beschrieben. Klicken Sie auf die Schaltfläche ÄNDERN. Wenn Sie den neuen Schema-master ausgewählt haben, klicken Sie auf OK.

Überprüfen von RID-Master, PDC-Emulator und Infrastrukturmater

Um die Rollen des RID-Masters, PDC-Emulators und Infrastrukturmasters zu überprüfen und anschließend zu ändern, sind die Schritte identisch. Als Beispiel wird hier der RID-Master überprüft und geändert.

- Öffnen Sie die Konsole ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
- Klicken Sie mit der rechten Maus auf ACTIVE DIRECTORY-BENUTZER UND -COMPUTER und wählen aus dem Kontextmenü BETRIEBSMASTER. Es wird der aktuelle Betriebsmaster angezeigt (siehe Abbildung 11.6).

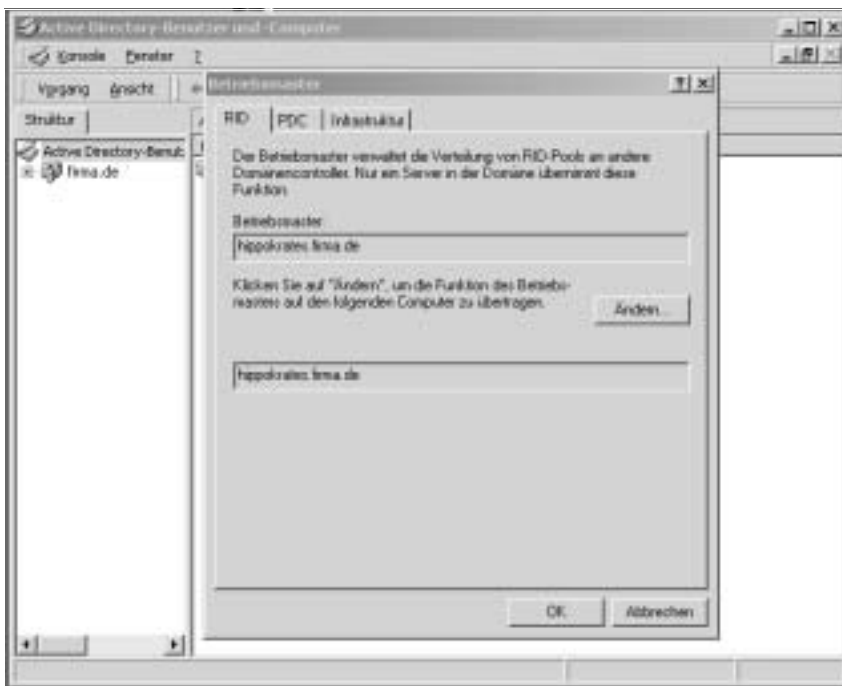


Abbildung 11.6: Überprüfen des RID-Masters

- Um den RID-Master zu ändern, klicken Sie in der Baumstruktur auf den Domänencontroller, der neuer RID-Master werden soll. Wählen Sie aus dem Kontextmenü VERBINDUNG MIT DOMÄNE HERSTELLEN. Es erscheint das in Abbildung 11.5 dargestellte Fenster.
- Geben Sie nun im Feld DOMÄNE den Namen der gewünschten Domäne an, oder klicken Sie auf DURCHSUCHEN. Unten werden die in der Domäne verfügbaren Domänencontroller aufgelistet. Wählen Sie den gewünschten Domänencontroller aus und klicken auf OK.

5. Wählen Sie nun wieder **BETRIEBSMASTER** aus dem Kontextmenü, wie in Schritt 2 beschrieben. Klicken Sie auf **ÄNDERN**. Wenn Sie den neuen RID-Master ausgewählt haben, klicken Sie auf **OK**.

11.1.5 Ausfälle von Betriebsmastern

In diesem Kapitel werden Sie erfahren, wie Sie auf den Ausfall von Betriebsmastern reagieren sollten. Hierbei gleich eines vorweg: Der Ausfall eines Betriebsmasters wird immer erst in dem Moment sichtbar, wenn eine seiner Funktion aufgerufen wird und aufgrund des Ausfalls nicht zur Verfügung steht. Wenn Sie für die Betriebsmaster Standby-Betriebsmaster eingerichtet haben, werden diese die Funktion übernehmen.

Sie können auch eine erzwungene Übertragung der Betriebsmasterrolle herbeiführen. Zuvor sollte jedoch immer geklärt werden, wo das Problem für den Ausfall des Betriebsmasters liegt. Erst wenn dabei klar wird, dass der Rechner nicht wieder in seiner alten Funktion arbeiten wird, sollten Sie zu diesem drastischen Schritt greifen.



Wenn Sie die Übertragung des DNS-Masters, Schemamasters oder RID-Masters erzwungen haben, dürfen die Computer, auf denen ursprünglich eine der Rollen ausgeführt wurde, nicht wieder ins Netzwerk integriert werden, bevor nicht die Festplatten neu formatiert und das Betriebssystem neu installiert worden sind. Alternativ dazu können Sie den alten Betriebsmaster aus dem Netzwerk entfernen und den Befehl **DCPROMO** ausführen. Dadurch wird er zu einem allein stehenden Server herabgestuft, auf dem alle Einträge bezüglich Active Directory gelöscht werden. Sobald Sie ihn wieder online geschaltet haben, führen Sie erneut **DCPROMO** aus, um den Server wieder zum Domänencontroller heraufzustufen.

Die Übernahme von Betriebsmasterrollen geschieht mithilfe des Kommandozeilenprogramms **NTDSUTIL**. Weitere Hinweise zu diesem Programm finden Sie in Kapitel 23.1.18. Der Vorgang ist für die Übernahme aller fünf Rollen identisch bis auf den Aufruf in Schritt 6.

1. Geben Sie an der Eingabeaufforderung `ntdsutil` ein. Es erscheint die Eingabeaufforderung `ntdsutil:`
2. Geben Sie nun den Befehl `roles` ein. Es erscheint die Eingabeaufforderung `fsmo maintenance:`
3. Geben Sie nun den Befehl `connections` ein. Es erscheint die Eingabeaufforderung `server connections:`
4. Geben Sie nun den Befehl `connect to server` und dahinter den vollqualifizierten Domännennamen (FQDN) des Domänencontrollers ein, der der neue Master werden soll, hier z.B. `hippokrates.firma.de` . Es erscheint wieder die Eingabeaufforderung `server connections:`
5. Geben Sie nun den Befehl `quit` ein. Es erscheint wieder die Eingabeaufforderung `fsmo maintenance:`
6. Geben Sie hier nun einen Befehl aus der Tabelle 11.1 an. Es erscheint wieder die Eingabeaufforderung `fsmo maintenance:`

7. Geben Sie hier den Befehl `quit`  ein. Es erscheint die Eingabeaufforderung `ntdsutil:`
8. Geben Sie zum Verlassen der Eingabeaufforderung abermals `quit`  ein.

Tabelle 11.1 zeigt den entsprechenden Befehl für Schritt 6 für die Rollenübernahme der verschiedenen Betriebsmaster.

Rollenübernahme des ...	Befehl für Schritt 6
DNS-Masters	<code>seize domain naming master</code>
Schemamasters	<code>seize schema master</code>
RID-Masters	<code>seize RID master</code>
PDC-Emulators	<code>seize PDC</code>
Infrastrukturmasters	<code>seize infrastructure master</code>

Tabelle 11.1: Rollenübernahmen der Betriebsmaster

12 Vertrauensstellungen

Vertrauensstellungen sind Beziehungen zwischen Domänen, wobei der Domänencontroller der einen Domäne die Authentifizierung von Benutzern einer anderen Domäne durchführen kann. Dieser Weg der Authentifizierung erfolgt nach einem festen Ablauf, der im Vertrauenspfad festgelegt ist.

12.1 Grundlagen der Vertrauensstellungen

In diesem Zusammenhang sind die Begriffe vertrauende Domäne und vertrauenswürdige Domäne wichtig. Die vertrauende Domäne ist diejenige, in der die Ressource vorhanden ist, auf die zugegriffen werden soll. Die vertrauenswürdige Domäne ist die Anmeldedomäne des Benutzers, der Zugriff auf eine Ressource haben möchte. Die vertrauenswürdige Domäne wird zuweilen auch als vertraute Domäne bezeichnet. Wenn beispielsweise ein Benutzer, der Mitglied der Domäne *firma.de* (vertrauenswürdige Domäne) ist, auf einen Drucker in der Domäne *filiale.de* (vertrauende Domäne) zugreifen möchte, wird zuvor vom Windows 2000-Sicherheitssystem geprüft, ob zwischen den beiden Domänen eine Vertrauensstellung besteht oder nicht. Dabei wird der Vertrauenspfad (siehe Abbildung 12.1) zwischen zwei Domänencontrollern der vertrauenden und vertrauenswürdigen Domäne berechnet.

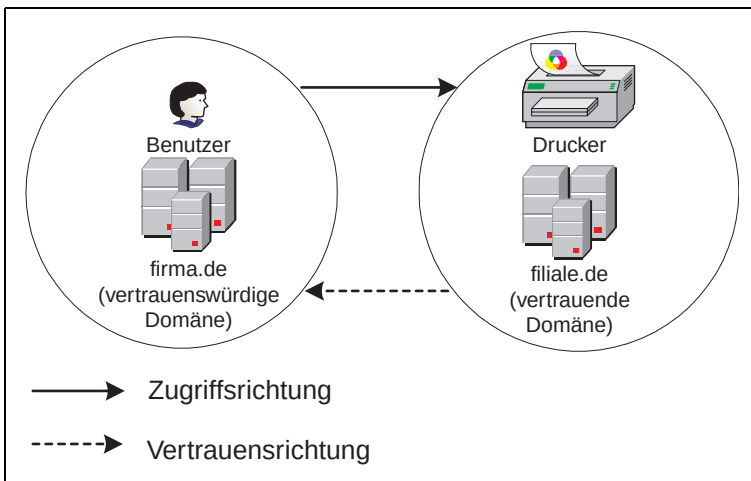


Abbildung 12.1: Der Vertrauenspfad zwischen Domänen

Der Vertrauenspfad kann in die Vertrauensrichtung oder die Zugriffsrichtung verlaufen.

Die Vertrauensstellungen können zwei verschiedene Authentifizierungsarten durchführen. Dies sind die Kerberos V5-Authentifizierung und die NTLM-Authentifizierung. Kerberos V5-Authentifizierung ist der Standard für Windows 2000 Clients und Clients, auf denen Windows 2000-Client-Software ausgeführt wird. Die NTLM-Authentifizierung wird verwendet, wenn einer der beiden an der Authentifizierung beteiligten Computer das Kerberos V5-Protokoll nicht unterstützt. Die Funktionsweise der beiden Authentifizierungsarten wurde bereits in Kapitel 2.2.3 abgehandelt.

Bei der Kerberos V5-Authentifizierung fordert der Client bei dem Domänencontroller, auf dem sein Benutzerkonto liegt, ein Ticket für den Ressourcenserver einer anderen vertrauenden Domäne an. Das Ticket wird von einem neutralen Vermittler ausgestellt. Mit diesem Ticket kann sich der Client an dem Ressourcenserver der anderen vertrauenden Domäne authentifizieren und auf die Ressourcen zugreifen.

Wenn ein Client über die NTLM-Authentifizierung auf einen Ressourcenserver einer anderen vertrauenden Domäne zugreifen möchte, muss der Ressourcenserver eine Anfrage an den Domänencontroller der Domäne senden, auf dem das Benutzerkonto des Clients liegt. An diesem Domänencontroller wird dann überprüft, ob die Authentifizierungsinformationen des Clients richtig oder falsch sind.

Es gibt insgesamt fünf verschiedene Möglichkeiten, nach denen Vertrauensstellungen zwischen Domänen aufgebaut werden können. Es gibt transitive, nicht transitive, bidirektionale und unidirektionale sowie explizite Vertrauensstellungen.

12.1.1 Transitive Vertrauensstellungen

Sämtliche Vertrauensstellungen von Domänen innerhalb einer Windows 2000-Gesamtstruktur sind transitiv. Die transitive Vertrauensstellung ist auf Windows 2000-Domänen beschränkt, und innerhalb einer Windows 2000-Gesamtstruktur können keine nicht transitiven Vertrauensstellungen hergestellt werden. Außerdem sind transitive Vertrauensstellungen stets bidirektional, d.h., die Vertrauensstellung funktioniert in beide Richtungen zwischen zwei Domänen. Näheres dazu lesen Sie in Kapitel 12.1.3.

Diese transitive Vertrauensstellung wird in folgenden beiden Fällen jedes Mal automatisch eingerichtet:

- ▶ wenn eine neue untergeordnete Domäne unter einer bestehenden Domäne erstellt wird und
- ▶ wenn eine neue Domänenstruktur in einer Gesamtstruktur erstellt wird.

Dieser automatische Vorgang wird auch als implizit bezeichnet. Damit wird gewährleistet, dass sich beim Erstellen neuer untergeordneter Domänen die transitiven Vertrauensstellungen in der Hierarchie bis zur Stammdomäne der Domänenstruktur fortsetzen. Besonders in einer großen und stetig wachsenden Domänenstruktur entfällt so die unter NT noch notwendige manuelle Erstellung von Vertrauensstellungen.

Auch beim Integrieren einer Domänenstruktur in eine Gesamtstruktur wird eine transitive Vertrauensstellung zwischen der Stammdomäne der Gesamtstruktur und der Stammdomäne der neuen Domäne hergestellt. Wenn der neuen Domäne untergeordnete Domänen hinzugefügt werden und somit die neue Domäne zur Domänenstruktur wird,

setzt sich die Vertrauensstellung auch innerhalb dieser untergeordneten Domänen bis zur Stammdomäne fort. Hiermit ist eine implizite transitive Vertrauensstellung zwischen allen Domänen der Gesamtstruktur sichergestellt.

Es ist auch möglich, zwischen Windows 2000-Domänen in einer Domänen- oder Gesamtstruktur explizite Vertrauensstellungen einzurichten. Dies ist z.B. dann sinnvoll, wenn in einer komplexen Struktur der Vertrauenspfad zwischen zwei bestimmten Domänen verkürzt werden soll. Näheres dazu erfahren Sie in Kapitel 12.1.5.

Da über die Vertrauenspfade auch die Authentifizierung geregelt wird, kann ein Benutzer einer beliebigen Domäne der Gesamtstruktur an jeder anderen Domäne der Gesamtstruktur authentifiziert werden. Außerdem ist es ihm so möglich, mit nur einer Anmeldung an der Domäne auf sämtliche Ressourcen in der Gesamtstruktur zugreifen zu können, für die ihnen Zugriffsberechtigungen erteilt worden sind.

12.1.2 Nicht transitive Vertrauensstellungen

Eine nicht transitive oder intransitive Vertrauensstellung ist auf zwei Domänen beschränkt und wird nicht an untergeordnete Domänen weitervererbt. Die Einrichtung von nicht transitiven Vertrauensstellungen erfolgt nicht automatisch, sondern muss manuell eingerichtet werden. Lesen Sie hierzu das Kapitel 12.1.6. Weiterhin sind nicht transitive Vertrauensstellungen unidirektional. Näheres dazu in Kapitel 12.1.4.

Eine nicht transitive Vertrauensstellung kann zwischen den folgenden Domänen hergestellt werden:

- ▶ Windows 2000- und Windows NT-Domäne im gemischten Modus. Wird die NT-Domäne auf Windows 2000 aktualisiert, bleiben die existierenden NT-Vertrauensstellungen erhalten.
- ▶ Zwei Windows 2000-Domänen in verschiedenen Gesamtstrukturen

12.1.3 Bidirektionale Vertrauensstellungen

Sämtliche impliziten transitiven Vertrauensstellungen einer Windows 2000-Gesamtstruktur sind bidirektional. Dies bedeutet, dass sich zwei Domänen gegenseitig vertrauen und somit Anfragen zur Authentifizierung in beide Richtungen zwischen den Domänen ausgetauscht werden können.

Eine nicht transitive bidirektionale Vertrauensstellung kann aufgebaut werden, indem zwischen den beiden Domänen zwei explizite unidirektionale Vertrauensstellungen in jeweils eine Richtung aufgebaut werden. Eine doppelte unidirektionale Verbindung wird zu einer bidirektionalen Verbindung. Lesen Sie hierzu das Kapitel 12.1.6.

12.1.4 Unidirektionale Vertrauensstellungen

Eine unidirektionale Vertrauensstellung ist eine einseitige Vertrauensstellung. Hierbei sieht zwar die Domäne 1 die Domäne 2 als vertrauenswürdig an, aber Domäne 2 sieht damit nicht automatisch Domäne 1 als vertrauenswürdig an. Unidirektionale Vertrauensstellungen können nur intransitiv sein. Die Anforderungen zur Authentifizierung

werden nur von der vertrauenden Domäne an die vertrauenswürdige geleitet, aber nicht umgekehrt. Wenn Domäne 1 und Domäne 2 sowie Domäne 2 und Domäne 3 über eine unidirektionale Vertrauensstellung untereinander verfügen, besteht dennoch keine Vertrauensstellung zwischen Domäne 1 und 3.

Unidirektionale Vertrauensstellungen sind nie implizit, sondern müssen immer manuell erstellt werden.

Unidirektionale Vertrauensstellungen können wie nicht transitive Vertrauensstellungen zwischen den folgenden Domänen hergestellt werden:

- ▶ Windows 2000- und Windows NT-Domäne im gemischten Modus. Wird die NT-Domäne auf Windows 2000 aktualisiert, bleiben die existierenden NT-Vertrauensstellungen erhalten.
- ▶ Zwei Windows 2000-Domänen in verschiedenen Gesamtstrukturen

Zwischen Windows 2000-Domänen in einer Gesamtstruktur können keine unidirektionalen Verbindungen hergestellt werden, da diese Verbindungen alle bidirektional sind.

12.1.5 Explizite Vertrauensstellungen

Explizite Vertrauensstellungen werden ausschließlich manuell eingerichtet und können nicht automatisch implizit erstellt werden. Das Einrichten expliziter Vertrauensstellungen wird im nächsten Kapitel beschrieben. Explizite Vertrauensstellungen werden unterschieden in externe Vertrauensstellungen und verknüpfte Vertrauensstellungen.

Externe Vertrauensstellungen

Externe Vertrauensstellungen dienen der Authentifizierung von Benutzern einer Domäne, die nicht in der Gesamtstruktur liegt. So kann der Zugriff auf Ressourcen einer bestimmten Domäne außerhalb der Gesamtstruktur sichergestellt werden, die nicht in den Vertrauenspfaden innerhalb der Gesamtstruktur eingetragen ist. Sie sind grundsätzlich unidirektional und intransitiv.

Bei einer externen Vertrauensstellung kann über zwei unidirektionale intransitive Pfade eine explizite bidirektionale Vertrauensstellung hergestellt werden.

Verknüpfte Vertrauensstellungen

Über verknüpfte Vertrauensstellungen wird innerhalb einer komplexen Windows 2000-Gesamtstruktur ein direkter und damit stark verkürzter Vertrauenspfad zwischen zwei Domänen hergestellt. Es entfällt ein langer vom Windows 2000-Sicherheitssystem zu berechnender Vertrauenspfad, um zu prüfen, ob das Konto der Quelldomäne Zugriffsrechte auf die Ressource in der Zieldomäne besitzt. Der Pfad kann nun direkt geprüft werden. Sehr effektiv ist diese Verknüpfung zwischen Domänen der mittleren oder unteren Hierarchieebenen, da hier der Vertrauenspfad enorm verkürzt wird.

Verknüpfte Vertrauensstellungen sind stets bidirektional und transitiv.

Nachdem nun alle Varianten von Vertrauensstellungen unter Windows 2000 vorgestellt worden sind, soll die folgende Abbildung einen abschließenden Überblick geben.

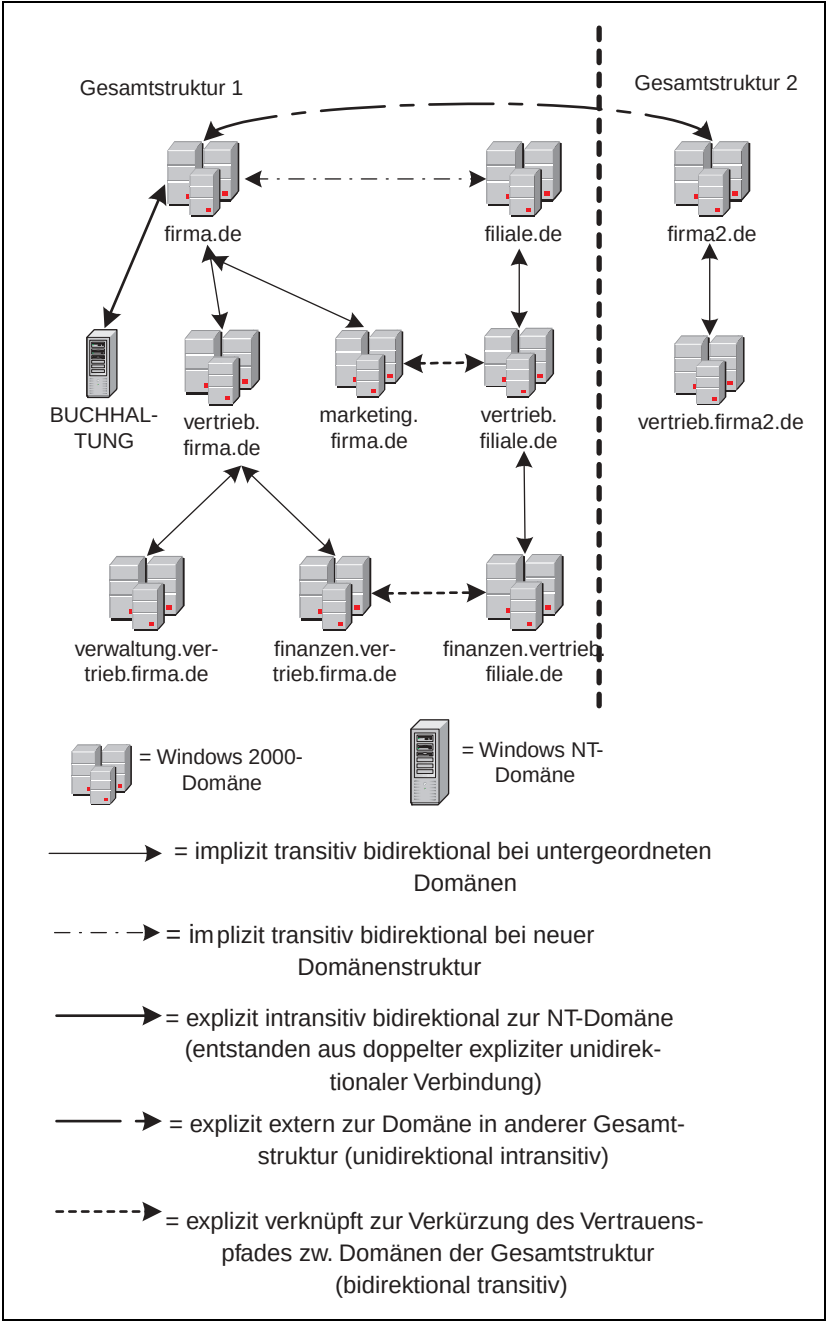


Abbildung 12.2: Übersicht über die verschiedenen Vertrauensstellungen

Innerhalb der Gesamtstruktur 1 verfügen die untergeordneten Domänen von *firma.de* und *filiale.de* jeweils über implizite transitive bidirektionale Vertrauensstellungen. Diese wurden bei der Installation der Domänen automatisch erstellt. Die beiden Stammdomänen *firma.de* und *filiale.de* verfügen ebenfalls über eine implizite transitive bidirektionale Vertrauensstellung. Diese wurde bei der Eingliederung der Domänenstruktur *filiale.de* in die Struktur *firma.de* eingerichtet.

Weiterhin befindet sich in der Gesamtstruktur 1 noch eine NT-Domäne BUCHHALTUNG. Zwischen dieser Domäne und *firma.de* wurden manuell zwei explizite unidirektionale intransitive Verbindungen erstellt. Daraus wurde eine explizite intransitive bidirektionale Verbindung.

Um den Vertrauenspfad zu verkürzen, wurde zwischen den Domänen zweiter und dritter Ebene eine explizite verknüpfte Vertrauensstellung eingerichtet. Die Domänen *marketing.firma.de* und *vertrieb.filiale.de* sind auf der zweiten Ebene, die Domänen *finanzen.vertrieb.firma.de* und *finanzen.vertrieb.filiale.de* auf der dritten Ebene direkt miteinander verbunden.

Außerdem wurde zu der Domäne *firma2.de* in der separaten Gesamtstruktur eine explizite externe unidirektionale Verbindung zur Domäne *firma.de* hergestellt. Diese Vertrauensstellung wird nicht auf die untergeordneten Domänen vererbt.

Wenn Sie über eine reine Windows 2000/2003-Domänenlandschaft verfügen, wird die häufigste Konstellation die der impliziten transitiven Vertrauensstellungen zwischen Domänen oder zu einer Domänenstruktur sein.

12.1.6 Erstellen expliziter Vertrauensstellungen

Das Erstellen und Verwalten expliziter Vertrauensstellungen geschieht über die Konsole Active Directory-Domänen und Vertrauensstellungen. Um eine Vertrauensstellung zwischen zwei Domänen manuell zu erstellen, führen Sie folgende Schritte durch:

1. Öffnen Sie die Konsole ACTIVE DIRECTORY-DOMÄNEN UND -VERTRAUENSSTELLUNGEN.
2. Klicken Sie mit der rechten Maus auf die gewünschte Domäne und wählen aus dem Kontextmenü EIGENSCHAFTEN. Klicken Sie dann auf die Registerkarte VERTRAUENSSTELLUNGEN.
3. Wählen Sie hier entweder HINZUFÜGEN im Bereich DOMÄNEN, DENEN DIESE DOMÄNE VERTRAUT oder im Bereich DOMÄNEN, DIE DIESER DOMÄNE VERTRAUEN (siehe Abbildung 12.3).



Abbildung 12.3: Einrichten expliziter Vertrauensstellungen

4. Geben Sie nun den Namen der vertrauten Domäne an. Sofern es sich um eine Windows 2000-Domäne handelt, geben Sie den vollständigen DNS-Namen an, bei einer Windows NT-Domäne den NetBIOS-Namen. Geben Sie außerdem das Kennwort für die vertraute Domäne ein. Dieses Kennwort muss identisch sein mit dem Kennwort, das Sie für die zu vertrauende Domäne eingegeben haben (siehe Abbildung 12.4).



Abbildung 12.4: Hinzufügen der vertrauten Domäne

5. Wiederholen Sie danach dieselben Schritte für die Domäne, die den zweiten Part der Vertrauensstellung ausmachen soll.

Die folgende Tabelle gibt Ihnen nochmals eine Zusammenfassung aller möglichen Vertrauensstellungen sowie deren Spezifikationen.

Vertrauensstellung	Merkmale
Transitiv	Nicht für NT-Domänen Stets bidirektional Wird automatisch (implizit) erstellt beim Hinzufügen untergeordneter Domänen sowie Domänen(strukturen) zur Gesamtstruktur
Intransitiv	Für 2003-, 2000- und NT-Domänen oder zwei Domänen in verschiedenen Gesamtstrukturen Stets unidirektional; wird bidirektional, wenn zwei explizite unidirektionale intransitive Verbindungen zwischen zwei Domänen hergestellt werden Nur manuell erstellbar, nicht automatisch Auf jeweils zwei Domänen beschränkt, keine Vererbung
Bidirektional	Alle impliziten transitiven Vertrauensstellungen Authentifizierungsinformationen können zwischen zwei Domänen in beide Richtungen ausgetauscht werden. Nur transitiv
Unidirektional	Für 2003-, 2000- und NT-Domänen oder zwei Domänen in verschiedenen Gesamtstrukturen Nur einseitige Vertrauensrichtung Nur intransitiv; wird transitiv, wenn zwei explizite unidirektionale intransitive Verbindungen zwischen zwei Domänen hergestellt werden
Explizit	Wird unterschieden in: Extern: Unidirektional Intransitiv Zur Verknüpfung mit Domänen außerhalb der Gesamtstruktur Verknüpft: Bidirektional Transitiv Zur Verkürzung des Vertrauenspfades von zwei Domänen in der Gesamtstruktur

Tabelle 12.1: Die verschiedenen Vertrauensstellungen

12.1.7 Erweiterte Vertrauensstellungen unter Windows Server 2003

Der Windows Server 2003 kann neben den eben beschriebenen Vertrauensstellungen auch eine Vertrauensstellung zu einer Domäne in einer anderen Gesamtstruktur herstellen. Dabei können sämtliche Domänen einer Gesamtstruktur zu allen Domänen einer anderen Gesamtstruktur eine transitive Vertrauensstellung besitzen. Hierzu ist lediglich eine Verknüpfung der Vertrauensstellungen zwischen den beiden Root-Domänen der beiden Gesamtstrukturen erforderlich. Bei einer die Gesamtstrukturübergreifenden Vertrauensstellung von drei oder mehr Gesamtstrukturen sind die Vertrauensstellungen

nicht mehr transitiv. Wenn Gesamtstruktur 1 eine Vertrauensstellung zu Gesamtstruktur B besitzt und Gesamtstruktur B zu C, so wird nicht automatisch eine Vertrauensstellung zwischen Gesamtstruktur A und C eingerichtet. Die die Gesamtstruktur übergreifenden Vertrauensstellungen können unidirektional und bidirektional sein.

Zusätzlich steht Ihnen unter 2003 ein verbesserter Wizard zur Verfügung, mit dem Sie sämtliche Arten von Vertrauensstellungen einrichten können. Sie erreichen diesen Wizard über die mmc ACTIVE DIRECTORY-DOMÄNEN UND VERTRAUENSSTELLUNGEN. Dort wählen Sie aus den Eigenschaften der Domäne die Registerkarte VERTRAUENSSTELLUNGEN und klicken auf NEUE VERTRAUENSSTELLUNG. Ein Assistent leitet Sie durch die einzelnen Konfigurationsschritte. Sie haben die Möglichkeit, eine Vertrauensstellung zwischen der aktuellen Domäne und einer Windows-Domäne derselben bzw. einer anderen Gesamtstruktur, einer Windows NT 4.0-Domäne oder einem Kerberos V5-Bereich herzustellen.

1. Nach der Willkommensmeldung geben Sie den Namen der Domäne ein, mit der die neue Vertrauensstellung eingerichtet werden soll (siehe Abbildung 12.5). Der Name sollte als DNS-Name angegeben werden. Klicken Sie dann auf WEITER.

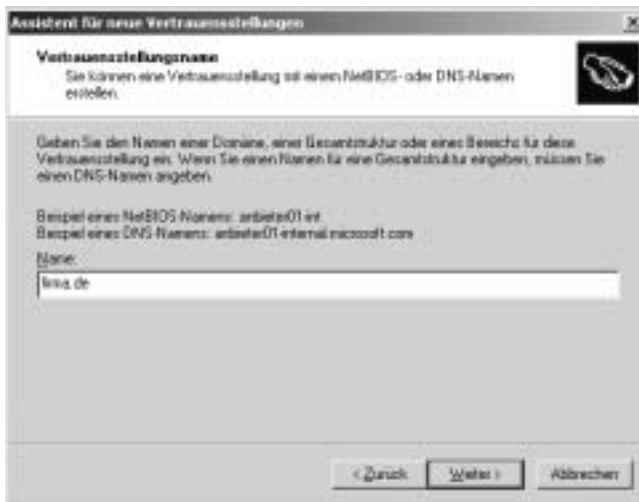


Abbildung 12.5: Auswahl der Domäne für die Vertrauensstellung

2. Sie müssen nun entscheiden, ob die Vertrauensstellung mit einer Windows-Domäne hergestellt werden soll (siehe Abbildung 12.6). Ist dies der Fall, markieren Sie die Checkbox VERTRAUENSSTELLUNG MIT EINER WINDOWS-DOMÄNE und geben den Namen der Domäne ein. Handelt es sich bei dem Server nicht um einen Windows-Domänencontroller, so können Sie eine Vertrauensstellung zu einem Kerberos V5-kompatiblen Bereich herstellen. Aktivieren Sie in diesem Fall die Checkbox BEREICHS-VERTRAUENSSTELLUNG. Klicken Sie dann auf WEITER.

12 Vertrauensstellungen

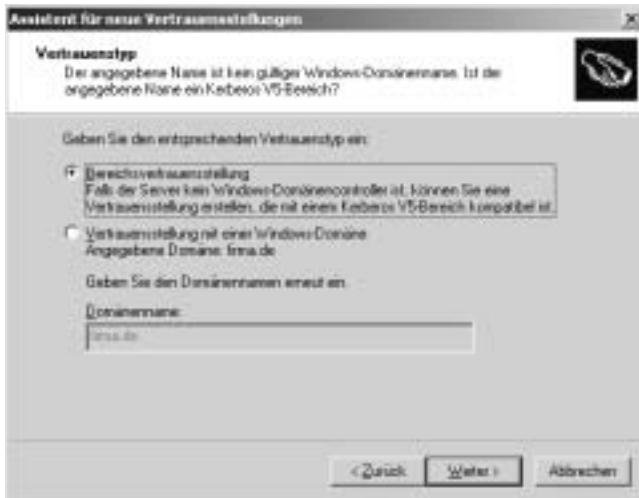


Abbildung 12.6: Auswahl des Vertrauensstyps

3. Als Nächstes bestimmen Sie, ob die Vertrauensstellung transitiv oder intransitiv werden soll (siehe Abbildung 12.7). Die Unterschiede sind in Kapitel 12.1.1 und 12.1.2 erläutert. Klicken Sie dann auf WEITER.



Abbildung 12.7: Auswahl zwischen transitiver und intransitiver Vertrauensstellung

4. Dann wird die Richtung der Vertrauensstellung festgelegt (siehe Abbildung 12.8). Sie können zwischen bidirektional (siehe Kapitel 12.1.3), unidirektional eingehend sowie unidirektional ausgehend wählen. Bei der Wahl UNIDIREKTIONAL EINGEHEND können die Benutzer der aktuellen Domäne in der angegebenen Domäne authentifiziert werden, bei UNIDIREKTIONAL AUSGEHEND authentifiziert die aktuelle Domäne Benutzer der angegebenen Domäne. Klicken Sie dann auf WEITER.



Abbildung 12.8: Die Richtung der Vertrauensstellung wählen

5. Im nächsten Schritt wird ein Kennwort für die Vertrauensstellung festgelegt (siehe Abbildung 12.9). Dasselbe Kennwort wird benötigt, wenn Sie die Vertrauensstellung der angegebenen Domäne mit der aktuellen Domäne einrichten. Klicken Sie dann auf WEITER.

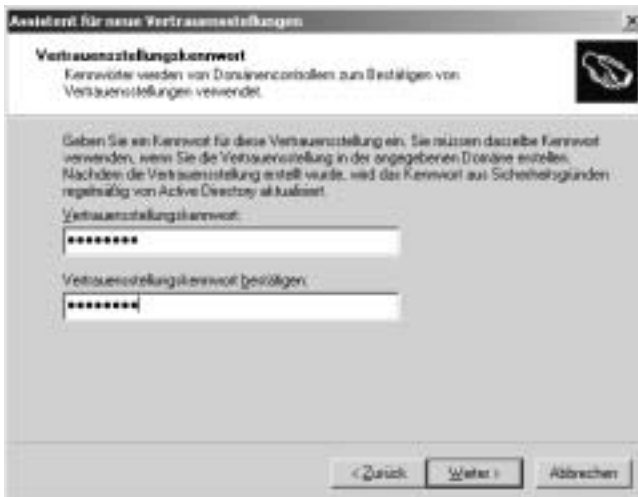


Abbildung 12.9: Festlegen eines Kennworts für die Vertrauensstellung

- Es erscheint eine Zusammenfassung der Einstellungen (siehe Abbildung 12.10). Um Einstellungen zu ändern, gehen Sie über die Schaltfläche ZURÜCK bis an die gewünschte Stelle. Klicken Sie hier auf FERTIG STELLEN.



Abbildung 12.10: Fertigstellen der neuen Vertrauensstellung

Die neu eingerichtete Vertrauensstellung befindet sich nun in der Liste der vorhandenen Vertrauensstellungen. Diese finden Sie auf der Registerkarte VERTRAUENSSTELLUNGEN in den Eigenschaften der Domäne.

13

Die Datenbank NTDS und der Systemdatenträger SYSVOL

Im Rahmen der Installation von Active Directory wurden kurz die Begriffe NTDS-Verzeichnisdatenbank und Systemdatenträger *SYSVOL* angesprochen.

13.1 NTDS und SYSVOL im Überblick

Diese beiden Komponenten sollen nun näher erläutert werden. Beide Elemente werden während der Installation eines Domänencontrollers angelegt. Die Verzeichnisdatenbank kann auf einem beliebigen FAT16-, FAT32- oder NTFS-Datenträger erstellt werden, der Ordner *SYSVOL* nur auf einem NTFS-Datenträger. Standardmäßig werden sie in die Verzeichnisse *%SYSTEMROOT%\NTDS* sowie *%SYSTEMROOT%\SYSVOL* installiert. Dieser Pfad kann aber während der Installation geändert werden. Auch nach der Installation des Active Directory haben Sie noch die Möglichkeit, das *SYSVOL*-Verzeichnis zu verschieben. Dieser Vorgang wird in Kapitel 13.1.3 und Kapitel 13.1.4 erläutert.

13.1.1 Die Verzeichnisdatenbank NTDS

Die Verzeichnisdatenbank *NTDS* wird auf allen Domänencontrollern gespeichert. Sie wird zuweilen auch nur als Verzeichnis bezeichnet. In dieser Datenbank befinden sich die replizierten Daten. Diese Daten enthalten Informationen zu sämtlichen Objekten im Verzeichnis, z.B. zu Computern, Benutzern, OUs oder auch den Gruppenrichtlinien. Diese Inhalte stehen damit sämtlichen Netzwerkbenutzern zur Verfügung.

Die Datei *NTDS.dit* ist der physische Speicherort der Datenbank. Die Dateierendung *.dit* bedeutet Directory Information Tree. Dieser Ordner ist nicht freigegeben und bietet somit einen geschützten Speicherort für die nicht öffentlichen Daten im Gegensatz zu den öffentlichen Daten im freigegebenen Ordner *SYSVOL*.

Ist die *NTDS.dit*-Datei auf einem Domänencontroller nicht mehr vorhanden, so ist diese nicht wieder herstellbar und auch durch eine Replikation nicht aktualisierbar. Außerdem kann nur noch im Reparaturmodus eine Anmeldung an dem Domänencontroller erfolgen, auf dem die Datenbankdatei fehlt.

Jeder Domänencontroller in der Domäne besitzt eine Kopie des Verzeichnisses. Somit ist eine hohe Verfügbarkeit der Verzeichnisdaten für die Benutzer in der Domäne gewährleistet. Werden auf einem Domänencontroller Änderungen am Verzeichnis durchgeführt, so werden von diesem Domänencontroller aus die Änderungen auf die übrigen Domänencontroller innerhalb der Domäne, Domänenstruktur oder Gesamtstruktur repliziert. Die Replikation von Daten zwischen den Domänencontrollern umfasst drei unterschiedliche Gruppen von Verzeichnisdaten: Domänen-, Konfigurations- und Schemadaten.

Die Domänenendaten enthalten Informationen zu den Objekten in einer Domäne, z.B. Attribute zu Benutzerkonten, Kontakte usw. Alle Änderungen an den Objekten werden in den Domänenendaten gespeichert. Hierzu zählen das Löschen oder Erstellen von Objekten oder das Ändern der Objektattribute. So werden beispielsweise für jedes neue Benutzerkonto ein Objekt für das Konto selbst angelegt sowie die Attributdaten gespeichert.

Konfigurationsdaten listen sämtliche Gesamtstrukturen, Strukturen, Domänen und Standorte der Domänencontroller sowie globalen Kataloge auf. Diese Daten spiegeln den strukturellen Aufbau des Verzeichnisses wider.

Die Schemadaten dienen der Definition der Objekt- und Attributdaten, die standardmäßig im Verzeichnis gespeichert werden können. Das Standardschema ist dynamisch erweiterbar. Es können sowohl für bereits vorhandene Objekte neue Attribute erstellt als auch ganz neue Attribute oder Objekttypen definiert werden. Nähere Details zum Ändern des Schemas finden Sie in Kapitel 24.3.

Wenn auf dem Domänencontroller auch der globale Katalog angesiedelt ist, beinhaltet er auch einen Teil der Verzeichnisdaten der übrigen Domänen in der Gesamtstruktur. Der globale Katalog wurde ausführlich in Kapitel 3.3 erläutert.

13.1.2 Der Systemdatenträger SYSVOL

Im Gegensatz zu den nicht öffentlichen Daten im Ordner *NTDS* beinhaltet der freigegebene Datenträger die öffentlichen Verzeichnisdaten. Auch diese werden auf andere Domänencontroller repliziert.

SYSVOL beinhaltet eine Ordnerstruktur, die auf allen Domänencontrollern vorhanden ist. Der Datenträger umfasst Skripte sowie einige Gruppenrichtlinienobjekte der aktuellen Domäne. Abbildung 13.1 zeigt die Ordnerstruktur des Domänencontrollers für die Domäne *firma.de*.



Abbildung 13.1: Die Ordnerstruktur von SYSVOL

Die Replikation von *SYSVOL* geschieht in demselben Intervall wie die Replikation des Active Directory. Standardmäßig liegt dieser bei zehn Minuten. Es kann jedoch vorkommen, dass die Dateireplikation auf oder von dem neu erstellten Systemdatenträger erst

beim zweiten Replikationsdurchlauf erfolgt, weil bei der ersten Replikation die übrigen Systemdatenträger erst über das Vorhandensein eines neuen SYSVOL-Ordners in Kenntnis gesetzt werden müssen.

Der oder die Datenträger, auf denen sich die Verzeichnisse *NTDS* und *SYSVOL* befinden, müssen regelmäßig einem Backup unterzogen werden und idealerweise auf RAID-Datenträgern liegen, um die Ausfallsicherheit zu erhöhen. Weitere Hinweise zum Backup des Active Directory finden Sie in Kapitel 21.6.

13.1.3 Verschieben von SYSVOL per Active Directory-Installations-Wizard

Das Verschieben des *SYSVOL*-Verzeichnisses kann erforderlich werden, wenn auf dem Datenträger nicht mehr genügend Speicherplatz zur Verfügung steht. Zum Verschieben können Sie entweder den Active Directory-Installations-Wizard benutzen oder den gesamten Prozess manuell durchführen. Der Wizard bietet zwar die einfachere Methode, doch ist bei diesem Verfahren immer das Herunterstufen des jeweiligen Domänencontrollers impliziert. Beim Verschieben über den Installations-Wizard wird nämlich zunächst das Active Directory vom Domänencontroller entfernt und dann neu installiert, wobei Sie den Speicherort des *SYSVOL*-Verzeichnisses neu angeben können.

Dieses Verfahren, das Active Directory neu zu installieren, ist jedoch nur bedingt praktikabel. Werden auf dem Domänencontroller zahlreiche weitere Dienste ausgeführt, die vom Active Directory abhängig sind, so müssen Sie diese ebenfalls neu installieren. Je umfangreicher und größer der Inhalt des Verzeichnisses ist, desto länger wird es auch dauern, bis der wieder neu installierte Domänencontroller sämtliche Informationen von seinen Replikationspartnern erhalten hat. Grundvoraussetzung ist, dass sich in der Domäne zumindest ein weiterer Domänencontroller befindet, der zur Verfügung steht, während auf einem Domänencontroller das *SYSVOL*-Verzeichnis verschoben wird. Bedenken Sie auch, dass Sie bei der Deinstallation des Active Directory die in Kapitel 9.3 beschriebenen Punkte beachten. Denken Sie daran, eventuelle Betriebsmasterrollen sowie die Rolle des globalen Katalogservers auf andere Domänencontroller zu übertragen. Prüfen Sie auch, ob der Domänencontroller als DNS-Server für die Domäne konfiguriert ist. In diesem Fall muss ein anderer Domänencontroller diese Rolle übernehmen. Überprüfen Sie auch die Kommunikation mit den übrigen Domänencontrollern. Verwenden Sie hierzu das Kommandozeilenprogramm *netdiag* mit folgendem Befehl:

```
netdiag /test:dsgetdc 
```

Um zusätzliche Informationen zu erhalten, benutzen Sie zusätzlich den Parameter */v*. Sie sollten als Ergebnis `DC discovery test: Passed` erhalten.

Haben Sie alle diese Schritte erfolgreich vorbereitet, können Sie das Active Directory vom Domänencontroller entfernen sowie das Serverobjekt in der mmc *ACTIVE DIRECTORY-STANDORTE UND -DIENSTE* löschen. Danach können Sie das Active Directory neu installieren und einen neuen Speicherort für das *SYSVOL*-Verzeichnis festlegen. Überprüfen Sie danach über die mmc *ACTIVE DIRECTORY-STANDORTE UND -DIENSTE*, ob sich der Domänencontroller am korrekten Standort befindet. Bei Bedarf verschieben Sie diesen an den gewünschten Standort (siehe Kapitel 14.1.4). Abschließend prüfen Sie die DNS-Konfiguration.

13.1.4 Manuelles Verschieben des SYSVOL-Ordners

Alternativ zu der eben beschriebenen Methode können Sie den *SYSVOL*-Ordner auch manuell verschieben. Hierbei müssen Sie entscheiden, ob Sie den gesamten *SYSVOL*-Ordner oder nur den Ordner *Staging Area* verschieben möchten. Letzteres Verfahren wird in Kapitel 13.1.6 beschrieben.

SYSVOL verwendet eine komplexe Ordnerstruktur mit zahlreichen Unterordnern. Wenn Sie diese Struktur über den Windows Explorer kopieren, achten Sie darauf, dass Sie auch sämtliche versteckte Ordner kopieren. Achten Sie auch auf die Aktualisierung der sog. *Junction Points*. Weitere Hinweise zu diesen speziellen Ordnern finden Sie im nächsten Kapitel.

Nachdem Sie die neue Ordnerstruktur erstellt und die Verknüpfungen der *Junction Points* aktualisiert haben, müssen Sie diese wieder mit Daten füllen. Dies geschieht bei der Replikation des Domänencontrollers mit einem seiner Replikationspartner. Achten Sie nach dem Verschieben des *SYSVOL*-Verzeichnisses darauf, ob sich relevante Sicherheitseinstellungen geändert haben. Sie sollten die Sicherheitseinstellungen wieder auf den Stand bringen, der bei der ursprünglichen Installation eingerichtet worden ist. Andernfalls kann es zum unerlaubten Zugriff auf An- und Abmeldeskripte oder Gruppenrichtlinienobjekte kommen.

Die speziellen Ordner „Junction Points“

Eine weitere Besonderheit im *SYSVOL*-Ordner sind die sog. *Junction Points*. Hierbei handelt es sich um spezielle Ordner, die Verknüpfungen zu anderen Ordnern enthalten. Im Windows Explorer erscheinen diese wie herkömmliche Ordner und werden auch vom Dateisystem entsprechend behandelt. Den Unterschied sehen Sie am besten, wenn Sie an der Eingabeaufforderung über den `dir`-Befehl den Inhalt eines Ordners anzeigen. Herkömmliche Ordner werden dort mit `<DIR>` beschrieben, während die *Junction Points* mit `<JUNCTION>` bezeichnet werden.

Ein Problem ergibt sich jedoch, wenn Sie diese Ordner an einen anderen Ort kopieren oder verschieben. Dabei wird zwar der Ordner an sich verschoben oder kopiert, aber die in ihm enthaltene Verknüpfung bezieht sich immer noch auf die Position des ursprünglichen Speicherorts.

Sobald ein Programm auf einen *Junction Point* zugreift, findet automatisch eine Weiterleitung an das in der Verknüpfung angegebene Ziel statt. *Junction Points* können nur mit dem Programm *LINKD* erstellt, gelöscht und aktualisiert werden. Auch die Verknüpfung an sich kann mit diesem Programm betrachtet werden. *LINKD* ist Bestandteil des Server Resource Kits.

Im Verzeichnis *SYSVOL* sind zwei *Junction Points* enthalten, die auf Ordner innerhalb von *SYSVOL* verweisen. Um die Verknüpfung zu aktualisieren, müssen Sie die Pfadinformation im Active Directory sowie in der Registry neu angeben.



Da für das manuelle Verschieben kein Assistent oder Ähnliches zur Verfügung steht, müssen Sie unbedingt die Reihenfolge der hier beschriebenen Arbeitsschritte einhalten.

1. Überprüfen Sie auf dem Domänencontroller, auf dem der Ordner verschoben werden soll, sowie auf einigen Replikationspartnern den ordnungsgemäßen Zustand der Ordner SYSVOL und NETLOGON. Wählen Sie aus der Ereignisanzeige die Kategorie DATEIREPLIKATIONSDIENST und suchen nach der Ereignis-ID 13516. Dieses Ereignis sollte denselben Zeitstempel tragen wie der letzte Neustart des Servers. Diese ID gibt an, dass der Dateireplikationsdienst erfolgreich gestartet wurde und die beiden Ordner SYSVOL und NETLOGON freigegeben worden sind, sodass der Domänencontroller ordnungsgemäß ausgeführt wird. Zusätzlich können Sie auch nach den IDs 13508 und 13509 suchen. 13509 zeigt an, dass der Dateireplikationsdienst erfolgreich gestartet wurde, 13508, dass der Dienst gerade gestartet wird. Zusätzlich können Sie an der Eingabeaufforderung `net share`  starten. Dies zeigt alle Freigaben des Domänencontroller an. In der Liste sollten sich die Ordner SYSVOL und NETLOGON befinden.
2. Im zweiten Schritt testen Sie die Replikationstopologie. Verwenden Sie hierzu das Support-Tool *DCDIAG*. Weitere Hinweise zu diesem Programm finden Sie in Kapitel 23.1.4. Geben Sie an der Eingabeaufforderung den Befehl `dcdiag /test:replications`  ein. Um zusätzlich die korrekten Berechtigungen für die Replikation zu prüfen, geben Sie den Befehl `dcdiag /test:netlogons`  ein.
3. Vor dem Verschieben des SYSVOL-Ordners müssen Sie die Ordnerstruktur an sich sowie die im Active Directory und in der Registry gespeicherten Pfadinformationen verstehen. Wird der Ordner verschoben, so müssen auch die entsprechenden Pfadinformationen aktualisiert werden. Andernfalls können Dateien aus einer falschen Quelle oder an ein falsches Ziel repliziert werden, ohne dass Sie Fehlermeldungen im Ereignisprotokoll erhalten, da ja die Replikation an sich korrekt abläuft.

Beim Verschieben müssen Sie besonders auf die Unterordner der ersten drei Level von SYSVOL achten, bei denen die entsprechenden Parameter aktualisiert werden müssen, damit der Dateireplikationsdienst korrekt auf sie zugreifen kann. Hierbei handelt es sich um die folgenden zehn Unterordner von %SYSTEMROOT%\SYSVOL sowie %SYSTEMROOT%\SYSVOL selbst:

- ▶ \DOMAIN
- ▶ \DOMAIN\DO_NOT_REMOVE_NTFRS_PREINSTALLED_DIRECTORY
- ▶ \DOMAIN\POLICIES
- ▶ \DOMAIN\SCRIPTS
- ▶ \STAGING
- ▶ \STAGING\DOMAIN
- ▶ \STAGING AREAS
- ▶ \STAGING AREAS FQDN
- ▶ \SYSVOL
- ▶ \SYSVOL FQDN

Einige dieser Ordner sind versteckt, sodass Sie erst die entsprechenden Ansichtsoption aktivieren müssen, bevor Sie die Ordner im Windows Explorer sehen können. FQDN steht für den vollqualifizierten Domänennamen der aktuellen Domäne dieses Domänencontrollers.

Bei den Ordnern \SYSVOL sowie \STAGING AREAS handelt es sich um *Junction Points*. \SYSVOL enthält eine Verknüpfung auf den Ordner \DOMAIN, \STAGING AREAS eine Verknüpfung zu \STAGING DOMAIN. Ändern sich die Pfadangaben der beiden Zielordner, müssen die Einträge der beiden *Junction Points* angepasst werden. Weiterhin muss im Active Directory auch die Variable *fRSRootPath* angepasst werden. Diese befindet sich im Ordner %SYSTEMROOT%\SYSVOL\DOMAIN. Mit dieser Variablen wird auf die in SYSVOL gespeicherten Richtlinien und Skripte gezeigt. Die zweite Variable *fRSStagingPath* befindet sich im Ordner %SYSTEMROOT%\SYSVOL\STAGING\DOMAIN und verweist auf die Ordner der Staging Area (siehe Kapitel 13.1.5). Schließlich muss auch in der Registry der Pfad für den Ordner %SYSTEMROOT%\SYSVOL\SYSVOL angepasst werden, auf den der Dienst Netlogon zugreift. Dies ist der Ordner, der die beiden Freigaben SYSVOL und NETLOGON erstellt.

Zunächst müssen Sie die bisherigen Werte für einige Parameter bestimmen. Wollen Sie den gesamten SYSVOL-Ordner verschieben, benötigen Sie alle fünf Parameter, soll nur die Staging Area verschoben werden, benötigen Sie lediglich die beiden ersten Parameter. Dabei handelt es sich um die Parameter: *fRSStagingPath*, *Staging Junction*, *fRSRootPath*, *Sysvol Junction* und *Sysvol* in der Registry.

- ▶ *fRSStaging Path*: Um diesen Wert zu ermitteln, benutzen Sie das Windows-Support-Tool *ADSIEDIT*. Weitere Hinweise zu diesem Programm finden Sie in Kapitel 23.1.2. Navigieren Sie in der mmc zum Container des aktuellen Domänencontrollers. Öffnen Sie dort den Container CN=NTFRS SUBSCRIPTIONS und darunter CN=DOMAIN SYSTEM VOLUME. Unter den Eigenschaften wählen Sie unter SELECT WHICH PROPERTIES TO VIEW den Eintrag MANDATORY. Unter SELECT A PROPERTY TO VIEW wählen Sie *fRSStagingPath*. Notieren Sie sich diesen Wert.
 - ▶ *Staging Junction*: Wechseln Sie an der Eingabeaufforderung zum Ordner %SYSTEMROOT%\SYSVOL\STAGING AREAS und geben DIR  ein. Sie sollten den vollqualifizierten Domänennamen (FQDN) für den Typ <JUNCTION> erhalten. Geben Sie dann den Befehl linkd FQDN  ein, wobei FQDN für den unter <JUNCTION> angegebenen Pfad steht. Notieren Sie sich diesen Wert.
 - ▶ *FRSRootPath*: Um diesen Wert zu ermitteln, benutzen Sie wiederum das Windows-Support-Tool *ADSIEDIT*. Navigieren Sie in der mmc zum Container des aktuellen Domänencontrollers. Öffnen Sie dort den Container CN=NTFRS SUBSCRIPTIONS und darunter CN=DOMAIN SYSTEM VOLUME. Unter den Eigenschaften wählen Sie unter SELECT WHICH PROPERTIES TO VIEW den Eintrag MANDATORY. Unter SELECT A PROPERTY TO VIEW wählen Sie *fRSROOTPath*. Notieren Sie sich diesen Wert.
 - ▶ *SYSVOL Junction*: Wechseln Sie an der Eingabeaufforderung zum Ordner %SYSTEMROOT%\SYSVOL\SYSVOL und geben DIR  ein. Sie sollten den vollqualifizierten Domänennamen (FQDN) für den Typ <JUNCTION> erhalten. Geben Sie dann den Befehl linkd FQDN  ein, wobei FQDN für den unter <JUNCTION> angegebenen Pfad steht. Notieren Sie sich diesen Wert.
 - ▶ *Sysvol in der Registry*: Starten Sie *regedit* und öffnen den Schlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters. Notieren Sie sich den Wert des Schlüssels *Sysvol*.
4. Als Nächstes müssen Sie den Dateireplikationsdienst beenden. Geben Sie dazu an der Eingabeaufforderung den Befehl `net stop ntfrs`  ein.

5. Nun wird die Ordnerstruktur des alten SYSVOL-Ordners an die neue Lokation kopiert. Öffnen Sie dazu im Windows Explorer den Ordner %SYSTEMROOT%\SYSVOL. Kopieren Sie diesen Ordner und fügen den Inhalt an der gewünschten Stelle ein. Überprüfen Sie die Struktur der beiden SYSVOL-Ordner miteinander. Sollten dem neuen SYSVOL einige Unterordner fehlen, so erstellen Sie diese neu.
6. Nachdem Sie SYSVOL an den gewünschten Ort kopiert haben, muss der neue Pfad in der Registry eingetragen werden. Navigieren Sie zu dem Schlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters und doppelklicken auf Sysvol. Geben Sie als Wert den neuen Pfad zum Unterordner SYSVOL in der Freigabe SYSVOL an.
7. Alternativ zum Verschieben des gesamten SYSVOL-Verzeichnisses können Sie auch nur den Ordner Staging Area verschieben. Dabei müssen der Parameter *fRSStagingPath* sowie der Junction Point %SYSTEMROOT%\SYSVOL\STAGING AREAS angepasst werden.

Um den *fRSStagingPath* zu ändern, benutzen Sie das Windows-Support-Tool *ADSI-EDIT*. Navigieren Sie in der mmc zum Container des aktuellen Domänencontrollers. Öffnen Sie dort den Container CN=NTFRS SUBSCRIPTIONS und darunter CN=DOMAIN SYSTEM VOLUME. Unter den Eigenschaften wählen Sie unter SELECT WHICH PROPERTIES TO VIEW den Eintrag MANDATORY. Unter SELECT A PROPERTY TO VIEW wählen Sie *fRSStagingPath*. Geben Sie in der Box EDIT ATTRIBUTE den Laufwerksbuchstaben sowie den Pfad zum Ordner STAGING AREA an.

Danach aktualisieren Sie die Verknüpfung des Junction Points. Wechseln Sie an der Eingabeaufforderung zum Ordner %SYSTEMROOT%\SYSVOL\STAGING AREAS und überprüfen mit DIR den Eintrag <JUNCTION>. Danach geben Sie folgenden Befehl ein: linkd Name des Junction Point neuer Pfad . Geben Sie hier denselben Pfad an wie im letzten Schritt unter *fRSStagingPath*.

8. Als Nächstes wird das Active Directory-Attribut *fRSRootPath* geändert. Dieses Attribut beschreibt die Lokation des SYSVOL-Ordners für den Domänencontroller.

Um diesen Wert zu ändern, benutzen Sie das Windows-Support-Tool *ADSIEDIT*. Navigieren Sie in der mmc zum Container des aktuellen Domänencontrollers. Öffnen Sie dort den Container CN=NTFRS SUBSCRIPTIONS und darunter CN=DOMAIN SYSTEM VOLUME. Unter den Eigenschaften wählen Sie unter SELECT WHICH PROPERTIES TO VIEW den Eintrag MANDATORY. Unter SELECT A PROPERTY TO VIEW wählen Sie *fRS-ROOTPath*. Geben Sie in der Box EDIT ATTRIBUTE den Laufwerksbuchstaben sowie den Pfad zum Ordner SYSVOL an.

Wechseln Sie dann an der Eingabeaufforderung zum Ordner %SYSTEMROOT%\SYSVOL\SYSVOL und überprüfen mit DIR den Eintrag <JUNCTION>. Danach geben Sie folgenden Befehl ein: linkd Name des Junction Point neuer Pfad . Geben Sie hier denselben Pfad an wie im letzten Schritt unter *fRSRootPath*.

9. In diesem Schritt sorgen Sie dafür, dass der Domänencontroller beim Neustart automatisch eine nicht autorisierende Wiederherstellung von SYSVOL durchführt. Hierzu wird in der Registry der Wert für die Backup-Restore-Flags (*BurFlags*) umgesetzt. An welcher Stelle der Registry der Wert umgesetzt wird, ist davon abhängig, ob auf dem Domänencontroller nur ein Satz von Repliken vorhanden ist (globaler BurFlags-Eintrag) oder mehrere (Replica-spezifischer BurFlags-Eintrag).

Um den BurFlags-Wert zu ändern, starten Sie *regedit* und navigieren zum Schlüssel HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NtFrs\Parameters. Um den globalen BurFlags-Eintrag zu ändern, erweitern Sie Backup/Restore-Process at Startup. Wollen Sie den Replica-spezifischen BurFlags-Eintrag ändern, erweitern Sie Cumulative Replica Sets sowie Replica Sets. Tragen Sie unter Replica Sets als Wert dieselbe GUID ein wie unter Cumulative Replica Sets. Klicken Sie dann die GUID unter Cumulative Replica Sets bzw. unter Process at Startup an und doppelklicken im Detailbereich auf BurFlags. Tragen Sie dort den dezimalen Wert 210 oder den hexadezimalen Wert D2 ein.

10. Abschließend müssen am neuen SYSVOL-Ordner wieder dieselben Sicherheitseinstellungen konfiguriert werden, wie sie bei der Erstinstallation am ursprünglichen SYSVOL erstellt worden sind. Wurden die Sicherheitseinstellungen am ursprünglichen SYSVOL nach der Installation manuell modifiziert, so müssen diese Modifikationen nach Abschluss der folgend beschriebenen Schritte durchgeführt werden.

1. Zunächst starten Sie *regedit* und navigieren zum Schlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters. Notieren Sie sich den unter Sysvol eingetragenen Pfad.
2. Öffnen Sie in der Systemsteuerung den Menüpunkt SYSTEM. Auf der Registerkarte ERWEITERTE klicken Sie auf UMGEBUNGSVARIABLEN. Erstellen Sie eine neue Systemvariable mit dem Namen Sysvol. Als Pfad der Variablen tragen Sie den im ersten Schritt notierten Pfad ein. Schließen Sie danach alle Eigenschaftsseiten.
3. Starten Sie dann einen beliebigen Texteditor und erstellen eine Datei namens *sysvol.inf*. Diese Datei übernimmt die Sicherheitseinstellungen für den neuen SYSVOL-Ordner. In die Datei *sysvol.inf* schreiben Sie den folgenden Inhalt:

```
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[Profile Description]
Description=Standardberechtigung für SYSVOL
[File Security]
; "%SystemRoot%\SYSVOL", 0, "D:AR(A;OICI;FA;;;BA)"
"%Sysvol%", 2, "D:P(A;CIOI;GRGX;;;AU)(A;CIOI;GRGM;;;SO)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
"%Sysvol%\domain\policies", 2, "D:P(A;CIOI;GRGX;;;AU)(A;CIOI;GRGM;;;SO)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)(A;CIOI;GRGWGXSD;;;PA)"
```

Listing 13.1: Die Datei *sysvol.inf*

4. Öffnen Sie eine neue Eingabeaufforderung, sodass für diese die neuen Umgebungsvariablen wirksam werden. Geben Sie dort den folgenden Befehl ein: `Secedit /configure /cfg Pfadangabe\sysvol.inf /db Pfadangabe\sysvol.db/overwrite` . Die Pfadangabe bezieht sich auf den Speicherort der *sysvol.inf*.

11. Als Letztes muss der Dateireplikationsdienst wieder gestartet werden. Geben Sie dazu an der Eingabeaufforderung den Befehl `net start ntfrs`  ein. Anschließend suchen Sie im Ereignisprotokoll des Dateireplikationsdienstes nach der Ereignis-ID 13516. Zusätzlich müssen Sie nach den IDs 13553 und 13556 suchen. Diese geben an, dass das Verschieben von SYSVOL bzw. des *Staging Area*-Ordners erfolgreich ausgeführt wurde.

13.1.5 Der Ordner Staging Area

Der Ordner *Staging Area* ist ein Unterordner des SYSVOL-Verzeichnisses. In diesem Ordner befinden sich die Kopien aller Dateien, die vom Dateireplikationsdienst (FRS, File Replication Service) repliziert werden. Dazu zählen einerseits die Dateien, die repliziert werden sollen, andererseits aber auch die Dateien, die gerade repliziert worden sind. Durch die Benutzung von Kopien während der Replikation ist sichergestellt, dass die Originaldatei während des Replikationsprozesses zur Verfügung steht.

Obwohl die Kopien alle vom Dateireplikationsdienst komprimiert werden, damit der benötigte Festplattenplatz reduziert und die Übertragung der zu replizierenden Dateien beschleunigt wird, kann es dennoch vorkommen, dass eine nicht unbeträchtliche Menge an Speicherplatz vom Ordner *Staging Area* belegt wird. Außer vom Dateireplikationsdienst wird der Ordner *Staging Area* auch vom DFS (Distributed File System / verteiltes Dateisystem) benutzt.

Standardmäßig liegt die Größe der *Staging Area* bei 675 MB. Dieser Wert kann jedoch über die Registry modifiziert werden. Der Minimalwert muss dabei bei 10 MB liegen, und maximal 2 Terabyte (TB) dürfen nicht überschritten werden. Dieser Wert kann in dem Schlüssel `HKEY_Local_Machine\System\CurrentControlSet\Services\NtFrs\Parameters` angepasst werden. Bedenken Sie beim Ändern des Wertes, dass neben dem vom FRS benutzten Speicherplatz auch genügend Speicherplatz für DFS zur Verfügung steht.

13.1.6 Verschieben des Staging Area-Ordners

Standardmäßig werden die Ordner *Staging Area* sowie *Staging* vom Active Directory-Installationsassistenten im SYSVOL-Verzeichnis angelegt. Da dieser Ordner aber den meisten Speicherplatz innerhalb des SYSVOL-Verzeichnisses benötigt, kann es sinnvoll sein, nur diesen Unterordner anstatt des gesamten SYSVOL zu verschieben, wenn der Speicherplatz auf dem ursprünglichen Laufwerk nicht mehr ausreichend ist. Wenn Sie den Ordner *Staging Area* verschieben, kann dieser sogar umbenannt werden. Die neue Position des Ordners wird anhand von zwei Parametern bestimmt. Im Active Directory ist die Variable `frsStagingPath` gespeichert. Diese enthält die Pfadangabe des Ordners, sodass FRS darauf zugreifen kann. Zusätzlich ist im *Staging Area*-Ordner ein *Junction Point* enthalten. Dieser stellt eine Verknüpfung zum aktuellen Speicherort dar. Wird der Ordner *Staging Area* verschoben, müssen diese beiden Variablen aktualisiert werden.

Bevor Sie den Ordner verschieben, müssen Sie im Großen und Ganzen dieselben Punkte überprüfen und Vorbereitungen treffen wie beim Verschieben des kompletten SYSVOL-Verzeichnisses. Hierzu zählen die in Kapitel 13.1.4 ausführlich beschriebenen Schritte 1,

Überprüfen von FRS, SYSVOL und NETLOGON, Schritt 2, Testen der Replikation, Schritt 3, Ermitteln bisheriger SYSVOL-Parameter, sowie Schritt 4, Beenden des Dateireplikationsdienstes.

Danach wird der neue *Staging Area*-Ordner angelegt. Erstellen Sie den neuen Ordner auf dem gewünschten Datenträger und geben entweder den Namen Staging Area oder einen beliebigen anderen Namen an.

Führen Sie nun die in Kapitel 13.1.4 beschriebenen Schritte 7, Schritt 9, Vorbereiten der nicht autorisierenden Wiederherstellung, sowie Schritt 11, Starten des Dateireplikationsdienstes und Überprüfen von SYSVOL aus.

14 Standorte und Organisationseinheiten

Dieses Kapitel zeigt Ihnen die nächsten Schritte, die Sie nach der Installation des Active Directory durchführen sollten. Sie müssen nun entsprechend Ihrer Unternehmensstruktur Standorte und Organisationseinheiten anlegen und konfigurieren.

14.1 Konfiguration von Standorten

Standorte unter Active Directory beruhen auf der physischen Struktur – im Gegensatz zu Domänen, die die logische Struktur eines Unternehmens widerspiegeln. So kann eine Domäne mehrere Standorte umfassen und umgekehrt ein Standort auch mehrere Domänen oder Teile von Domänen. Die wichtigste Aufgabe der Standorte ist die Bereitstellung einer schnellen Netzwerkverbindung. Durch die Einrichtung von Standorten werden sowohl die Anmeldung und Authentifizierung als auch der Replikationsprozess beeinflusst. Bei der Anmeldung sucht der Client zunächst an seinem Standort nach einem Domänencontroller, der ihn authentifizieren kann. Die Replikation zwischen zwei Standorten kann von Ihnen im Gegensatz zur standortinternen Replikation bezüglich der Zeit und der Route geplant werden. Auch andere in Active Directory integrierte Anwendungen, wie beispielsweise Exchange 2000, werden durch die Konfiguration von Standorten tangiert.

Das Einrichten eines neuen Standorts gliedert sich in vier Arbeitsschritte. Zunächst müssen Sie einen neuen Standort erstellen. Dieser Standort muss mit einem Subnetz verknüpft werden. Danach müssen Sie noch Standortverknüpfungen einrichten und einen Standortlizenzserver auswählen und konfigurieren.

Beginnen wir also mit der Beschreibung und Einrichtung eines neuen Standorts. Ein Standort umfasst eine Gruppe von Computern, die untereinander über eine gute Netzwerkverbindung verfügen. Diese Computer am Standort befinden sich in einem Satz von einem oder mehreren Subnetzen.

Innerhalb eines Standorts müssen somit keine Aspekte bezüglich Kosten oder Geschwindigkeit berücksichtigt werden. Dies ist wichtig für die Replikation innerhalb eines Standorts. Die Replikation am Standort wird immer durchgeführt, sobald an einem Domänencontroller Änderungen vorgenommen worden sind. Dieser Domänencontroller benachrichtigt seine Replikationspartner, und diese fordern dann die geänderten Informationen an. Die standortübergreifende Replikation findet nur zu den festlegbaren Intervallen statt, da hier die Kostenaspekte beachtet werden müssen.

Sämtliche Einstellungen dieses Kapitels werden, wenn nicht ausdrücklich anders erwähnt, über die mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE vorgenommen. Die Standorte werden zuweilen auch als Sites bezeichnet. Der übergeordnete Standortcontainer in der mmc heißt ebenfalls SITES.

Nachdem Sie auf dem ersten Domänencontroller Active Directory installiert haben, finden Sie im Container SITES den Standort STANDARDNAME-DES-ERSTEN-STANDORTS. Dort wird unter SERVER der erste Domänencontroller eingetragen. Ist dieses erledigt, kann der Standort in den gewünschten Namen umbenannt werden. Weitere Domänencontroller können Sie entweder an demselben Standort wie der Quell-Domänencontroller einrichten, sofern dessen IP-Adresse dem Standort zugeordnet ist, oder an anderen neu eingerichteten Standorten.

Um einen neuen Standort zu erstellen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE und wählen aus dem Kontextmenü von SITES den Eintrag NEUER STANDORT (siehe Abbildung 14.1).

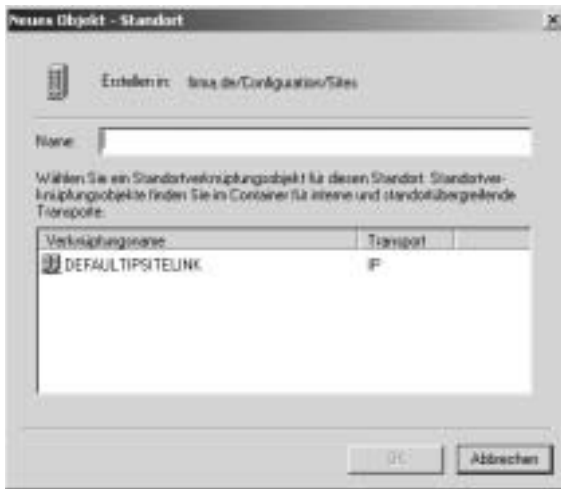


Abbildung 14.1: Einrichten eines neuen Standorts

2. Geben Sie einen Namen für den neuen Standort ein. In den weiteren Beispielen dieses Kapitels heißt dieser Standort Dortmund. Im unteren Konfigurationsfenster wird der Verknüpfungsname DEFAULTSITEIPLINK automatisch angegeben. Markieren Sie diesen und klicken dann auf OK.
3. Sie erhalten dann noch Hinweise, welche Schritte für den Abschluss der Standortkonfiguration notwendig sind. Dem neuen Standort muss ein Domänencontroller hinzugefügt werden. Außerdem benötigt er eine Standortverknüpfung, ein Subnetz und einen Lizenzserver.
4. Um den ersten Standort mit dem wenig aussagekräftigen Namen STANDARDNAME-DES-ERSTEN-STANDORTS umzubenennen, wählen Sie aus dem Kontextmenü dieses Objekts den Eintrag UMBENENNEN. Geben Sie dann den neuen Namen ein. In unserem Beispiel wird der Standard-Standortname in Barsinghausen umbenannt.
5. Damit ist das Erstellen eines neuen Standorts abgeschlossen. Im nächsten Schritt muss dem Standort nun ein Subnetz zugewiesen werden.

14.1.1 Festlegen von Subnetzen

Dieses Kapitel beschreibt, wie Sie den eben erstellten Standort mit einem oder mehreren Subnetzen verbinden können. Hierzu erfolgt zunächst eine Beschreibung über den Aufbau und das Berechnen von Subnetzen.

Die Subnetze werden oft in der Form von Bit-Werten angegeben, z.B. 172.20.20.106/16. Dieser kleine Exkurs soll Ihnen zeigen, wie eine dezimale Subnetzadresse in den Binärwert übersetzt werden kann.

Bleiben wir bei unserem Beispiel 172.20.20.106/16. Interessant für die Berechnung des Subnetzes ist nur der Wert 16. Die 16 steht für eine 16-Bit-Subnetzmaske. Anhand des Netzwerkteils der IP-Adresse lässt sich bestimmen, welcher Subnetzklasse der Bereich zuzuweisen ist. Es gibt drei Klassen von Subnetzbereichen. In der folgenden Tabelle bedeutet NW = Netzwerkteil und Host = Hostteil der IP-Adresse.

Subnetzklasse	Bereich	Netzwerk-/Hostteil der IP-Adresse
A	1.x.x.x bis 126.x.x.x	NW.Host.Host.Host
B	128.0.x.x bis 191.255.x.x	NW.NW.Host.Host
C	192.0.0.x bis 223.255.255.x	NW.NW.NW.Host

Tabelle 14.1: Die Bereiche der Subnetzklassen

Wir sehen also, dass der Netzwerkbereich 172.20.x.x in den Bereich eines Subnetzes der Klasse B fällt. 172.20. ist in der Klasse B der Netzwerkteil der IP-Adresse. Es ist aber möglich, Subnetze zuzuweisen, die nicht zu der jeweiligen Klasse gehören. Die IP-Adresse 172.20.20.106 kann sich auch ebenso gut in einem Klasse-C-Subnetz befinden. Dann lautet der Netzwerkteil der IP-Adresse 172.20.20.

Eine Subnetzadresse besteht aus vier Oktetten zu je 8 Bit. Im Binärsystem gibt es nur die Werte 1 und 0. Aus diesen beiden Werten werden alle Zahlen zwischen 0 und 255 zusammengestellt. Eine Binärzahl von 8 Bit Länge entspricht der Dezimalzahl 255. Stellen Sie sich dieses folgendermaßen vor:

Bit-Nummer	1	2	3	4	5	6	7	8
Dezimalwert	128	64	32	16	8	4	2	1
Binärwert	1	1	1	1	1	1	1	1

Tabelle 14.2: Dezimalzahlen als Binärwerte

Jede Bit-Nummer kann den Wert 1 oder 0 haben. In der Tabelle hat jede Bit-Nummer den Wert 1. Also müssen Sie alle Bit-Nummern, die den Wert 1 haben, anhand des Dezimalwerts zusammenzählen. Dies ergibt in unserem Beispiel:

als Binärwert 11111111 und als Dezimalwert $128+64+32+16+8+4+2+1 = 255$

Eine Subnetzmaske von 8 Bit würde also 255.0.0.0 lauten, da nur die ersten 8 Bits einen Wert haben. Die 16-Bit-Subnetzmaske setzt sich somit aus zweimal 8 Bit zusammen, lautet damit also 255.255.0.0. Die folgende Tabelle gibt eine Übersicht über die gebräuchlichsten Dezimal-/ Binärzahlen.

	Bit-Nummer								
	1	2	3	4	5	6	7	8	
Dezimalwert	128	64	32	16	8	4	2	1	Dezimalzahl
	1	1	1	1	1	1	1	1	255
	1	1	1	1	1	1	1	0	254
	1	1	1	1	1	1	0	0	252
	1	1	1	1	1	0	0	0	248
	1	1	1	1	0	0	0	0	240
	1	1	1	0	0	0	0	0	224
	1	1	0	0	0	0	0	0	192
	1	0	0	0	0	0	0	0	128
	0	1	0	0	0	0	0	0	64
	0	0	0	0	0	0	0	0	0

Tabelle 14.3: Berechnungsbeispiele für Subnetze

Ein Subnetz von beispielsweise 12 Bit hat also die Maske 255.240.0.0. Die 12 Bit setzen sich zusammen aus den 8 Bit des ersten Oktetts (255) und den 4 Bit des zweiten Oktetts (240).

Weiterhin können Sie nun die Anzahl der Subnetze und der Computer pro Subnetz berechnen.

Anzahl der Hosts pro Subnetz

Beginnen wir damit zu berechnen, wie viele Computer in einem bestimmten Subnetz enthalten sein können.

1. Hierzu werfen Sie zunächst einen Blick in die Tabelle 14.1 und entscheiden, welcher Subnetzklasse Ihre IP-Adresse angehört oder tatsächlich zugeordnet ist. Ermitteln Sie die letzte Zahl des Netzwerkbereichs Ihrer Subnetzadresse. In unserem Beispiel der 172.20.20.106/16 handelt es sich um das Subnetz 255.255.0.0 der Klasse B. Die letzte Zahl des Netzwerkbereichs ist die 255. Wenden Sie dann die folgende Formel an:

$$256 - (\text{letzte Zahl des Netzwerkbereichs}) = X; \text{ hier } 256 - 255 = 1$$

Merken Sie sich dieses Ergebnis.

2. Dann betrachten Sie die Oktette der Host-Teile Ihrer Subnetzadresse, in unserem Beispiel also 0.0. Die Anzahl der Oktette variiert je nach Subnetzklasse. In der Klasse B sind es zwei Oktette. Der Maximalwert je Host-Oktett kann 256 betragen. Dies wäre der Fall bei 255.255.0.0. Subtrahieren Sie den Wert des Host-Teils von 256.

Nehmen Sie den Wert aus Schritt 1 (im Beispiel 1), und multiplizieren Sie ihn mit der Anzahl der freien Oktette des Hostbereichs für jedes Oktett. In unserem Beispiel ergibt das:

$$1 * (256 - 0) * (256 - 0) = 1 * 256 * 256 = 65\,536$$

3. Subtrahieren Sie von dem Wert aus Schritt 2 die 2. Dies ergibt in unserem Beispiel: $65\,536 - 2 = 65\,534$

Dies ist die maximale Anzahl der Hosts in dem Subnetz 255.255.0.0. Die IP-Adressen können zwischen 172.20.0.1 und 172.20.255.254 liegen.

Gibt es im Hostbereich der Subnetzadresse kein freies Oktett mehr, z.B. bei 255.255.255.250, so nehmen Sie den letzten Teil des Netzwerkbereichs, hier also 250, und subtrahieren diesen von 256. Dies ergibt 6. Dieser Wert wird nicht mit 0 multipliziert, da es keine freien Host-Oktette mehr gibt, sondern direkt von diesem Wert wird die 2 subtrahiert. In dem Subnetz 255.255.255.250 kann es also nur vier Hosts geben.

Vereinfacht lautet die Formel:

$256 - (\text{letzte Zahl des Netzwerkbereichs}) = X$

$X * (256 - \text{freie Oktette Hostbereich}) * (256 - \text{freie Oktette Hostbereich}) = Y$

$Y - 2 = \text{Anzahl der Hosts pro Subnetz}$

Zur Berechnung von Subnetzen, der Bitlänge von Subnetzen, deren Anzahl sowie der Anzahl der Hosts pro Subnetz stehen Ihnen verschiedene nützliche Programme im Free- und Shareware-Sektor bzw. zum Kauf zur Verfügung.

Erstellen eines neuen Subnetzes

Nach diesem Exkurs soll nun endlich dem Standort ein Subnetz zugewiesen werden. Die Subnetzinformationen benutzt jeder Active Directory-Client zur Suche nach einem Domänencontroller an seinem Standort. Anhand dieser Informationen wird von Active Directory auch automatisch die beste Replikationsroute ermittelt.

Um ein neues Subnetz zu erstellen, führen Sie die folgenden Schritte aus:

1. Doppelklicken Sie auf den Ordner SITES. Wählen Sie dann aus dem Kontextmenü des Ordners SUBNETS den Eintrag NEUES SUBNETZ (siehe Abbildung 14.2). Geben Sie im Feld ADRESSE den Netzwerkteil der IP-Adresse für diesen Standort und im Feld MASKE die Subnetzmaske ein. Diese Angaben werden automatisch in das Format Netzwerk/Bit übersetzt. In unserem Beispiel haben wir den Bereich 172.20.20. in einer Subnetzklasse C. Dies ergibt 172.20.20/24.
2. Haben Sie bereits mehrere Standorte erstellt, markieren Sie hier das gewünschte Standortobjekt, dem Sie das Subnetz zuweisen möchten, und klicken dann auf OK.



Abbildung 14.2: Erstellen eines neuen Subnetzes

- Um ein Subnetz nachträglich einem anderen Standort zuzuweisen, wählen Sie die Eigenschaften aus dem Kontextmenü des betreffenden Subnetzes. Sie können dann in dem Listefeld STANDORT alle verfügbaren Standorte sehen und den neuen Standort auswählen, mit dem das Subnetz verknüpft werden soll.

14.1.2 Erstellen von Standortverknüpfungen

In diesem Schritt werden die Verknüpfungen zwischen einzelnen Standorten eingerichtet. Diese Verknüpfungen sind notwendig, damit die standortübergreifende Replikation durchgeführt werden kann. Ohne eine Standortverknüpfung kann keine Verbindung zwischen den Computern beider Standorte eingerichtet werden. Eine Standortverknüpfung kann zwei oder mehr Standorte miteinander verbinden. Im letzten Fall werden alle Standorte gleich gut miteinander verbunden.

Für jede Standortverknüpfung wird ein Zeitplan erstellt, nach dem die Replikation zwischen den Standorten stattfinden soll.

Um eine Standortverknüpfung zwischen zwei Standorten zu erstellen, führen Sie die folgenden Schritte aus:

- Doppelklicken Sie auf den Ordner INTER-SITE-TRANSPORTS. Dort befinden sich die beiden Unterordner IP und SMTP. Dabei handelt es sich um die beiden zur Verfügung stehenden Replikationsprotokolle. Sie haben folgende Funktionen:

Protokoll	Funktion
IP (Internet Protocol)	Dieses Protokoll kann sowohl für die standortinterne als auch für die standortübergreifende Replikation verwendet werden. Bei der IP-Replikation werden RPCs (Remote Procedure Calls) verwendet. Diese Replikationsart findet im Rahmen der konfigurierten Zeitpläne statt.
SMTP (Simple Mail Transfer Protocol)	SMTP wird ausschließlich für die standortübergreifende Replikation verwendet. Da SMTP asynchron arbeitet, werden eventuell vorhandene Zeitpläne ignoriert. Wenn Sie das SMTP-Protokoll einsetzen möchten, müssen Sie erstens SMTP auf allen Domänencontrollern dieser Standortverknüpfung SMTP installieren und zweitens eine Zertifizierungsstelle einrichten. Darüber werden die SMTP-Nachrichten zwischen den Domänencontrollern signiert und die Echtheit sichergestellt.

Tabelle 14.4: Die Replikationsprotokolle IP und SMTP

- Nachdem Sie sich für ein Protokoll entschieden haben, wählen Sie aus dem Kontextmenü des Ordners NEUE STANDORTVERKNÜPFUNG.



Bei der Installation von Active Directory wurde im Ordner IP automatisch die Standortverknüpfung DEFAULTSITEPLINK für den ersten Standort mit dem Namen STANDARDNAME-DES-ERSTEN-STANDORTS eingerichtet. Diese Verknüpfung sollten Sie sinnvoll umbenennen. In ihr ist standardmäßig der erste Standort enthalten.

3. Geben Sie danach (siehe Abbildung 14.3) im Feld NAME einen Namen für die Verknüpfung an. Sinnvollerweise kommen darin die Namen der verknüpften Standorte vor. Die Erstellung der Standortverknüpfung ist für IP und SMTP identisch.



Abbildung 14.3: Erstellen einer Standortverknüpfung

4. In der Liste links sehen Sie alle konfigurierten Standorte. Um die gewünschten Standorte zur Verknüpfung hinzuzufügen, markieren Sie diese und fügen sie der Liste rechts hinzu. Von dort können Sie auch wieder Standorte entfernen. Das Hinzufügen und Entfernen von Standorten funktioniert jedoch erst, wenn Sie mindestens drei Standorte konfiguriert haben.

Falls Sie zu einem späteren Zeitpunkt weitere Standorte zu einer Verknüpfung hinzufügen möchten, doppelklicken Sie die gewünschte Standortverknüpfung. Sie erhalten dadurch dasselbe Fenster wie in Abbildung 14.3 dargestellt. Der einzige Unterschied besteht darin, dass sich rechts bereits mindestens zwei Standorte in der Liste befinden. Fügen Sie alle gewünschten Standorte der linken Liste hinzu.

14.1.3 Einrichten von Standortlizenzservern

In jedem Unternehmen sollte an zentraler Stelle ein Überblick über vorhandene, vergabene und gelöschte Lizenzen der Microsoft-Produkte gewährleistet sein. Auf jedem Windows 2000 und 2003 Server läuft der Lizenzprotokollierdienst. Über diesen Dienst ist es möglich, Lizenzinformationen zentral auf einem Server zu sammeln. Sie können Lizenzen für Windows, Microsoft BackOffice oder auch weitere Server, wie z.B. den Systems Management Server, verwalten.

Für jeden Active Directory-Standort können Sie einen Server bestimmen, der als Standortlizenzserver agieren soll. Standardmäßig wird dazu der erste Domänencontroller eines Standorts eingerichtet. Diese Einstellung kann jedoch nachträglich geändert werden. Es muss sich bei dem Computer auch um keinen Domänencontroller handeln, der als Standortlizenzserver arbeiten soll.

In einem großen Unternehmen ist es sinnvoll, an jedem Standort einen separaten Lizenzserver zu unterhalten. Der Zugriff auf nur einen zentralen Lizenzserver würde eine zu hohe Netzwerklast auf dem Server verursachen. In kleineren Umgebungen können jedoch alle Standorte gemeinsam denselben Lizenzserver an einem Standort verwenden.

Um zu überprüfen, welcher Computer für einen Standort der aktuelle Lizenzserver ist, oder um einen anderen Computer als Standortlizenzserver zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Doppelklicken Sie auf den Standort, für den Sie einen Lizenzserver einrichten möchten. Im Ergebnisabschnitt erscheint nun das Objekt LICENSING SITE SETTINGS. Wählen Sie aus dessen Kontextmenü den Eintrag EIGENSCHAFTEN, oder führen Sie einen Doppelklick darauf aus.
2. In Abbildung 14.4 sehen Sie auf der Registerkarte LIZENZIERUNGSEINSTELLUNGEN im Feld COMPUTER den Rechner HIPPOKRATES mit seiner zugehörigen Domäne *firma.de* angegeben. Hierbei handelt es sich um den ersten Domänencontroller des Standorts, der standardmäßig als Lizenzserver eingerichtet wird.



Abbildung 14.4: Einrichten eines Standortlizenzservers

3. Um einen anderen Computer als Lizenzserver auszuwählen, klicken Sie auf die Schaltfläche ÄNDERN. Sie erhalten dann eine Liste aller im Verzeichnis verfügbaren Computer. Die Domänencontroller sind dort in Großbuchstaben hervorgehoben. Wählen Sie dort einen Windows 2000 Server aus und bestätigen mit OK.

4. Um die gesammelten Lizenzinformationen anzuzeigen, wählen Sie auf dem eingerichteten Lizenzserver STARTMENÜ / PROGRAMME / VERWALTUNG / LIZENZIERUNG. Dort erhalten Sie eine Übersicht über alle erworbenen Lizenzen und Produkte. Auch die Lizenzierungsform für den Clientzugriff pro Server oder pro Arbeitsplatz kann dort geändert werden. Sie können standardmäßig die Informationen für die gesamte erreichbare Netzwerkumgebung abrufen oder über das Menü LIZENZ nur eine bestimmte Domäne oder Arbeitsgruppe anzeigen, deren Lizenzinformationen Sie betrachten oder ändern möchten.

14.1.4 Konfigurieren der Server am Standort

In diesem Kapitel werden Ihnen einige Arbeitsschritte vorgestellt, die bei der Konfiguration von Standorten immer wieder auftreten. Dazu gehören das Erstellen neuer Serverobjekte, das Entfernen von Serverobjekten sowie das Verschieben von Serverobjekten zwischen Standorten.

Erstellen neuer Serverobjekte

Gleich das Wichtigste vorweg: Mit diesem Vorgang können Sie keinen neuen Domänencontroller einrichten wie mit dem Installationsassistenten für Active Directory. Vielmehr geht es hier um das Erstellen bereits vorhandener Domänencontroller und Mitgliedsserver in einem Standort.

Um ein neues Serverobjekt zu erstellen, führen Sie die folgenden Schritte aus:

1. Doppelklicken Sie auf den Standort, dem Sie ein neues Serverobjekt hinzufügen wollen.
2. Wählen Sie aus dem Kontextmenü des Ordners SERVER den Eintrag NEU und dann SERVER.
3. Geben Sie in dem folgenden Fenster im Feld NAME den Namen für den Server ein und klicken dann auf OK.

Löschen von Serverobjekten

Bevor Sie das Serverobjekt löschen, überlegen Sie, ob Sie den Server verbindlich aus dem Standort entfernen möchten, etwa weil er außer Betrieb gesetzt wurde, oder ob der Server nur temporär entfernt und später wieder an dem Standort in Betrieb genommen werden soll. Dafür gibt es verschiedene Wege. Wollen Sie ein Serverobjekt dauerhaft löschen, führen Sie die folgenden Schritte aus:

1. Markieren Sie an dem Standort den zu löschenden Server und wählen aus dem Kontextmenü LÖSCHEN. Bestätigen Sie die Sicherheitsabfrage mit JA.

Wollen Sie das Serverobjekt nur temporär löschen, führen Sie die folgenden Schritte aus:

1. Doppelklicken Sie am Standort den gewünschten Server. Im Ergebnisabschnitt sehen Sie nun das Objekt NTDS SETTINGS. Löschen Sie dieses Objekt.
2. Wenn der Server später wieder im Netzwerk zur Verfügung steht, wird das NTDS Settings-Objekt automatisch von Active Directory neu erstellt. Der Server wird auch wieder automatisch in die Replikationstopologie eingegliedert.

Verschieben von Serverobjekten zwischen Standorten

Sie haben die Möglichkeit, Server von einem Standort an den anderen zu verschieben. Dies kann erforderlich werden, um so geänderten Unternehmensstrukturen zu genügen. Sie können Domänencontroller und Mitgliedsserver zwischen Standorten verschieben. Um einen Server zwischen zwei Standorten zu verschieben, führen Sie die folgenden Schritte aus:

1. Markieren Sie den Server an seinem ursprünglichen Standort und wählen aus dem Kontextmenü VERSCHIEBEN. Sie erhalten das Fenster SERVER VERSCHIEBEN (siehe Abbildung 14.5).



Abbildung 14.5: Verschieben eines Servers zwischen zwei Standorten

2. Sie sehen in der Liste alle vorhandenen Standorte. Klicken Sie den gewünschten neuen Standort an und bestätigen mit OK. Damit ist der Server an den neuen Standort verschoben.

14.1.5 Ein Server als Mitglied mehrerer Standorte

Diese Konfigurationsmöglichkeit mag auf den ersten Blick paradox klingen, da der Standort als ein Verbund von Computern innerhalb eines schnellen LAN definiert worden ist. Allerdings kann sich innerhalb eines LAN-Verbundes, z.B. einem Verwaltungs- oder Firmengebäude, eine große Anzahl von Clients und dementsprechend auch Domänencontrollern befinden. Um hier den Überblick zu behalten, welche Benutzer sich an welchem Domänencontroller anmelden, oder um die Replikation effektiv zu gestalten, kann die Einteilung in mehrere Standorte die beste Lösung sein. Gehört hierbei der Domänencontroller eines Standorts gleichzeitig auch zu einem oder mehreren anderen, so kann er für diese(n) als Backup-Domänencontroller zur Verfügung stehen, falls an einem Standort Probleme am Active Directory auftreten. Weiterhin kann ein Domänencontroller als Bridgehead-Server für jeden Standort konfiguriert werden. Dies bringt den Vorteil, dass der Domänencontroller für alle Standorte als Erster die Replikationsinformationen erhält und somit die Netzwerklast verringert.

Um einen Domänencontroller zum Mitglied mehrerer Standorte zu machen, müssen Sie lediglich einen Registry-Schlüssel unter Windows 2000 über *regedt32* bzw. unter Windows 2003 über *regedit* hinzufügen. Öffnen Sie den Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters` und fügen einen neuen Wert mit dem Namen `SiteCoverage` hinzu. Wählen Sie als Datentyp `REG_MULTI_SZ` und geben als Daten die Namen der Standorte an. Als Trennzeichen können Sie ein Leerzeichen oder ein Komma verwenden. Starten Sie danach den Domänencontroller neu. Dieser Vorgang muss unter Windows 2000 mit *regedt32* durchgeführt werden, da *regedit* keine `REG_MULTI_SZ`, sondern lediglich `REG_SZ`-Werte erstellen kann.

14.2 Konfiguration von Organisationseinheiten

Über Organisationseinheiten können Sie die Struktur Ihres Unternehmens unter funktionalen oder geschäftsinternen Aspekten abbilden. In jeder Domäne können Sie eine andere Hierarchie, Struktur und Benennung Ihrer Organisationseinheiten vornehmen. Jetzt erfahren Sie, wie die Organisationseinheiten erstellt und konfiguriert werden.

Um eine neue Organisationseinheit zu erstellen, müssen Sie über Administratorrechte verfügen. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie die *mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER* und wählen dort die Position, an der die neue Organisationseinheit erstellt werden soll. Eine Organisationseinheit kann entweder in einer Domäne oder einer bereits bestehenden Organisationseinheit erstellt werden.
2. Wählen Sie aus dem Kontextmenü des gewählten Objekts den Eintrag *NEU* und dann *ORGANISATIONSEINHEIT*.
3. Geben Sie dann einen Namen für diese Organisationseinheit ein (siehe Abbildung 14.6).

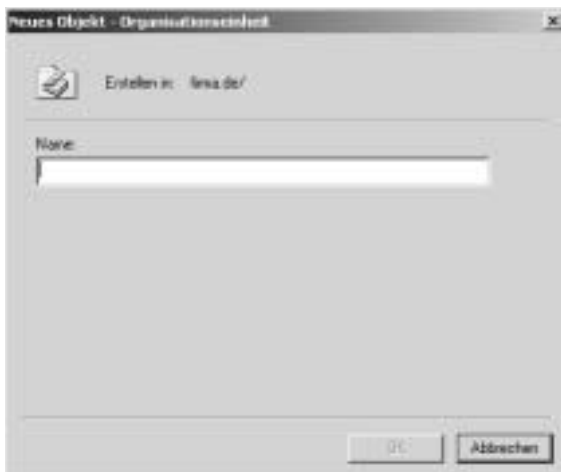


Abbildung 14.6: Erstellen einer Organisationseinheit

Die neu erstellte Organisationseinheit wird an der gewünschten Position in der mmc hinzugefügt. Sie trägt dasselbe Symbol wie die Domänencontroller in dieser mmc.

Zur genaueren Beschreibung einer Organisationseinheit können Sie einige Eigenschaften festlegen. Da Sie mit Sicherheit eine Reihe von Organisationseinheiten anlegen werden, sollten Sie sich die Zeit nehmen und die Eigenschaften ausfüllen. Dies erleichtert später die Suche nach bestimmten Eigenschaften. Sie finden die Eigenschaften im gleichnamigen Kontextmenüeintrag jeder Organisationseinheit. Die Eigenschaften gliedern sich in die drei Registerkarten ALLGEMEIN, VERWALTET VON sowie GRUPPENRICHTLINIE (siehe Abbildung 14.7).



Abbildung 14.7: Die Eigenschaften einer Organisationseinheit

Auf den Registerkarten können Sie Einträge zu folgenden Punkten vornehmen:

Registerkarte	Mögliche Einträge
Allgemein	Hier können Sie eine Beschreibung für die Organisationseinheit sowie die komplette Adresse eintragen.
Verwaltet von	Hier können Sie alle Daten wie Anschrift, E-Mail-Adresse, Telefon usw. des OU-Verwalters eintragen.
Gruppenrichtlinie	Hier werden alle Gruppenrichtlinien aufgelistet, mit denen die Organisationseinheit verbunden ist.

Tabelle 14.5: Die Einträge der Registerkarten für OU-Eigenschaften

Um eine Organisationseinheit wieder zu löschen, sie umzubenennen oder in einen anderen Container zu verschieben, wählen Sie den jeweiligen Eintrag aus dem Kontextmenü.

15 Einrichten von globalen Katalogservern

Jeder Active Directory-Client muss für seine Anmeldung Zugriff auf einen globalen Katalog haben. Aus dem globalen Katalog liest der Domänencontroller die Informationen über die Mitgliedschaften des Benutzers in universellen Gruppen aus. Kann er diese Informationen nicht beziehen, scheitert die Anmeldung des Benutzers an der Domäne. Deshalb sollten Sie pro Standort mindestens einen globalen Katalogserver einrichten. Andernfalls würden Sie durch den Zugriff des Clients auf einen Katalogserver an einem fremden Standort unnötig den Netzwerkverkehr erhöhen, obwohl Sie die Standorte bewusst zur Verringerung des Netzwerkverkehrs eingerichtet haben. Um einen Server als globalen Katalogserver einzurichten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE. Markieren Sie dort die NTDS SETTINGS des Servers am gewünschten Standort.
2. Wählen Sie aus dem Kontextmenü EIGENSCHAFTEN. Auf der Registerkarte ALLGEMEIN befindet sich die Checkbox GLOBALER KATALOG (siehe Abbildung 15.1). Markieren Sie diese, wenn der ausgewählte Domänencontroller den globalen Katalog verwalten soll, andernfalls deaktivieren Sie diese Checkbox.



Abbildung 15.1: Ein Domänencontroller als globaler Katalogserver

3. Um den globalen Katalog zu einem späteren Zeitpunkt wieder von dem Domänencontroller zu entfernen, müssen Sie lediglich die Checkbox GLOBALER KATALOG deaktivieren. Die Aktivierung des globalen Katalogs ist nur sinnvoll, wenn Ihr Unternehmen mehr als eine Domäne umfasst. Dabei sollte an jedem Standort ein Katalogserver vorhanden sein.

15.1 Verbesserungen unter Windows Server 2003

Sofern also für einen Client kein globaler Katalogserver der Gesamtstruktur zur Verfügung steht, können die Mitgliedschaften in universellen Gruppen für diesen Benutzer nicht ausgelesen werden, und der Domänencontroller verweigert die Anmeldung des Benutzers. Unter Windows Server 2003 wurde dieses Verhalten verbessert. Der Windows Server 2003 besitzt die neue Funktion *Zwischenspeichern der universellen Gruppenmitgliedschaften* (*Universal Group Membership Caching*). Dies ermöglicht einem Domänencontroller, bei der ersten Anmeldung eines Benutzers sämtliche Mitgliedschaften in universellen Gruppen aus dem globalen Katalog auszulesen und diese Informationen in einem lokalen Cache vorzuhalten. Sobald sich der Benutzer erneut anmeldet, kann der Domänencontroller auf seine lokalen Informationen zurückgreifen und muss nicht mehr einen Katalogserver abfragen. Um mögliche Änderungen an den Mitgliedschaften zu ermitteln, führt der Domänencontroller automatisch alle acht Stunden einen Abgleich seines lokalen Caches mit den Einträgen des nächsten Katalogservers durch. Somit werden einerseits die Anmeldezeiten der Benutzer verkürzt, andererseits müssen Sie nicht mehr für jeden Standort einen globalen Katalogserver bereitstellen.

Dieses Feature aktivieren Sie über die mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE. Öffnen Sie dort einen Standort und wählen das Objekt NTDS SITE SETTINGS. Öffnen Sie die Registerkarte STANDORTEINSTELLUNGEN (siehe Abbildung 15.2).



Abbildung 15.2: Das Zwischenspeichern der universellen Gruppenmitgliedschaften aktivieren

Aktivieren Sie dort die Checkbox ZWISCHENSPEICHERN DER UNIVERSELLEN GRUPPENMITGLIEDSCHAFT AKTIVIEREN. Aus der Listbox CACHE AKTUALISIEREN VON können Sie entweder einen speziellen Standort oder die Option STANDARD auswählen. Bestätigen Sie dann mit OK.



Zur Verwendung des Zwischenspeicherns der universellen Gruppenmitgliedschaften muss pro Standort mindestens ein Domänencontroller unter Windows Server 2003 ausgeführt werden.

15.2 Replikation der globalen Katalogserver

Sobald ein globaler Katalogserver zu einem Standort hinzugefügt wird, berechnet der KCC eine neue Replikationstopologie. Diese neu berechnete Topologie wird standortintern sofort umgesetzt. Die standortübergreifende Replikation beginnt zum nächsten festgelegten Intervall. Werden weitere globale Katalogserver an einem Standort hinzugefügt, wird wiederum eine neue Replikationstopologie berechnet.

Nachdem sich der neue globale Katalogserver repliziert hat, ist er bereit für Abfragen. Hierfür werden die Ports 3268 und 3269 benutzt. Allerdings unterscheiden sich die Anforderungen für die Abfragebereitschaft bei einem globalen Katalogserver unter Windows 2000 SP2 und SP3 bzw. höher. Unter Windows 2000 SP2 muss eine Replikation mit allen Domänen-Verzeichnispartitionen innerhalb des Standorts stattgefunden haben. Unter Windows 2000 SP3 und höher muss zusätzlich auch eine Replikation mit allen Domänendaten-Verzeichnispartitionen der übrigen Standorte erfolgt sein. Unter SP2 besteht deshalb die Gefahr, dass durch das zu frühe Repräsentieren als Domänencontroller Clients falsche Informationen beziehen können, wenn sie auf dem neuen globalen Katalogserver gesamtstrukturweite Suchabfragen durchführen.

Globale Katalogserver unter Windows Server 2000 replizieren grundsätzlich den kompletten globalen Katalog. Unter Windows Server 2003 hingegen replizieren globale Katalogserver lediglich die Änderungen am Katalog. Dies gilt jedoch nur, wenn alle Replikationspartner unter Windows Server 2003 betrieben werden. Sind globale Katalogserver beider Betriebssysteme vorhanden, wird weiterhin eine vollständige Replikation des globalen Katalogs durchgeführt.

Wird ein globaler Katalogserver entfernt, stoppt auch gleichzeitig dessen Darstellung als Katalogserver. Die schreibgeschützten Repliken werden vom KCC auf dem Domänencontroller entfernt. Sobald Sie einem Katalogserver unter Windows Server 2000 dessen Funktionalität entziehen, dauert es jedoch, bis dieser Vorgang endgültig abgeschlossen ist. Dies liegt darin begründet, dass nur alle 50 Minuten maximal 5000 Objekte aus der Kopie des globalen Katalogs des Domänencontrollers gelöscht werden können. Wird hingegen ein globaler Katalogserver unter Windows Server 2003 entfernt, so werden alle Objekte nacheinander aus dessen lokaler Kopie des globalen Katalogs entfernt.

15.3 Der Occupancy-Level des globalen Katalogservers

Auf jedem globalen Katalogserver kann ein sog. „Occupancy-Level“ festgelegt werden. Dieser Level gibt an, wie sich der globale Katalogserver selbst im DNS darstellt. Der Occupancy-Level sollte jedoch erst dann eingestellt werden, wenn alle schreibgeschützten Repliken der Verzeichnispartitionen synchronisiert worden sind, damit die Clients keine falschen Daten erhalten. Insgesamt gibt es sechs verschiedene Level. Diese werden über die Registry eingestellt. Öffnen Sie dazu in der Registry den Schlüssel `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters`. Fügen Sie dort einen Wert mit den folgenden Daten hinzu:

- ▶ Value name: Global Catalog Partition Occupancy
- ▶ Data type: REG_DWORD
- ▶ Radix: Hexadecimal
- ▶ Value data: Ein Wert aus der folgenden Tabelle.

Die folgende Tabelle beschreibt die möglichen Occupancy-Levels. Jeder höhere Level beinhaltet automatisch einen niedrigeren Level. Für Windows 2000 SP2 und früher können Sie maximal den Wert 4 festsetzen, erst unter SP3 und höher sind auch die Werte 5 und 6 möglich.

Occupancy-Level	Beschreibung
0	Keine Anforderung an einen bestimmten Occupancy-Level.
1	Der KCC fügt die Verbindung zu mindestens einer schreibgeschützten Verzeichnispartition des aktuellen Standorts hinzu. Die Ereignis-ID 1264 kennzeichnet die erfolgreiche Ausführung.
2	Mindestens eine schreibgeschützte Verzeichnispartition des aktuellen Standorts wird mit dem globalen Katalogserver repliziert.
3	Der KCC stellt Verbindungen zu sämtlichen schreibgeschützten Verzeichnispartitionen des aktuellen Standorts her, und mit mindestens einer erfolgt eine Replikation.
4	Alle schreibgeschützten Verzeichnispartitionen des aktuellen Standorts werden auf den Katalogserver repliziert.
5	Der KCC stellt Verbindungen zu sämtlichen schreibgeschützten Verzeichnispartitionen der Gesamtstruktur her, und mit allen erfolgt eine Replikation.
6	Alle schreibgeschützten Verzeichnispartitionen der Gesamtstruktur werden auf den Katalogserver repliziert.

Tabelle 15.1: Die Occupancy-Level eines globalen Katalogservers

16 DNS und Active Directory

In diesem Kapitel wird Ihnen die Funktionsweise von DNS (Domain Name Service) vorgestellt. Active Directory und DNS sind so eng miteinander verzahnt, dass Active Directory nicht ohne den DNS-Dienst arbeiten kann. DNS muss für Active Directory zwangsläufig implementiert werden. Zunächst erhalten Sie einen Überblick über die Funktionsweise des DNS-Dienstes und die DNS-Abfragen. Danach werden Ihnen verschiedene DNS-Zonen, deren Konfiguration sowie Übertragung und Replikation vorgestellt. Eine Verbesserung und Neuheit unter Windows 2000 ist das dynamische DNS (DDNS). Auch dessen Funktionen und Einrichtung werden ausführlich erläutert.

Bei einem derartig komplexen Prozess wie dem DNS-Dienst kann es auch Probleme geben. Dafür erhalten Sie abschließend eine Übersicht mit möglichen Problemen, deren Ursachen sowie selbstverständlich auch Lösungen.

16.1 Das Prinzip von DNS

Durch die Installation von Active Directory wird ein Windows 2000 Server zum Domänencontroller heraufgestuft. Dabei geben Sie einen DNS-Namen für die Domäne an. Hierfür wird geprüft, ob für die Domäne bereits ein autorisierender DNS-Server, der dynamische Aktualisierungen unterstützt, vorhanden ist oder nicht. Ist dies nicht der Fall, werden Sie aufgefordert, im Zuge der Installation einen DNS-Server einzurichten.

Bei einem Verzeichnisdienst handelt es sich um einen definierbaren Namensraum. Innerhalb dieses Namensraumes können in einem TCP/IP-Netzwerk die Namen von Hosts in numerische IP-Adressen aufgelöst werden. Active Directory arbeitet zur Namensauflösung mit DNS zusammen oder genauer gesagt mit jeder neuen BIND-(Berkeley Internet Name Domain-)DNS-Implementierung, sofern diese dynamisches DNS (siehe Kapitel 16.4) und SRV-Ressourceneinträge (siehe Kapitel 16.2.5) unterstützt. So ist es auch möglich, Active Directory in Kombination mit Unix-basierten DNS-Servern zu betreiben (siehe Kapitel 29.8). Bei DNS handelt es sich um einen Internetstandard. Über DNS können sowohl Computer, Drucker, Router usw. in einem privaten Netzwerk als auch Hosts im Internet gesucht werden.

Für die Netzwerkbenutzer bietet DNS den Vorteil, dass sie nach benutzerfreundlichen DNS-Namen suchen können, anstatt sich die numerischen IP-Adressen merken zu müssen. Auch gerade bei Verwendung von DHCP im Netzwerk kann sich eine IP-Adresse schnell ändern und ist den Benutzern nicht bekannt, der Hostname aber bleibt bestehen. Bei der Suche nach Computern im Netzwerk können die Benutzer bei DNS dieselben Benennungskonventionen verwenden, wie sie es von der Suche von Internet-Hosts gewohnt sind.

Ein vollständiges DNS setzt sich aus den folgenden vier Komponenten zusammen:

DNS-Komponente	Funktion
Domänen-Namensraum	Begrenzt einen Bereich, in dem die Namen aufgelöst werden können, und bestimmt eine strukturierte Hierarchie der Domänen
DNS-Server	Speichert die Ressourceneinträge und beantwortet Client-Anfragen
DNS-Client	Senden Ihre Anfragen nach Ressourcen an den DNS-Server
Ressourceneinträge	Ordnen die Domännennamen bestimmten Ressourceninformationen zu, siehe Kapitel 3.2.5.

Tabelle 16.1: Die DNS-Komponenten

Die explizite technische Definition von DNS kann in RFC 1034 und 1035 nachgelesen werden.

Ein Namensraum oder Namespace gliedert sich in eine hierarchisch angeordnete Struktur von Domänen und deren Namen. In Teil B, Kapitel 3.1.2, wurde bereits diskutiert, ob für das interne Netzwerk derselbe Namensraum verwendet werden soll wie der im Internet veröffentlichte. Für die Beschreibung der Namespace-Struktur macht es keinen Unterschied, für welche der beiden Möglichkeiten Sie sich dort entschieden haben.

Die DNS-Namen werden in insgesamt fünf Hierarchieebenen untergliedert. Hierbei handelt es sich um den Domänenstamm, Domänen erster und zweiter Ebene, Subdomänen sowie den eigentlichen Hostnamen. Diese Elemente machen den vollqualifizierten Domännennamen (FQDN = Fully Qualified Domain Name) einer Ressource aus. Alle diese Elemente werden Domänenbezeichner genannt. Als Trennelemente zwischen den Bezeichnern werden Punkte benutzt. Also könnte beispielsweise ein vollständiger Domänenname eines Hosts *hippokrates.firma.de* lauten.

Die Domänenbezeichner werden in der folgenden Tabelle näher beschrieben.

Domänenbezeichner	Beschreibung
Stammdomäne oder Root-Domäne	Dies ist die oberste Ebene der Struktur, die jedoch keinen Namen trägt. Dieser Nullwert wird zuweilen auch durch zwei Anführungszeichen markiert (""). Bei einem DNS-Domännennamen wird die Stammdomäne durch einen nachgestellten Punkt (.) markiert. Hiermit wird der höchste Punkt der Hierarchieebene gekennzeichnet. Durch den Verweis auf diesen expliziten Punkt wird der Domänenname als vollständig angesehen.
Domäne erster Ebene	Eine Abkürzung aus zwei oder drei Buchstaben, die das Länderkürzel oder eine Organisationsart kennzeichnet. Beispiele wären .de, .us, .com, .org, .net, .gov, .edu usw.

Domänenbezeichner	Beschreibung
Domäne zweiter Ebene	Der Domänenname beliebiger Länge vor dem Länder- oder Organisationskürzel. Dieser Name kann sowohl im Internet registriert werden, als auch nur dem lokalen Intranet dienen. Ein Beispiel wäre <i>microsoft.de</i> .
Subdomäne	Die vom Unternehmen definierten Namen, um den Namensraum zu vergrößern und weitere Domänen nach regionalen oder organisatorischen Aspekten in den Namespace einzugliedern.
Hostname	Der Name einer Ressource im Netzwerk, dem Endknoten in der DNS-Struktur. Anhand dieses Hostnamens sucht DNS nach der IP-Adresse des Computers. Der Hostname ist immer der am weitesten links stehende Teil des vollständigen Domänennamens. Der Hostname muss nicht mit dem NetBIOS-Namen identisch sein.

Tabelle 16.2: Die Domänenbezeichner

Die Namen im DNS-Namespace setzen sich also aus der umgekehrten hierarchischen Baumstruktur der DNS-Namensstruktur zusammen.

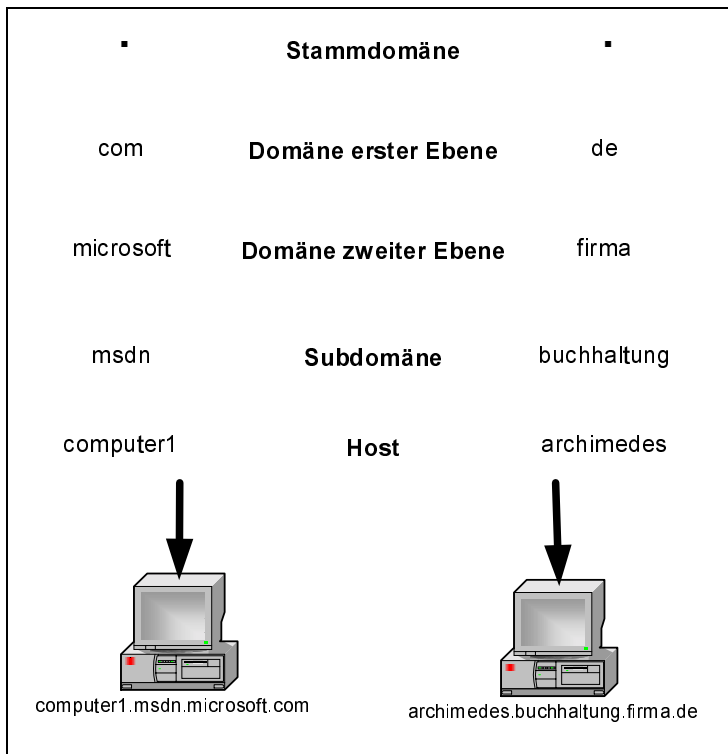


Abbildung 16.1: Der DNS-Namensraum in seiner Struktur

Abbildung 16.1 zeigt zwei Beispiele für einen Namensraum. Links sehen Sie eine Struktur für einen im Internet registrierten Domänennamen, hier *microsoft*, rechts sehen Sie einen Namensraum *firma.de*, der nur für ein Intranet gültig ist. Der letztendlich gesuchte Hostname setzt sich aus den Elementen in einer umgekehrten Baumstruktur zusammen.

Ein vollständig qualifizierter Pfad eines DNS-Domänennamens wird von Windows analog zu einem Verzeichnispfad im Windows Explorer interpretiert und verfolgt.

Obwohl Windows 2000 auf DNS aufbaut, kann es aus Gründen der Abwärtskompatibilität zu älteren Windows-Versionen auch mit NetBIOS-Namen arbeiten. Beide Namenssysteme arbeiten jedoch völlig getrennt voneinander. Theoretisch müssen somit der DNS- und der NetBIOS nicht identisch sein, aber dies sollte aus Gründen der Übersichtlichkeit vermieden werden, obwohl es rein technisch gesehen kein Problem wäre. Deshalb wird auch bei der DNS-Namensvergabe eines neuen Computers standardmäßig das Feld NetBIOS-Name automatisch mit demselben Namen ausgefüllt.

16.1.1 Was bedeutet Namensauflösung?

Wie schon erwähnt, ist es für die Netzwerkbenutzer wesentlich einfacher, über einen eindeutigen Namen als über die IP-Adresse nach einem Rechner, Drucker usw. im Netzwerk zu suchen. Auch bei der Verwendung von DHCP kommt dem DNS-Dienst eine wichtige Rolle zu, da in diesem Fall die IP-Adressen der Computer den Benutzern nicht unbedingt bekannt sind.

Über den DNS-Dienst werden die Hostnamen vom Computern oder auch Internetseiten in IP-Adressen aufgelöst. Jeder Host, der TCP/IP als Kommunikationsprotokoll benutzt, besitzt eine IP-Adresse. Über die Hostkennung der IP-Adresse wird jeder Computer, Drucker usw. im Netzwerk eindeutig bestimmt. Angenommen, Sie haben einen Host mit der IP-Adresse 172.20.20.106. Die IP-Adressen in diesem Bereich gehören zur Klasse B. Näheres dazu finden Sie in Kapitel 14.1.1. Im Bereich der Klasse B besteht der Hostbereich der IP-Adresse aus den beiden letzten Oktetten, also 20.106. Damit ist der Computer in seinem Netzwerk eindeutig identifiziert.

Auf jedem Computer kann die so genannte *HOSTS*-Datei eingerichtet werden. Diese Datei befindet sich im Verzeichnis `%SYSTEMROOT%\SYSTEM32\DRIVERS\ETC`. Die auch dort befindliche Datei *LMHOSTS* wird vom WINS-Dienst verwendet. In der Datei *HOSTS* werden lokal statische IP-Adressen und deren zugehörige Hosts eingetragen. Die Hosts-Datei kann mit jedem beliebigen Texteditor bearbeitet werden. Beim Start des DNS-Client-Dienstes werden diese Einträge in den DNS-Namenscache des jeweiligen Computers geladen. Die Hosts-Datei ist die traditionelle Methode zur Pflege der DNS-Namen. Es ist jedoch ein großer Aufwand, sämtliche Computer eines Netzwerks in diese Tabelle einzupflegen und dann an alle Rechner weiterzugeben. Verwenden Sie in Ihrem Netzwerk DHCP, kann die Hosts-Datei ohnehin nicht verwendet werden. Sie sollten bei DHCP das dynamische DNS (siehe Kapitel 16.4) einsetzen.

16.1.2 Wie funktionieren DNS-Abfragen?

Ein DNS-Server verarbeitet die Anfragen nach IP-Adressen, die die Clients an ihn stellen. Er kann aber umgekehrt auch IP-Adressen in Hostnamen auflösen. Das Auflösen von Hostnamen in IP-Adressen wird als Forward-Lookup bezeichnet, das Auflösen einer IP-Adresse in einen Hostnamen als Reverse-Lookup.

Ein DNS-Server kann bei der Clientabfrage gleichzeitig auch als DNS-Client fungieren, der die angeforderte Anfrage an einen anderen DNS-Server weitersendet. Deshalb läuft auf jedem DNS-Server gleichzeitig auch der Dienst „DNS-Client“.

Jede DNS-Anfrage eines Clients an einen Server besteht aus insgesamt drei Teilen:

- ▶ dem vollständigen Domännennamen (FQDN),
- ▶ einem bestimmten Abfragetyp, der einen Ressourceneintrag (siehe Kapitel 16.2.5) oder einen Abfragetyp angibt (meist A-Ressourceneintrag für die Adresse), sowie
- ▶ der Klasse für den Domännennamen, die unter Windows stets auf Internetklasse (IN-Klasse) gesetzt werden sollte.

Angenommen, ein Client sendet eine Anfrage nach der IP-Adresse des Hosts *archimedes.firma.de* an einen DNS-Server. Hierbei wird geprüft, ob für den Host mit dem FQDN *archimedes.firma.de* Ressourceneinträge für die Adresse bestehen (A-Ressourceneintrag). Ist die Antwort des DNS-Servers positiv, erhält der Client den Wert des A-Ressourceneintrags und damit die gewünschte IP-Adresse.

Eine DNS-Abfrage kann auf vier verschiedene Arten durchgeführt werden. Zum einen kann ein Client auf lokal zwischengespeicherte Daten zurückgreifen. Dies ist der Fall, wenn er bereits eine Anfrage nach einem bestimmten Host gesendet und eine Antwort empfangen hat. Zum anderen kann auch der DNS-Server selbst auf zwischengespeicherte Daten zurückgreifen, wenn er bereits die Anfrage nach diesem Host erhalten hat. Weiterhin gibt es die Verfahren Rekursion und Iteration. Bei der Rekursion leitet der DNS-Server die Anfrage des Clients an andere DNS-Server weiter. Dabei fungiert der Server selbst als Client. Hat er schließlich eine Antwort erhalten, so sendet er diese an den Client zurück. Stellt dagegen der Client selbst eine Verbindung zu anderen DNS-Servern her und benutzt dabei eigene Abfragen, die der Server mit Referenzantworten beantworten kann, so spricht man von Iteration. Die Funktionsweise dieser Verfahren wird nun kurz erläutert. Die Betonung liegt hierbei auf kurz, da nicht vom eigentlichen Thema Active Directory abgewichen werden soll. Für weitere Informationen sei auf die Windows 2000/2003-Server-Hilfe verwiesen.

Lokale DNS-Abfragen

Bevor die DNS-Abfragen an einen Server weitergeleitet werden, versucht der Client, die Adressen lokal aufzulösen. Für diese Aufgabe ist der DNS-Clientdienst zuständig. Findet der DNS-Clientdienst lokal zwischengespeicherte Einträge, so wird keine Anfrage über das Netzwerk weitergeleitet. Die zwischengespeicherten Einträge können entweder aus vorherigen DNS-Abfragen stammen, die für einen bestimmten Zeitraum – standardmäßig eine Stunde – lokal vorgehalten werden, oder aber die Einträge werden aus der lokalen *HOSTS*-Datei beim Start des DNS-Clientdienstes in den Zwischenspeicher geladen. Die *HOSTS*-Datei kann auf jedem Rechner eingerichtet und gepflegt werden.

Sie befindet sich im Verzeichnis %SYSTEMROOT%\SYSTEM32\DRIVERS\ETC. Diese Datei erhält Verknüpfungen zwischen Hostnamen und den dazugehörigen Adressen. Die Zeitspanne für das lokale Vorhalten von vorherigen DNS-Abfragen wird über den TTL-(Time To Live-)Wert vorgegeben. Sobald ein Eintrag zwischengespeichert wird, wird der Zeitwert herabgerechnet. Ist die TTL-Dauer abgelaufen, wird die Information aus dem Cache gelöscht. Wenn Sie den TTL-Wert herabsetzen, führt dies zu einer erhöhten Datenlast auf dem DNS-Server, aber auch zu aktuelleren Daten im Namensraum. Erhöhen Sie hingegen den TTL-Wert, so verringern Sie zwar die Last auf dem DNS-Server, haben aber unter Umständen nicht immer die aktuellen Daten. Die Daten werden auf dem Client nicht vor Ablauf der TTL-Dauer aktualisiert.

DNS-Server-Abfragen

Empfängt der DNS-Server eine Abfrage, so sucht er zunächst in seiner lokal konfigurierten Zone nach den entsprechenden Ressourceneinträgen. Kann er hier keine Einträge finden, so sucht er weiter in seinen zwischengespeicherten Daten. Diese sind analog zu denen des Clients auf dem Server vorhanden. Werden über eine der beiden Methoden Ergebnisse gefunden, werden diese an den Client gesendet. Andernfalls wird die Rekursion gestartet.

Rekursion

Wenn ein Client die Anfrage an den DNS-Server schickt, wird damit standardmäßig gleichzeitig auch die Rekursion beantragt. Bei der Rekursion leitet der erste DNS-Server die Anfrage an einen oder mehrere andere DNS-Server weiter. Hierfür benötigt er zunächst Informationen über die anderen DNS-Server des Namensraumes. Diese erhält er über die *Hinweise auf den Stammserver*. Hierbei handelt es sich um eine spezielle Liste, die der DNS-Dienst für die Suche nach autorisierenden DNS-Servern des Domänenstammes und der Domänen erster Ebene benutzt. Der DNS-Server sendet dann seine Anfragen hierarchisch vom autorisierenden Server der Domäne erster Ebene bis zu der Ebene, wo der entsprechende DNS-Server über die angeforderten Daten verfügt. Dieser sendet die Daten an den ursprünglich fragenden DNS-Server, der die Antwort an den Client weiterleitet. Damit ist die Rekursion abgeschlossen. Das Wiederholungsintervall der rekursiven Abfrage liegt bei drei Sekunden, das Zeitüberschreitungsintervall bei 15 Sekunden. Die Rekursion kann auch deaktiviert werden. Wählen Sie dazu aus der mmc DNS den entsprechenden Server. Unter den Eigenschaften wählen Sie die Registerkarte ERWEITERT und aktivieren dort die Checkbox REKURSIONSVORGANG DEAKTIVIERT.

Iteration

Die Iteration ist ein vom Client ausgehender Prozess an jeweils einen DNS-Server. Hierbei verlangt der Client eine sofort verfügbare Antwort und unterbindet Abfragen weiterer Server. Die Iteration wird eingeleitet, wenn entweder die Rekursion auf dem DNS-Server deaktiviert ist oder das Verwenden der Rekursion bei der Anfrage an den Server vom Client aus nicht gefordert wird. Ein Client sollte über eine lokale Liste von DNS-Servern verfügen, die er der Reihe nach abfragen kann, wenn der primäre DNS-Server keine Antwort auf die Abfrage liefern kann.

16.2 DNS-Zonen

Der DNS-Namensraum lässt sich zur besseren Verwaltung in verschiedene DNS-Zonen unterteilen. Eine Zone enthält Namensinformationen für eine oder mehrere DNS-Domänen. Sie ist die autorisierende Quelle aller Informationen für alle in ihr enthaltenen DNS-Domänennamen. Jede Zone muss einen zusammenhängenden DNS-Namensraum haben. Die Verknüpfungen zwischen den Hostnamen und IP-Adressen werden für jede Zone in einer Zonendatenbankdatei gespeichert. Für jede Zone gibt es eine fest verbundene Domäne, die als Stammdomäne der Zone bezeichnet wird. Hier befinden sich nur die Informationen zu den Teildomänen der Zone, aber nicht zwangsläufig zu allen Teildomänen der Stammdomäne. Dies soll Abbildung 16.2 verdeutlichen.

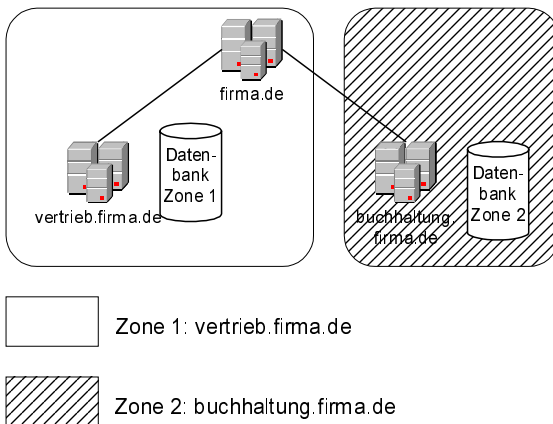


Abbildung 16.2: Zonen im DNS-Namensraum

Für Zone 1 ist *firma.de* die Stammdomäne. In der Zonendatenbankdatei befinden sich die Zuordnungen für die Domänen *firma* und *vertrieb*. Hier sind jedoch nicht die Zuordnungen der Domäne *buchhaltung* enthalten, die eine Teildomäne von *firma* ist. Diese befinden sich nur in Zone 2. Die Stammdomäne dieser Zone ist *buchhaltung.firma.de*.

Die Zonendatenbankdatei befindet sich auf einem DNS-Server. Auf einem DNS-Server können eine oder mehrere Zonen gespeichert werden. Er wird als autorisierender Server für den Namensraum bezeichnet, zu dem die Zone gehört. Für jede Zone muss mindestens ein DNS-Server vorhanden sein. Dieser enthält die primäre Zonendatenbankdatei. Er wird deshalb auch als der primäre DNS-Server bezeichnet. An diesem Server werden sämtliche Änderungen wie das Hinzufügen von neuen Hosts oder Domänen vorgenommen. Darüber hinaus können Sie für jede Zone zusätzliche DNS-Server implementieren. Diese sekundären DNS-Server dienen der Entlastung des primären DNS-Servers. Die sekundären DNS-Server erhalten eine Kopie der primären Zonendatenbank. Hierbei spricht man auch von Zonenübertragung. Die sekundären Datenbankdateien sind schreibgeschützt.

Der DNS-Namensraum gibt die logische Struktur Ihres Netzwerks wider. Die Zonen sind dabei die physischen Speicherplätze für die Ressourcen der Domänen.

Es ist nicht unbedingt erforderlich, eine Domäne in mehrere DNS-Zonen aufzuteilen. Dies ist z.B. dann sinnvoll, wenn Sie eine große Zone erstellt haben und zur Reduzierung

der Netzlast auf die DNS-Server diese in mehrere kleine Zonen unterteilen möchten. Auch zur Verbesserung der Fehlertoleranz ist die Einteilung in mehrere kleine Zonen eine gute Lösung. Ein dritter Grund für das Erstellen neuer Zonen kann der Umzug eines DNS-Namensraumes an einen anderen Standort sein, der über keine schnelle Verbindung mehr zur ursprünglichen Stammdomäne verfügt.

Wie bereits erwähnt, gibt es zwei Arten von DNS-Zonen, nämlich die Forward Lookup-Zonen und die Reverse Lookup-Zonen. Diese werden in den beiden nächsten Kapiteln nun näher erläutert.

16.2.1 Forward Lookup-Zonen

Über die Forward Lookup-Zonen werden IP-Adressen in Namen aufgelöst. Auf jedem DNS-Server muss mindestens eine Forward Lookup-Zone vorhanden sein. Wenn Sie DNS über Installationsassistenten von Active Directory einrichten, wird eine Forward Lookup-Zone erstellt, die auf dem DNS-Namen des Servers basiert. In unserem Beispiel für die Installation der Domäne *firma.de* in Kapitel 9 heißt der Server *hippokrates*. Eine Forward Lookup-Zone für *firma.de* ist bei der Installation eingerichtet und konfiguriert worden.

Bei der Einrichtung einer neuen Zone werden Sie über einen Installationsassistenten durch eine Reihe von notwendigen Angaben wie Zonentyp, Zonenname sowie Zonen-datei geleitet. In unserem Beispiel soll nun eine neue Forward Lookup-Zone für *vertrieb.firma.de* eingerichtet werden. Um eine neue Forward Lookup-Zone zu erstellen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie die mmc DNS. Wählen Sie aus dem Kontextmenü des DNS-Servers den Eintrag **NEUE ZONE**. Damit wird der Assistent gestartet. Klicken Sie auf **WEITER**. Alternativ können Sie auch aus dem Kontextmenü des Ordners **FORWARD-LOOKUP-ZONEN** den Eintrag **NEUE ZONE** wählen. Hierbei entfällt der hier beschriebene zweite Schritt, bei dem Sie entscheiden müssen, ob Sie eine Forward oder Reverse Lookup-Zone erstellen möchten.

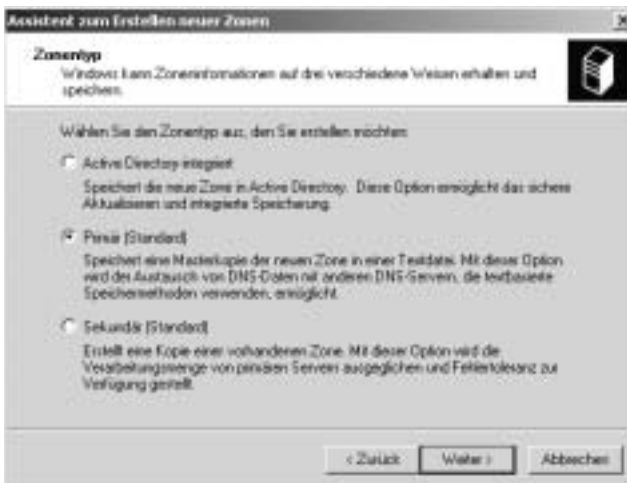


Abbildung 16.3: Auswahl des DNS-Zonentyps

2. Sie müssen nun den Zonentyp der Zone auswählen (siehe Abbildung 16.3). Es gibt die drei Typen Active Directory-integriert, Primär (Standard) sowie Sekundär (Standard). Diese Zonentypen gibt es sowohl für Forward als auch für Reverse Lookup-Zonen. Sie haben die folgenden Bedeutungen:

Zonentyp	Beschreibung
Active Directory-integriert	Hierbei handelt es sich um die Masterkopie einer neuen Zone, die von Active Directory zum Speichern und Replizieren der Zonendaten verwendet wird. Die Zone wird als dns-Containerobjekt gespeichert. Dieser Zonentyp sollte der Standardtyp bei einer Active Directory-Implementierung sein. Die Inhalte der Active Directory-integrierten Zone werden innerhalb der Domänenstruktur, nicht aber der Gesamtstruktur repliziert.
Standard (Primär)	Auch hierbei handelt es sich um eine Masterkopie einer neuen Zone. Hiermit wird die primäre Zone auf dem Computer verwaltet, auf dem die Zone erstellt wurde. Das Format dieser Datei ist eine Textdatei.
Standard (Sekundär)	Eine sekundäre Zone ist ein Replikat einer vorhandenen Zone. Eine sekundäre Zone kann erst erstellt werden, wenn bereits eine primäre Zone besteht. Auch hierbei handelt es sich um eine Textdatei, jedoch ist sie schreibgeschützt. Bei der Erstellung muss der Server angegeben werden, von dem die Zoneninformationen übertragen werden sollen.

Tabelle 16.3: Die DNS-Zonentypen

Der Vorteil Active Directory integrierter DNS-Zonen

Die Active Directory-integrierten Zonen unterstützen Multimaster-Aktualisierungen, während die Standardzonen nur Einzelmaster-Aktualisierungen verarbeiten können. Dort gibt es nur einen Server mit der Masterkopie der Zonendatenbank, der die autorisierende Quelle für die Zone ist. Fällt dieser aus, können die Clients keine aktualisierten DNS-Informationen für diese Zone erhalten. Bei den Active Directory-integrierten Zonen ist jeder DNS-Server eine primäre Quelle. Die Masterkopie der Zonendatenbank wird von der Active Directory-Datenbank verwaltet und auf alle Domänencontroller repliziert. Also kann jeder als DNS-Server konfigurierte Domänencontroller die Zonendaten aktualisieren. Die Clients erhalten so lange aktualisierte DNS-Informationen, während noch ein Domänencontroller für sie erreichbar ist. Weiterhin können Sie über die Zugriffssteuerungslisten (ACL, siehe Kapitel 19.1.1) festlegen, welche Personen die Zonen bearbeiten dürfen oder welche DNS-Clients dynamische Aktualisierungen durchführen dürfen. Die integrierten Zonen sind bereits auf jedem Domänencontroller gespeichert, auch wenn der DNS-Dienst nicht konfiguriert ist. Damit ist es möglich, die Einstellungen der Zonen automatisch auf neue Domänencontroller zu replizieren und diese zu synchronisieren. Die Aktualität der Daten ist höher, da die Verzeichnisreplikation schneller ist als die herkömmliche DNS-Replikation. Weiterhin vereinfachen Sie Ihre Verwaltung, da Sie DNS- und Active Directory-Informationen in einer Verwaltungsebene zusammenfassen können.

3. Als Nächstes müssen Sie sich entscheiden, ob Sie eine Forward oder Reverse Lookup-Zone erstellen möchten. Klicken Sie nach Ihrer Auswahl auf WEITER.
4. Danach müssen Sie einen Namen für die Zone angeben (siehe Abbildung 16.4). Sie sollten die Zone nach der hierarchisch ranghöchsten Domäne benennen, zu der die Zone gehört, also der Stammdomäne für diese Zone. In unserem Beispiel wählen wir den Namen *vertrieb.firma.de*. Dadurch können die Zonen schnell und übersichtlich verwaltet werden. Haben Sie im ersten Schritt eine Active Directory-integrierte Zone gewählt, haben Sie nun alle notwendigen Einstellungen getroffen, und der Installationsassistent zeigt Ihnen eine Zusammenfassung an.

Einstellungen für eine primäre Standardzone

Haben Sie die Erstellung einer primären Standardzone gewählt, müssen Sie nun die Angaben zur Zonendatei vornehmen (siehe Abbildung 16.4).

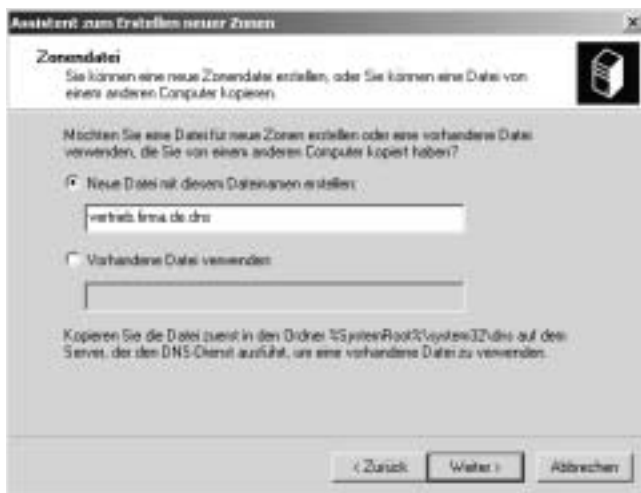


Abbildung 16.4: Einstellungen für eine primäre Standardzone

1. Hierbei müssen Sie entscheiden, ob Sie eine neue Datei erstellen oder eine vorhandene Datei verwenden möchten. Wenn Sie eine neue Zonendatei erstellen, markieren Sie die Checkbox **NEUE DATEI MIT DIESEM DATEINAMEN ERSTELLEN**. Damit wird der Name der Zonendatenbankdatei festgelegt. Standardmäßig wird der Zonename aus dem vorhergehenden Schritt vorgeschlagen und an diesen die Dateiergung *.dns* angefügt. In unserem Beispiel heißt die Zonendatei also *vertrieb.firma.de.dns*.
2. Entscheiden Sie sich, eine vorhandene Zone von einem anderen DNS-Server zu migrieren, markieren Sie die Checkbox **VORHANDENE DATEI VERWENDEN**. Sie müssen zunächst die entsprechende *.dns*-Datei aus dem Verzeichnis *%SYSTEMROOT%\SYSTEM32\DNS* des Quellservers in das entsprechende Verzeichnis auf dem neuen DNS-Server kopieren. Danach können Sie die neue Zonendatei erstellen.
3. Klicken Sie abschließend auf **WEITER**. Der Installationsassistent zeigt Ihnen eine Zusammenfassung Ihrer Einstellungen.

Einstellungen für eine sekundäre Standardzone

Haben Sie sich für die Einrichtung einer sekundären Standardzone entschlossen, so müssen Sie die Angaben für die sekundäre Standardzone vornehmen (siehe Abbildung 16.5).

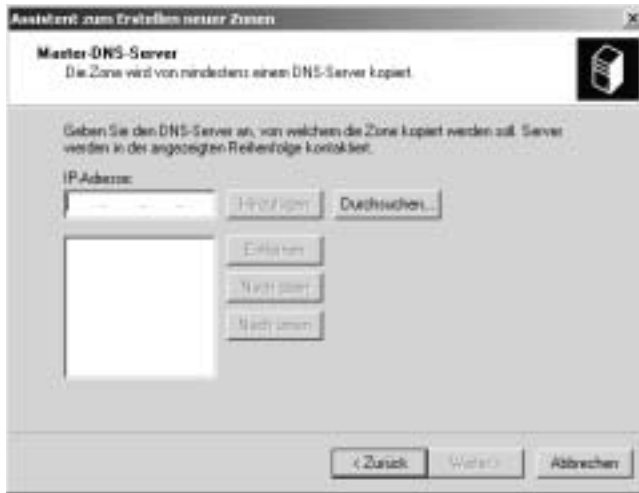


Abbildung 16.5: Einstellungen für eine sekundäre Standardzone

1. Sie müssen die IP-Adresse des DNS-Servers angeben, von dem die Zone kopiert werden soll. Dies ist der Master-DNS-Server. Geben Sie die IP-Adresse an und klicken dann auf die Schaltfläche HINZUFÜGEN. Wenn Sie mehrere Server angeben, wiederholen Sie diesen Vorgang. Die Reihenfolge der Server können Sie nachträglich über die Schaltflächen NACH OBEN und NACH UNTEN ändern.
2. Klicken Sie abschließend auf WEITER. Der Installationsassistent zeigt Ihnen eine Zusammenfassung Ihrer Einstellungen.

16.2.2 Funktionsweise des Forward Lookup

In diesem Kapitel wird an einem praktischen Beispiel die Funktionsweise des Forward Lookup erläutert. Ein Client, der nicht der Zone *firma.de* angehört, stellt eine Anfrage an den lokalen DNS-Server nach der IP-Adresse des Clients *archimedes.firma.de*.

Die Nummern in der Abbildung haben folgende Bedeutung:

1. Ein Client außerhalb der Zone *firma.de* fragt seinen lokalen DNS-Server nach der IP-Adresse von *archimedes.firma.de*. Dies ist eine Forward Lookup-Abfrage. Dabei wird gleichzeitig eine rekursive Abfrage beantragt.
2. Der DNS-Server sieht in seiner Zonendatenbankdatei nach, ob diese die gewünschte Namen-Adressen-Zuordnung enthält. Da dieser DNS-Server nicht für die Zone *firma.de* autorisiert ist, leitet er die Anfrage an den DNS-Stammserver weiter. Dieser antwortet mit dem Verweis auf den DNS-Server für *.de*. Damit sind die rekursiven Abfragen eingeleitet.

3. Der DNS-Server stellt seine Anfrage an den .de-DNS-Server. Dieser gibt einen Verweis auf den firma-Namensserver aus.
4. Der DNS-Server stellt seine Anfrage an den .firma-DNS-Server. Dies ist der autorisierende DNS-Server für diesen Teil des Namensraums und enthält somit auch die angeforderte IP-Adresse, die an den lokalen DNS-Server zurückgegeben wird.
5. Der lokale Namensserver gibt die Adresse an den Client weiter. Damit ist die Forward Lookup-Abfrage erfolgreich beendet worden.
6. Der Client hat nun Zugriff auf *archimedes.firma.de*.

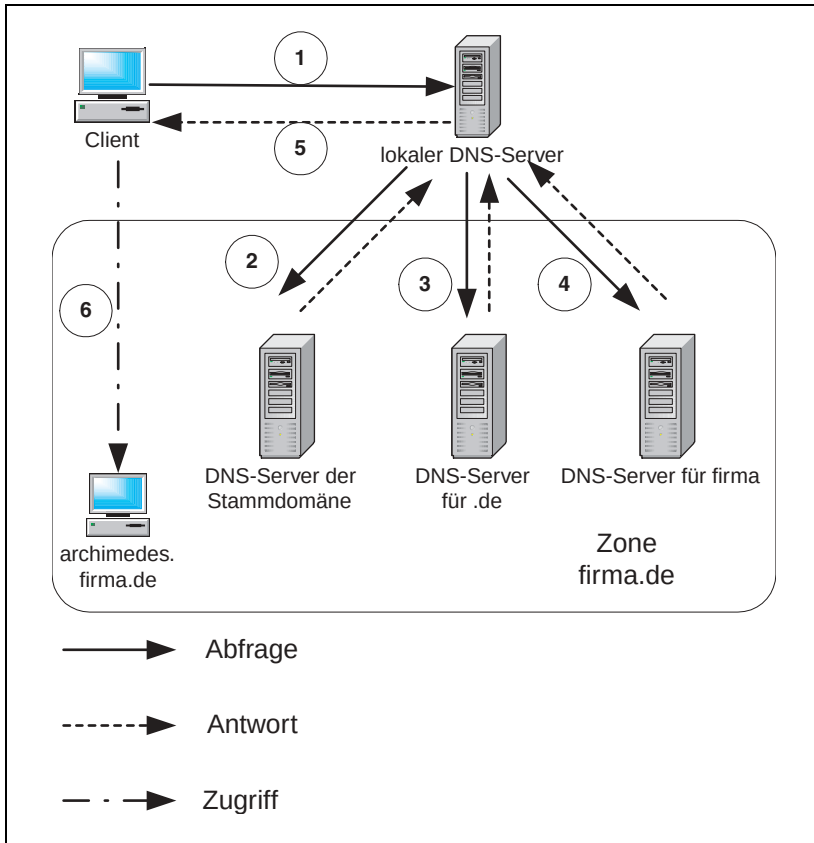


Abbildung 16.6: Die Funktionsweise des Forward Lookup

16.2.3 Reverse Lookup-Zonen

Über eine Reverse Lookup-Zone werden IP-Adressen in DNS-Namen aufgelöst. Dieser Vorgang findet nicht so häufig statt wie das Forward Lookup. Im Gegensatz zu den Forward Lookup-Zonen sind sie jedoch nicht unbedingt erforderlich. Jedoch greifen Diagnoseprogramme wie etwa NSLOOKUP (siehe Kapitel 16.6.3) auf die Reverse Lookup-Zonen zurück.

Eine Reverse Lookup-Zone wird ähnlich wie eine Forward Lookup-Zone erstellt.

1. Öffnen Sie die mmc DNS und wählen aus dem Kontextmenü des DNS-Servers den Eintrag NEUE ZONE. Alternativ können Sie auch aus dem Kontextmenü des Ordners REVERSE-LOOKUPZONEN den Eintrag NEUE ZONE wählen. Hierbei entfällt der folgend beschriebene zweite Schritt, bei dem Sie entscheiden müssen, ob Sie eine Forward- oder Reverse-Lookup-Zone erstellen möchten.
2. Wählen Sie dann den Zonentyp. Es gibt auch hier Active Directory-integrierte sowie primäre und sekundäre Standardzonen.
3. Nun müssen Sie die Netzwerkkennung der Zone angeben (siehe Abbildung 16.7). Geben Sie dazu in die Textbox NETZWERKKENNUNG den Netzwerkbereich der IP-Adresse ein. In unserem Beispiel lautet der Netzwerkteil 172.20, da es sich um ein Netzwerk der Klasse B handelt. Dadurch wird automatisch das Feld NAME DER REVERSE LOOKUP-ZONE ausgefüllt.



Abbildung 16.7: Die Netzwerkkennung einer Reverse Lookup-Zone

4. Dadurch werden alle Reverse Lookup-Abfragen im Netzwerkbereich 172.20 in dieser Zone in Namen aufgelöst. Klicken Sie anschließend auf WEITER. Haben Sie eine Active Directory-integrierte Zone gewählt, erscheint nun die Zusammenfassung.

Einstellungen für eine primäre Standardzone

1. Als Nächstes müssen Sie die Zonendatei angeben (siehe Abbildung 16.8). Markieren Sie dazu die Checkbox **NEUE DATEI MIT DIESEM DATEINAMEN ERSTELLEN**. Standardmäßig wird der Name in dem Format **UMGEKEHRTE IP-OKTETTE.IN-ADDR.ARPA.DNS** vorgegeben. In unserem Beispiel ist dies **20.172.in-addr.arpa.dns**.

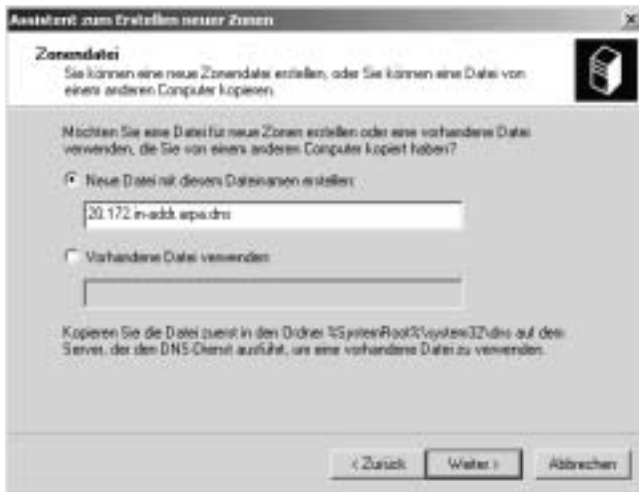


Abbildung 16.8: Die Zonendatei der Reverse Lookup-Zone

2. Sie haben auch hier analog zur Forward Lookup-Zone die Möglichkeit, eine vorhandene Datei zu benutzen. Markieren Sie in diesem Fall die Checkbox **VORHANDENE DATEI VERWENDEN**. Diese Datei muss zuvor vom Quell-DNS-Server in das Verzeichnis **%SYSTEMROOT%\SYSTEM32\DNS** kopiert worden sein. Klicken Sie auf **WEITER**. Es wird die Zusammenfassung angezeigt.

Einstellungen für eine sekundäre Standardzone

1. Haben Sie sich für die Einrichtung einer sekundären Zone entschlossen, erscheint nach der Eingabe des Zonnennamens ein Fenster, in dem Sie den DNS-Server angeben, von dem die Zone kopiert werden soll, siehe Abbildung 16.5. Klicken Sie auf **WEITER**, und es erscheint eine Zusammenfassung.

16.2.4 Funktionsweise des Reverse Lookup

Beim Reverse Lookup wird der Name eines Hosts abgefragt, dessen IP-Adresse bekannt ist. Diese Abfrage ist nicht so häufig wie das Forward Lookup. Die DNS-Datenbank ist deshalb auch für die Forward Lookup-Abfrage optimiert, da die Namen der Hosts und nicht deren IP-Adressen als Primärschlüssel indiziert sind. Somit würde eine Reverse Lookup-Abfrage sehr lange dauern, da sämtliche Namen durchsucht werden müssten.

Um die Suche nach Hostnamen dennoch ebenso schnell wie die Suche nach IP-Adressen durchführen zu können, wird eine spezielle Domäne der zweiten Ebene namens *in-addr.arpa* angelegt. Diese dient ausschließlich dem Reverse Lookup. Auch diese Domäne ist hierarchisch aufgebaut, allerdings basiert sie auf den IP-Adressen anstatt auf den Namen. Die einzelnen Domänen werden nach den IP-Adressen der Netzwerkbereiche benannt.

In unserem Beispiel umfasst unser Unternehmen den IP-Bereich 172.20.20.0 bis 172.20.20.255 der Klasse B mit dem Subnetz 255.255.0.0. Somit ist die Autorität für die Zone 20.172.in-addr.arpa gegeben.

Angenommen, es wird der Hostname für die IP-Adresse 172.20.20.172 gesucht. Die Suche wird in den folgenden Ebenen ausgeführt:

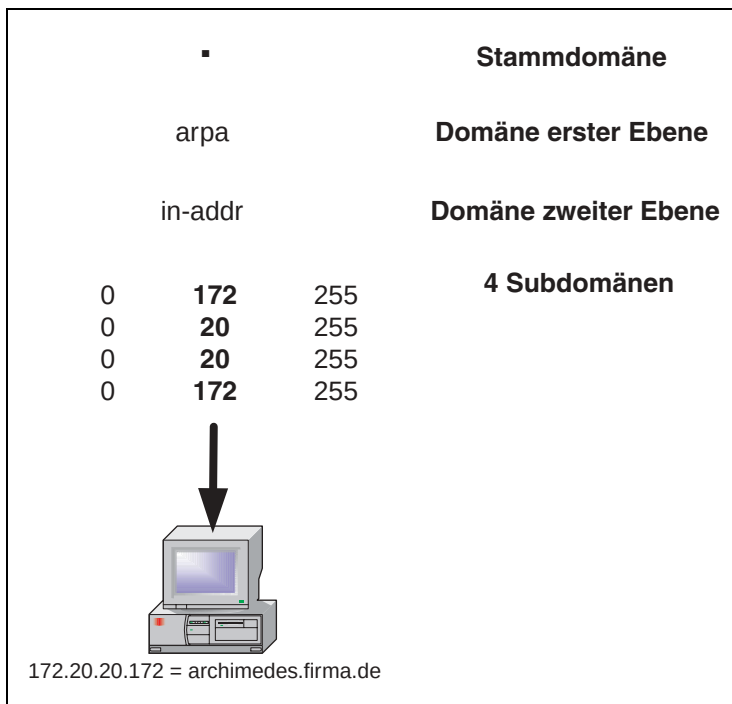


Abbildung 16.9: Funktionsweise einer Reverse Lookup-Abfrage

Das Ergebnis der Suche bringt den vollständigen Hostnamen *archimedes.firma.de*.

16.2.5 Ressourceneinträge

Die Ressourceneinträge befinden sich in der Zonendatenbankdatei. Sie sind Verknüpfungen zwischen den DNS-Domännennamen und Daten für Netzwerkressourcen.

Der häufigste Eintrag ist der Host (A)-Eintrag, der die Zuordnung von Hostnamen und IP-Adresse enthält. Insgesamt gibt es 19 verschiedene Ressourceneinträge. Die wichtigsten zeigt die folgende Tabelle. Für alle übrigen gibt das jeweilige Dialogfeld nähere Angaben oder Quellen an.

Ressourceneintrag	Beschreibung
Alias (CNAME)	Zum Festlegen alternativer Hostnamen, um mit mehreren Namen auf eine Adresse zeigen zu können. Dies ist dann sinnvoll, wenn Sie z.B. auf demselben Computer einen Webserver mit dem Namen <i>www.firma.de</i> sowie einen FTP-Server mit dem Namen <i>ftp.firma.de</i> haben.
Dienstidentifizierung (SRV)	Gibt an, welche Server bestimmte Dienste ausführen, z.B. primäre Dientserver oder Sicherungsserver. Ein Client kann auch eine Liste der IP-Adressen der Domänencontroller vom DNS-Server für die Anmeldung anfordern.
Host (A)	Gibt die Zuordnungen zwischen Hostnamen und IP-Adressen für die Forward Lookup-Zone an.
Hostinformationen (HINFO)	Kann zur Ressourcenüberwachung eingesetzt werden. Sie können für jeden Host das Betriebssystem und die CPU angeben.
Namensserver (NS)	Gibt alle DNS-Server an, die der Domäne zugeteilt sind.
SOA (Source of authority/ Autoritätsursprung)	Gibt den DNS-Server an, der die autorisierende Quelle innerhalb der Domäne ist.
Zeiger (PTR)	Das Gegenstück zum Hosteintrag. Hier werden für die Reverse Lookup-Zone die Verknüpfungen zwischen Adresse und Name angegeben.

Tabelle 16.4: Die wichtigsten Ressourceneinträge

Um einen neuen Ressourceneintrag zu erstellen, wählen Sie aus dem Kontextmenü der entsprechenden Zone den Eintrag NEUER HOST, NEUER ALIAS oder NEUER MAIL-EXCHANGER. Für alle übrigen Einträge wählen Sie ANDERE NEUE EINTRÄGE. Aus der Liste können Sie dann den Ressourcentyp auswählen. Wenn Sie im Bereichsabschnitt eine Zone markieren, sehen Sie im Ergebnisabschnitt alle Ressourceneinträge, die für diese Zone existieren. Sie können auch manuell neue Einträge an der Datei *netlogon.dns* vornehmen. Diese Textdatei befindet sich in %SYSTEMROOT%\SYSTEM32\CONFIG\.

Beim Erstellen einer neuen Zone werden automatisch die Namensserver (NS)- und SOA-Einträge erstellt. Diese können nicht wie alle anderen Einträge manuell erstellt werden. Der SOA-Eintrag muss dabei der erste Eintrag in der Zonendatenbankdatei sein. Über die Eigenschaften des SOA-Eintrags können Sie verschiedene Optionen einstellen. Die Eigenschaftsseite gliedert sich in sechs Tabsheets. Dies sind:

TabSheet	Beschreibung	
Allgemein	Status und Typ der Zone sowie Einstellungen zur dynamischen Aktualisierung, siehe Kapitel 3.4.	
Autoritätsursprung	Seriennummer	Revisionsnummer, die sich bei jeder Änderung eines Ressourceneintrags erhöht. Anhand dieser Nummer werden die Änderungen für die Replikation auf andere Server verfolgt.
	Primärer Server	Hostname des primären DNS-Servers
	Verantwortliche Person	E-Mail-Adresse des Administrators. Statt @ wird . verwendet.
	Aktualisierungsintervall	So lange wartet ein sekundärer DNS-Server, ehe er die Zone erneuert. Dabei holt er sich eine Kopie des SOA-Eintrags. Unterscheiden sich die beiden Seriennummern, leitet er eine Zonenübertragung ein.
	Wiederholungsintervall	Wartezeitraum bei Mißerfolg der Zonenübertragung
	Läuft ab nach	Nach diesem Wert beantwortet der sekundäre Server keine Anfragen mehr, nachdem das Aktualisierungsintervall abgelaufen ist, in dem die Zone nicht erfolgreich übertragen wurde.
	Minimum TTL	So lange wird ein Wert von anderen Servern zwischengespeichert.
	TTL für diesen Eintrag	Benutzerdefinierte Werte, die vom Minimum TTL abweichen.
Namensserver	Eine Liste aller verfügbaren DNS-Server der Domäne. Sie können weitere hinzufügen.	
WINS	Sie können einen oder mehrere WINS-Server angeben, die die Namen auflösen, die nicht im DNS-Namensraum gefunden werden konnten.	
Zonenübertragungen	Optionen zur Zonenübertragung. Es ist einstellbar, ob sie zugelassen sind und, wenn ja, an welchen primären und sekundären Server sie stattfinden sollen. Vergleiche Kapitel 3.3.	
Sicherheitseinstellungen	Einstellungen für die Zugriffsrechte auf die Zone.	

Tabelle 16.5: Die SOA-Eigenschaften

16.2.6 Delegieren von Zonen

Standardmäßig werden in einer Zone die Daten für einen DNS-Domännennamen gespeichert. Wenn Sie nun Unterdomänen dieser Domäne erstellen, können die Unterdomänen derselben oder auch einer eigenen Zone angehören. Die neue Unterdomäne kann entweder in die bereits vorhandenen Zoneneinträge integriert oder in eine neue Zone delegiert werden, die Sie für die neue Unterdomäne eingerichtet haben. Bei der Delegation einer Zone müssen auch die SOA-Ressourceneinträge erstellt werden. Es muss im SOA-Eintrag auf den autorisierenden DNS-Server verwiesen werden. Ansonsten kann nicht ordnungsgemäß auf andere DNS-Server und -Clients verwiesen werden.

Für die Delegation von Zonen steht Ihnen ein Assistent zur Verfügung. Führen Sie dazu die folgenden Schritte durch:

1. Öffnen Sie die mmc DNS. Erstellen Sie gegebenenfalls über den Eintrag **NEUE DOMÄNE** die neue Unterdomäne an der gewünschten Position.
2. Wählen Sie aus den Eigenschaften der neuen Domäne **NEUE DELEGIERUNG**. Damit wird der Assistent gestartet. Klicken Sie auf **WEITER**.
3. Geben Sie nun den Namen der zu erstellenden Unterdomäne an (siehe Abbildung 16.10). Dabei wird im unteren Feld automatisch der vollqualifizierte Domänenname vervollständigt. Klicken Sie danach auf **WEITER**.

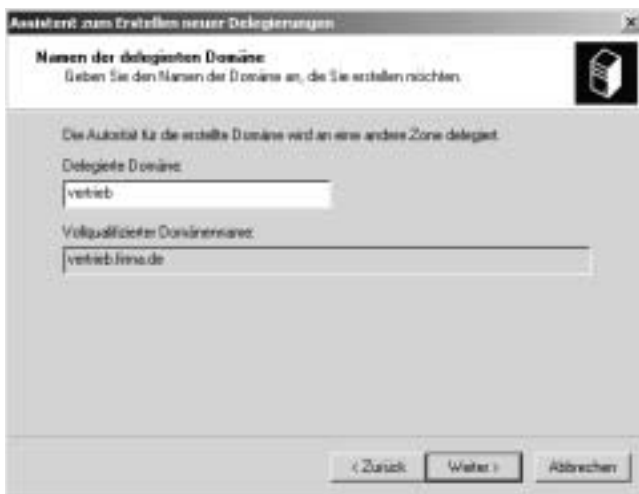


Abbildung 16.10: Der Delegierungsassistent

4. Nun müssen Sie die Namen der DNS-Server angeben, die die delegierte Zone verwalten sollen. Klicken Sie dazu auf **HINZUFÜGEN**. Geben Sie nun entweder direkt den Namen ein, oder wählen Sie über **DURCHSUCHEN** den oder die gewünschten Server aus. Klicken Sie dann auf **WEITER**.
5. Zum Abschluss sehen Sie eine Übersicht der getroffenen Einstellungen. Über **ZURÜCK** können Sie Einstellungen korrigieren. Nachdem Sie die neue Zone über **FERTIG STELLEN** eingerichtet haben, erscheint diese mit einem neuen Symbol im Bereichsabschnitt der DNS-Zone.

16.2.7 DNS-Weiterleitungen

Bei der Installation des DNS-Dienstes über DCPROMO wird standardmäßig die Root-DNS-Zone angelegt. Diese Zone trägt den Namen . (Punkt). Wenn diese Zone beibehalten wird, kann es unter Umständen zu Problemen bei der Namensauflösung von externen Ressourcen wie Internetadressen kommen. Solange der DNS-Server über die Root-Zone verfügt, betrachtet er sich selbst als quasi allwissend für alle Anfragen und leitet keine Anfragen an andere DNS-Server weiter. Ist dieser Server nun so konfiguriert, dass er nur die internen Hosts auflösen kann, wird kein Client in der Lage sein, auf Internetressourcen zuzugreifen, da deren Namen vom DNS-Server nicht aufgelöst werden können.

Um dieses Problem zu umgehen, müssen Sie zuerst die Root-Zone des DNS-Servers löschen. Danach wählen Sie aus den Eigenschaften des Servers die Registerkarte WEITERLEITUNGEN. Dort markieren Sie die Checkbox WEITERLEITUNG AKTIVIEREN und tragen die IP-Adressen der Komponenten ein, die die externen Adressen auflösen können. Dabei kann es sich um weitere DNS-Server handeln oder um einen Router. Für die Weiterleitungen kann zusätzlich ein Zeitlimit definiert werden. Außerdem können Sie festlegen, ob für diese Weiterleitungen die Rekursion verwendet werden soll oder nicht.

Die konfigurierten Weiterleitungen sind nun für alle Zonen aktiv, die auf diesem DNS-Server eingerichtet worden sind bzw. später zusätzlich eingerichtet werden. Solange die Root-Zone nicht gelöscht ist, ist die Checkbox WEITERLEITUNG AKTIVIEREN nicht anwählbar.

16.3 Zonenübertragungen

Sie sollten aus Redundanzgründen sowie auch zur besseren Fehlertoleranz mehrere DNS-Server in Ihrem Netzwerk einsetzen. Auch für die Verbesserung der Zugriffsgeschwindigkeit für Remote-Standorte ist die Einrichtung von zusätzlichen DNS-Servern sinnvoll. Da die Verwaltung des DNS somit auf mehrere Server verteilt wird, müssen diese Zonenübertragungen durchführen. Durch Zonenübertragungen wird die Replikation und Synchronisation aller Zonenkopien auf allen DNS-Servern ermöglicht. Die Zonenübertragung findet zwischen dem primären DNS-Server und den sekundären DNS-Servern statt. Es gibt zwei Arten der Zonenübertragung, nämlich die vollständige und inkrementelle Zonenübertragung.

Sobald Sie einen neuen sekundären DNS-Server zu einer bestehenden Zone hinzugefügt haben, wird die vollständige Zonenübertragung (AXFR) durchgeführt. Hierbei erhält der neue sekundäre DNS-Server eine vollständige Kopie der Ressourceneinträge für diese Zone und kann diese nun replizieren. AXFR ist der von allen DNS-Servern unterstützte Standardabfragetyp.

Windows 2000/2003 unterstützt als Neuerung auch die inkrementelle Zonenübertragung (IXFR). Diese Zonenübertragung wird zum Aktualisieren von Änderungen benutzt. In früheren DNS-Implementierungen wurde auch dafür eine vollständige Zonenübertragung durchgeführt. Zur Nutzung der inkrementellen Zonenübertragung müssen sowohl der Quellserver als auch der Zielserver dieses Feature unterstützen. IXFR ist wesentlich effektiver, schneller und weniger netzwerkbelastend als AXFR. Nur für die Zonenreplikation wird auch weiterhin AXFR verwendet.

Bei der inkrementellen Zonenübertragung erhält ein DNS-Server nur die Änderungen, die für die Synchronisierung seiner Datenbankdatei mit der des Quellservers erforderlich sind. Die Änderungen werden anhand des Seriennummereintrags (siehe Tabelle 16.5) im SOA-Ressourceneintrag vorgenommen. Ist diese bei Ziel und Quelle identisch, findet keine Übertragung statt. Besitzt der Quellserver eine höhere Seriennummer, werden nur die geänderten Einträge der inkrementellen Versionen übertragen. Hierzu führt der DNS-Quellserver eine chronologische Liste der inkrementellen Zonenänderungen. Der Quellserver ist entweder der primäre DNS-Server oder ein anderer sekundärer DNS-Server, der die zu übertragende Zone enthält.

Zur Erhöhung der Sicherheit können Sie die Server auflisten, die an der Zonenübertragung teilnehmen dürfen. Damit wird verhindert, dass nicht autorisierte DNS-Server Zonen übertragen. Treffen Sie dazu die folgenden Einstellungen:

1. Öffnen Sie in der mmc DNS die Zone, für die die Zonenübertragung konfiguriert werden soll, und wählen aus dem Kontextmenü EIGENSCHAFTEN.
2. Wählen Sie dort die Registerkarte ZONENÜBERTRAGUNGEN. Dort haben Sie drei verschiedene Optionen, an welche Server die Übertragung stattfinden darf (siehe Abbildung 16.11).



Abbildung 16.11: DNS-Zonenübertragungen

- ▶ **AN JEDEN SERVER:** Die Übertragung findet an alle Server statt, auch an nicht autorisierte DNS-Server. Dies ist die Standardeinstellung.
- ▶ **SERVER, DIE UNTER „NAMENSER“ AUFGEFÜHRT SIND:** Auf der Registerkarte derselben Eigenschaftsseite können Sie alle DNS-Server der Zone angeben. Die Übertragung erfolgt an alle der dort von Ihnen angegebenen Server.
- ▶ **NUR AN FOLGENDE SERVER:** Hier können Sie beliebige Server eintragen. Es müssen nicht alle Server enthalten sein, die unter Namenserver aufgelistet sind.

Eine inkrementelle Zonenübertragung wird grundsätzlich vom Sekundärserver aus eingeleitet. Es ist also ein Pull-Verfahren. Sie findet statt, wenn das Aktualisierungsintervall einer Zone abgelaufen ist oder wenn der DNS-Dienst für eine Zone auf dem sekundären Server gestartet wird. Außerdem können Sie eine Benachrichtigungsliste der Server (siehe Kapitel 16.3.1) konfigurieren, die bei Änderungen an der primären Zone eine Zonenübertragung durchführen sollen. Zusätzlich können Sie den Vorgang auch jederzeit manuell einleiten.

16.3.1 Die DNS-Benachrichtigungsliste

Die DNS-Benachrichtigung ist ein Push-Verfahren, bei dem die Änderungen an den Zonen-daten vom Quellserver den Sekundärservern einer einstellbaren Liste mitgeteilt werden. Diese Server leiten dann ihrerseits im Pull-Verfahren die Zonenübertragung ein. Die DNS-Benachrichtigung wird nur für sekundäre Server benötigt. Die Active Directory-integrierten Zonen werden automatisch standardmäßig alle 15 Minuten auf Änderungen hin abgefragt. Eine Benachrichtigung ist hier überflüssig und könnte zu unnötiger Netzwerklast führen.

Nachdem eine Zone auf dem Quellserver geändert wurde, wird die Seriennummer im SOA-Ressourceneintrag erhöht. Damit wird gezeigt, dass eine neue Version der Zone vorhanden ist. Daraufhin sendet der Quellserver eine Benachrichtigung an alle angege-benen Server, die dann ihrerseits eine IXFR-Zonenübertragung durchführen.

Um eine Benachrichtigungsliste zu erstellen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die Registerkarte ZONENÜBERTRAGUNGEN aus den Eigenschaften der Zone (siehe Abbildung 16.11).
2. Klicken Sie dort auf die Schaltfläche BENACHRICHTIGEN. Es erscheint das Fenster BENACHRICHTIGEN (siehe Abbildung 16.12).
3. Aktivieren Sie hier die Checkbox AUTOMATISCH BENACHRICHTIGEN und wählen dann die Server, die benachrichtigt werden sollen. Sie können entweder die unter Namen-server aufgelisteten Server wählen oder selbst einen Satz von Servern festlegen. Kli-cken Sie dann auf OK.



Abbildung 16.12: Die DNS-Benachrichtigungsliste

16.4 Dynamisches DNS

Windows 2000 und 2003 unterstützen neben dem herkömmlichen DNS auch dynamisches DNS, das auch als DDNS bezeichnet wird. Beim dynamischen DNS werden Änderungen an den IP-Adressen, die der Client per DHCP zugewiesen bekommt, automatisch in der Zonendatenbankdatei durchgeführt und aktualisiert. Dies ist ein entscheidender Vorteil von Windows 2000 bezüglich des Verwaltungsaufwandes, da Sie die geänderten Adressen nicht mehr manuell pflegen müssen.

Der DHCP-Dienst ist unter Windows 2000 und 2003 eng mit dem DDNS verknüpft. Dem DHCP-Client wird vom DHCP-Dienst gestattet, seinen Host (A)-Ressourceneintrag in die Zonendatenbank zu schreiben, während der DHCP-Dienst selbst den zugehörigen Zeiger (PTR)-Eintrag für die Reverse Lookup-Zone erstellt. Sobald die Gültigkeitsdauer des DHCP-Tickets für den Client abgelaufen ist, entfernt der DHCP-Dienst den A- sowie PTR-Eintrag wieder aus der Zonendatenbankdatei. Damit sind keine ungültigen Einträge in der Zonendatenbankdatei enthalten. DHCP-Clients mit einem nicht DDNS-fähigen Client-Betriebssystem unterstützen nicht die direkte Interoperabilität mit DDNS. In diesem Fall sendet anstelle des Clients der DHCP-Server sowohl den Host- als auch den Zeigereintrag an den DNS-Server.

	Statische IP-Adressen	Windows 2000-DHCP-Server
DDNS-fähiger Client	Der Client registriert den A- und PTR-Eintrag.	Der Client registriert den A-Eintrag, der DHCP-Server den PTR-Eintrag. Beide Einträge werden vom DHCP-Server wieder entfernt.
nicht-DDNS-fähiger Client	Es findet keine automatische Registrierung statt.	Der DHCP-Server registriert und entfernt den A- und PTR-Eintrag.

Tabelle 16.6: Die DDNS-Funktionalitäten der Clients

Tabelle 16.6 gibt Ihnen einen Überblick über die Funktionen des Windows 2000-DHCP-Servers im Zusammenspiel mit DDNS-fähigen und nicht-DDNS-fähigen Clients sowie den Funktionen der Clients, wenn statische IP-Adressen vergeben werden. DDNS-fähig sind die Windows-Versionen 2003, XP, 2000 sowie 98, nicht DDNS-fähig sind die Versionen 3.x, 95, NT 3.x sowie NT 4.0.

Damit der DHCP-Server die dynamischen Aktualisierungen an den DNS-Server senden kann, muss in der Konfiguration des DHCP-Servers auf die entsprechenden DNS-Server verwiesen werden. Dies geschieht in der mmc DHCP über die Optionen. Die weiteren Schritte hierzu finden Sie in der Windows-Hilfe beschrieben. Weiterhin muss es sich um einen DHCP-Server der Version Windows 2000 oder 2003 handeln. Ein DHCP-Server unter Windows NT bietet nicht die Funktionalitäten zur Registrierung der Clients im DNS.

Falls Sie keinen Windows 2000-basierten DNS-Server, sondern beispielsweise einen Unix-Server einsetzen möchten, so vergewissern Sie sich vordem anhand der RFCs 2052 (Unterstützung von SRV-Einträgen) und besonders 2136, ob dieser die Spezifikationen zur Unterstützung des DDNS erfüllt oder nicht. Die Unterstützung von SRV-Einträgen

ist zwingend notwendig. Ansonsten kann der Unix DNS-Server nicht in einer Windows 2000-Domäne betrieben werden. Unterstützt er lediglich die Spezifikationen für DDNS nicht, so kann er wenigstens als herkömmlicher DNS-Server eingesetzt werden.

16.4.1 Einrichten von dynamischem DNS

Dieses Kapitel beschreibt die Einrichtung von DDNS auf Ihrem DNS-Server.

1. Wählen Sie aus dem Kontextmenü der Forward oder Reverse Lookup-Zone den Eintrag EIGENSCHAFTEN und dort die Registerkarte ALLGEMEIN (siehe Abbildung 16.13).



Abbildung 16.13: Die Konfiguration des dynamischen DNS

2. In der Listbox DYNAMISCHE AKTUALISIERUNG ZULASSEN haben Sie drei Auswahlmöglichkeiten. Dies sind:
 - ▶ NEIN: In dieser Zone sind keine dynamischen Aktualisierungen möglich.
 - ▶ JA: Alle dynamischen Aktualisierungen dieser Zone werden durchgeführt
 - ▶ NUR GESICHERTE AKTUALISIERUNGEN: Diese Option ist nur bei Active Directory-integrierten Zonen verfügbar und dort die Standardeinstellung. In dieser Einstellung wird über einen speziellen Mechanismus geprüft, ob der Sender der Abfrage berechtigt ist, Aktualisierungen an der Zonendatenbank durchzuführen. Dieser Mechanismus ist fest in einem gesicherten DNS-Aktualisierungsprotokoll enthalten. Die technischen Details dazu entnehmen Sie den RFCs 2136 und 2137.

16.5 Standorte von DNS-Servern

Nachdem Sie bereits Informationen zum Einrichten und Konfigurieren der DNS-Server erhalten haben, soll Ihnen dieses Kapitel zeigen, wie Sie die DNS-Server am effektivsten in Ihrem Netzwerk platzieren. Hierfür gibt es sicher nicht nur einen Weg, aber die folgenden Hinweise sollen Ihnen bei der Erstellung nützlich sein.

- ▶ Normalerweise sind an einem Standort zwei DNS-Server zur Redundanz ausreichend. Sie sollten jedoch weitere Server zu Remote-Standorten hinzufügen, sofern Ihr Unternehmen über solche verfügt.
- ▶ Bei der Verwendung von Active Directory-integrierten Zonen müssen die DNS-Server auf den Domänencontrollern eingerichtet werden. Das heißt aber nicht, dass zwangsläufig jeder Domänencontroller an einem Standort für den DNS-Dienst konfiguriert sein muss.
- ▶ Wenn Sie standardmäßige DNS-Zonen verwenden, können Sie nur einen primären DNS-Server einrichten. Am Standort des Primärservers sollte höchstens ein sekundärer Server hinzukommen, an den anderen Standorten jeweils maximal zwei sekundäre Server.
- ▶ Da DDNS-Aktualisierungen nur am primären Server vorgenommen werden können, kann dies gerade zu Stoßzeiten wie morgens zu einer erhöhten Auslastung des Servers führen. Untergliedern Sie den Namensraum in weitere Unterdomänen, die ihrerseits jeweils eine primäre Zone haben können. Bei Active Directory-integrierten Zonen entfällt dieses, da jeder Server die DDNS-Aktualisierungen verarbeiten kann.
- ▶ Wenn Sie den Clients die DNS-Server lokal zuweisen oder die DHCP-Server-Optionen konfigurieren, sollten Sie darauf achten, welche und wie viele DNS-Server Sie den Clients zuweisen. Die Anzahl der DNS-Server sollte selbst in einem großen Netzwerk nicht drei übersteigen. Sobald der erste eingetragene DNS-Server keine Anfragen des Clients mehr beantwortet, benutzt er künftig ausschließlich den zweiten angegebenen Server, selbst wenn der erste nach einiger Zeit wieder funktionsfähig sein sollte. Um die Clients dazu zu zwingen, dass sie wieder den ersten DNS-Server benutzen, müssen Sie den zweiten herunterfahren.
- ▶ Sie sollten ferner darauf achten, dass der sekundäre Server nicht unbedingt ein DNS-Server eines Remote-Standortes ist. Ansonsten werden Sie nach dem Ausfall des ersten DNS-Servers den Effekt haben, dass sämtliche Clients über ein möglicherweise langsames WAN ihre DNS-Informationen beziehen und damit das WAN lahm legen können. Haben Sie als zweiten DNS-Server nur einen im WAN verfügbar, so müssen Sie regelmäßig anhand des WAN-Verkehrs prüfen, ob die Clients nicht zwischenzeitlich diesen DNS-Server als den primären benutzen.

16.6 Fehlersuche bei DNS-Problemen

Dieses Kapitel beschäftigt sich mit der Fehlersuche und deren Behebung bei DNS-Problemen. Zunächst werden Ihnen einige Optionen vorgestellt, mit denen Sie auf Probleme aufmerksam werden können. Hierzu zählen das DNS-Ereignisprotokoll, das DNS-Logfile sowie einige Befehlszeilenprogramme. Danach werden einige häufig auftretende DNS-Fehler-Szenarios beschrieben und jeweils ein Lösungsansatz dafür geboten.

16.6.1 Das DNS-Ereignisprotokoll

Für die Meldungen des DNS-Serverdienstes gibt es ein separates Ereignisprotokoll. In diesem werden von Windows vordefinierte Ereignisse des DNS-Serverdienstes protokolliert. Jedem Ereignis wird dabei eine bestimmte ID zugewiesen. Die Ereignisse werden in Hinweise, Warnungen und Fehlermeldungen unterteilt. Zu den Informationen zählen das Starten und Beenden des Dienstes. Auch über Ereignisse wie z.B. den Abschluss eines Aufräumzyklus wird eine Informationsmeldung ausgegeben. Diese Ereignisse sind nicht kritisch, sondern dienen nur der Information.

- ▶ Warnmeldungen sind kritischer und sollten anhand der im Protokoll gegebenen Hinweise schnellstmöglich beseitigt werden.
- ▶ Auch bei Fehlermeldungen wird ein Hinweis auf eine mögliche Abhilfe gegeben. Bei zonenbezogenen Fehlern reicht oftmals das Neuladen der jeweiligen Zone. Auch die Fehlermeldungen des DDNS werden hier aufgezeichnet.
- ▶ Die Ereignismeldungen des DNS-Clientdienstes befinden sich im Systemprotokoll des jeweiligen Computers.
- ▶ Das Ereignisprotokoll ist der erste schnelle Weg, um sich einen Überblick zu verschaffen, ob und, wenn ja, welche DNS-Probleme vorliegen. Sollten die in der Ereignisbeschreibung gegebenen Hinweise nicht zur Beseitigung des Problems führen, so können Sie im nächsten Schritt Debug-Optionen Debug-Optionen einstellen. Dies beschreibt das nächste Kapitel.

16.6.2 Das DNS-Logfile

Im Verzeichnis %SYSTEMROOT%\SYSTEM32\DNS befindet sich die Datei DNS.LOG. In ihr werden die Ereignisse des DNS-Servers ab dem aktuellen Start protokolliert. Im selben Verzeichnis befindet sich ein Ordner namens BACKUP. Dieser enthält das DNS-Protokoll seit dem letzten Start des DNS Server-Dienstes bis zum Beenden des Dienstes.

Standardmäßig sind jedoch alle Debug-Protokollierungsinformationen deaktiviert. Das Debuggen kann sich negativ auf die Leistung des DNS-Servers auswirken und auf diesem Festplattenkapazität belegen. Deshalb sollten die Debug-Optionen Debug-Optionen nur eingeschaltet werden, wenn Sie ein spezielles Problem lösen möchten.

Um die Protokollierung zu aktivieren, führen Sie folgende Schritte durch:

1. Öffnen Sie in der mmc DNS den DNS-Server und wählen aus dem Kontextmenü den Eintrag EIGENSCHAFTEN.
2. Wählen Sie dort die Registerkarte PROTOKOLLIERUNG (siehe Abbildung 16.14). Aktivieren Sie dort die Checkboxes der gewünschten Optionen und klicken auf OK.



Abbildung 16.14: Die Optionen für die DNS-Debugprotokollierung

- Um das Debuggen zu beenden, klicken Sie auf die Schaltfläche STANDARD. Damit werden alle Debug-Optionen wieder deaktiviert.

Die Debug-Optionen haben die folgenden Bedeutungen:

Debugoption	Protokolliert Folgendes:
Abfragen	von den DNS-Clients an den Server gesendete Abfragen
Benachrichtigungen	Benachrichtigungen, die der DNS-Server von anderen Servern erhält
Aktualisieren	dynamische Aktualisierungen, die von anderen DNS-Servern gesendet werden
Fragen	Inhalt des Fragenabschnitts aller DNS-Abfragen, die der Serverdienst bearbeitet
Antworten	Inhalt des Antwortabschnitts aller DNS-Abfragen, die der Serverdienst bearbeitet
Senden	Anzahl der vom DNS-Dienst gesendeten Abfragen
Empfangen	Anzahl der vom DNS-Dienst empfangenen Abfragen
UDP	Anzahl der über den UDP-Port empfangenen Abfragen
TCP	Anzahl der über den TCP-Port empfangenen Abfragen
Vollständige Pakete	Anzahl vollständiger Pakete, die der DNS-Server erstellt und versendet hat
Protokollierung fortsetzen	Anzahl der Pakete, die weiter zurück in die Zone protokolliert werden

Tabelle 16.7: Bedeutung der Debug-Informationen

16.6.3 DNS-Befehlszeilenprogramme

Dieses Kapitel beschreibt die drei Befehlszeilenprogramme für DNS. Dies sind *NSLOOKUP*, *IPCONFIG* sowie *DNSCMD*. Die beiden ersten werden von der Eingabeaufforderung aus ausgeführt, *DNSCMD* bietet zahlreiche Befehle, die in Form von Batchdateien ausgeführt werden können.

NSLOOKUP

Mit diesem Programm können Sie die Bereitschaft eines DNS-Servers, die DNS-Registrierung der Domänencontroller sowie die Zonendelegierung überprüfen. Die einzelnen Befehle für diese Aufgaben werden in der folgenden Tabelle beschrieben:

Prüfung von	Befehl und Parameter
Bereitschaft eines DNS-Servers	Nslookup [IP-Adresse des DNS-Servers] 127.0.0.1  Ist der Server bereit zur Antwort, wird der Name des DNS-Servers ausgegeben, ansonsten erhalten Sie eine Fehlermeldung
DNS-Registrierung der Domänencontroller	Geben Sie nacheinander die folgenden Befehle ein: • Nslookup  • set type=srv  (Damit wird die Suche nur nach Ressourceneinträgen für die Dienstidentifizierung (SRV) gefiltert) • _ldap._tcp.dc._msdcs.[Domänenname der Active Directory-Domäne und deren Domänencontroller]  (in unserem Beispiel wäre dies _ldap._tcp.dc._msdcs.firma.de) Das Ergebnis der SRV-Abfrage sollte dabei den Hostnamen mit Port angeben.
Zonendelegierung	Geben Sie nacheinander die folgenden Befehle ein: • nslookup [IP-Adresse des Stammservers]  • set norecursion  • set type =[Ressourceneintragstyp des Namens, dessen Auflösung misslang]  (meist A für den Hostnamen) • Eingabe des FQDN des Namens, dessen Auflösung mißlang. Am Ende muss ein . stehen. Sie sollten nun eine Liste mit NS-Ressourceneinträgen (Namensserver) für die delegierten Server erhalten. Ist dies nicht der Fall, entnehmen Sie die weiteren Schritte der Windows-Hilfe zu nslookup.

Tabelle 16.8: NSLOOKUP-Befehle

IPCONFIG

Mit diesem Programm können Sie die lokale IP-Konfiguration auf einem Computer anzeigen und bearbeiten. Im Zusammenhang mit DNS können Sie über IPCONFIG einen DNS-Client neu registrieren oder den Inhalt des DNS-Cache des Clients anzeigen sowie leeren und wieder zurücksetzen. Die Befehle dafür zeigt die folgende Tabelle.

Funktion	Befehl und Parameter
DNS-Client neu registrieren	Geben Sie den folgenden Befehl ein: <pre>Ipconfig /registerdns</pre> Optional können Sie nach registerdns auch noch den Netzwerkadapter angeben, für den die Aktualisierungen vorgenommen werden sollen. Damit werden bei Verwendung von DHCP die Adress-Leases aktualisiert und die DNS-Namen des Clients neu registriert. Sollten dabei Fehler auftreten, werden diese nach 15 Minuten in dem Ereignisprotokoll des Clients angezeigt. Dieser Befehl ist nur auf Windows 2000-Rechnern mit gestartetem DNS-Clientdienst verfügbar.
Anzeigen des DNS-Cache	Geben Sie den folgenden Befehl ein: <pre>Ipconfig /displaydns</pre> Dies zeigt den kompletten Inhalt des DNS-Auflösungscache an.
Leeren und Zurücksetzen des DNS-Cache des Clients	Geben Sie den folgenden Befehl ein: <pre>Ipconfig /flushdns</pre> Hiermit können Sie unbeantwortete oder dem Cache dynamisch hinzugefügte Einträge löschen. Dadurch werden jedoch keine Einträge der Hosts-Tabelle gelöscht. Dieser Befehl ist nur auf Windows 2000-Rechnern mit gestartetem DNS-Clientdienst verfügbar.

Tabelle 16.9: IPCONFIG-Befehle

DNSCMD

Um dieses Programm nutzen zu können, müssen Sie zunächst die Windows 2000 Support-Tools aus dem Resource Kit installieren. Diese installieren Sie über die Datei *2000rskt.msi*, die sich auf der Windows 2000 Server-CD im Verzeichnis `\SUPPORT\TOOLS\` befindet. *DNSCMD* umfasst einen großen Satz von Befehlen zur Verwaltung von DNS-Servern. Diese Befehle sind geeignet, um sie einerseits lokal auf einem DNS-Server auszuführen oder aber auch in Batchdateien für Verwaltungsaufgaben, Konfiguration neuer DNS-Server oder deren unbeaufsichtigter Installation zu nutzen. Es können dieselben Verwaltungsaufgaben erledigt werden, die Sie alternativ auch an der GUI der DNS-mmc durchführen können.

Mit *DNSCMD* können Sie DNS-Zonen und ihre Inhalte ansehen, erstellen oder löschen, Zonen-Updates durchführen, Zonen aktualisieren und anhalten, den DNS-Dienst starten und anhalten sowie DNS-Statistiken betrachten. Eine Übersicht über die umfangreichen Befehle von *DNSCMD* finden Sie im Rahmen der Beschreibung der Support-Tools in Kapitel 23.1.5.

16.6.4 DNS-Fehlerszenarien

In diesem Kapitel wird Ihnen eine Reihe typischer Fehlerszenarien im Zusammenhang mit DNS vorgestellt. Die Fehlerszenarien sind unterteilt in Fehler des DNS-Servers, Fehler bei DNS-Zonenübertragungen und Fehler bei DDNS. Zu jedem Szenario wird mindestens ein Lösungsansatz vorgeschlagen.

Fehler des DNS-Servers

1. Der DNS-Server kommuniziert nicht mit seinen Clients.

- ▶ So trivial es auch erscheinen mag, überprüfen Sie zunächst, ob der DNS-Server netzwerktechnisch seine Clients erreichen kann und umgekehrt. Setzen Sie hierzu einen Ping ab und prüfen die Einstellungen der Netzwerkkarte.
- ▶ Der Server ist zwar netzwerktechnisch erreichbar, aber bearbeitet dennoch keine DNS-Abfragen. Prüfen Sie, ob der DNS-Serverdienst gestartet ist. Überprüfen Sie mit *NSLOOKUP*, ob der Server Clientabfragen beantworten kann. Geben Sie von einem Client aus den Befehl

```
nslookup <IP-Adresse des DNS-Servers> 127.0.0.1 ↵
```

ein. Sie sollten als Antwort den DNS-Servernamen erhalten.

- ▶ Möglicherweise ist der DNS-Server nur für einen ausgewählten Satz von IP-Adressen zur Antwort konfiguriert. Öffnen Sie in der mmc DNS den DNS-Server, wählen aus dem Kontextmenü *EIGENSCHAFTEN* und dann die Registerkarte *SCHNITTSTELLEN*. Dort können entweder alle dem DNS-Server zugeordneten IP-Adressen oder nur ausgewählte für die DNS-Abfragen bestimmt werden. Fügen Sie im Bedarfsfall fehlende Adressen hinzu.
- ▶ Möglicherweise verwendet der DNS-Server nicht den Standard-UDP-Port 53. Alle nslookup-Abfragen werden über diesen Port gesendet. Dies könnte der Fall sein, wenn auf den DNS-Server über eine Firewall, einen Proxy-Server oder einen Router mit Paketfiltern zugegriffen wird. Ist dieser Port nicht absichtlich gesperrt, können Sie einen Paketfilter einrichten, der den Datenverkehr über den UDP-Port 53 zulässt.
- ▶ Sehen Sie im DNS-Ereignisprotokoll nach, ob Sie dort die Meldung mit der ID 414 finden. Ist dies der Fall, verfügt der DNS-Server über keinen vollständigen DNS-Domänennamen. Der Name wird in der Form *Computername.* anstatt *Computername.Domäne.de* angegeben. Dieser fehlerhafte Eintrag wird in die SOA- und NS-Ressourceneinträge geschrieben. Damit erhalten die Zonen den falschen Eintrag. Um dem Computer einen Domänennamen zu geben, wählen Sie die Eigenschaften des Arbeitsplatzes und dort die Registerkarte *NETZWERKIDENTIFIKATION*. Geben Sie dort unter *EIGENSCHAFTEN* einen vollständigen DNS-Namen an.

2. Der DNS-Dienst lässt keine administrativen Aufgaben zu.

- ▶ Der DNS-Dienst startet zwar, aber sobald Sie versuchen, mit der DNS-mmc oder dem Kommandozeilenprogramm DNS zu konfigurieren, erhalten Sie eine Fehlermeldung, z.B. Error 0x11d603. Dies ist der Fall, wenn auf dem DNS-Server das Sicherheitsauditing aktiviert ist. Um das Problem zu beheben, müssen Sie Windows 2000 Servicepack 2 oder später installieren.

3. Es gibt Probleme bei der Namensauflösung der Clients.

- ▶ Der DNS-Server beantwortet zwar die Abfragen, gibt aber leider falsche Daten an die Clients aus. Hier ist der Fehler seitens des Servers in falschen Ressourceneinträgen zu suchen. Entweder sind Ihnen beim manuellen Hinzufügen von Einträgen zu einer Zone Fehler unterlaufen, oder die dynamischen Aktualisierungen werden nicht korrekt durchgeführt. Möglicherweise enthält die Zone auch veraltete Ressourceneinträge. Entweder sind es Einträge, die noch nicht entfernt wurden, oder Einträge aus der Lookup-Zwischenspeicherung. Löschen Sie den Cache über den Eintrag CACHE LÖSCHEN aus dem Menü VORGANG des DNS-Servers, oder entfernen Sie die veralteten Einträge über `dnscmd <Server> /StartScavenging` .
- ▶ Der DNS-Server kann keine Anfragen weiterleiten oder die Rekursion initiieren. Standardmäßig sind alle DNS-Server zur Durchführung der Rekursion konfiguriert. Prüfen Sie in den erweiterten Eigenschaften des DNS-Servers in der mmc unter SERVEROPTIONEN, ob das Kontrollkästchen REKURSIONSVORGANG DEAKTIVIERT aktiviert wurde. Deaktivieren Sie es wieder. Zur Aktivierung der Weiterleitung klicken Sie in den erweiterten Eigenschaften auf der Registerkarte WEITERLEITUNGEN das Kontrollkästchen WEITERLEITUNG AKTIVIEREN an. Soll nur dieser DNS-Server Weiterleitungen ausführen, so aktivieren Sie das Feld KEINE REKURSION VERWENDEN. Geben Sie dann die Liste der IP-Adressen der DNS-Server an, über die Weiterleitungen für diesen DNS-Server ausgeführt werden sollen.
- ▶ Der DNS-Server löst nur die Namen im LAN, nicht aber in Remote-Netzwerken oder im Internet richtig auf. Hierbei handelt es sich um einen Fehler bei der Rekursion, die für alle Abfragen verwendet wird, die außerhalb der Domäne des DNS-Servers und -Clients liegen. Überprüfen Sie, ob alle autorisierenden Server die rekursiven Anfragen weiterleiten. Möglicherweise ist in der Kette einer der Remote-DNS-Server netzwerktechnisch nicht verfügbar oder kann aufgrund von Zeitüberschreitung die Abfrage nicht vollständig durchführen.
- ▶ Möglicherweise sind die Hinweise auf das Stammverzeichnis fehlerhaft. Diese finden Sie unter der gleichnamigen Registerkarte in den Eigenschaften des DNS-Servers. Es wird auf die DNS-Server verwiesen, die für die Zone des Domänenstammes und der Domänen der ersten Ebene autorisierend sind. Die Einstellungen sind beim ersten DNS-Server im Netzwerk deaktiviert, da er automatisch zum Stammserver wird und keine Hinweise benötigt. Bei zusätzlich eingerichteten DNS-Servern prüfen Sie die angegebenen Server und fügen fehlende hinzu oder entfernen fehlerhafte Einträge aus der Liste.

Fehler bei DNS-Zonenübertragungen

1. Der DNS-Serverdienst oder die DNS-Zone wurden angehalten.
 - ▶ Überprüfen Sie, ob auf dem Quell- und Zielserver der DNS-Serverdienst gestartet ist und ob die Zonen auf keinem der beiden Server angehalten sind. Den Status der Zone sehen Sie unter den Eigenschaften der jeweiligen Zone.

2. Es wird keine Zonenübertragung durchgeführt, da die Seriennummer von Quell- und Zielservers identisch ist.
 - ▶ Navigieren Sie in der mmc DNS zur Registerkarte AUTORITÄTSURSPRUNG (SOA). Setzen Sie dort in das Feld der Seriennummer für die Zone auf dem Quellserver einen Wert ein, der höher ist als auf dem Zielservers. Starten Sie dann auf dem sekundären Servers die Zonenübertragung.
3. Der DNS-Servers kann Ressourceneinträge der Zone nicht verarbeiten.
 - ▶ Wenn Sie nicht nur Windows 2000-basierte DNS-Servers einsetzen, prüfen Sie zunächst, ob die problemlose Interoperabilität gewährleistet ist. Finden Sie heraus, welche BIND-Versionen die Nicht-Windows-Servers verwenden.
 - ▶ Ist die Interoperabilität gewährleistet, prüfen Sie, ob nicht unterstützte Ressourceneintragstypen verwendet werden. Die unterstützten Typen finden Sie in Kapitel 3.2.5 aufgelistet.
4. Die autorisierenden DNS-Zonendaten sind fehlerhaft.
 - ▶ Sehen Sie im Ereignisprotokoll des DNS-Servers nach, ob falsche Zonendaten die Zonenübertragung scheitern lassen. Stellen Sie sicher, dass die Zone nur über standardmäßige Ressourceneinträge verfügt. Entfernen Sie die nicht standardmäßigen Einträge.

Fehler beim dynamischen DNS

1. Der Client oder dessen DHCP-Servers unterstützen keine dynamischen Aktualisierungen.
 - ▶ Stellen Sie sicher, dass sich in Ihrem Netzwerk Windows 2000-DHCP-Servers befinden und die Clients für die dynamische Aktualisierung ebenfalls Windows 2000 ausführen. Andere Windows-Versionen unterstützen kein DDNS.
2. Der DNS-Servers unterstützt keine dynamischen Aktualisierungen.
 - ▶ Prüfen Sie, ob der DNS-Servers DDNS unterstützen kann. Aus der Windows-Welt kann dies nur ein 2000-Servers, jedoch kein NT-Servers. Verwenden Sie einen Unix-basierten DNS-Servers, so überprüfen Sie anhand der Spezifikationen von RFC 2136, ob der Servers DDNS unterstützt. Unterstützt der Servers keine SRV-Ressourceneinträge (siehe RFC 2052), kann er generell nicht als DNS-Servers im Active Directory agieren.
3. Der DNS-Servers unterstützt zwar DDNS, nimmt aber keine Einträge an.
 - ▶ Standardmäßig wird DDNS für die primäre Zone von Windows nicht zugelassen. Prüfen Sie in den Eigenschaften der Zone auf der Registerkarte ALLGEMEIN, ob die dynamischen Aktualisierungen aktiviert sind.
4. Der Client kann sich nicht bei seinem DNS-Servers registrieren oder aktualisieren.
 - ▶ Überprüfen Sie in den Eigenschaften der LAN-Verbindung die DNS-Konfiguration des Clients. Vergeben Sie an den Client ein primäres DNS-Suffix, wenn Sie statische Adressen verwenden oder ein verbindungspezifisches DNS-Suffix für eine installierte Netzwerkverbindung.

5. Der Client hat versucht, die aktualisierten DNS-Informationen zu erhalten, aber der Versuch ist seitens des Servers gescheitert.
 - ▶ Wenn der Client seinen DNS-Server netzwerktechnisch erreichen kann, sehen Sie im Systemprotokoll des Clients nach, welche Fehlermeldungen bezüglich DNS erstellt worden sind. Der Client ist nicht in der Lage, seine Host (A)- oder Pointer (SRV)-Einträge zu aktualisieren.
6. Die DNS-Zonendatenbank ist nicht verfügbar.
 - ▶ Bei Active Directory-integrierten Zonen muss der DNS-Server als Domänencontroller konfiguriert sein und auf die Verzeichnisdatenbank Zugriff haben. Überprüfen Sie in der DNS-Konsole, ob die Zone vorhanden und nicht angehalten ist.

17 Die Replikation

Über die Replikation wird gewährleistet, dass die Änderungen an einem Domänencontroller an alle anderen innerhalb der Domäne weitergeleitet werden und somit alle Domänencontroller stets über die aktuellen Informationen verfügen.

17.1 Der Replikationsablauf im Detail

In diesem Kapitel wird Ihnen ein kompletter Replikationsvorgang erläutert, in dem alle wichtigen Schlagwörter erläutert werden. Zunächst wird als Grundlage beschrieben, wie die Replikation jedes Objekts über dessen Metadaten gesteuert wird. Danach wird an einem Beispiel vorgestellt, wie sich diese Metadaten während der Replikation ändern. Weiterhin wird auch die Konfiguration der standortübergreifenden Replikation abgehandelt.

17.1.1 Die Metadaten zur Replikationssteuerung

Bei der Replikation zwischen Domänencontrollern werden Verzeichnispitionen ausgetauscht, die auch als Namenskontext (NC) bezeichnet werden. Diese NCs können Schemainformationen, Konfigurationsinformationen oder Domänendaten sein. Sie werden alle getrennt voneinander repliziert. Damit nun diese NCs nicht in Endlosschleifen oder – als anderes Extrem – gar nicht übertragen werden, wird die Replikation über die Metadaten der NCs gesteuert. In jedem NC sind mehrere Metadaten enthalten. Hierbei handelt es sich um den High-Watermark-Vektor und den Up-toto-Dateness-Vektor sowie deren zugehörige Tabellen.

Der High-Watermark-Vektor

Für jeden NC auf einem Domänencontroller liegt eine eindeutige Sequenznummer (USN = Update Sequence Number) vor. Die USN ist ein Wert von 64 Bit Größe. Beim Erstellen eines Objekts wird der Wert für USN-Created angelegt. Über die USN wird angegeben, wie viele Änderungen eines NC auf einem Domänencontroller stattgefunden haben. Die jeweils aktuelle Änderungsversion gibt der Wert uSN-Changed an. Der USN-Zählerwert der Aktualisierungen wird als High-Watermark-Vektor bezeichnet. Zum schnelleren Auffinden der USN-Werte sind diese in der Active Directory-Datenbank indiziert. Die Replikation kennt zwei verschiedene Arten von Aktualisierungen. Es gibt einerseits die Änderungen, die entweder auf dem Domänencontroller selbst vollzogen werden oder durch eine mit ihm verbundene Applikation. Hierbei spricht man von ausgehender Aktualisierung oder Schreibvorgang (Originating Update). Andererseits gibt es auch Änderungen, die der Domänencontroller während der Replikation von seinen Partnern

empfängt. Hierbei spricht man von replizierter Aktualisierung oder Schreibvorgang (Replicated Update).

Sollte beim Ändern eines Objekts ein Datenbankfehler in Active Directory auftreten, so wird die für diesen Vorgang vorgesehene USN als fehlerhaft markiert. Dieser Wert wird ausgeklammert und bei der nächsten Änderung nicht mehr neu verwendet.

Auf jedem Domänencontroller sind die Datensätze mit den Änderungen an den USNs aller NCs vorhanden. Damit ist es möglich, dass andere Domänencontroller spezielle Änderungen anfordern können, die auf einer bestimmten USN basieren. Außerdem verfügt jeder Domänencontroller über eine Tabelle mit der Liste der High-Watermark-Vektoren aller seiner Replikationspartner. Diese Tabelle heißt High-Watermark-Vektor-Tabelle. Sobald sich der High-Watermark-Vektor lokal ändert, wird er dort sofort geändert, aber auf den Replikationspartnern findet die Aktualisierung erst beim nächsten Replikationsdurchlauf statt. Über den High-Watermark-Vektor wird die höchste USN angegeben, die im Active Directory für einen bestimmten NC vorhanden ist. Dabei ist es gleichgültig, ob die USN durch ausgehende oder replizierte Aktualisierungen heraufgesetzt wurde.

Der Up-to-Dateness-Vektor

Der Up-to-Dateness-Vektor gibt den Wert der höchsten USN an, die durch ausgehende Aktualisierungen erhöht wurde. Zusätzlich wird auch der GUID (Global Unique Identifier) des Domänencontrollers dazugeschrieben, der die Änderung vorgenommen hat. Angenommen, die USN eines NC liegt bei 1000. Auf dem Domänencontroller wurde dann eine Änderung lokal vorgenommen, also eine ausgehende Aktualisierung durchgeführt. Danach haben die USN des Up-to-Dateness-Vektors und des High-Watermark-Vektors jeweils den Wert 1001. Bei der nächsten Replikation empfängt der Domänencontroller 3 replizierte Aktualisierungen. Dadurch ändert sich nicht der Up-to-Dateness-Vektor, da dieser nur die ausgehenden Aktualisierungen aufzeichnet, sondern nur der High-Watermark-Vektor, der beide Aktualisierungsarten verfolgt, und zwar auf den Wert 1004.

Analog zur High-Watermark-Vektor-Tabelle gibt es auf jedem Domänencontroller auch eine Up-to-Dateness-Vektor-Tabelle. In ihr werden die Up-to-Dateness-Vektoren sämtlicher Replikationspartner gepflegt, die mindestens eine ausgehende Aktualisierung durchgeführt haben. Solange ein Domänencontroller noch keine ausgehende Aktualisierung durchgeführt hat, enthält der Up-to-Dateness-Vektor keinen Wert. Außerdem werden dort auch die GUIDs der Domänencontroller gepflegt, die die jeweilige ausgehende Änderung durchgeführt haben. Lokal wird der Up-to-Dateness-Vektor sofort geändert, die Replikationspartner empfangen den neuen Wert erst bei der nächsten Replikation. Der Up-to-Dateness-Vektor gibt den höchsten Wert der ausgehenden Aktualisierungen auf allen Domänencontrollern an.

Durch das Hinzufügen der GUIDs zu den Up-to-Dateness-Vektoren wird sichergestellt, dass der Domänencontroller, der ursprünglich die ausgehende Aktualisierung vorgenommen hat, nicht erneut diese Information repliziert und somit in eine Endlosschleife laufen würde, da der GUID für jeden Domänencontroller unterschiedlich ist.

17.1.2 Das Ändern der Metadaten während der Replikation

Nachdem Sie eben erfahren haben, wie über die Metadaten in Form der beiden Vektoren mit ihren zugehörigen Tabellen die Replikation gesteuert wird, soll nun anhand eines Beispiels veranschaulicht werden, wie die Metadaten von Eigenschaften eines Objekts beim Verändern sowie während der Replikation geändert werden.

Unser Beispiel besteht aus insgesamt vier Schritten, die alle ausführlich beschrieben werden. Diese Schritte sind:

1. Auf dem Domänencontroller 1 wird ein neues Benutzerobjekt angelegt.
2. Dieses Benutzerobjekt wird auf den Domänencontroller 2 repliziert.
3. Auf dem Domänencontroller 2 wird das Objekt geändert.
4. Das geänderte Objekt wird wieder auf den Domänencontroller 1 repliziert.

Zunächst erhalten Sie eine grafische Übersicht dieser Schritte. Anhand der beiden Bilder (siehe Abbildung 17.1 und Abbildung 17.2) können Sie alle nachfolgend beschriebenen Verfahren und Änderungen nachvollziehen. Seien Sie nicht weiter besorgt, wenn Sie zunächst mit den Begrifflichkeiten und Zahlen noch nicht viel anfangen können. Alle Unklarheiten sollten im Laufe dieses Kapitels beseitigt werden.

	Domänencontroller 1		Domänencontroller 2	
Transaktions-USN	USN 1000 DC 1		USN 2200 DC 2	
Metadaten	Eig. Name	Eig. Passwort	Eig. Name	Eig. Passwort
Zeitstempel	Z1	Z1	Z2	Z2
Ausgebende USN	1000	1000	1000	1000
Ausgebender GUID	GUID DC 1	GUID DC 1	GUID DC 1	GUID DC 1
Versionsnummer	1	1	1	1
USN der Eigenschaft	1000	1000	2200	2200

10:00 h

Neu-Erstellung des Benutzerobjekts

10:15 h

Replikation auf DC 2

Abbildung 17.1: Das Ändern der Metadaten während der Replikation – Bild 1

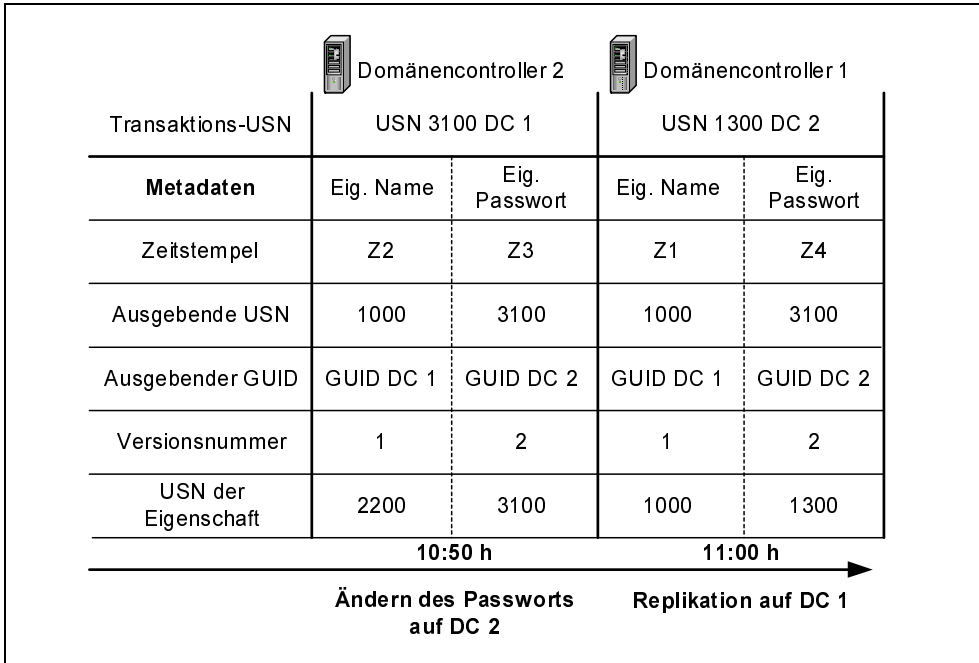


Abbildung 17.2: Das Ändern der Metadaten während der Replikation – Bild 1

Die Metadaten von Eigenschaften können über Active Directory-Support-Tools wie *REPADMIN* oder *LDP* eingesehen werden. Auch der Status der Replikation kann über diese beiden Tools oder noch komfortabler über das Freewaretool *ADCheck* von NetIQ geprüft werden.

1. Schritt: Anlegen eines Objekts auf Domänencontroller 1

Sie erstellen auf Domänencontroller 1 um 10:00 h ein neues Benutzerobjekt. Damit ist dieser Domänencontroller der Server der ausgehenden Aktualisierungen und wird damit auch ausgebender Server für dieses Objekt genannt. Das Erstellen des neuen Benutzers ist eine Datenbanktransaktion im Active Directory. Diese Transaktion erhält die USN 1000. Entsprechend dieser USN erhalten alle Benutzereigenschaften auch die USN 1000. Auch die ausgehende USN erhält auf Basis der Transaktions-USN den Wert 1000. In unserem Schaubild werden zwei Eigenschaften eines Benutzers exemplarisch herausgegriffen, nämlich sein Name und das Passwort.

Jede Eigenschaft enthält fünf verschiedene Metadaten, die sich beim Ändern der Objekteigenschaften ebenfalls mitändern. Dies sind:

- Zeitstempel
- Ausgebende (Originating) USN
- Ausgebender GUID des Domänencontrollers
- Versionsnummer der Eigenschaft
- USN der Eigenschaft

Bei jeder Änderung oder dem Erstellen eines Objekts wird ein Zeitstempel hinzugefügt. Dieser Zeitstempel wird bei Replikationskonflikten herangezogen, wenn zwei USNs identisch sind. Es wird dann die Änderung mit dem neueren Zeitstempel übernommen. Die ausgebende USN wird auf Basis der Transaktions-USN der aktuellen Datenbankänderung am ausgebenden Domänencontroller vergeben. Sie erhält nur dann einen neuen Wert, wenn auf einem anderen Domänencontroller eine Änderung vorgenommen wurde. Dieser neue Wert basiert wiederum auf der aktuellen Transaktions-USN. Der ausgebende GUID eines Domänencontrollers wird entsprechend dem Server hinzugefügt, auf dem die Änderung lokal vorgenommen wurde. Die Versionsnummer der Eigenschaft wird bei jeder Änderung um 1 heraufgesetzt. Die USN der Eigenschaft basiert auf der Transaktions-USN des jeweiligen Domänencontrollers, an dem die Eigenschaft gerade bearbeitet wird. Die Eigenschafts-USN ändert sich nur, wenn die Eigenschaft geändert wird.

Der Zeitstempel bekommt einen Wert, der hier mit einer Variablen Z1 angegeben wird. Die ausgebende und Eigenschafts-USN erhalten beide analog zur Transaktions-USN den Wert 1000. Der ausgebende GUID ist der von Domänencontroller 1, da auf diesem das Objekt mit seinen Eigenschaften erstellt wurde. Die Versionsnummer ist 1, da noch keine Änderungen durchgeführt sind. Im ersten Schritt sind alle Metadaten für die Eigenschaften Name und PasswortPasswort identisch, da sie auf einer gemeinsamen Quelle beruhen und noch nicht geändert wurden.

2. Schritt: Replikation auf Domänencontroller 2

Um 10:15 h wird das Objekt mit seinen Eigenschaften auf Domänencontroller 2 repliziert. Die Transaktions-USN für diesen Zeitpunkt liegt bei 2.200. Auf diesem Domänencontroller erhalten beide Eigenschaften den neuen Zeitstempel Z2. Die ausgebende USN bleibt bei beiden Eigenschaften 1.000, da allein durch die empfangene Replikation der Domänencontroller 2 keine Änderungen vorgenommen hat, für die er der ausgebende Server sein könnte. Deshalb behalten auch beide Eigenschaften den GUID von Domänencontroller 1. Durch diese beiden Eigenschaften wird gekennzeichnet, dass die Eigenschaften zuletzt von Domänencontroller 1 festgelegt worden sind. Die Versionsnummer bleibt ebenfalls bei 1, da keine Änderungen durchgeführt worden sind. Es ändert sich aber die Eigenschafts-USN. Sie hat nun auf Basis der Transaktions-USN von Domänencontroller 2 ebenfalls den Wert 2.200. Im Zuge der Transaktion 2.200 wurde der Benutzer auf Domänencontroller 2 übertragen und dort verfügbar.

3. Schritt: Ändern des Benutzerkennworts auf Domänencontroller 2

Um 10:50 h wird auf dem Domänencontroller 2 das Kennwort des Benutzers geändert, aber nicht der Benutzername selbst. Damit behalten sämtliche Metadaten für die Eigenschaft „Name“ dieselben Werte wie in Schritt 2. Die Eigenschaft „Passwort“ bekommt den neuen Zeitstempel Z3 für den Zeitpunkt der Änderung. Zwischen dem Empfang des replizierten Objekts um 10:15 h und dem Ändern um 10:50 h ist ein längerer Zeitraum vergangen, sodass die aktuelle Transaktions-USN den Wert 3.100 hat. Auf dieser Basis wird der neue Wert für die ausgebende USN festgelegt. Da die Änderung lokal auf dem Domänencontroller 2 durchgeführt wurde, wird auch der Wert des GUID auf den von Domänencontroller 2 geändert. Durch die Änderung des PasswortPassworts hat dieses nun eine neue Version. Diese Version ist die 2. Der Zähler für die Version wird bei jeder Änderung erhöht. Dabei ist es gleichgültig, auf welchem Domänencontroller sie durchgeführt wird. Die USN

der Eigenschaft wird auf 3.100 geändert, da zu diesem Transaktions-Zeitpunkt die Änderung auf Domänencontroller 2 durchgeführt wurde.

4. Schritt: Replizieren des geänderten Objekts an Domänencontroller 1

Für 11:00 h steht die nächste Replikation zwischen den beiden Domänencontrollern an. Dabei werden die geänderten Passwort-Eigenschaften des Benutzerobjekts an Domänencontroller 1 übertragen. Dieser Zeitpunkt wird durch die Transaktions-USN 1.300 auf Domänencontroller 1 markiert. Die Namenseigenschaft nimmt wieder den ursprünglichen Zeitstempel Z1 an, da sie seit ihrer ersten Erstellung nicht geändert wurde. Da ausschließlich geänderte Eigenschaften bei der Replikation übertragen werden und nicht das komplette Objekt, wird kein neuer Wert für den Zeitstempel geliefert. Also behält die Namenseigenschaft auf Domänencontroller 1 ihren alten Wert Z1. Es wird also aufgrund fehlender Änderungen überhaupt kein neuer Wert für irgendeine Namenseigenschaft geliefert. Damit behalten auch die ausgehende USN, der ausgehende GUID, die Versionsnummer sowie die USN der Eigenschaft den alten Wert, der beim Erstellen des Objekts um 10:00h aktuell war.

Anders sieht es beim Passwort aus. Da dieses zwischenzeitlich geändert wurde, werden die geänderten Werte übertragen. Damit erhält die Passwort-Eigenschaft den aktuellen Zeitstempel Z4 des Domänencontrollers 1. Die ausgehende USN ändert sich nicht durch die Replikation, ebenso wenig auch der Wert des ausgehenden GUID. Sie behalten beide den Wert aus Schritt 3. Damit ist der Domänencontroller 2 als der Server gekennzeichnet, der die letzten Änderungen der Eigenschaft vorgenommen hat. Auch die Versionsnummer ändert sich bei der Replikation nicht. Sie bleibt bei der Nummer 2. Als Eigenschafts-USN wird der Wert 1.300 festgelegt. Dieser Wert basiert auf der aktuellen Transaktions-USN von Domänencontroller 1.

17.1.3 Die Replikation eines Objekts

In diesem Kapitel wird vorgeführt, welche Schritte die Domänencontroller bei der Replikation durchführen, um herauszufinden, welche aktualisierten Daten der Quellserver senden muss, wie diese Daten auf dem Zielsystem verarbeitet werden und wie dieser schließlich überprüft, ob er alle notwendigen Daten erhalten hat und damit auf demselben Stand ist wie der Quellserver.

Stellen Sie sich für unsere Beispielkonstellation ein Netzwerk mit fünf Domänencontrollern vor. Der detaillierte Replikationsprozess wird nur zwischen den Servern 1 und 2 beschrieben, da das Prinzip bei allen Replikationspartnern dasselbe ist. Die drei anderen Server liefern uns im Beispiel lediglich Werte für die High-Watermark-Vektor-Tabelle sowie die Up-to-Dateness-Vektor-Tabelle.

Unsere Beispielreplikation durchläuft insgesamt fünf Schritte. Dies sind:

1. Die Replikation von Domänencontroller 1 wird eingeleitet.
2. Der Domänencontroller 2 ermittelt die zu sendenden Informationen.
3. Der Domänencontroller 2 sendet die erforderlichen Daten an Domänencontroller 1.
4. Der Domänencontroller 1 verarbeitet die empfangenen Daten.
5. Der Domänencontroller 1 prüft, ob er alle Daten erhalten hat.

1. Schritt: Der Replikationsprozess wird von DC 1 eingeleitet

Sobald ein Replikationsintervall abgelaufen ist, leitet der Domänencontroller 1 die Replikation ein. Dabei fordert er von Domänencontroller 2 alle neuen Informationen für die NCs an, über die er noch nicht verfügt. Auf diesem Weg erhält zwar Domänencontroller 1 Daten von Domänencontroller 2 (DC 2), letzterer jedoch nicht von Domänencontroller 1 (DC 1). Die Anforderung neuer Informationen umfasst die folgenden Replikationsmetadaten:

- ▶ Name des NC, für den aktualisierte Daten angefordert werden. Es kann sich dabei um den Schema- oder Konfigurationsinformationen- oder den Domänendaten-NC handeln. In unserem Beispiel ist es der Domänendaten-NC.
- ▶ Maximalanzahl von zu empfangenden Aktualisierungen für ein Objekt
- ▶ Maximalanzahl aller zu empfangenden Werte
- ▶ High-Watermark-Vektor dieses NC auf DC 2
- ▶ Up-to-Dateness-Vektor-Tabelle dieses NC von DC 1

Diese Daten sendet Domänencontroller 1 an Domänencontroller 2. Die eigentliche Replikation findet aber in die Gegenrichtung statt. Die Maximalanzahl der Aktualisierungen für ein Objekt und für alle Werte zusammen, die DC 1 bei einer Replikationsdurchführung empfangen möchte, sorgen dafür, dass das Netzwerk während der Replikation nicht überlastet wird, wenn sich eine sehr große Menge zu replizierender Daten angesammelt hat. Dies ist beispielsweise der Fall, wenn ein Domänencontroller längere Zeit nicht im Netzwerk verfügbar war. Wird das Maximum für diese Werte überschritten, wird nur der Maximalwert der Daten übertragen. Der Rest wird bei der nächsten Replikation übertragen.

2. Schritt: DC 2 ermittelt die an DC 1 zu sendenden Daten

Anhand der von DC1 empfangenen Metadaten ermittelt DC 2 die Aktualisierungen, die an DC 1 zu senden sind. Dieses ist der komplexeste aller fünf Schritte und damit auch recht lang in der Beschreibung. Zur Vereinfachung gehen wir aber davon aus, dass die zu übertragenden Daten nicht die Maximalwerte übersteigen und somit alle Daten in einem Stück übertragen werden.

Als Erstes vergleicht DC 2 seinen eigenen aktuellen High-Watermark-Vektor (1.301) für den Domänendaten-NC mit dem von DC 1 empfangenen Vektor, der den Wert für DC 2 bei der letzten Replikation enthält (1.305). Wurden seit der letzten Replikation zwischen DC 1 und DC 2 Änderungen am Schema-NC durchgeführt, kann DC 2 herleiten, wie viele Änderungen es waren. Stimmen die beiden Werte nicht überein, kann DC 2 anhand seiner Tabelle mit allen Änderungen der USNs ablesen, welche USNs auf DC 1 fehlen. Um nicht unnötig Daten zu übertragen, muss DC 2 herausfinden, ob DC 1 einen Teil oder möglicherweise alle fehlenden Daten bereits von einem anderen DC bezogen hat.

Hierfür wird die an DC 2 gesendete Up-to-Dateness-Vektor-Tabelle auf DC 1 benutzt. In dieser Tabelle untersucht DC 2 für jede als auf DC 1 fehlend ermittelte USN die Einträge der ausgehenden USN sowie den GUID des Domänencontrollers. Bleiben wir nun bei dem Beispiel eines geänderten Passworts. Angenommen, ein Passwort wurde ursprünglich auf DC 4 geändert. Die Passwortheigenschaft trägt die GUID von DC 4 und dessen USN 2.345.

Diese Änderung ist auf DC 2 unter der USN 1.112 mit der GUID von DC 4 hinterlegt. Um herauszufinden, ob DC 1 diese Änderung bereits kennt, schlägt DC 2 in der Up-to-Dateness-Vektor-Tabelle von DC 1 nach, um den Up-to-Dateness-Vektor für den ursprünglich ausgebenden Server, also DC 4, zu finden. Ist dieser Wert (2.402) gleich oder größer der ausgebenden USN auf DC 4 (2.391), kennt DC 1 bereits die Änderung, und sie muss nicht erneut übertragen werden. Diese Überprüfung anhand der Up-to-Dateness-Vektor-Tabelle zur Vermeidung unnötiger Netzwerklast durch überflüssige Datenübertragung wird auch als Propagationsdämpfung (Propagation Dampening) bezeichnet.

Nehmen wir an, von DC 2 wurden insgesamt vier Aktualisierungen ermittelt, die an DC 1 zu übertragen sind. Hierbei handelt es sich um die laut High-Watermark-Vektor fehlenden USNs auf DC 1. Dies sind die Werte 1.302 bis 1.305. Bei der USN 1.302 handelt es sich um eine von DC 2 ausgehende Aktualisierung mit dem GUID von DC 2. Da diese Änderung direkt von DC 2 ausgeht, muss nicht die Up-to-Dateness-Vektor-Tabelle verwendet werden, um herauszufinden, ob DC 1 die Änderung bereits von einem anderen DC empfangen hat. Die USNs 1.303 bis 1.305 sind replizierte Aktualisierungen. Bei den USNs 1.303 und 1.304 handelt es sich um Einträge mit dem GUID von DC 3 und der ausgebenden USN von 1.605 und 1.711 auf DC 3. Über die Up-to-Dateness-Vektor-Tabelle wurde ermittelt, dass der USN-Eintrag für DC 3 bei 1.513 liegt. Da der Wert aus der Up-to-Dateness-Vektor-Tabelle von DC 1 niedriger ist, müssen beide Änderungen übertragen werden. Bei der vierten Aktualisierung handelt es sich um die im letzten Absatz beschriebene USN 1.305, die jedoch nicht an DC 1 geschickt werden muss. Um die Verwirrung bezüglich der USNs ein wenig in Grenzen zu halten, fasst Tabelle 17.1 die bisherigen Erkenntnisse zusammen:

Zu übertragende USN auf DC 2	GUID des ausgebenden DCs	USN des ausgebenden Servers	Eintrag in UTDV-Tabelle für DC der GUID	Senden der Änderung an DC 1 nötig?
1302	DC 2	1302	1301	Ja
1303	DC 3	1711	1513	Ja
1304	DC 3	1605	1513	Ja
1305	DC 4	2391	2402	Nein

Tabelle 17.1: Zusammenfassung der Beispiel-USNs

DC 2 weiß also nun anhand der beiden Vektor-Tabellen, dass er drei Änderungen an DC 1 senden muss. Im Folgenden werden nun die Vorgänge beschrieben, wie DC 2 die Daten aus den Tabellen ermittelt.

Sobald DC 2 die Aktualisierungsanfrage von DC 1 erhält, legt er eine Kopie seiner eigenen Up-to-Dateness-Vektor-Tabelle für DC 1 an. Diese Tabelle wird zwar gleich bei der Aktualisierungsanfrage erstellt, aber es dauert noch, bis diese mit neuen Daten gefüllt wird. DC 2 sucht im kompletten Domänendaten-NC nach Objekten, die eine Eigenschaft haben, deren USN-Changed-Wert höher ist als der High-Watermark-Vektor von DC 1 für DC 2 (1.301). Der USN-Changed-Wert ist in jeder Eigenschaft vorhanden und gibt geänderte USN-Einträge an. DC 2 erstellt dann eine Liste aller gefundenen Objekte dieser Suche. Die Sortierreihenfolge entspricht den gefundenen USN-Changed-Werten in aufsteigender Reihe.

Dann wird von DC 2 ein leerer Ausgabezwischenspeicher angelegt. In diesen werden alle Änderungseinträge für DC 1 geschrieben. Dann bereitet DC 2 als Teil der Replikationsmetadaten einen Wert namens Last-Object-USN-Changed vor. Dieser Wert wird die USN des Objekts enthalten, das als Letztes während dieser Replikation geschickt werden wird. Hierbei handelt es sich um den aktuellen High-Watermark-Vektor von DC 2, hier also 1.305. Um es nochmals klarzustellen: Dieser Wert ist nicht die Eigenschaft irgendeines Objekts, sondern nur ein Bestandteil der Replikationsmetadaten. DC 2 beginnt dann, für alle gefundenen Objekte einen bestimmten Satz an fest vorgegebenen Schritten abzuarbeiten. Begonnen wird mit dem Objekt, das den kleinsten geänderten USN-Eintrag besitzt. Damit wird sichergestellt, dass keine Konflikte entstehen, falls sich eine neuere Änderung auf ein Objekt bezieht, das dem Domänencontroller noch nicht bekannt ist oder in anderer Weise Probleme bereiten könnte. Es werden für jedes abzuarbeitende Objekt von DC 2 die folgenden Schritte durchgeführt:

Zunächst prüft DC 2, ob sich das Objekt bereits im Ausgabezwischenspeicher befindet. Ist das Objekt bereits im Zwischenspeicher, setzt DC 2 den Wert von Last-Object-USN-Changed auf den Wert des USN-Changed-Wertes des aktuell bearbeiteten Objekts. Angenommen, das letzte zu übertragende Objekt trägt den Last-Object-USN-Changed-Wert 1.305. Ein aktuell zu übertragendes Objekt mit dem Wert 500 befindet sich bereits im Zwischenspeicher. Also wird als der Last-Object-USN-Changed-Wert 500 eingetragen. Dann wird das nächste Objekt abgearbeitet.

Ist das aktuell bearbeitete Objekt noch nicht im Zwischenspeicher vorhanden, prüft DC 2, ob darin Änderungen enthalten sind, die DC 1 noch nicht von einem anderen DC erhalten hat. Dazu werden in der Up-to-Dateness-Vektor-Tabelle für jede Eigenschaft der GUID des ausgebenden DCs sowie die zugehörige ausgebende USN nachgeschlagen und mit dem Eintrag der ausgebenden USN für den entsprechenden DC in der Up-to-Dateness-Vektor-Tabelle auf DC 1 verglichen. Sind die Werte der ausgebenden USN auf DC 2 kleiner oder gleich dem Wert in der Tabelle auf DC 1, werden keine Daten für diese Eigenschaft übertragen. Ist der Wert auf DC 2 größer, müssen Daten gesendet werden. Die zu sendenden Informationen werden dann in den Zwischenspeicher geschrieben, und der Wert Last-Object-USN-Changed wird durch den des aktuellen Objekts ersetzt. Dann wird mit dem nächsten Objekt fortgefahren.

Wird beim Hinzufügen der zu sendenden Daten das Limit erreicht, werden keine weiteren Daten in die Liste geschrieben. Es wird nur noch abschließend ein Flag mit dem Wert More-Data=TRUE gesetzt. Damit wird gekennzeichnet, dass bei der nächsten Replikation vor dem Übertragen der dann neuen Aktualisierungen zunächst der Rest der alten Änderungen an DC 1 übertragen werden muss. Wird beim Hinzufügen der Daten zum Zwischenspeicher das Limit nicht erreicht, wird das Flag More-Data=FALSE angefügt.

3. Schritt: Senden der Aktualisierungen an DC 1

Wenn DC 2 die Liste der zu sendenden Informationen fertig gestellt hat, sendet er sowohl die Aktualisierungen als auch Metadaten an DC 1. Um in unserem Beispiel zu bleiben, sendet DC 2 die folgenden Daten an DC 1:

- Alle geänderten Eigenschaften aus dem Ausgabezwischenspeicher von DC 2, hier sind es drei geänderte Eigenschaften.

- ▶ Seinen eigenen aktuellen High-Watermark-Vektor (also den Last-Object-USN-Changed-Wert), also 1.305.
- ▶ Das Flag More-Data, hier mit dem Wert FALSE, da alle Daten in einem einzigen Vorgang übertragen wurden.
- ▶ Die Up-to-Dateness-Vektor-Tabelle auf DC 2 für den aktuellen NC, hier also die Domänen Daten. Diese Tabelle wird erst in dem Replikationsdurchlauf mitgeschickt, der auch das Flag More-Data=FALSE enthält.

Befindet sich DC 1 bereits auf dem aktuellen Stand, werden keine geänderten Daten übertragen. Dies ist entweder dann der Fall, wenn der aktuelle High-Watermark-Vektor von DC 2 mit dem von DC 1 gesendeten übereinstimmt oder wenn sich die beiden High-Watermark-Vektoren zwar unterscheiden, DC 1 aber dennoch aus anderen Replikationen bereits über alle aktuellen Daten verfügt. Bei einem solchen Replikationsvorgang werden nur die Metadaten, d.h. der High-Watermark-Vektor sowie die Up-to-Dateness-Vektor-Tabelle, an DC 1 übertragen.

4. Schritt: DC 1 verarbeitet die von DC 2 empfangenen Daten

Nachdem DC 1 die Daten empfangen hat, speichert er diese in der lokalen Kopie der Active Directory-Datenbank. Dabei wird für jede Änderung eine Transaktions-USN verwendet. Die jeweilige Transaktions-USN wird für den Wert USN-Changed der geänderten Eigenschaft eingetragen. Sind alle Eigenschaften aktualisiert, wird auf DC 1 der High-Watermark-Wert für DC 2 anhand des eben empfangenen Last-Object-USN-Changed-Wertes aktualisiert. Damit weiß DC 1, dass er auf demselben Stand ist wie DC 2. In unserem Beispiel war der von DC 2 gesendete Last-Object-USN-Changed-Wert 1305, obwohl diese Änderung nicht übertragen wurde, da sie DC 1 bereits bekannt war. Die letzte ausgeführte Änderung hatte die USN 1304 des GUID DC 3. Dennoch wird der höchste Wert übertragen, damit die „Änderung“ mit der USN 1.305 nicht beim nächsten Replikationsvorgang erneut abgearbeitet wird, wenn der High-Watermark-Vektor für DC 2 nur auf 1304 stehen würde.

5. Schritt: DC 1 prüft, ob er alle Daten erhalten hat

Hierzu prüft DC 1 den Wert des Flags More-Data. Steht dieses Flag auf FALSE, weiß er, dass er alle aktuellen Daten von DC 2 erhalten hat. Trägt das Flag jedoch den Wert TRUE, werden weitere Änderungsinformationen von DC 2 angefordert. Hat DC 1 alle erforderlichen Daten bekommen, wird die Up-to-Dateness-Vektor-Tabelle bearbeitet. Anhand dieser von DC 2 gesendeten Tabelle weiß DC 1, welchen Stand DC 2 hat. Alle Einträge der neu empfangenen Up-to-Dateness-Vektor-Tabelle werden nacheinander geprüft. Ist der Wert in der empfangenen Tabelle höher als in seiner eigenen, übernimmt DC 1 den höheren Wert. Dieser Wert kann gefahrlos übernommen werden, da DC 1 und DC 2 nun miteinander abgeglichen sind. Findet DC 1 in der von DC 2 gesendeten Tabelle eine Eintragung für einen DC, den seine eigene Tabelle noch nicht kennt, wird auch dieser Eintrag hinzugefügt. Auf diese Weise werden von Active Directory automatisch neu erstellte Domänencontroller in die bestehende Replikationstopologie eingegliedert.

Nach dem Abgleichen der Up-to-Dateness-Vektor-Tabelle könnte diese Tabelle auf DC 1 die folgenden Einträge haben (siehe Tabelle 17.2); in der ersten Zeile werden zum Vergleich die Werte vor der Replikation angegeben): Sie sehen, dass lediglich die Werte für DC 4 und 5 nicht geändert wurden. Die Änderungen von DC 4 waren DC 1 bereits vor der Replikation bekannt, und an DC 5 sind keine ausgehenden Änderungen durchgeführt worden. Er kam in unserer Beschreibung deshalb auch nicht weiter vor.

	High-Watermark-Vektor für DC 2	UTDV-Tabelle fürDC 2	UTDV-Tabelle fürDC 3	UTDV-Tabelle fürDC 4	UTDV-Tabelle fürDC 5
Ursprünglicher Eintrag	1301	1301	1513	2402	125
Eintrag nach der Replikation	1305	1305	1714	2402	125

Tabelle 17.2: Ursprüngliche und aktualisierte Einträge der Up-to-Dateness-Vektor-Tabelle

Sie haben nun den kompletten Prozess der Replikation kennen gelernt. Bei den hier beschriebenen Abläufen handelt es sich um interne tiefgreifende LDAP-Prozesse. Aber dennoch ist zu einem guten Verständnis von Active Directory auch dieses tiefgehende Wissen notwendig. Besonders in Bezug auf eine Fehlersuche bei der Replikation oder anderen Replikationsproblemen kann dieses tiefe Verständnis von Vorteil sein.

In den beiden folgenden Kapiteln werden Ihnen einige Konstellationen gezeigt, bei denen die einfache Regel „jeder Domänencontroller verfügt stets über alle aktuellen Informationen“ nur eingeschränkt gilt. So kann es notwendig werden, dass Sie zwischen den Domänencontrollern die Systemzeit synchronisieren müssen (siehe Kapitel 17.1.5) oder sich eine Strategie überlegen müssen, an welchem Domänencontroller Sie Änderungen durchführen, damit diese möglichst zeitnah für die Clients an einem bestimmten Standort verfügbar sind (siehe Kapitel 17.1.6).

17.1.4 Die Linked-Value Replication unter Windows Server 2003

Das Replikationsverhalten wurde unter Windows Server 2003 gegenüber Windows 2000 verbessert. Diese Änderung betrifft die Replikation von Attributen mit mehreren Werten. Unter Windows 2000 wurden sämtliche Werte eines Attributs repliziert, auch wenn nur ein einziger Wert des Attributs geändert wurde. Dies führte zu unnötigem Replikationsverkehr und erhöhte auch das Risiko von Replikationskonflikten, wenn gleichzeitig Änderungen an einem Attributwert vorgenommen worden sind. Windows Server 2003 wurde um das Feature der Linked-Value Replication erweitert. Dieses Feature ermöglicht, dass lediglich der geänderte Wert eines Attributs repliziert wird, nicht jedoch die unverändert gebliebenen Werte. Damit diese neue Funktionalität verfügbar ist, muss der Gesamtstrukturmodus auf Windows Server 2003 eingestellt sein (siehe Kapitel 10.1.5). Die Windows 2000-Betriebsmodi unterstützen die neue Funktion nicht.

17.1.5 Synchronisieren der Systemzeit zwischen Domänencontrollern

Damit die Replikation auch bei eventuell auftretenden Sonderfällen von Änderungen an Domänencontrollern einwandfrei funktioniert, sollte die Systemzeit zwischen den Domänencontrollern synchronisiert werden. Zwar besitzt jeder Domänencontroller einen Zähler für die Änderungen, die an ihm vorgenommen wurden, und jede Änderung bekommt vom Active Directory automatisch eine eindeutige Sequenznummer (USN = Update Sequence Number) sowie einen Zeitstempel zugewiesen, aber dennoch kann die Synchronisierung sinnvoll sein. Die USN mit dem höheren Wert ist immer die aktuellere. Diese Sequenznummern finden Sie unter den Eigenschaften jedes Objekts, das geändert werden kann, auf der Registerkarte **OBJEKT**.

Normalerweise erhält ein Domänencontroller, der länger nicht verfügbar war, die Änderungen mit der höchsten Sequenznummer. Dabei kann noch kein Problem auftreten. Komplizierter wird es, wenn der seltenere, aber dennoch nicht auszuschließende Fall eintritt, dass dieselbe Änderung von zwei verschiedenen Benutzern innerhalb eines Replikationsintervalls an zwei verschiedenen Domänencontrollern durchgeführt wurde. In diesem Fall muss zusätzlich der Zeitstempel entscheiden, welche Änderung als die aktuelle zu replizierende angesehen wird. Hierbei wird dann die Synchronisierung wichtig. Auch für andere seltene Fälle, in denen ein Konflikt der Änderungen nicht über die USN gelöst werden kann, kann eine Zeitsynchronisierung die Lösung sein.

Angenommen, Sie führen auf dem Domänencontroller 1 eine Änderung durch, und die aktuelle Systemzeit dieses Domänencontrollers ist genau 10:00 h. Diese Änderung soll beim nächsten Replikationsintervall repliziert werden. Die nächste Replikation steht um 10:05 h an. Währenddessen führt Ihr Kollege dieselbe Änderung auf dem Domänencontroller 2 durch, dessen Systemzeit bei 10:03 h steht. Also erhält die Änderung Ihres Kollegen den neueren Zeitstempel. Die Änderungen wurden bereits von beiden Domänencontrollern übernommen, bevor eine der Änderungen repliziert werden konnte. Beim Replikationsvorgang werden beide Änderungen als neu auf jeweils den anderen Domänencontroller repliziert, und auf beiden wird der Zähler für die USN um eins heraufgesetzt. Um den Konflikt zu lösen, werden von dem Domänencontroller die Zeitstempel seiner lokalen Änderung und der empfangenen Änderung überprüft. Es wird die Änderung mit dem neueren Zeitstempel übernommen.

In der Ereignisanzeige des Systemprotokolls finden Sie regelmäßig Warnungs- bzw. Fehlerereignisse der Quelle *W32Time*, wenn der erste Domänencontroller feststellt, dass er mit keiner externen Zeitquelle synchronisiert ist. Die Ereignisse tragen die IDs 54 und 62. Sie sollten alle Domänencontroller mit einer bestimmten Zeitquelle synchronisieren. Somit ist auf allen Domänencontrollern sichergestellt, dass sie alle exakt dieselbe Systemzeit haben. Die Synchronisierung geschieht mittels des Befehls `net time` an der Eingabeaufforderung.

Bei `net time` haben Sie die folgenden wichtigsten Optionen und Parameter zur Verfügung:

```
Net time [\\Computername] [/Domänenname] [/set]
```

`Net time` ohne weitere Parameter zeigt die Uhrzeit des Servers, der als Zeitserver für die Domäne arbeitet. Ist kein Zeitserver konfiguriert, erhalten Sie eine Fehlermeldung.

Ohne den Befehl `/set` erhalten Sie die Zeit des unter Computernamen angegebenen Rechners. Den Computernamen können Sie als DNS-Namen oder als IP-Adresse angeben, wenn sich die Einstellungen nicht auf den lokalen Computer beziehen sollen. Die Angabe des Domänennamens ist optional.

Mit dem Befehl `/set` können Sie auf dem lokalen Computer die Zeit des angegebenen Computers übernehmen.

Um einen Domänencontroller mit einer externen Zeitquelle zu synchronisieren, geben Sie den Befehl

```
Net time [\\Computername] /setsntp[:NTP-Serverliste] 
```

ein.

Setsntp gibt eine Liste der NTP-(Network Time Protocol-)Server an, die der Domänencontroller zur Synchronisierung verwenden soll. Sie können die NTP-Server als DNS-Namen oder in Form von IP-Adressen angeben. Wenn Sie mehrere Server angeben, müssen die Namen von Anführungszeichen eingeschlossen sein. Selbstverständlich können Sie nicht nur Domänencontroller, sondern auch andere Server oder Clients über diesen Befehl zur Zeitsynchronisierung zwingen.

Mit folgendem Befehl können Sie später den Namen des oder der NTP-Server(s) anzeigen, der für den unter Computernamen angegebenen Rechner konfiguriert ist:

```
Net time [\\Computername] /querysnTP 
```

Der NTP-Server wird dabei als aktueller SNTP-Wert ausgegeben.

17.1.6 Beschleunigen der Replikation

In diesem Kapitel wird ein weiteres häufiges Problem beschrieben, das streng genommen gar kein Problem der Replikation, sondern eher der Standorte der vorhandenen Domänencontroller ist. Stellen Sie sich das folgende Szenario vor:

Ihr Unternehmen verfügt über eine Domäne mit den vier Standorten der Zentrale in Barsinghausen und den Filialen in Dortmund, Oberhausen und Wolfsburg. Als Administrator haben Sie an Ihrem ersten Domänencontroller in Barsinghausen das Passwort eines Benutzers in der Filiale Dortmund zurückgesetzt, der sein altes Passwort vergessen hat. Sie teilen ihm mit, dass Sie das Passwort zurückgesetzt haben, woraufhin er sich sofort in Dortmund erneut an der Domäne, aber genauer gesagt an Domänencontroller 4, mit dem zurückgesetzten Passwort anzumelden versucht, jedoch ohne Erfolg. Die Standorte sind jedoch korrekt konfiguriert, jeder hat sein eigenes Subnetz. Sie wissen, dass das Problem nicht in der Konfiguration der Standorte zu suchen ist.

Dieses Problem kann in jedem Unternehmen auftreten, das über mehr als einen Domänencontroller verfügt, die über das WAN miteinander verbunden sind.

Die Ursache, dass sich der Benutzer in Dortmund nicht sofort nach der am Domänencontroller in Barsinghausen durchgeführten Änderung anmelden kann, liegt darin, dass sein Client für die Anmeldung und Authentifizierung zunächst einen Domänencontroller am Standort sucht – und diesen in Form von Domänencontroller 4 auch findet. Für den

Anmeldeprozess an sich ist es dabei auch gleichgültig, ob der Domänencontroller alle geänderten Informationen bereits als Replikat erhalten hat oder nicht. Bemerkenswert ist dieses Problem natürlich am schnellsten, wenn die für den Anmeldevorgang nötige Passwortinformation noch nicht repliziert wurde. Der Domänencontroller in Wolfsburg wird die neue Passwortinformation aber erst bei einem neu anstehenden Replikationsdurchlauf empfangen – und dies kann dauern, falls die standortübergreifende Replikation für die Domänencontroller 1 bis 4 über die Standortverknüpfungen der Reihe nach festgelegt wurde.

Sie haben zwei verschiedene Möglichkeiten, um die Replikation zwischen den beiden Standorten zu beschleunigen. Zum einen können Sie die Werte für die Replikationshäufigkeit umsetzen. Da aber mit einer höheren Replikationshäufigkeit auch höhere Kosten verbunden sind, sollten Sie lieber das zweite Verfahren anwenden.

Wie schon am Anfang erwähnt, ist dieses nicht direkt ein Problem der Replikation, sondern eher ein Problem des Domänencontrollers, da dieser nicht das Passwort besitzt. Wenn Sie die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER öffnen, um das Passwort für den Benutzer in Dortmund zurückzusetzen, verbindet sich die mmc mit dem nächsten verfügbaren Domänencontroller, in unserem Beispiel also dem in Barsinghausen, sofern Sie die Änderungen nicht direkt am Domänencontroller durchführen. Sie haben also das Passwort auf dem Domänencontroller zurückgesetzt, der Ihnen am nächsten ist, aber nicht dem Benutzer, der die geänderten Informationen sofort benötigt.

Um dieses Problem zu umgehen, können Sie von Ihrer Zentrale aus die Änderungen auch direkt auf dem Domänencontroller des Standorts vornehmen, an dem die Informationen sofort verfügbar sein müssen. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
2. Markieren Sie dort Ihre aktuelle Domäne und wählen aus dem Kontextmenü VERBINDUNG MIT DOMÄNENCONTROLLER HERSTELLEN. Sie erhalten nun eine Liste aller verfügbaren Domänencontroller dieser Domäne. Bei jedem ist zusätzlich der Standort angegeben. Wählen Sie hier den Domänencontroller vom Standort des Benutzers aus.

Nun werden die Änderungen direkt auf dem Domänencontroller, in unserem Fall also in Dortmund vorgenommen. Für den Benutzer sind die Änderungen dort sofort verfügbar. An die anderen Standorte wird die Änderung beim nächsten Replikationsintervall geschickt. An den anderen Standorten spielt es nicht die entscheidende Rolle, wann die Information des zurückgesetzten Passworts übermittelt wird, da sich derselbe Benutzer wohl kaum innerhalb eines Replikationsintervalls von einem Standort an den anderen bewegen wird, um sich dort an einem Domänencontroller zu authentifizieren.

17.1.7 Bearbeiten der Replikationszeiten über die Registry

Wie Sie bereits gesehen haben, wird der Replikationsprozess automatisch in Gang gesetzt, sobald Änderungen am Verzeichnis aufgetreten sind. Standardmäßig ist eine Verzögerungszeit vordefiniert, bevor ein Domänencontroller darüber informiert wird, dass eine Replikation ansteht. Diese Verzögerungszeit der Benachrichtigung wird auch als Hold-back Time bezeichnet und liegt standardmäßig bei 300 Sekunden (= fünf Minuten). Erst nach Ablauf dieser 5 Minuten teilt das Active Directory dem ersten Domänencontroller

mit, dass Änderungen vorgenommen worden sind. Wollen Sie diesen Wert ändern, so modifizieren Sie in dem Registry-Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters` den Wert für `REPLICATOR NOTIFY PAUSE AFTER MODIFY`. Der Wert ist in Sekunden anzugeben. Bedenken Sie aber, dass ein zu hoher Wert Inkonsistenzen im Verzeichnis hervorrufen kann, da vor einer Replikation zu viele Änderungen vorgenommen worden sind. Setzen Sie den Wert hingegen zu niedrig an, findet eine dauernde Replikation statt, die auf Kosten der Netzwerkauslastung geht, aber keine Vorteile mit sich bringt. Im Idealfall sollten Sie diesen Wert also nicht modifizieren.

Sobald der erste Domänencontroller über eine anstehende Replikation benachrichtigt worden ist, gibt dieser die Benachrichtigung an seine Replikationspartner weiter. Dabei wird der erste Partner standardmäßig nach 30 Sekunden informiert, nach weiteren 30 Sekunden der nächste usw. Damit wird verhindert, dass alle Domänencontroller zeitgleich die Änderungen anfordern und damit das Netzwerk überlasten. Soll dieser Wert bearbeitet werden, so ändern Sie im Registry-Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters` den Wert `REPLICATOR NOTIFY PAUSE BETWEEN DSAs`. Auch dieser Wert ist in Sekunden anzugeben.

Die standortinternen Replikationsrouten werden automatisch berechnet. Hierfür ist der Knowledge Consistency Checker (KCC, Konsistenzprüfung) zuständig. Der KCC berechnet standardmäßig alle 15 Minuten neue Routen. Um diesen Wert zu ändern, modifizieren Sie im Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters` den Wert `REPL TOPOLOGY UPDATE PERIOD`.

Für die Replikation wird von Windows 2000 der RPC-(Remote Procedure Call-)Port dynamisch festgelegt. Aus Sicherheitsaspekten sollten Sie auch nie einen festen Port angeben. Wollen Sie aber beispielsweise für Diagnosezwecke einen bestimmten Port angeben, den Sie überwachen möchten, so müssen Sie im Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters` einen Wert mit dem Namen `TCP/IP PORT` (Typ `REG_DWORD`) hinzufügen und dort den gewünschten Port angeben. Damit diese Änderung wirksam wird, muss der Computer neu gestartet werden. Haben Sie Ihre Diagnose beendet, sollten Sie die Registry-Änderung wieder rückgängig machen, damit der Port wieder dynamisch gewählt werden kann.

17.2 Standortübergreifende Replikation

Der wichtigste Aspekt bei der standortübergreifenden Replikation ist die Vermeidung von hohen Kosten beim Netzwerkverkehr über das WAN. Deshalb werden bei der standortübergreifenden Replikation die Kosten für die Replikation, die Replikationsintervalle sowie die Replikationsverfügbarkeit konfiguriert.

Beim Datenaustausch der standortübergreifenden Replikation werden die zu übertragenen Daten vorher auf dem Domänencontroller komprimiert und vom Ziel-Domänencontroller wieder entpackt. Damit wird sichergestellt, dass eine kleinere Menge an Daten schneller und damit auch kostengünstiger zwischen den Standorten ausgetauscht werden kann. Dabei wird in Kauf genommen, dass die Domänencontroller Rechenkapazität für das Ein- und Entpacken der Daten benötigen. Bei der standortinternen Replikation werden

die Daten nicht komprimiert. Hier ist es innerhalb eines schnellen LANs nicht relevant, wie groß die zu übertragende Datenmenge ist. Damit entfällt auf den Domänencontrollern auch die zusätzliche Rechenzeit zum (De-)Komprimieren der Datenpakete.

Für die standortübergreifende Replikation müssen Sie drei Komponenten einrichten und konfigurieren. Hierbei handelt es sich um Standortverknüpfungsattribute, Standortverknüpfungsbrücken und Bridgehead-Server/Bridgehead-Server. Das Einrichten dieser Objekte wird in den folgenden Kapiteln erläutert.

Bei der Replikation werden zwei verschiedene Ports benutzt. LDAP benutzt den Port 389 und SMTP, das ausschließlich bei der standortübergreifenden Replikation verwendet wird, den Port 25. Diese beiden Ports müssen bei der Konfiguration einer Firewall entsprechend freigeschaltet werden.

17.2.1 Standortverknüpfungsattribute

Für alle Standortverknüpfungen sollten Sie Standortverknüpfungsattribute konfigurieren. Diese Attribute umfassen die Standortverknüpfungskosten, die Replikationshäufigkeit sowie die Replikationsverfügbarkeit. Sämtliche Einstellungen dieses Kapitels werden über die Eigenschaften der Standortverknüpfung vorgenommen. Die Standortverknüpfungen finden Sie in der mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE im Container INTER-SITE-TRANSPORTS und dort entweder unter IP oder SMTP – je nachdem, für welches Transportprotokoll Sie sich entschieden haben. Für jede Standortverknüpfung können alle Werte unabhängig konfiguriert werden.

Standortverknüpfungskosten

Auf der Eigenschaftsseite einer Standortverknüpfung sehen Sie das Eingabefeld KOSTEN (siehe Abbildung 17.3). Als Standard ist dort der Wert 100 vorgegeben.

Legen Sie den Wert für die Kosten anhand der Leistung der Netzwerkbandbreite zwischen den Standorten fest. Wenn Sie über mehrere Netzwerkverbindungen zwischen den Standorten verfügen, konfigurieren Sie für jede Verbindung eine separate Standortverknüpfung. Active Directory wählt immer automatisch die Verbindung, für die die niedrigsten Kosten angegeben sind, solange sie verfügbar ist. Ist innerhalb eines Replikationsintervalls die kostengünstigste Verbindung ausgefallen, so wird die Alternativverbindung benutzt. Ist die günstige Verbindung nach einiger Zeit wieder verfügbar, so wird sie ab diesem Zeitpunkt wieder benutzt. Der Standardwert für die Kosten liegt bei 100. Je geringer der Kostenwert ist, desto höher ist die Priorität, mit der diese Verbindung genutzt wird. Falls Sie beispielsweise über eine T1-Standleitung und eine DFÜ-Verbindung zwischen zwei Standorten verfügen, so können Sie für die Standleitung einen Kostenwert von 100 festlegen, während der Wert für die DFÜ-Verbindung 150 beträgt.



Abbildung 17.3: Konfiguration der Replikationskosten

Je schneller und damit auch kostengünstiger eine Verbindung ist, desto geringer ist der Wert, den Sie im Kosten-Feld festlegen müssen. Bevor Sie mit der Angabe von Kostenwerten beginnen, sollten Sie sich einen Überblick über alle vorhandenen Verbindungen zwischen sämtlichen Standorten verschaffen und dann anhand dieser Ergebnisse die zu vergebenden Kostenwerte kalkulieren.

Replikationsintervalle

Unter dem Eingabefeld für die Kosten befindet sich das Feld REPLIZIEREN ALLE ... MINUTEN. Standardmäßig ist hier der Wert 180 eingetragen, was einem Replikationsintervall von drei Stunden entspricht. Der Maximalwert der Eingabe liegt bei 10.080 Minuten, was einer Woche entspricht. Der Minimalwert liegt bei 15. Für alle möglichen Replikationen muss eine Standortverknüpfung eingerichtet sein. Wollen Sie aus bestimmten Gründen verhindern, dass eine Replikation zwischen zwei Standorten stattfindet, so erstellen Sie keine Verknüpfung für diese beiden Standorte.

Bedenken Sie beim Festlegen der Werte für das Replikationsintervall die folgenden Punkte:

- ▶ Wenn Sie einen sehr niedrigen Wert (unter 100 Minuten) festlegen, so erzielen Sie damit zwar stets sehr aktuelle Verzeichnisinformationen, auf der anderen Seite erhöhen Sie aber auch die Netzwerklast und damit auch die Kosten für den WAN-Verkehr.
- ▶ Setzen Sie den Wert hingegen zu hoch an (über 200 Minuten), verringern Sie zwar den WAN-Verkehr, aber für die Benutzer bedeutet dies ein langes Warten auf aktualisierte Verzeichnisdaten. In dieser Wartezeit können die Benutzer möglicherweise nicht produktiv arbeiten.

Replikationsverfügbarkeit

Als letzte Option können Sie die Zeitpläne festlegen, zu welchen Zeiten die Replikation durchgeführt werden soll. Diese Option kommt im Prinzip nur für das IP-Replikationsprotokoll in Frage, da SMTP asynchron arbeitet. Sie können die Replikationshäufigkeit nur dann für SMTP durchsetzen, wenn folgende Punkte erfüllt sind:

- ▶ Sie verwenden nur durch den Zeitplan bestimmte Verbindungen zwischen den Standorten.
- ▶ Die SMTP-Warteschlange richtet sich nach keinem Zeitplan.
- ▶ Die Replikationsinformationen müssen direkt zwischen den Servern ausgetauscht werden und nicht über zwischengeschaltete Server, wie es bei einer Ethernet-Backbone-Verbindung der Fall ist.

Damit alle im folgenden Abschnitt beschriebenen Einstellungen wirksam werden, prüfen Sie zunächst, ob auf der Eigenschaftsseite von IP und SMTP die Checkbox ZEITPLAN IGNORIEREN aktiviert ist oder nicht. Standardmäßig ist sie nur unter SMTP aktiviert. Dort muss sie deaktiviert werden, wenn Sie die Zeitpläne für SMTP durchsetzen wollen. Wollen Sie hingegen alle Zeitpläne deaktivieren, so aktivieren Sie bei dem jeweiligen Transportprotokoll die Checkbox.

Um die Replikationsverfügbarkeit zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der Eigenschaftsseite der Standortverknüpfung auf die Schaltfläche ZEITPLAN ÄNDERN. Standardmäßig ist die Replikation die ganze Woche rund um die Uhr verfügbar.

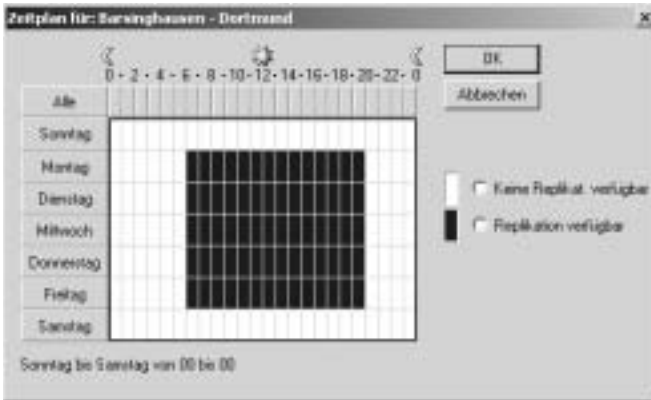


Abbildung 17.4: Verfügbarkeitszeiträume der Replikation

2. Um Zeiten zu bestimmen, zu denen keine Informationen repliziert werden sollen, markieren Sie die entsprechenden Zeiten und Tage und klicken dann auf KEINE REPLIK. VERFÜGBAR (siehe Abbildung 17.4). Es ist beispielsweise nicht sinnvoll, die Replikation die ganze Nacht über oder an den Wochenenden durchzuführen. Dies verursacht nur unnötige Kosten, da zu diesen Zeiten in der Regel die Benutzer nicht arbeiten und somit aktualisierte Verzeichnisinformationen benötigen. Eine Replikationsverfügbarkeit könnte wie in der oberen Abbildung auf die Werktage zwischen 6:00 am Morgen und 20:00 am Abend eingeschränkt werden.

17.2.2 Standortverknüpfungsbrücken (Site Link Bridges)

Wenn Sie zwei oder mehr Standorte über Standortverknüpfungen für die Replikation verbunden haben und für alle Verknüpfungen dasselbe Replikationsprotokoll verwendet wird, gelten die Standorte als überbrückt. Eine einzige Standortverknüpfungsbrücke umfasst somit alle Standortverknüpfungen, die entweder über das IP- oder das SMTP-Transportprotokoll miteinander verbunden sind. Innerhalb einer solchen Standortverknüpfungsbrücke spricht man von transitiven Standortverknüpfungen. Manuell müssen Sie nur in dem Fall Standortverknüpfungsbrücken einrichten, falls Ihr Netzwerk nicht vollständig geroutet ist. Verwenden Sie im Netzwerk Router, die redundante WAN-Verbindungen bereitstellen, so müssen Sie im Active Directory keine Standortverknüpfungsbrücken konfigurieren. In diesem Fall laufen beide WAN-Verbindungen über einen Router. Ist dabei die erste Verbindung nicht mehr verfügbar, so leitet der Router automatisch den gesamten WAN-Verkehr über die zweite Leitung. Richten Sie in diesem Fall dennoch eine Standortverknüpfungsbrücke ein, so besteht die Gefahr, dass die Replikation fehlschlägt, wenn die erste Verbindung des Routers nicht mehr verfügbar ist.

Ist Ihr Netzwerk nicht vollständig geroutet, müssen Sie Standortverknüpfungsbrücken manuell erstellen. Die Brücke entspricht dann einem getrennten Netzwerk. Sämtliche Verknüpfungen innerhalb der Standortverknüpfungsbrücke werden als transitiv angesehen und geroutet, alle außerhalb der Brücke liegenden intransitiven Verknüpfungen werden nicht geroutet.



Überprüfen Sie zunächst, ob im Eigenschaftsfeld des Transportprotokolls die Checkbox BRÜCKE ZWISCHEN ALLEN STANDORTVERKNÜPFUNGEN HERSTELLEN aktiviert ist. Standardmäßig ist dies bei beiden Protokollen der Fall. Ist diese Option aktiviert, werden automatisch alle vorhandenen Standortverknüpfungen eines Transportprotokolls überbrückt. Wenn Sie dennoch Standortverknüpfungsbrücken einrichten, erzielen Sie damit lediglich Redundanz.

Um eine neue Standortverknüpfungsbrücke zu erstellen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie den Ordner des bevorzugten Transportprotokolls (IP oder SMTP) und wählen dann aus dem Kontextmenü den Eintrag NEUE STANDORTVERKNÜPFUNGSBRÜCKE.
2. Geben Sie in dem neuen Fenster im Feld NAME einen Namen für die neue Standortverknüpfungsbrücke ein (siehe Abbildung 17.5).
3. In der Liste links sehen Sie alle eingerichteten Standortverknüpfungen. Wählen Sie alle Verknüpfungen aus, die unter der neuen Brücke zusammengefasst werden sollen, und bringen Sie diese über HINZUFÜGEN in die rechte Liste.

Sie können auch Standortverknüpfungsbrücken zur zuverlässigeren Übertragung der Active Directory-Daten einrichten. In diesem Fall ist die gebrückte Verbindung eine redundante Verbindung zu einer bereits bestehenden Standortverknüpfung. Angenommen, die Standorte Barsinghausen und Dortmund sind über eine Verknüpfung direkt miteinander verbunden. Zusätzlich implementieren Sie eine Brücke dieser Verbindung über den Standort Oberhausen. Sollte nun die direkte Verbindung zwischen Barsinghausen

und Dortmund nicht verfügbar sein, so wird die Verbindung zwar über den Umweg Oberhausen geleitet, aber trotzdem können Barsinghausen und Dortmund miteinander Daten austauschen.



Abbildung 17.5: Einrichten einer Standortverknüpfungsbrücke

Außer den Standortverknüpfungen und Standortverknüpfungsbrücken können Sie auch manuelle Verbindungen zwischen Domänencontrollern herstellen. Sie sollten aber lieber Active Directory die Auswahl und Optimierung der Replikationspfade überlassen. Wenn Sie manuelle Verbindungen einrichten, sollten diese nicht länger als notwendig bestehen bleiben, da sie sich eher negativ auf die Replikations-Performance auswirken können. Weiterhin kann auch die Replikation manuell erzwungen werden.

Um entweder eine Verbindung manuell herzustellen oder die Replikation zu erzwingen, führen Sie die folgenden Schritte aus:

1. Navigieren Sie in der mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE auf den Standort des Servers und dort auf den Ordner NTDS SETTINGS.
2. Für die manuelle Herstellung einer Verbindung wählen Sie aus dessen Kontextmenü NEUE ACTIVE DIRECTORY-VERBINDUNG. In dem dann folgenden Fenster sehen Sie unten eine Liste aller Server an allen Standorten. Wählen Sie hier den gewünschten aus und klicken auf OK.
3. Um die Replikation zwischen zwei Domänencontrollern zu erzwingen, wählen Sie aus dem Ergebnisabschnitt der NTDS SETTINGS die Verbindung aus, über die die geänderten Daten repliziert werden sollen. Standardmäßig finden Sie unter den Verbindungen nur die automatisch erstellte Standortverknüpfungsbrücke.

17.2.3 Bridgehead-Server

Ein Bridgehead-Server ist an einem Standort derjenige Domänencontroller, der bevorzugt als erster die Replikationsdaten erhält. Durch das Bestimmen eines Bridgehead-Servers können Sie also das normale Replikationsverhalten beeinflussen, bei dem alle Domänencontroller ihre Daten zwischen den Standorten austauschen. Die Implementierung macht selbstverständlich nur dann Sinn, wenn an den Standorten mehr als ein Domänencontroller vorhanden ist. Da der Bridgehead-Server der einzige Kommunikationspunkt zu anderen Standorten ist, sollten Sie einen Computer mit geeigneter Bandbreite auswählen. Über den Bridgehead-Server allein wird die standortübergreifende Replikation abgewickelt. Hat er dabei alle Daten empfangen, leitet er diese standortintern an die restlichen Domänencontroller weiter.

Sie können für einen Standort einen oder mehrere Bridgehead-Server angeben. Es kann aber nur einer zur Zeit von Active Directory benutzt werden. Dieser ist der aktive Bridgehead-Server. Die Liste der alternativen Bridgehead-Server wird abgearbeitet, wenn der erste konfigurierte nicht erreichbar ist. Ist keiner der angegebenen Bridgehead-Server mehr verfügbar, wählt Active Directory automatisch einen anderen Domänencontroller. Falls dieser jedoch nicht genügend Bandbreite bietet, kann es bei der Replikation zu Problemen kommen. Bis Active Directory einen anderen Domänencontroller ausgewählt hat, findet keine standortübergreifende Replikation statt. Um dieses Problem zu mildern, könnten Sie einen großen Standort in mehrere kleine aufteilen. Fällt nun der Bridgehead-Server für einen Teil-Standort aus, so ist nur eine kleinere Anzahl Ihrer Clients betroffen. Würde die standortübergreifende Replikation hingegen für den gesamten Standort ausfallen, wäre die negative Auswirkung größer. Um es nochmals klarzustellen: Diese Lücken in der standortübergreifenden Replikation entstehen nur, sobald der bevorzugte Bridgehead-Server ausgefallen ist und bis Active Directory einen alternativen Bridgehead-Server ausgewählt hat.

Die Einrichtung eines Bridgehead-Servers ist notwendig, wenn Ihr Standort von einer Firewall geschützt wird. Sie sollten dann den Firewall-Proxy-Server als den bevorzugten Bridgehead-Server einrichten. Um einen Bridgehead-Server einzurichten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE. Wählen Sie dort aus einem Standort den gewünschten Domänencontroller aus und klicken im Kontextmenü auf EIGENSCHAFTEN.
2. Wählen Sie im Eigenschaftsfenster (siehe Abbildung 17.6) aus dem Feld TRANSPORTE FÜR DIE STANDORTÜBERGREIFENDE DATENÜBERMITTLUNG das gewünschte Transportprotokoll, also IP oder SMTP, und klicken auf HINZUFÜGEN. Damit wird der gewählte Computer zum bevorzugten Bridgehead-Server.



Abbildung 17.6: Der bevorzugte Bridgehead-Server

3. Um eine Liste alternativer Bridgehead-Server zu erstellen, wiederholen Sie diesen Vorgang für die restlichen Server, die Sie konfigurieren möchten. Der erste konfigurierte Bridgehead-Server wird so lange von Active Directory verwendet, wie er erreichbar ist. Nur einer dieser Server ist gleichzeitig aktiv.

17.2.4 Einstellungen standortübergreifender Replikationstopologie

Wie nun schon mehrfach erwähnt, wird die standortinterne Replikation von Active Directory automatisch gesteuert. Nachdem Sie nun für die standortübergreifende Replikation einen bevorzugten Bridgehead-Server erstellt haben, muss für diesen das geeignete Verbindungsobjekt mit einem Zeitplan erstellt werden. Dafür ist der Inter-Site Topology Generator (ISTG) zuständig – der Generierer der standortübergreifenden Topologie. Der ISTG wird standardmäßig auf dem ersten am Standort eingerichteten Domänencontroller erstellt. Für einen Standort kann es nur einen ISTG geben, selbst dann, wenn Ihr Standort über mehrere Domänen verfügt.

1. Um zu überprüfen, welcher Domänencontroller der aktuelle ISTG ist, öffnen Sie die Eigenschaften der NTDS SETTINGS am Standort (siehe Abbildung 17.7).



Abbildung 17.7: Der aktuelle ISTG

2. Dort sehen Sie den Namen und Standort des ISTG. Über die Schaltfläche ZEITPLAN ÄNDERN können Sie einen Zeitplan festlegen, an welchen Tagen und zu welchen Intervallen die standortübergreifende Replikation stattfinden soll. Die Standardeinstellung sieht folgendermaßen aus (siehe Abbildung 17.8):

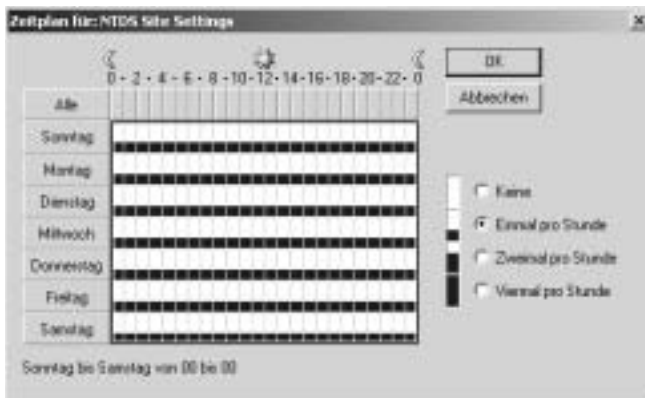


Abbildung 17.8: Der Zeitplan für die standortübergreifende Replikation

3. Sie können das Replikationsintervall auf alle 15, 30 oder 60 Minuten festlegen oder aber auch die Replikation deaktivieren. Diese Einstellung kann für jede einzelne Stunde jedes Tages separat eingestellt werden. Markieren Sie dazu die gewünschten Zeitfelder und wählen dann rechts aus der Liste das gewünschte Intervall aus. Bestätigen Sie abschließend mit OK.

Zur Prüfung der Replikationstopologie läuft ein Hintergrundprozess im Active Directory ab, bei dem die folgenden Kriterien analysiert werden:

- ▶ Sind noch alle Domänencontroller im Active Directory vorhanden und auch verfügbar?
- ▶ Sind seit der letzten Replikation neue Domänencontroller ins Active Directory integriert worden?
- ▶ Sind bei standortübergreifenden Replikationen die als kostengünstigsten definierten Verbindungen noch verfügbar oder muss eine teurere Verbindung benutzt werden? Die Replikationstopologie wird alle 15 Minuten über den KCC (Knowledge Consistency Checker) neu berechnet. Die Replikationstopologie wird zuweilen auch als RepsFrom und RepsTo bezeichnet. Wird dabei festgestellt, dass die kostengünstigste Verbindung zwischen zwei Standorten nicht mehr verfügbar ist, so wird diese Verknüpfung vom KCC so lange nicht mehr benutzt, bis sie wieder als funktionierend erkannt wird. Danach wird selbstverständlich wieder die kostengünstigste Verbindung benutzt.

Diese geprüften Informationen werden ausgelesen. Auf Basis dieser Informationen wird die optimale, effiziente Replikationsroute festgelegt. Dabei werden neue Verbindungsobjekte integriert oder veraltete entfernt. Von diesem Prozess sind jedoch nicht die manuell erstellten Verbindungen betroffen.

Normalerweise wird dieser Prüfprozess automatisch durchgeführt. Sie können die Überprüfung der Replikationstopologie aber auch manuell initiieren. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie in der mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE den Domänencontroller, für den die Topologie geprüft werden soll.
2. Markieren Sie dessen NTDS-Settings und wählen aus dem Kontextmenü den Eintrag REPLIKATIONSTOPOLOGIE ÜBERPRÜFEN. Damit wird der Prüfvorgang eingeleitet, und die Verbindungsobjekte können bei Bedarf angepasst werden.

Der Inter-Site Topology Generator (ISTG) des 2003 Servers wurde gegenüber dem ISTG des Windows 2000 Servers verbessert. Er verwendet nun verbesserte Algorithmen und ist besser skalierbar für eine größere Anzahl von Standorten als unter Windows 2000. Damit Sie die verbesserte Performance der neuen ISTG-Algorithmen ausnutzen können, müssen alle Domänencontroller im Windows 2003-Betriebsmodus der Gesamtstruktur ausgeführt werden.

17.2.5 Wann wird welcher Replikationszeitplan benutzt?

Wie Sie in den vorangegangenen Kapiteln gelesen haben, kann an zwei Stellen ein Replikationszeitplan konfiguriert werden. Zum einen kann ein Zeitplan unter INTER-SITE-TRANSPORTS/IP/DEFAULTSITEPLINK editiert werden, zum anderen unter STANDORT-NAME/NTDS-SITE-SETTINGS. Hier erfahren Sie, wann welcher Zeitplan benutzt wird.

Sobald an einem Domänencontroller eine Änderung vorgenommen wurde, benachrichtigt er standardmäßig nach fünf Minuten die anderen Domänencontroller, die sich am selben Standort befinden. Dann erfolgt die standortinterne Replikation. An Domänencontroller außerhalb des Standorts können keine Benachrichtigungen gesendet werden. Sollte ein

Domänencontroller innerhalb dieses Standorts die Änderungsbenachrichtigung nicht erhalten haben, etwa weil das Netzwerk überlastet war, so fragt jeder Domänencontroller stündlich bei seinen Replikationspartnern an, ob ihm eine Änderung entgangen ist. Diese Einstellung wird unter den NTDS-Settings des Standorts vorgenommen.

Über den DEFAULTSITEPLINK wird die standortübergreifende Replikation eingerichtet. Nach jedem Ablauf des konfigurierten Zeitfensters bauen die Bridgehead-Server der beiden Standorte eine Verbindung miteinander auf und replizieren die Änderungen.

17.3 Fehler bei der Replikation

Bei einem so komplexen Vorgang wie der Replikation oder unter Windows 2000 sogar der Multimaster-Replikation können natürlich leider auch Probleme nicht generell ausgeschlossen werden. In diesem Kapitel wird Ihnen zunächst erläutert, wie Sie auf fehlerhafte Replikation aufmerksam werden können. Danach wird Ihnen eine Beschreibung möglicher Replikationskonflikte geboten, die teilweise auch schon die Lösung beschreiben. Damit ist ein fließender Übergang zum Abschluss des Kapitels gegeben, wo Sie eine Liste weiterer häufiger Probleme mit jeweils zugeordneten Lösungsansätzen erhalten.

Um herauszufinden, ob es in Ihrem Active Directory Replikationsprobleme gibt, sollten Sie das Active Directory-Support-Tool *DCDIAG* aufrufen. Auch dieses Kommandozeilenprogramm ist Bestandteil des Windows 2000 Resource Kit. Sollten Sie dort eine Meldung wie `failed test kccevent` finden, wissen Sie, dass Replikationsprobleme vorliegen. KCC bedeutet Knowledge Consistency Checker. Es ist ein in Windows 2000 Active Directory fest integriertes Stück Software, mit dem die Konsistenz der Active Directory-Datenbank überprüft wird. Über den KCC wird ermittelt, wann eine Replikation notwendig ist. Weiterhin besteht seine Funktion auch darin, sich bei einer anstehenden Replikation mit einem anderen Domänencontroller zu verbinden und von diesem dann die benötigten Daten abzufordern.

Außerdem ist der KCC für die Bandbreitenüberwachung bei der Replikation zuständig. Er sorgt dafür, dass bei der Multimaster-Replikation innerhalb eines Standorts ein Domänencontroller nicht mehr als drei gleichzeitige Replikationsverbindungen zu anderen Domänencontrollern unterhält. Würde ein Domänencontroller mit allen seinen Replikationspartnern gleichzeitig kommunizieren, wäre der übrige Netzwerkverkehr für die Zeit der Replikation sehr stark beeinträchtigt.

Um einen Domänencontroller zur sofortigen Replikation seiner Änderungen zu zwingen, verwenden Sie das Support-Tool *REPADMIN*. Verwenden Sie dazu die Syntax

```
repadmin /kcc Servername.Domäne.xy ↵, also etwa  
repadmin /kcc hippokrates.firma.de ↵.
```

17.3.1 Mögliche Replikationskonflikte

Eine gute Nachricht gleich vorweg: Ein großer Teil der Replikationsprobleme beruht lediglich auf Verbindungsproblemen zwischen den Replikationspartnern. Sobald Sie festgestellt haben, dass sie keine Verbindung zueinander herstellen können, lösen Sie dieses Problem. Danach wird auch die Replikation wieder funktionieren.

Sollten große Replikationsprobleme zwischen einer Vielzahl von Domänencontrollern aufgetreten sein, so sollten Sie als letzten Ausweg die autorisierende Wiederherstellung des Active Directory in Betracht ziehen. Wenn Sie die autorisierende Wiederherstellung auf einem Domänencontroller durchführen, wird dieser zu einem speziellen Master. Auf ihm werden sämtliche UNSs so weit heraufgesetzt, dass sie einen höheren Wert haben als auf den anderen Domänencontrollern. Alle anderen Domänencontroller beziehen danach ihre Informationen von diesem Master.

Ein unlösbares Problem haben Sie, wenn Sie auf einem Domänencontroller neue Objekte erstellen, aber dieser Domänencontroller vor dem nächsten Replikationsintervall einen Absturz erleidet und sich danach beharrlich und erfolgreich weigert, seinen Dienst wieder aufzunehmen. In diesem Fall sind alle noch nicht replizierten Änderungen unwiderruflich verloren. Es ist zwar nicht gerade wahrscheinlich, dass dieser Fall eintritt, aber man sollte die Konsequenzen kennen.

Nun werden Ihnen einige Beispiele aufgelistet, bei denen es zwangsläufig zu Problemen bei der nächsten Replikation kommen wird.

Erstellen eines gleichnamigen Objekts auf mehreren Domänencontrollern

Angenommen, zwei Administratoren erstellen ein auf zwei verschiedenen Domänencontrollern ein Objekt, das sie beide mit demselben Namen versehen. Bei der Replikation wird zunächst die Versionsnummer der beiden Objekte überprüft. Sind diese unterschiedlich, wird das Objekt mit der höheren Versionsnummer übernommen. Sind sie gleich, wird als Nächstes der Zeitstempel sämtlicher Eigenschaften betrachtet. Aus allen Eigenschaften der beiden Objekte wird dann jeweils der neueste Zeitstempel ausgelesen und miteinander verglichen. Sollten auch diese identisch sein, fällt spätestens beim nächsten Vergleich die Entscheidung, welches Objekt als das gültige angesehen wird. Nun wird nämlich der GUID des ausgehenden Servers betrachtet. Da GUIDS nicht gleich sein können, wird das Objekt vom Server mit der höheren GUID übernommen. Das nicht übernommene Objekt wird jedoch nicht gelöscht, sondern darf seinen Namen behalten, bekommt aber von Active Directory automatisch einen neuen eindeutigen GUID zugewiesen. Damit ist eine Koexistenz der beiden Objekte gewährleistet.

Anlegen eines Objekts in einem nicht mehr vorhandenen Container

Dieses Phänomen kann auftreten, wenn Sie eine neue Benutzergruppe in einer Organisationseinheit erstellt haben. Nach der Replikation der Domänencontroller stellen Sie fest, dass sowohl die eben erstellte Gruppe als auch die Organisationseinheit nicht mehr vorhanden sind. Allerdings ist diese Situation nun wirklich nicht die Regel, aber dennoch sollte man auch für diesen Fall gewappnet sein.

Stellen Sie sich vor, Sie haben an zwei verschiedenen Standorten zwei Administratoren. Am ersten Standort ist der Administrator damit beschäftigt, neue Gruppen in einer bestimmten Organisationseinheit zu erstellen. Jedoch hat zuvor ein anderer Administrator am anderen Standort genau diese Organisationseinheit innerhalb desselben Replikationsintervalls vollständig gelöscht. Wenn Active Directory nun diese beiden Änderungen replizieren will, so trifft er auf das Problem, dass gleichzeitig der Container der Organisationseinheit gelöscht, aber in diesem Container der Organisationseinheit neue Objekte, sprich die Benutzergruppen, angelegt werden sollen. Diese Situation kann auch

mit neu erstellten Benutzerkonten eintreten, wenn die Zieldomäne auf einem anderen Domänencontroller entfernt wurde, aber diese Änderungen noch nicht repliziert wurden.

Active Directory wendet in diesem Fall ein spezielles Verfahren an. Die neuen Benutzergruppen werden erstellt, obwohl ihr ursprünglich zugewiesener übergeordneter Container entfernt ist. Somit muss für diese Benutzergruppen ein neuer Container gesucht werden, wo sie erstellt werden können. Diesen bietet Active Directory in Form des Containers LOSTANDFOUND. Diesen Container finden Sie in den erweiterten Ansichtsoptionen der mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER. Aktivieren Sie dazu im Menü ANSICHT die Option ERWEITERTE FUNKTIONEN. Um die darin enthaltenen Objekte in einen anderen Container zu schieben, in unserem Beispiel also die Benutzergruppen in eine andere Organisationseinheit, wählen Sie aus dem Kontextmenü des verlorenen Objekts VERSCHIEBEN und wählen dann das neue Ziel.

Machen Sie jedoch nicht den Fehler, den Ordner LOSTANDFOUND mit einem herkömmlichen Windows-Papierkorb zu verwechseln. In diesem speziellen Ordner werden nicht die Objekte aufbewahrt, die Sie über den Kontextmenüeintrag LÖSCHEN entfernen. Diese Objekte sind endgültig gelöscht. Dieser Ordner enthält lediglich die Objekte, die aufgrund eines fehlenden Zielcontainers nicht erstellt werden konnten.

Gleichzeitige Änderung gleicher Objekteigenschaften

Angenommen, zwei Administratoren haben unabhängig voneinander die gleiche Objekteigenschaft bearbeitet und mit verschiedenen Werten versehen. In diesem Fall läuft der Prüfungs- und Entscheidungsprozess ähnlich ab wie nach dem Erstellen zweier gleichnamiger Objekte. Auch hier werden der Reihe nach die Versionsnummer, der Zeitstempel sowie der GUID des ausgebenden Servers verglichen. Es wird die Eigenschaft übernommen, die an der ersten Prüfstelle den höheren Wert besitzt. Jedoch geht die Objekteigenschaft mit dem kleineren Wert unwiederbringlich verloren, da nicht zwei gleiche Objekteigenschaften mit verschiedenen Werten existieren können.

Was tun, wenn die Konflikte repliziert werden?

Stellen Sie sich dazu das folgende Szenario vor: Sie verfügen über drei Domänencontroller DC 1 bis 3. Während der Replikation werden in folgender Weise Konflikte festgestellt: Zunächst erhält DC 1 von DC 2 Änderungen übermittelt. Diese Aktualisierungen führen noch zu keinen Konflikten. Dann aber fordert DC 1 auch die Änderungen von DC 3 an. Beim Verarbeiten dieser Informationen wird ein Konflikt zwischen den bereits empfangenen Änderungen von DC 2 und den aktuell verarbeiteten von DC 3 festgestellt. Zur Lösung des Konflikts werden die in den vorangegangenen Absätzen beschriebenen Methoden verwendet. Gehen wir in unserem Beispiel davon aus, dass die Änderungen von DC 3 für neuer erachtet wurden als die von DC 2. So sind nach Abschluss der Replikation mit DC 3 zwar DC 1 und DC 3 auf demselben Stand und haben keine konfliktbehafteten Einträge mehr, jedoch muss nun noch DC 2 die Änderungen von DC 3 erhalten und übernehmen. DC 2 kann diese Aktualisierungen aber auch von DC 1 empfangen, da dort die korrigierten Einträge von DC 3 enthalten sind. DC 2 findet dieselben Konflikte zwischen sich und DC 1 bzw. DC 3, wie sie ursprünglich zwischen DC 1 und DC 3 aufgetreten sind. DC 2 löst die Konflikte und übernimmt dabei die Einträge von DC 1 bzw. 3. Damit sind alle Konflikte behoben, und die Active Directory-Datenbank ist wieder konsistent.

Besonders häufig kann es zu den eben aufgeführten Konflikten führen, wenn ein Domänencontroller über einen langen Zeitraum vom Netzwerk getrennt war. Je länger er keine Replikation durchgeführt hat, desto höher ist die Wahrscheinlichkeit, dass in der Zwischenzeit Änderungen vorgenommen wurden, die mit den veralteten Daten in Konflikt stehen werden.

17.3.2 Replikationsprobleme mit DNSLint beheben

Microsoft stellt das kostenlose Tool DNSLint zur Verfügung, mit dem neben weiteren DNS-Tests speziell auch DNS-Probleme im Active Directory überprüft werden können. DNSLint kann unter folgender Adresse heruntergeladen werden:

http://www.microsoft.com/serviceproviders/downloads/dnslint_P123867.asp

Dort finden Sie auch eine Übersicht über alle verfügbaren Parameter des Programms.

Mit dem Kommandozeilenprogramm DNSLint können Sie für jeden Domänencontroller im Active Directory prüfen, ob die DNS-Datensätze aufgelöst werden können, die für die Replikation benötigt werden. Alle nicht auflösbaren Datensätze werden anschließend von DNSLint aufgelistet. Weiterhin werden sämtliche für die Active Directory-Struktur autorisierenden DNS-Server daraufhin überprüft, ob sie tatsächlich über alle Datensätze verfügen, die für die Replikation erforderlich sind. Für jeden einzelnen autorisierenden DNS-Server werden die fehlenden Datensätze einzeln aufgelistet.

Im Folgenden werden die DNS-spezifischen Schritte aufgelistet, die bei der Replikation zwischen zwei Domänencontrollern durchgeführt werden. Einem Domänencontroller sind lediglich die Namen der Replikationspartner bekannt. Nach einem dieser Namen durchsucht er das Active Directory und findet dort die eindeutige GUID des Replikationspartners, nicht jedoch dessen IP-Adresse. Um die IP-Adresse zu ermitteln, stellt der Domänencontroller eine rekursive Anfrage nach einem CNAME-Eintrag an den lokalen DNS-Server. Dieser Eintrag liegt in dem Format `BEKANNTE GUID._MSDCS.FIRMA.DE` vor, wobei *firma.de* durch den Stamm der jeweiligen Active Directory-Struktur zu ersetzen ist. Der DNS-Server sollte auf die Abfrage hin den Aliasnamen des Domänencontrollers, also etwa *hippokrates.firma.de* ausgeben.

Sobald der Domänencontroller diesen Aliasnamen erhalten hat, schickt er wiederum eine rekursive Abfrage nach dem Hosteintrag für den Aliasnamen an seinen DNS-Server. Der DNS-Server übermittelt dem Domänencontroller die zugehörige IP-Adresse. Damit kann der Domänencontroller eine Verbindung zum Replikationspartner herstellen.

Funktioniert dieser Vorgang nicht, kann keine Replikation durchgeführt werden. Zur Fehlersuche setzen Sie DNSLint ein, sodass Sie herausfinden können, ob sich alle benötigten DNS-Datensätze an der korrekten Stelle befinden. Verwenden Sie dazu den Befehl

```
dnslint /ad 172.20.20.177 /s 172.20.20.1 
```

Der Parameter `/ad` gibt die IP-Adresse eines Domänencontrollers an, mit `/s` wird die IP-Adresse des autorisierenden DNS-Servers für die Zone `_msdcs.firma.de` angegeben. Mit diesem Befehl wird auf dem Domänencontroller 172.20.20.177 das Active Directory nach sämtlichen GUIDs innerhalb der Gesamtstruktur abgefragt. Genauer gesagt werden die Inhalte des Containers `CN=NTDS Settings,CN=Sites,CN=Configuration,DC=firma,dc=de` geprüft. Wird vom Domänencontroller eine Auflistung von GUIDs zurückgesendet, so

sendet DNSLint die entsprechende DNS-Abfrage an den DNS-Server, der unter /s angegeben ist. Ist der DNS-Server nicht autorisierend, werden keine DNS-Datensätze für die GUIDs gefunden. DNSLint stellt dann Anfragen an weitere für den Domänenstamm autorisierende DNS-Server. Wie bei einer herkömmlichen Replikationsanfrage wird der CNAME-Eintrag abgefragt sowie der zugehörige Aliasname. Am Ende erstellt DNSLint einen Bericht im HTML- oder Textformat. Dort sind sämtliche GUIDs, die für den Stamm autorisierenden DNS-Server sowie die Ergebnisse der CNAME- und Aliasnamen-Abfragen enthalten. Zudem wird angegeben, ob und, wenn ja, welche CNAME und Aliasnamen-Einträge auf welchem DNS-Server fehlen.

17.3.3 Fehlerbehebung bei der Replikation

Hier werden Ihnen einige Hilfestellungen gegeben, was zu tun ist, wenn die Replikation entweder gar nicht oder nur sehr verlangsamt stattfindet.

1. Die Replikation zwischen zwei Standorten findet nicht statt.
 - ▶ Prüfen Sie, ob Sie für die betreffenden Standorte Standortverknüpfungen eingerichtet haben. Ohne diese Verknüpfungen können die Domänencontroller nicht miteinander kommunizieren und somit auch keine Replikationsdaten austauschen. Erstellen Sie also neue Standortverknüpfungen zwischen dem aktuellen Standort und bereits verbundenen Standorten. Sollten noch gar keine Standorte verbunden sein, müssen Sie diesen Schritt jetzt komplett nachholen.
2. Die Replikation sowie weiterer Netzwerkverkehr ist deutlich langsamer geworden, findet aber noch statt.
 - ▶ Prüfen Sie zunächst, ob die vorhandenen Netzwerkressourcen dem Replikationsverkehr durch Active Directory noch gewachsen sind. Um die Netzwerkressourcen zu entlasten, können Sie das Replikationsintervall herabsetzen. Dadurch wird aber auch die Aktualität Ihrer Daten herabgesetzt.
 - ▶ Die standortinterne Replikation findet wie erwartet statt, aber die Domänencontroller an anderen Standorten erhalten zu selten die Aktualisierungen. In diesem Fall sollten Sie das Replikationsintervall erhöhen. Prüfen Sie außerdem, ob die Verbindung über eine Standortverknüpfungsbrücke hergestellt wird. Ist dies der Fall, stellen Sie in den darüber gebrückten Verknüpfungen fest, welche der Verknüpfungen das längste Replikationsintervall und die geringste Replikationsverfügbarkeit besitzt. Ändern Sie diese Werte, bis Sie ein zufrieden stellendes Ergebnis haben.
 - ▶ Prüfen Sie, ob die kostengünstige schnelle Verbindung, die Sie als Primärverbindung eingerichtet haben, möglicherweise ausgefallen ist. In diesem Fall würde Active Directory eine langsamere Verbindung benutzen, sofern Sie eine redundante Verbindung eingerichtet haben.
 - ▶ Clients müssen lange auf die Bestätigung der Authentifizierung und auf andere Verzeichnisinformationen von einem Domänencontroller warten. Überprüfen Sie, zu welchem Subnetz der betreffende Client gehört und ob dafür ein besserer Standort als der aktuelle vorhanden ist. Baut der Client seine Verbindung zum Domänencontroller über eine langsame WAN-Verbindung auf, sollten Sie darüber nachdenken, für diese Clients einen eigenen Standort mit einem eigenen Domänencontroller einzurichten.

17.3.4 FRS-Fehler im Ereignisprotokoll

In diesem Kapitel werden Ihnen die häufigsten Fehler des File Replication Service (FRS) mit ihren IDs im Ereignisprotokoll vorgestellt.

Weitere Informationen zu den IDs im Ereignisprotokoll – und zwar zu sämtlichen Quellen – finden Sie auf der Website www.eventid.net.

Ereignis-ID 13508

Die ID 13508 besagt, dass der Replikationsdienst eine RPC-Verbindung zu einem Replikationspartner nicht herstellen konnte. Das Wiederherstellen der Verbindung wird jedoch weiterhin versucht. Die Informationen zur Replikationstopologie bezieht FRS grundsätzlich vom nächstgelegenen Domänencontroller am Standort. Replikationspartner innerhalb eines Standortes replizieren sich standardmäßig alle fünf Minuten, Replikationspartner an zwei verschiedenen Standorten frühestens nach 15 Minuten. Findet sich im Ereignisprotokoll auch die ID 13509, so müssen Sie keine weiteren Schritte unternehmen, da 13509 besagt, dass das Problem behoben wurde.

Um das Problem zu beheben, überprüfen Sie auf dem im Ereignisprotokoll angegebenen Domänencontroller, ob dort der Dateireplikationsdienst korrekt ausgeführt wird. Verwenden Sie hierzu das Kommandozeilen-Programm `ntfrsutl`. Dieses ist Bestandteil des Windows 2000 Resource Kit. Geben Sie an der Eingabeaufforderung den Befehl `Ntfrsutl version <Vollqualifizierter Name des Remote-DCs>`  ein.

Schlägt dieser Versuch fehl, überprüfen Sie zunächst, ob der Remote-Domänencontroller per Ping erreichbar ist, und verifizieren dann die DNS-Einstellungen. Sobald Sie den Domänencontroller netzwerktechnisch erreichen können, stellen Sie sicher, dass auf diesem der Dateireplikationsdienst läuft und nicht angehalten wurde. Prüfen Sie dann, ob beispielsweise ein umkonfigurierter Router oder eine Firewall die RPC-Verbindung blockiert.

Ereignis-ID 13511

Diese ID besagt, dass für die FRS-Datenbank kein weiterer Speicherplatz zur Verfügung steht. Versuchen Sie zunächst, auf dem Laufwerk der Datenbank nicht mehr benötigte Dateien zu löschen. Andernfalls müssen Sie die Datenbank auf eine andere Partition oder einen anderen Datenträger verschieben. Die zu verschiebenden Daten sind zum einen die `Ntfrs.jdb` Jet-Datenbank sowie eine Reihe von Logdateien. Nach dem Verschieben sind Änderungen an der Registry notwendig.

Um die Datenbank zu verschieben, führen Sie die folgenden Schritte aus:

1. Beenden Sie den Dateireplikationsdienst mit dem Befehl `net stop ntfrs` .
2. Kopieren Sie den NTFRS-Ordner aus `%SYSTEMROOT%\NTFRS` an die gewünschte Stelle.
3. Tragen Sie den neuen Pfad in die Registry ein. Hierzu öffnen Sie den Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters` und editieren den Schlüssel `WORKING DIRECTORY`. Selbst wenn Sie lediglich das Arbeitsverzeichnis ändern und nicht den NTFRS-Ordner verschieben, wird die Ordnerstruktur beim Starten des Dateireplikationsdienstes automatisch an der neuen Lokation angelegt.
4. Überprüfen Sie die Berechtigungen für den Ordner NTFRS sowie dessen Unterordner. Für das Administrator- sowie Systemkonto muss Vollzugriff für sämtliche Ordner und Dateien bestehen.

5. Starten Sie dann wieder den Dateireplikationsdienst mit dem Befehl `net start ntfrs` .

Ereignis-ID 13522

Diese ID besagt, dass für die Staging Area kein Speicherplatz mehr zur Verfügung steht. In der Staging Area werden die geänderten Dateien gespeichert, die bei der nächsten Replikation an die Replikationspartner weitergegeben werden sollen oder während der letzten Replikation empfangen worden sind. Ein möglicher Grund könnte darin bestehen, dass die Replikationspartner die geänderten Daten nicht verarbeiten. Prüfen Sie, warum die Replikation nicht durchgeführt werden kann. Möglicherweise wurden auch so viele Änderungen vorgenommen, dass diese innerhalb eines oder mehrerer Replikationsintervalle nicht verarbeitet werden können. Weitere Hinweise finden Sie unter der Ereignis-ID 13567.

Verwenden Sie Windows 2000 SP3 oder höher, so müssen Sie die Staging Area manuell löschen. Unter Windows 2000 SP2 und früher wird die Replikation automatisch fortgesetzt, sobald wieder Speicherplatz für die Staging Area zur Verfügung steht.

Ereignis-ID 13526

Diese ID gibt an, dass ein Domänencontroller nicht mehr erreichbar ist. Standardmäßig wird alle fünf Minuten vom FRS eine Abfrage ans Active Directory gesendet, um die FRS-Konfigurationsinformationen auszulesen. Dabei wird die SID (Security Identifier) eines Replikationspartners aufgelöst. Ist der Domänencontroller nicht erreichbar, kann die entsprechende Bindung nicht durchgeführt werden. Als Abhilfe müssen Sie den Dateireplikationsdienst auf dem Server, der die ID protokolliert hat, beenden und wieder neu starten.

Ereignis-ID 13548

Diese ID wird ausgegeben, wenn die Zeiteinstellungen zweier Replikationspartner um mehr als eine halbe Stunde voneinander abweichen. Prüfen Sie zunächst, ob auf einem der Replikationspartner eine falsche Zeitzone eingestellt ist, sodass eine dermaßen große Abweichung auftritt. Ist dies nicht der Fall, müssen Sie die Systemzeit auf den Replikationspartnern synchronisieren.

Ereignis-ID 13557

Diese Ereignis-ID gibt an, dass zwischen zwei Replikationspartnern doppelte Verbindungen ermittelt worden sind. Die betroffenen Verbindungsobjekte werden aufgelistet, sodass Sie das überflüssige Verbindungsobjekt löschen können.

Ereignis-ID 13567

Diese Ereignis-ID wird auf Domänencontrollern ausgegeben, die Windows 2000 SP3 oder höher verwenden, sobald vom Dateireplikationsdienst exzessive unnötige Änderungen an Dateien entdeckt werden. Dabei wird eine Datei von einer Applikation oder einem Benutzer neu geschrieben, ohne dass an ihr Änderungen durchgeführt worden sind. Die Datei wird also von einer gleichnamigen Kopie und identischen Zugriffsberechtigungen überschrieben. FRS prüft, ob diese Änderungen häufiger als 15 Mal pro Stunde auftreten. Ist dies der Fall, wird die Ereignis-ID 13567 ins Ereignisprotokoll geschrieben.

Finden Sie also heraus, welche Applikation diese ungewünschten Änderungen an den Dateien vornimmt. Um die identischen Dateien zur Replikation zu zwingen, müssen Sie die Registry bearbeiten. Öffnen Sie den Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters` und erstellen dort den Schlüssel `SUPPRESS IDENTICAL UPDATES TO FILES` mit dem Wert 0 bzw. ändern diesen von der Standardeinstellung 1 auf 0 ab.

Ereignis-ID 13568

Diese ID wird bei Problemen im Zusammenhang mit dem NTFS Journal ausgegeben. NTFS besitzt eine spezielle Datei namens NTFS USN-JOURNAL. In diesem Journal befindet sich eine Liste aller Änderungen an Dateien und Verzeichnissen der NTFS-Partition. Der Dateireplikationsdienst benutzt dieses Journal, um relevante Änderungen auszulesen, die an die Replikationspartner repliziert werden müssen. Die Größe des Journals ist fest vorgegeben. Die Maximalgröße unter Windows 2000 mit SP2 und früher liegt bei 128 MB, die Standardgröße bei 32 MB. Unter Windows 2000 SP3 und höher liegt die Standardgröße bei 128 MB und die Maximalgröße bei 10 GB. Der entsprechende Wert wird in der Registry im Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters` unter `NTFS JOURNAL SIZE IN MB` angegeben. Wenn Sie die Größe bereits heraufgesetzt haben, sollten Sie diesen Wert später nicht wieder minimieren. Jede Dateiänderung belegt im Journal ungefähr 100 Byte. Ältere Einträge im Journal werden durch neuere überschrieben.

Sind dabei Einträge, die vom FRS noch benötigt werden, bereits überschrieben, wird die Journal Wrap Condition eingeleitet. Dabei wird vom Dateireplikationsdienst der aktuelle Replikationsstatus in Hinblick auf die Replikationspartner sowie NTFS neu geordnet. Dieser Vorgang wird auch eingeleitet, wenn Sie die Größe des Journals auf einen niedrigeren Wert herabsetzen oder komplett löschen. Die Journal Wrap Condition kann aber auch aus mehreren anderen Gründen vom Dateireplikationsdienst eingeleitet werden.

- ▶ Auf dem NTFS-Datenträger wurden von Checkdisk Fehler am Dateisystem behoben. Dabei wird ein neues NTFS-Journal geschrieben, und korrupte Einträge werden gelöscht.
- ▶ Eine große Anzahl an Dateien wurde der Replik hinzugefügt, während der Dateireplikationsdienst nicht verfügbar oder ausgelastet war.
- ▶ Der Dateireplikationsdienst wird nicht fehlerfrei ausgeführt, sodass keine Änderungen im NTFS-Journal verarbeitet werden können.

Die Replikation auf dem betroffenen Domänencontroller kann erst fortgesetzt werden, wenn die Journal Wrap Condition nicht mehr besteht. Hierzu müssen Sie den Replikationsdienst beenden und auf dem Domänencontroller eine nicht autorisierende Wiederherstellung (siehe Kapitel 21.7.1) durchführen.



Die autorisierende Wiederherstellung (siehe Kapitel 21.7.2) wird lediglich auf Windows 2000 Server mit SP2 automatisch durchgeführt. Unter Windows 2000 Server mit SP1, SP3 und SP4 müssen Sie die autorisierende Wiederherstellung manuell durchführen. Wollen Sie auch unter SP3 die automatische autorisierende Wiederherstellung ermöglichen, so öffnen Sie in der Registry den Schlüssel `HKEY_LOCAL_MACHINE\System\Ccs\Services\Ntfrs\Parameters` und setzen dort den Schlüssel `ENABLE JOURNAL WRAP AUTOMATIC RESTORE` auf den Wert 1.

18 Benutzer, Gruppen und Profile

Nachdem Sie in den vorangegangenen Kapiteln erfahren haben, wie Sie Domäne, Standorte und Organisationseinheiten anlegen, ist es nun an der Zeit, diese Strukturelemente mit Leben zu füllen, d.h. Benutzer- und Gruppen- sowie Computerkonten anzulegen und zu konfigurieren. In diesem Kapitel lernen Sie neben dem Erstellen der eben genannten Objekte Grundlagen von Benutzer- und Gruppenkonten kennen. Ebenfalls werden routinemäßige Aufgaben an den Konten, wie z.B. das (De-)Aktivieren oder (Ent-)Sperren von Konten vorgeführt. Auch die Einrichtung von Benutzerprofilen sowie die Zuordnung von Basisverzeichnissen zu Benutzern wird erläutert. Außerdem erhalten Sie Hinweise zum Schutz des Administratorkontos.

18.1 Arten von Benutzerkonten

In diesem Kapitel werden Ihnen zunächst nur die verschiedenen Arten von Benutzerkonten vorgestellt. Gruppenkonten werden gesondert in Kapitel 18.4 vorgestellt. Mehrere Benutzerkonten mit ähnlichen Aufgaben und Berechtigungen können zu einem Gruppenkonto zusammengefasst werden. Über ein Benutzerkonto bekommt der betreffende Benutzer die Möglichkeit, sich entweder lokal oder an einer Domäne zu authentifizieren und danach auf Daten zuzugreifen. Hierbei wird unterschieden, ob es sich bei dem Konto um ein Domänenbenutzerkonto, um ein lokales Konto oder um ein integriertes Konto handelt. Diese Arten von Konten werden Ihnen im Folgenden vorgestellt.

18.1.1 Domänenbenutzerkonten

Mit einem Domänenbenutzerkonto authentifiziert sich der Benutzer gegenüber einem Domänencontroller und bekommt damit Zugriff auf alle Ressourcen des Netzwerks, für die ihm die entsprechenden Rechte erteilt worden sind. Bei der erfolgreichen Authentifizierung erhält er einen Zugriffstoken mit seiner Benutzer- und Sicherheitskonfiguration. Mit diesem Token kann er sich an allen Windows NT, 2000, 2003 und XP-Computern identifizieren.

Neue Benutzerkonten werden in der Active Directory-Datenbank entweder direkt in einer Domäne oder in einer Organisationseinheit erstellt. Dieser Vorgang wird im nächsten Kapitel erläutert. Durch die Replikation des Konteneintrags kann sich der Benutzer von allen Clientcomputern in der Domäne an sämtlichen Domänencontrollern anmelden.

18.1.2 Lokale Benutzerkonten

Mit einem lokalen Benutzerkonto hingegen kann sich der Benutzer nur lokal an seinem Rechner identifizieren, auf dem das lokale Konto eingerichtet wurde. Er erhält damit nur Zugriff auf die Daten des lokalen Rechners. Die Sicherheitsinformationen zu einem loka-

len Konto werden in der lokalen Sicherheitsdatenbank gespeichert. Damit können diese Konten auch nicht repliziert werden. Für den Netzwerkzugriff ist eine gesonderte Anmeldung erforderlich. Lokale Benutzerkonten werden in Arbeitsgruppen eingesetzt. Sie können die lokal erstellten Benutzerkonten nicht in der Domäne verwenden. Um die lokalen Konten vom Domänenadministrator aus zu verwalten und Ressourcen zuzuweisen, muss er für jedes lokale Konto gesondert über **COMPUTERVERWALTUNG / VORGANG / VERBINDUNG ZU ANDEREM COMPUTER HERSTELLEN** eine Verbindung zu diesem Computer herstellen. Dazu müssen ihm die lokalen Kennwörter bekannt sein, da er sich mit seiner Domänen-Admin-Kennung natürlich nicht an einem lokalen Rechner außerhalb der Domäne anmelden kann.

18.1.3 Integrierte Benutzerkonten

Als Drittes gibt es die fest in Windows 2000 integrierten Benutzerkonten. Diese werden automatisch erstellt und können nicht gelöscht, sondern nur umbenannt oder deaktiviert werden. Dabei handelt es sich um die folgenden Konten Administrator und Gast.

Das Administratorkonto ist das Standardkonto für alle anfallenden Verwaltungsaufgaben auf dem Domänencontroller. Jeder Administrator sollte außerdem über ein alternatives zweites Konto verfügen, in dem er nicht über alle Rechte verfügt. Das echte Administratorkonto sollte nur benutzt werden, wenn die Rechte wirklich benötigt werden. Weitere Hinweise zum Administratorkonto finden Sie in Kapitel 18.6.

Das zweite integrierte Benutzerkonto ist das Gast-Konto. Dieses ist standardmäßig deaktiviert. Es verfügt nur über sehr eingeschränkte Berechtigungen und ist für Benutzer gedacht, die nur kurzzeitig auf die Netzwerkressourcen zugreifen müssen. Sobald das Konto aktiviert ist, sollte es immer mit einem Passwort versehen werden, um unberechtigtem Zugriff vorzubeugen.

Auf einem Windows 2000/2003 Server können auch noch drei weitere integrierte Benutzerkonten vorhanden sein, wenn weitere Windows-Komponenten installiert werden. Genaue Informationen entnehmen Sie in Tabelle 18.1.

Kontoname	Beschreibung
TsInternetUser	Dieses Konto wird erstellt, wenn die Terminaldienste installiert werden. Es handelt sich um das Dienstkonto der Terminaldienste.
IUSR_Computername	Hierzu muss der Internet Information Server (IIS) installiert sein. Dies ist das Konto für den anonymen Zugriff auf den IIS.
IWAM_Computername	Auch hierfür muss zunächst der IIS installiert sein. Von diesem Konto aus wird anonym auf prozessexterne IIS-Anwendungen zugegriffen.

Tabelle 18.1: Weitere integrierte Benutzerkonten

Alle integrierten Benutzerkonten finden Sie in der mmc **ACTIVE DIRECTORY-BENUTZER UND -COMPUTER** im Container **USERS**.

18.1.4 Das Zusammenspiel zwischen einer Domäne und Arbeitsgruppe

Für den Ressourcenzugriff ist es immer vorzuziehen, sämtliche Benutzer und Ressourcen wie Netzlaufwerke oder Drucker gemeinsam in eine Domäne zu bringen und nicht einzelne Ressourcen in einer Arbeitsgruppe zu belassen. Angenommen, Sie haben in einer Arbeitsgruppe unter Windows NT 4.0 freigegebene Ressourcen, z.B. Netzwerkdrucker, die von den Benutzern der Domäne benutzt werden sollen. Die Benutzung ist zwar theoretisch möglich, jedoch sehr aufwändig in der Administration.

So müssen Sie zunächst sämtliche Benutzer der Domäne, die auf die Drucker zugreifen sollen, auf dem Windows NT-Rechner als lokale Benutzer anlegen. Dabei müssen Sie denselben Anmeldenamen und vor allen Dingen auch dasselbe Passwort angeben, das für die Anmeldung an der Domäne verwendet wird. Hier beginnt jedoch schon das Problem: Der Administrator der Windows NT-Arbeitsgruppe muss sämtliche Kennwörter der Domänenbenutzer kennen. Dies dürfte aber in den meisten Fällen ein zu hohes Sicherheitsrisiko darstellen. Und sobald ein Domänenbenutzer sein Kennwort geändert hat, kann er nicht auf die Drucker zugreifen, bis der NT-Administrator das Benutzer-Passwort lokal aktualisiert hat. Da der Windows NT-Rechner lediglich Mitglied einer Arbeitsgruppe ist, besteht auch keine Möglichkeit, dass er mit dem Domänencontroller eine Vertrauensstellung eingeht. Somit ist es auch nicht möglich, eine globale Benutzergruppe der Domäne dem lokalen Rechner hinzuzufügen.

18.2 Einrichten von Benutzerkonten

Nachdem Sie im letzten Kapitel die verschiedenen Arten von Konten kennen gelernt haben, werden nun neue Konten erstellt und konfiguriert. Der Schwerpunkt liegt auf der Beschreibung der Domänenbenutzerkonten. Auf die Unterschiede zu den Einstellungen für ein lokales Konto wird an den betreffenden Stellen hingewiesen.

18.2.1 Einrichten von Benutzerkonten

Hier werden Sie nun Schritt für Schritt durch die Erstellung eines neuen Domänenbenutzerkontos geleitet. Von der Namensvergabe über Passwortooptionen bis zur Verfügbarkeit der Anmeldezeiten werden Ihnen alle Kontoeigenschaften vorgestellt.

Neue Domänenbenutzerkonten werden über die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER eingerichtet, lokale Konten am betreffenden Rechner über COMPUTER-VERWALTUNG/LOKALE BENUTZER UND GRUPPEN. Dieser Knoten ist in der Computerverwaltung eines Domänencontrollers zwar vorhanden, aber gesperrt, da auf einem Domänencontroller keine lokalen Konten erstellt werden können.

Um ein Domänenbenutzerkonto anzulegen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER. Sie können dort den Benutzer entweder im vorgegebenen Container USERS erstellen, im Container eines Standorts oder direkt unter der Domäne. Wählen Sie aus dem Kontextmenü des gewählten übergeordneten Objekts den Eintrag NEU/BENUTZER.

- Geben Sie zunächst die persönlichen Daten eines Benutzers an. Dazu zählen der Vor- und Nachname, aus denen sich der vollständige Name ergibt, sowie die Initialen. Zusätzlich geben Sie den Anmeldenamen für Windows 2000- und Windows NT-Domänen an (siehe Abbildung 18.1).

Abbildung 18.1: Anlegen eines Domänenbenutzerkontos

In diesem Zusammenhang werden nun die Namensanforderungen erläutert, die Sie bei der Namensvergabe bedenken sollten und müssen.

Ein Eintrag in die beiden Felder VORNAME und NACHNAME ist zwingend erforderlich. Aus diesen Eingaben setzt sich automatisch der vollständige Name zusammen. Der vollständige Name (Kontoname), also der relativ definierte Name (RDN), muss in dem Container eindeutig sein, in der der Benutzer erstellt wird. In welchem Container der neue Benutzer angelegt wird, sehen Sie im oberen Bereich des Fensters. In unserem Beispiel wird der Benutzer im Container firma.de/Users angelegt.

Für ein Domänenbenutzerkonto muss der Benutzeranmeldename im gesamten Verzeichnis eindeutig sein. Bei einem lokalen Konto muss der Anmeldename auf dem Computer eindeutig sein. Denken Sie sich eine bestimmte Konvention aus, nach der Sie die Anmeldenamen vergeben. Sie können sowohl den vollständigen Namen als auch beispielsweise den ersten Buchstaben des Vornamens und den kompletten Nachnamen oder auch den kompletten Vornamen und einen Teil des Nachnamens benutzen. Hierbei sind Sie frei in Ihrer Entscheidung. Die Groß- und Kleinschreibung wird bei der Angabe des Benutzernamens ignoriert. Außerdem dürfen die folgenden Sonderzeichen nicht im Benutzeranmeldenenamen enthalten sein: < > [] / \ : ; , , ? | + * =. Die Länge des Anmeldenamens ist nicht begrenzt. Allerdings werden von Windows nur die ersten 20 Zeichen gelesen und verarbeitet.

Sollten in Ihrem Unternehmen mehrere Benutzer mit demselben Namen arbeiten, so können Sie den Namen in den Feldern VORNAME und ZUNAME wie gewohnt eintragen. Lediglich für den Anmeldenamen müssen Sie sich ein System ausdenken, wie Sie gleichnamige Mitarbeiter unterscheiden. Eine Möglichkeit wäre es, an den jewei-

ligen Benutzernamen eine Zahl anzuhängen. In unserem Beispiel hätten wir dann einen pmustermann1 und einen pmustermann2.

Bei der Einrichtung eines lokalen Benutzers werden Sie nur nach dem Vor- und Nachnamen gefragt und können optional eine Beschreibung eingeben.

3. Haben Sie alle Namenseinstellungen vorgenommen, klicken Sie auf WEITER. Nun werden die Kennwortoptionen eingestellt (siehe Abbildung 18.2).

Abbildung 18.2: Das Einrichten der Kennwortoptionen

Die folgenden Hinweise zu Kennwörtern sollten oder müssen Sie beachten. Grundsätzlich sollten Sie jedem Konto ein Kennwort zuweisen. Selbst wenn ein Benutzer sein Kennwort vergessen sollte, kann der Administrator das Passwort jederzeit zurücksetzen. Das Passwort darf nicht Teile des Benutzernamens enthalten oder diesem entsprechen. Ebenfalls sollten keine leicht zu erratenen Passwörter wie Telefonnummern, Geburtstage oder Namen aus der Familie oder solche, die in anderer Weise leicht mit dem Benutzer in Verbindung zu bringen sind, verwendet werden.

Geben Sie in das Feld KENNWORT ein Kennwort ein, das die folgenden Anforderungen erfüllen sollte:

- Das Kennwort sollte mindestens acht Zeichen lang sein.
- Das Kennwort sollte sich aus verschiedenen Zeichen aus drei der folgenden vier Gruppen zusammensetzen: Großbuchstaben, Kleinbuchstaben, arabische Zahlen und Sonderzeichen, wie z.B. Interpunktionszeichen.

Im Feld KENNWORTBESTÄTIGUNG geben Sie das Passwort erneut ein. Zusätzlich haben Sie vier weitere Kennwortoptionen. Diese werden in der folgenden Tabelle beschrieben.

Kennwortoption	Beschreibung
Benutzer muss Kennwort bei der nächsten Anmeldung ändern	Bei der ersten Anmeldung erhält der Benutzer einen Hinweis, dass er sein Kennwort ändern muss. Damit liegt die Verantwortung für das Kennwort beim Benutzer.
Benutzer kann Kennwort nicht ändern	In diesem Fall kann nur der Administrator das Kennwort ändern. Diese Option ist beispielsweise für das Gast-Konto sinnvoll, da dieses von mehreren Benutzern verwendet werden kann.
Kennwort läuft nie ab	Das Kennwort muss nie, kann aber jederzeit geändert werden.
Konto ist deaktiviert	Das Konto ist zwar eingerichtet, kann aber noch nicht verwendet werden.

Tabelle 18.2: Die Kennwortoptionen für ein Benutzerkonto

Bei der Erstellung eines lokalen Benutzerkontos werden auch Eingaben zum Kennwort verlangt. Sie können hier nur das Passwort eingeben und haben die Optionen BENUTZER MUSS KENNWORT BEI DER NÄCHSTEN ANMELDUNG ÄNDERN sowie KONTO IST DEAKTIVIERT zur Verfügung. Die Kennwortoptionen werden in einem Fenster mit den Benutzerangaben vereinigt.

4. Haben Sie alle Kennwortoptionen für das Domänenbenutzerkonto festgelegt, klicken Sie auf WEITER. Sie erhalten dann eine Zusammenfassung Ihrer Angaben. Klicken Sie dort auf FERTIG STELLEN. Um Änderungen vorzunehmen, können Sie über ZURÜCK bis zur gewünschten Stelle zurückgehen. Dann wird das neue Benutzerobjekt in dem gewählten Container angelegt.

Über das Benutzerkonto kann nun die Authentifizierung an der Domäne erfolgen. Auch die Zugriffssteuerung auf freigegebene Netzwerkressourcen und Überwachungsaufgaben auf Kontenbasis werden über ein Konto durchgeführt.

18.2.2 Eigenschaften von Benutzerkonten

Nachdem Sie nun das neue Benutzerobjekt erstellt haben, finden Sie es in der mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER in dem gewählten Container. Jedes Benutzerkonto verfügt über einen vordefinierten Satz an Eigenschaften, den Sie für jeden Benutzer individuell konfigurieren können. Um auf die Eigenschaften eines Benutzers zuzugreifen, wählen Sie den gleichnamigen Eintrag aus dem Kontextmenü (siehe Abbildung 18.3).

Abbildung 18.3: Die Eigenschaften eines Domänenbenutzerkontos

Die Eigenschaften sind in zwölf Kategorien eingeteilt. Für jede Kategorie steht eine Registerkarte bereit. Ein lokales Benutzerkonto enthält nur drei Registerkarten, nämlich ALLGEMEIN, PROFIL und MITGLIED VON. Die Bedeutung der einzelnen Registerkarten wird in Tabelle 18.3 erläutert. Die wichtigsten dieser Eigenschaften werden im Anschluss detailliert vorgestellt.

Registerkarte	Beschreibung
Allgemein	Hier können Sie den Namen des Benutzers, eine optionale Beschreibung sowie Angaben zu seinem Büro, seiner Telefonnummer, E-Mail-Adresse und Webseite vornehmen. Einträge müssen nur in den Feldern „Vorname“, „Nachname“ und „Anzeigename“ vorhanden sein. Der Rest ist optional.
Adresse	Tragen Sie hier die Adresse (Straße, Postfach, Stadt, Bundesland, PLZ sowie Land/Region) ein. Auch diese Einträge sind optional.
Konto	Sie finden hier den Benutzeranmeldenamen sowie weitere Optionen zum Benutzerkonto. Diese werden weiter unten gesondert erklärt. Außerdem können Sie die Anmeldezeiten sowie die Liste der Computer, von denen aus sich der Benutzer anmelden darf, begrenzen.
Profil	Hier können Sie den Pfad zu einem Benutzerprofil, ein Anmeldeskript sowie einen Basisordner für Dokumente angeben. Die Profileinstellungen werden separat in Kapitel 18.3 besprochen.
Rufnummern	Hier können Sie zusätzliche Rufnummern des Benutzers angeben (Privat, Funkruf, Mobil, Fax und IP-Telefon).

Registerkarte	Beschreibung
Organisation	Hier können Sie firmenbezogene Angaben wie Anrede, Abteilung, Firma und Vorgesetzter eintragen.
Mitglied von	Hier können Sie festlegen, in welchen Gruppen der Benutzer Mitglied sein soll. Standardmäßig gehört er nur der Gruppe „Domänen-Benutzer“ an. Gruppen werden in Kapitel 18.4 behandelt. Jeder Benutzer hat eine Gruppe als seine primäre Gruppe definiert. Wenn er mehreren Gruppen angehört, können Sie die Einstellung über „Primäre Gruppe festlegen“ ändern.
Einwählen	Hier können Sie die Optionen für RAS-Zugriff konfigurieren. Standardmäßig ist kein RAS-Zugriff erlaubt.
Umgebung	Sie bestimmen hier, ob bei der Anmeldung Netzlaufwerke und Drucker automatisch verbunden werden und welche Programme beim Start der Terminalsitzungen ausgeführt werden sollen.
Sitzungen	Hier werden Optionen für die Terminalsitzungen vorgenommen.
Remoteüberwachung	Hier können Sie die Remote-Überwachung für die Terminalsitzungen aktivieren oder deaktivieren sowie die Benutzererlaubnis zur Überwachung ein- und ausschalten.
Terminalsitzungsprofile	Hier können Sie ein Benutzerprofil und das Basisverzeichnis für die Terminalsitzungen angeben.

Tabelle 18.3: Die Registerkarten der Kontoeigenschaften

Es können bei den Benutzereigenschaften weitere Registerkarten hinzukommen, wenn beispielsweise Komponenten wie Exchange 2000 oder die Services for Unix (SFU) installiert sind.

Die wichtigsten Registerkarten sind KONTO, PROFIL und MITGLIED VON. Die erweiterten Kontooptionen werden jetzt ausführlich beschrieben, die beiden anderen Themen in den Kapiteln 18.3 und 18.4.

Auf der Registerkarte KONTO finden Sie weitere Optionen zu den Kennworteigenschaften. Außerdem können Sie dort die Anmeldezeiten eines Benutzers beschränken und ebenso auch die Computer, von denen aus er sich an der Domäne anmelden darf.

Beginnen wir mit den erweiterten Kennworteigenschaften. Außer den vier bereits bekannten Optionen BENUTZER MUSS KENNWORT BEI DER NÄCHSTEN ANMELDUNG ÄNDERN, BENUTZER KANN DAS KENNWORT NICHT ÄNDERN, KENNWORT LÄUFT NIE AB und KONTO IST DEAKTIVIERT haben Sie hier sechs weitere Optionen. Diese werden in Tabelle 18.4 näher erläutert.

Kennwortoption	Beschreibung
Kennwort mit reversibler Verschlüsselung speichern	Standardmäßig sind die Kennwörter in der Kennwortdatenbank verschlüsselt. Die standardmäßige Verschlüsselung ist nicht umkehrbar. Bei Verwendung der reversiblen Verschlüsselung können Kennwörter aus der Datenbank wiederhergestellt werden. Bei Verwendung der reversiblen Verschlüsselung muss die Passwortdatenbank gut gegen Angriffe von außen abgesichert sein. Für Benutzer eines Apple Macintosh-Clients müssen Sie diese Option aktivieren, da diese Clients ausschließlich mit reversibler Verschlüsselung arbeiten.
Benutzer muss sich mit einer Smartcard anmelden	Der Benutzer muss sich anhand einer Smartcard über ein Kartenlesegerät authentifizieren.
Konto wird für Delegierungszwecke vertraut	Dieser Benutzer hat das Recht, anderen Benutzern oder Gruppen Teile des Domänen-Namensraums zur Verwaltung zu übergeben. Näheres dazu finden Sie in Kapitel 24.1.4).
Konto kann nicht delegiert werden	Diesem Konto kann von keinem anderen Benutzer die Delegierung von Verwaltungsaufgaben übergeben werden.
DES-Verschlüsselungstypen für dieses Konto benutzen	Hiermit können Sie die Unterstützung für DES (Data Encryption Standard) aktivieren. DES unterstützt verschiedene Verschlüsselungsmechanismen, z.B. MPPE 40, 64 und 128 Bit oder IPSec in verschiedenen Stufen.
Keine Kerberos-Präauthentifizierung erforderlich	Aktivieren Sie diese Option nur, wenn für das Konto nicht die Kerberos-Implementierung von Windows 2000 eingesetzt wird, sondern beispielsweise eine Unix-Implementierung, die einen anderen Zeitmechanismus für die Ausgabe des ticket-genehmigenden Tickets durch das KDC (Key Distribution Center) verwendet.

Tabelle 18.4: Erweiterte Kennwortoptionen

Außerdem können Sie festlegen, ob das Konto zu einem bestimmten Zeitpunkt ablaufen soll oder nicht (Letzteres ist Standard). Dies ist sinnvoll, wenn einige Mitarbeiter nur zeitweise beschäftigt sind. Soll das Konto zu einem bestimmten Zeitpunkt ablaufen, markieren Sie die entsprechende Checkbox und wählen aus dem Kalenderelement das gewünschte Datum.

Weiterhin befindet sich auf der Registerkarte KONTO auch die Schaltfläche ANMELDEZEITEN. Darüber können Sie festlegen, wann sich der Benutzer an der Domäne anmelden darf. Standardmäßig kann sich der Benutzer jeden Tag in der Woche rund um die Uhr anmelden. Um die Anmeldezeiten einzuschränken, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf die Schaltfläche ANMELDEZEITEN. Sie sehen, dass die Zeiten nicht eingeschränkt sind.
2. Markieren Sie nun die Zeiten, zu denen eine Anmeldung nicht notwendig ist, und markieren für diese die Checkbox ANMELDUNG VERWEIGERN. In unserem Beispiel (siehe Abbildung 18.4) ist die Anmeldezeit auf werktags von 8:00 h bis 18:00 h beschränkt. Für einen herkömmlichen Büroangestellten sollten diese Zeiten ausreichen.

3. Klicken Sie dann auf OK.

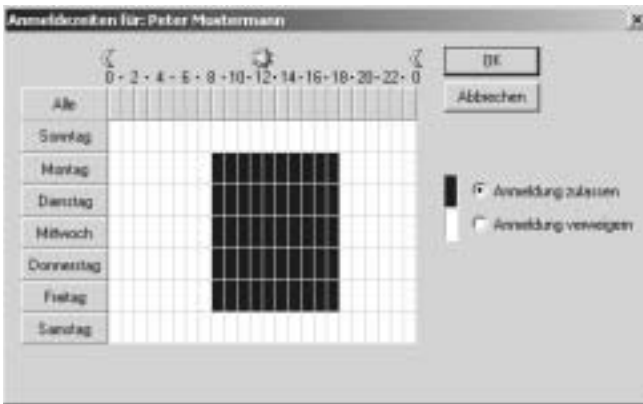


Abbildung 18.4: Festlegen der erlaubten Anmeldezeiten

Über die Schaltfläche ANMELDEN auf der Registerkarte KONTO können Sie bestimmen, von welchen Computern aus sich der Benutzer anmelden darf. Wenn ein Benutzer nur an einem festen Arbeitsplatz oder von seinem Laptop aus arbeitet, können Sie ihm nur diesen Rechner zuweisen. Standardmäßig kann er sich von allen Computern aus anmelden. Um die Anmelderechner einzuschränken, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf die Schaltfläche ANMELDEN. Sie sehen, dass die Option ALLE COMPUTER aktiviert ist.



Abbildung 18.5: Festlegen der erlaubten Anmeldecomputer

2. Um den Anmeldevorgang auf einen oder mehrere Computer zu beschränken, geben Sie in das Textfeld den Namen des Computers ein und klicken auf HINZUFÜGEN (siehe Abbildung 18.5). Wiederholen Sie diesen Prozess, bis Sie alle gewünschten

Rechner in die Liste aufgenommen haben. Um später wieder Rechner aus der Liste zu löschen, markieren Sie die gewünschten Computer und klicken auf ENTFERNEN. Über die Schaltfläche BEARBEITEN können Sie den Namen eines in der Liste vorhandenen Computers ändern.

3. Klicken Sie anschließend auf OK.

Sie können die gültigen Anmeldezeiten nur für alle gültigen Anmelderechner und nicht für jeden dieser Rechner einzeln festlegen.

Bedenken Sie auch Folgendes: Je restriktiver Sie die gültigen Anmeldezeiten und Anmelderechner für die Benutzer handhaben, desto geringer wird auch die Wahrscheinlichkeit, dass ein Konto zu Unrecht benutzt werden kann.

18.2.3 Die tägliche Arbeit mit Benutzerkonten

Zur täglichen Arbeit mit Konten zählen neben dem eben beschriebenen Erstellen und Konfigurieren noch weitere Tätigkeiten. Zu den weiteren administrativen Aufgaben gehören auch das Aktivieren bzw. Deaktivieren von Konten, das Kopieren, Verschieben, Löschen und Umbenennen von Konten sowie das Entsperren von Konten.

Um ein aktives Konto zu deaktivieren oder ein deaktiviertes Konto zu aktivieren, wählen Sie aus dem Kontextmenü des Benutzerkontos den Eintrag KONTO DEAKTIVIEREN bzw. KONTO AKTIVIEREN. Sie sollten ein Konto so lange deaktiviert lassen, bis es benötigt wird. Haben Sie beispielsweise Mitte des Monats bereits die Benutzerkonten für Mitarbeiter eingerichtet, die erst im nächsten Monat ihre Tätigkeit aufnehmen, so sollten diese Konten auch erst am 1. des Folgemonats aktiviert werden, um eventuellen Missbrauch zu verhindern. Deaktivierte Konten sind in der mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER gesondert gekennzeichnet.

Auch für das Kopieren, Verschieben, Löschen und Umbenennen von Konten wählen Sie den jeweiligen Eintrag aus dem Kontextmenü. Sie können ein Konto kopieren, um so die Einstellungen als Vorlage für ein neues Konto benutzen zu können, bei dem Sie nicht wieder alle Einträge neu vornehmen wollen. Sie müssen lediglich den Namen und die Kennwortoptionen neu angeben. Wollen Sie das Benutzerobjekt verschieben, können Sie aus Ihrer Domäne den neuen Container auswählen, in dem das Objekt liegen soll. Das Umbenennen eines Kontos ist sinnvoll, wenn ein neuer Mitarbeiter die Einstellungen seines Vorgängers bis auf den Namen übernehmen soll. Das Löschen von Objekten sollte eigentlich selbsterklärend sein.

Schließlich finden Sie im Kontextmenü noch den Eintrag KENNWORT ZURÜCKSETZEN. Auch wenn Sie bei den Kennwortoptionen die Passwortvergabe durch den Benutzer eingestellt haben (siehe Kapitel 18.2.1), können Sie als Administrator jederzeit das Passwort eines Benutzers zurücksetzen, falls dieser sich sein Kennwort nicht merken kann. Um ein Passwort wieder zurückzusetzen, wählen Sie den oben genannten Eintrag aus dem Kontextmenü, geben das neue Passwort ein und bestätigen es. Sie können auf diese Weise auch ein leeres Passwort vergeben. Teilen Sie dieses vorläufige Passwort dem ausgesperrten Benutzer mit und bitten ihn, sich künftig sein Passwort besser zu merken. Er kann nun, wenn die Option aktiviert ist, das Passwort bei der Anmeldung ändern.

18.2.4 Einrichten von Computerkonten

Nachdem Sie bereits das Erstellen von Benutzerkonten kennen gelernt haben, wird Ihnen nun das Einrichten von Computerkonten nahegebracht. Auch diese werden über die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER erstellt. Sie können einen neuen Computer entweder im vordefinierten Container COMPUTERS oder in jeder beliebigen Organisationseinheit oder direkt unter der Domäne erstellen.

Um einen neuen Computer zu erstellen, führen Sie die folgenden Schritte aus:

1. Wählen Sie an der gewünschten Stelle den Eintrag NEU / COMPUTER aus dem Kontextmenü. Sie erhalten das Fenster NEUES OBJEKT – COMPUTER (siehe Abbildung 18.6).

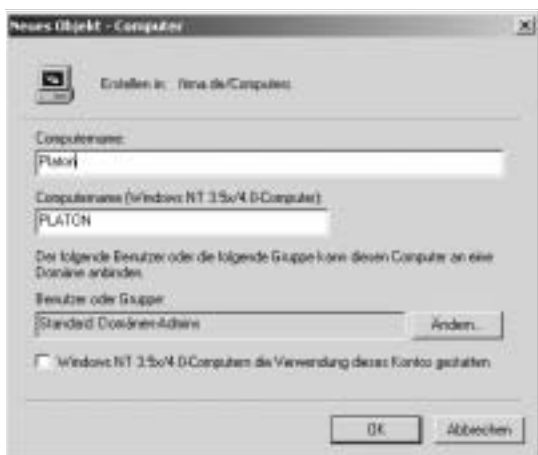


Abbildung 18.6: Einrichten eines Computerkontos

2. Geben Sie den Namen des Computers im Feld COMPUTERTNAME ein. Das Feld für den Windows NT-Computernamen wird dabei automatisch ausgefüllt.
3. Weiterhin können Sie angeben, welcher Benutzer oder welche Gruppe den Computer einer Domäne hinzufügen darf. Standardmäßig darf dies die Gruppe „Domänen-Admins“. Über ÄNDERN können Sie aber auch eine andere Einstellung treffen.
4. Außerdem können Sie festlegen, ob Windows NT-Computern die Verwendung dieses Kontos gestattet ist. Standardmäßig ist dies nicht der Fall. Klicken Sie zum Abschluss der Einstellungen auf OK.

18.2.5 Die tägliche Arbeit mit Computerkonten

Auch für die tägliche Arbeit mit den Computerkonten stehen Ihnen einige Möglichkeiten bereit. Über die Eigenschaften des Computers finden Sie Informationen zu seinem Betriebssystem. Dieser Eintrag erfolgt automatisch beim ersten Anmelden des Computers an der Domäne. Sie können auch die Gruppenmitgliedschaft des Computers (Standard: Domänencomputer) ändern sowie Angaben zu seinem Standort und der Person machen, die ihn verwaltet.

Im Kontextmenü finden Sie noch weitere Einträge, die nun kurz erläutert werden.

1. **KONTO DEAKTIVIEREN:** Hiermit wird das Computerkonto vorübergehend deaktiviert. Sie sollten diesen Schritt ausführen, wenn ein Computer später wieder ins Netzwerk hinzugefügt werden soll. Würden Sie ihn löschen, wären alle Einträge verloren.
2. **KONTO ZURÜCKSETZEN:** Über diese Option wird die Verbindung des Computerkontos zur Domäne getrennt. Der Computer muss anschließend der Domäne erneut beitreten.
3. **VERWALTEN:** Über diesen Punkt können Sie von jedem Rechner in der Domäne die Computerverwaltung aufrufen und die meisten Verwaltungsaufgaben auf dem Remote-Computer durchführen. Das Defragmentierungsprogramm kann jedoch nicht auf einem Remote-Computer gestartet werden. Sie können sich aber die Ereignisanzeige ansehen, Systeminformationen lesen, neue Freigaben erstellen, Informationen aus dem Gerätemanager lesen (Änderungen sind nicht möglich, da er auf einem Remote-Computer nur schreibgeschützt ausgeführt werden kann), neue lokale Benutzer und Gruppen anlegen, die Datenträgerverwaltung ausführen, die Eigenschaften der logischen Laufwerke und Wechselmedien betrachten, Dienste starten, beenden und konfigurieren sowie die Optionen des Indexdienstes einstellen.
4. Die Tasks **LÖSCHEN** und **VERSCHIEBEN** sind selbsterklärend.

18.2.6 Verhindern von Änderungen der Benutzerattribute

Standardmäßig ist es den Active Directory-Benutzern gestattet, dass sie ihre persönlichen Einstellungen im Benutzerprofil, wie z.B. Telefonnummer oder Adresse, selbst ändern können. Diese Änderungen können sie über die mmc **ACTIVE DIRECTORY-BENUTZER UND -COMPUTER** vornehmen. Damit wird sichergestellt, dass die Benutzer selbst für Ihre Angaben verantwortlich und diese stets aktuell sind. Sollten Sie jedoch nicht wünschen, dass die Benutzer ihre Angaben ändern können, haben Sie zwei Möglichkeiten. Zum einen können Sie über die Gruppenrichtlinie sicherstellen, dass die mmc **ACTIVE DIRECTORY-BENUTZER UND -COMPUTER** nicht an die Benutzer verteilt wird. Sie können aber auch den folgenden Weg wählen. Hierbei wird das Active Directory-Schema angepasst.

Um zu verhindern, dass die Benutzer ihre Daten selbst ändern können, haben Sie entweder die Möglichkeit, über die Gruppenrichtlinie festzulegen, dass die Benutzer nicht die mmc **ACTIVE DIRECTORY-BENUTZER UND -COMPUTER** nicht erhalten sollen, oder aber Sie ändern das Active Directory-Schema entsprechend ab. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie die mmc **ACTIVE DIRECTORY-SCHEMA**. Weitere Hinweise zum Öffnen dieser mmc finden Sie in Kapitel 24.1.4.
2. Wählen Sie aus dem Kontextmenü von Active Directory-Schema den Eintrag **BETRIEBSMASTER**. Hier sehen Sie, welcher Rechner die Rolle des Schemamasters (siehe Kapitel 1.3.1) innehat. Aktivieren Sie die Checkbox **SCHEMA KANN AUF DIESEM DOMÄNENCONTROLLER GEÄNDERT WERDEN**.
3. Auf dem Schemamaster muss ein zusätzlicher Registry-Schlüssel hinzugefügt werden. Unter dem Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\Current Control Set\Services\NTDS\Parameters` fügen Sie einen neuen **DWORD-Wert** mit dem Namen `SchemaUpdateAllowed` mit dem Wert **1** ein.

4. Nach dem Ändern des Schemas sollten Sie aus Sicherheitsgründen den Wert des Registry-Schlüssels wieder auf 0 setzen sowie die Checkbox SCHEMA KANN AUF DIESEM DOMÄNENCONTROLLER GEÄNDERT WERDEN wieder deaktivieren. Andernfalls könnten Sie versehentlich Änderungen am Schema durchführen.
5. Öffnen Sie im Active Directory-Schema den Container KLASSEN und dann den Container USER. Wählen Sie aus dem Kontextmenü den Eintrag EIGENSCHAFTEN.
6. Klicken Sie auf die Registerkarte SICHERHEITSEINSTELLUNGEN. Dort finden Sie die Berechtigungen für die spezielle Benutzergruppe SELBST. Sie können hier nun z.B. die Berechtigung TELEFON- UND POSTOPTIONEN SCHREIBEN oder PERSÖNLICHE INFORMATIONEN SCHREIBEN für die Benutzer selbst entfernen. Sobald Sie auf OK geklickt haben, wird die Schemaänderung sofort auf die anderen Server repliziert.

Im Gegensatz zur Replikation, wobei nur die geänderten Attribute übertragen werden, wird bei der Änderung am Active Directory-Schema unter Windows 2000 die gesamte Klasse und nicht nur das geänderte Attribut übertragen. Die Replikation der Schemaänderungen auf Attributebene ist erst unter Windows 2003-Servern möglich.



Führen Sie das eben beschriebene Verfahren aus, bevor Sie die Benutzerobjekte anlegen. Die Änderungen am Schema wirken sich nämlich nicht auf bereits bestehende Objekte aus.

Sie können auch nicht einmalig in einer übergeordneten Domäne oder Organisationseinheit eine Verweigerung für das Ändern der Benutzerrechte konfigurieren, da den Benutzern beim Erstellen Ihres Kontos dieses spezielle Recht automatisch zugeteilt wird. Haben Sie bereits Benutzerkonten angelegt und diesen noch keine speziellen Rechte zugewiesen, so können Sie über das Programm *DSACLs* (siehe Kapitel 23.1.7) alle Einstellungen an den Benutzerkonten auf den Status zurücksetzen, der durch das Schema vorgegeben wird. Ist über das Schema also definiert, dass die Benutzer keine Änderungen an ihren persönlichen Einstellungen vornehmen dürfen, so erhalten alle bereits bestehenden Konten auch diese Einstellung.



Es werden dabei auch alle anderen benutzerdefinierten Einstellungen aller Objekte – und nicht nur der Benutzerobjekte – auf die Standardvorgaben des Schemas zurückgesetzt!

Geben Sie an der Kommandozeile folgenden Befehl ein, um alle Einstellungen auf die Vorgabe des Schemas zurückzusetzen:

```
DSACLs dc=<Domänenname>, dc=<Name der Domäne erster Ebene> /s /t 
```

also beispielsweise

```
DSACLs dc=firma, dc=de /s /t 
```


18.3 Benutzerprofile und Basisverzeichnisse

In diesem Kapitel werden Ihnen die Grundlagen von Benutzerprofilen und Basisverzeichnissen nahegebracht. In einem Benutzerprofil werden diverse Ordner mit Daten und Konfigurationseinstellungen eines Benutzers gespeichert. Mit Benutzerprofilen kann die Konsistenz der Benutzereinstellungen sichergestellt werden. Bei einem Basisverzeichnis handelt es sich um einen alternativen Ordner zum Speicherort **EIGENE DATEIEN**. Zunächst lernen Sie die verschiedenen Arten von Benutzerprofilen kennen. Danach erfahren Sie, wie Benutzerprofile und Basisverzeichnisse eingerichtet und konfiguriert werden.

18.3.1 Arten von Benutzerprofilen

Ein Benutzerprofil umfasst alle persönlichen Einstellungen und Dateien eines Benutzers. Man spricht auch von den Desktop-Einstellungen auf dem lokalen Computer. Ein neues Benutzerprofil wird automatisch erstellt, sobald sich ein neuer Benutzer das erste Mal an einem Computer anmeldet. Bei der Installation werden standardmäßig die Profile für die folgenden Benutzer angelegt:

- ▶ für den Kontonamen des Benutzers, der bei der Installation angegeben wird,
- ▶ für Default User und
- ▶ All Users.

Durch den Einsatz von Profilen können mehrere Benutzer an einem Computer arbeiten, wobei jeder seine persönlichen Einstellungen bekommt und sich seine Änderungen nicht auf die Einstellungen der anderen Benutzer auswirken. Angenommen, Benutzer 1 möchte auf seinem Desktop große Icons verwenden und wählt diese Option. Bei der nächsten Anmeldung erhält ausschließlich Benutzer 1 die großen Icons, während Benutzer 2 weiterhin die herkömmlichen Windows-Icons behält. In einem Profil sind immer die Einstellungen und Daten enthalten, die beim letzten erfolgreichen Herunterfahren des Computers eingestellt und vorhanden waren. Das Profil beinhaltet also eine Momentaufnahme vom letzten Zustand vor dem Herunterfahren. Wird der Computer nicht ordnungsgemäß heruntergefahren, kann auch das Benutzerprofil Schaden nehmen, indem möglicherweise nicht alle Änderungen in das Profil eingetragen werden.

Jedes Profil beinhaltet dieselben Inhalte, nur hinsichtlich des Speicherortes und der Änderungsmöglichkeiten unterscheiden sie sich. Die lokalen Benutzerprofile befinden sich im Verzeichnis `%SYSTEM%\DOKUMENTE UND EINSTELLUNGEN\%BENUTZERANMELDENAME%`, z.B. `C:\DOKUMENTE UND EINSTELLUNGEN\ADMINISTRATOR`. Wurde der Computer von Windows NT auf Windows 2000 aktualisiert, so befindet sich das Profil in `%SYSTEMROOT%\PROFILES\%BENUTZERANMELDENAME%`. Servergespeicherte Profile befinden sich in einer Netzwerkfreigabe auf einem Server. Ein Profil enthält die persönlichen Ordner, individuelle Einstellungen, z.B. der Bildschirmauflösung, das Farbschema, Ansichtsoptionen im Windows Explorer, Favoriten usw. Diese Informationen befinden sich in den folgenden Ordnern:

Ordner	Inhalt
Anwendungsdaten ¹	Hier werden persönliche Einstellungen zu Applikationen gespeichert, beispielsweise die Office-Benutzerwörterbücher oder Office-Vorlagen. Alle Windows 2000-konformen Applikationen legen dort die persönlichen Einstellungen ab anstatt direkt im Programmverzeichnis.
Cookies	Hier befinden sich Informationen über besuchte Internet-Seiten.
Desktop	Hier werden alle Elemente des aktuellen Desktops wie Verknüpfungen oder auf dem Desktop gespeicherte Daten abgelegt.
Druckumgebung ¹	Hier befinden sich Verknüpfungen zu Objekten des Druckerordners.
Eigene Dateien	Eigene Dateien wird als das Standardverzeichnis für persönliche Dokumente benutzt. Microsoft-Applikationen, wie z.B. das Office-Paket, geben auch diesen Pfad vor. Darin enthalten ist auch der Ordner Eigene Bilder. Er ist der Speicherort für alle Grafikelemente des Benutzers.
Favoriten	Hier befinden sich die Verknüpfungen zu den als Favoriten gewählten Internetseiten.
Lokale Einstellungen ¹	Dieser Ordner beinhaltet vier weitere Ordner: Anwendungsdaten, z.B. Outlook-Archive, Temp für alle temporär verwendeten Dateien, Temporary Internet Files für zwischengespeicherte Internetdaten und Verlauf für eine Übersicht über besuchte Internetseiten.
Netzwerkumgebung ¹	Hier befinden sich Verknüpfungen zu Netzwerkelementen wie aktuell verbundene Netzlaufwerke.
Recent ¹	In diesem Ordner wird eine Liste der zuletzt geöffneten Dokumente und Ordner gepflegt.
Send to ¹	Hier befinden sich die Verknüpfungen zu Elementen, die Sie im Kontextmenü eines Objekts unter Senden an finden.
Startmenü	Hier befinden sich die Verknüpfungen zu allen Einträgen und Elementen des Startmenüs.
Vorlagen	Hier befinden sich Vorlagen für Dokumenttypen, die auf dem Computer geöffnet werden können.
NTUSER.DAT ¹	Diese Datei speichert Registry-Einstellungen wie Monitorauflösung, bevorzugtes Farbschema, Ansichtsoptionen des Explorers und der Ordner. Ist die NTUSER.DAT beschädigt oder fehlt sie, wird für den Benutzer ein neues Profil angelegt, obwohl die Verknüpfungen noch alle in den oben beschriebenen Ordnern vorhanden sind.

Tabelle 18.5: Die Inhalte eines Benutzerprofils

Die mit ¹ gekennzeichneten Ordner sind nur sichtbar, wenn Sie im Windows Explorer unter EXTRAS/ORDNEROPTIONEN/ANSICHT die Option ALLE DATEIEN UND ORDNER ANZEIGEN gewählt haben. Standardmäßig werden die versteckten Objekte nicht angezeigt.

Es gibt insgesamt drei Arten von Benutzerprofilen. Es handelt sich um lokale, servergespeicherte sowie verbindliche Benutzerprofile. Die folgende Tabelle gibt eine Übersicht über die verschiedenen Typen.

Benutzerprofil	Beschreibung
Lokal	Diese Art von Profilen wird angelegt, sobald sich ein neuer Benutzer das erste Mal an einem Computer anmeldet. Die in diesem Profil gespeicherten Einstellungen sind ausschließlich für den lokalen Computer gültig.
Servergespeichert	Die servergespeicherten Profile werden nicht lokal, sondern auf einem Server abgelegt. Sie sind stets verfügbar. Dabei ist es gleichgültig, von welchem Rechner im Netzwerk aus sich der Benutzer anmeldet, er bekommt immer seine persönlichen Einstellungen. Nimmt der Benutzer Änderungen vor, werden diese auch auf dem Server gespeichert. Ein servergespeichertes Profil muss vom Administrator eingerichtet werden.
Verbindlich	Auch dieses Profil wird auf einem Server gespeichert. Es ist somit auch immer verfügbar, egal an welchem Rechner sich der Benutzer anmeldet. Allerdings werden in diesem Profil seine Änderungen nicht gespeichert. Der Benutzer bekommt immer wieder die Einstellungen, die der Administrator einmal für ihn oder eine ganze Benutzergruppe festgelegt hat.

Tabelle 18.6: Arten von Benutzerprofilen

Ein lokales Profil muss im Gegensatz zu servergespeicherten und verbindlichen Profilen nicht explizit eingerichtet werden. Es wird automatisch bei jeder Anmeldung eines neuen Benutzers eingerichtet. Hierzu werden die Grundeinstellungen des Ordners `DEFAULT USER` in `\DOKUMENTE UND EINSTELLUNGEN` benutzt und mit einem neuen Namen versehen. Genauer wird dieser Vorgang in Kapitel 18.3.4 beschrieben.

18.3.2 Checkliste zum Einrichten von Benutzerprofilen

Die folgende Checkliste gibt Ihnen einen Überblick über die erforderlichen Schritte, die Sie zur Einrichtung und Konfiguration servergespeicherter Benutzerprofile bis hin zum Festlegen von Kontingentgrenzen für Benutzerprofile durchführen sollten. Da diese Schritte hier nicht chronologisch beschrieben werden, sondern in den jeweiligen Gesamtkontext eines Kapitels eingegliedert sind, werden die jeweils relevanten Kapitel angegeben.

1. Wählen Sie einen Dateiserver aus, und erstellen Sie auf diesem einen oder mehrere freigegebene Ordner, in dem/denen Sie die Benutzerprofile speichern möchten. Durch die Verwendung eines zentralen Speicherorts wird Ihnen auch die Datensicherung erleichtert (siehe Kapitel 18.3.3).
2. Richten Sie die servergespeicherten Benutzerprofile ein. Überlegen Sie sich, für welche Anwendergruppen welche Einstellungen sinnvoll sein können (siehe Kapitel 18.3.3 und 18.3.4).

3. Spezifizieren Sie die Benutzerordner, für die Sie Umleitungen einrichten möchten. Diese umgeleiteten Ordner stellen sich für die Benutzer wie lokale Ordner dar und belasten im Gegensatz zu Ordnern, die im servergespeicherten Profil liegen, nicht das Netzwerk (siehe Kapitel 20.3.1).
4. Aktivieren Sie die Option, Dateien und Ordner offline verfügbar zu machen. Damit kann einem Benutzer auch dann Zugriff auf die Daten gewährt werden, wenn er nicht am Netzwerk angemeldet ist (siehe Kapitel 20.3.3).
5. Legen Sie über Datenträgerkontingente Beschränkungen fest, wie groß die Benutzerprofile der Benutzer maximal sein dürfen (siehe Kapitel 19.3).
6. Erstellen Sie einen Plan, welche Optionen von Gruppenrichtlinien und anderen Konfigurationseinstellungen Sie als standardmäßige oder erweiterte Funktionen definieren möchten. Teilen Sie Ihre Angestellten in Gruppen ein, die auf deren Funktion basieren, und weisen Sie dann den Gruppen standardmäßige oder erweiterte Optionen zu (siehe Kapitel 20.2).

18.3.3 Einrichten eines servergespeicherten Profils

Das servergespeicherte Profil wird auf einem Server im Netzwerk abgelegt und ist somit immer verfügbar. Die persönlichen Einstellungen sind für den Benutzer an jedem Computer verfügbar, an dem er sich anmeldet, und nicht auf einen lokalen Rechner begrenzt. Bei der Anmeldung an einem Computer kopiert Windows die Daten des Profils auf den Client-Computer. Bei der ersten Anmeldung wird das Profil komplett kopiert, bei späteren Anmeldungen wird geprüft, ob Änderungen an dem Profil vorgenommen sind. Ist dies der Fall, werden ausschließlich die Änderungen auf den Client kopiert. Die Änderungen, die der Client während seiner Sitzung am Profil vorgenommen hat, werden während des Abmeldevorgangs auf den Server geschrieben. Der ideale Speicherort für die Profile ist ein Dateiserver, von dem regelmäßig Backups erstellt werden. Legen Sie die Profile nicht auf dem Domänencontroller ab, da beim Kopieren von Profilen verstärkt Netzwerkressourcen belegt werden, wodurch die Leistung des Domänencontrollers herabgesetzt werden kann.

Sie können ein servergespeichertes Profil nicht nur für einen einzelnen Benutzer, sondern auch für eine ganze Benutzergruppe einrichten. Dies ist sinnvoll, wenn z.B. alle Mitglieder einer Gruppe mit denselben Aufgaben dieselben Einstellungen erhalten sollen. Die Benutzer erhalten nur die Einträge und Verknüpfungen, die sie für ihre Arbeit benötigen. Auch die benötigten Netzwerkressourcen, wie z.B. ein bestimmtes Laufwerk für Daten und ein bestimmter Drucker, können ihnen gleich automatisch zugeteilt werden. Dabei handelt es sich um verbindliche, servergespeicherte Benutzerprofile.

Um ein neues servergespeichertes Benutzerprofil für einen Benutzer einzurichten, führen Sie die folgenden Schritte aus:

1. Richten Sie auf dem Dateiserver einen neuen Ordner ein und geben diesen frei. Wählen Sie als Freigabenamen beispielsweise Profile.
2. Wählen Sie am Domänencontroller über die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER das gewünschte Benutzerobjekt, und öffnen Sie über dessen Eigenschaften die Registerkarte PROFIL. Geben Sie hier im Feld PROFILPFAD einen Pfad im folgenden Format an: `\\SERVERNAME\FREIGABENAME\ANMELDENAME`, also etwa `\\BORUSSIA\PROFILE\PMUSTERMANN`.



Benutzen Sie statt des Anmeldenamens die Variable %username%. Windows kann diese Variable durch den Namen des Benutzerkontos ersetzen. Sie sparen sich dadurch Arbeit und können die Profile leichter kopieren. Meldet sich der Benutzer zum ersten Mal an, wird automatisch der Profilordner mit seinem Anmeldenamen eingerichtet.

Um ein servergespeichertes Profil für eine Gruppe von Benutzern einzurichten, führen Sie die folgenden Schritte aus. Man spricht in diesem Fall auch von einem standardmäßigen, servergespeicherten Benutzerprofil.

1. Erstellen Sie über die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER ein Benutzerkonto als Profilvorlage. Geben Sie einen beliebigen Vor- und Nachnamen ein und vergeben einen Benutzeranmeldenamen, z.B. Vorlage. Melden Sie sich mit diesem Vorlagennamen an und nehmen alle gewünschten Einstellungen und Änderungen am Desktop vor. Melden Sie sich dann wieder als Administrator an.
2. Richten Sie auf dem Dateiserver einen neuen Ordner ein und geben diesen frei. Wählen Sie als Freigabenamen beispielsweise Profile. In diesem Ordner werden alle Benutzerprofile angelegt.
3. Kopieren Sie von dem Rechner, an dem Sie eben die Änderungen am Profil vorgenommen haben, aus dem Verzeichnis %SYSTEM%\DOKUMENTE UND EINSTELLUNGEN\BENUTZERNAME den Profilordner in die Freigabe auf dem Dateiserver. Dies geschieht auf folgende Weise:
 1. Öffnen Sie in der Systemsteuerung den Eintrag SYSTEM.
 2. Wählen Sie die Registerkarte BENUTZERPROFILE (siehe Abbildung 18.7). Sie sehen hier eine Liste aller Benutzer, die sich bereits an diesem Computer angemeldet hatten.



Abbildung 18.7: Vorhandene lokale Profile

3. Sie sehen in der Liste auch das Vorlagenprofil mit dem Namen FIRMA\Vorlage. Markieren Sie dieses Profil und klicken auf die Schaltfläche KOPIEREN NACH.
4. Geben Sie den Pfad zu der im zweiten Schritt erstellten Freigabe auf dem Dateiserver an (siehe Abbildung 18.8) und geben einen Ordner für den Benutzer an, der das Profil erhalten soll, z.B. \\BORUSSIA\PROFILE\PMUSTERMANN. Nach dem Kopiervorgang befinden sich im Ordner pmustermann alle Ordner mit den zugehörigen Einstellungen aus %SYSTEM%\DOKUMENTE UND EINSTELLUNGEN\VORLAGE.



Abbildung 18.8: Pfad des Benutzerprofils

5. Um nun die Benutzer hinzuzufügen, die dieses Profil benutzen sollen, klicken Sie auf die Schaltfläche ÄNDERN (siehe Abbildung 18.8). Sie erhalten eine Liste aller vorhandenen Benutzer und Gruppen und können die gewünschten Personen auswählen. Bestätigen Sie mit OK.
6. Legen Sie über die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER in den Kontoeigenschaften für alle Benutzer den Profilpfad entsprechend fest, in unserem Beispiel also \\BORUSSIA\PROFILE\%USERNAME%.

Künftig werden alle Benutzer, die Sie eben für die Verwendung dieses Benutzerprofils ausgewählt haben, dieses Profil als Standardprofil bei der Anmeldung erhalten. Ihre Änderungen werden in ihrem jeweiligen Ordner %USERNAME% gespeichert.

Die Vorteile servergespeicherter Profile bestehen darin, dass sich ein Benutzer von jedem beliebigen Computer im Netzwerk aus anmelden kann und dabei immer seine persönlichen Einstellungen bekommt. Ein Nachteil besteht in dem dadurch verursachten Netzwerkverkehr. Sie sollten auch keine servergespeicherten Benutzerprofile für die Benutzer einrichten, die über langsame RAS-Verbindungen wie z.B. eine Telefonleitung auf das Netzwerk zugreifen.

18.3.4 Einrichten eines verbindlichen Profils

Bei einem verbindlichen Profil hat der Benutzer nicht die Möglichkeit, dauerhaft Änderungen an seinem Desktop vorzunehmen. Er kann nur temporär Einstellungen ändern. Diese werden aber nicht gespeichert und stehen damit bei der nächsten Anmeldung nicht mehr zur Verfügung. Mit dieser Methode haben Sie als Administrator die volle Kontrolle über die Desktop-Einstellungen Ihrer Benutzer.

Ein verbindliches Profil ist schreibgeschützt. Um ein verbindliches Profil einzurichten, führen Sie die folgenden Schritte aus:

1. In dem Profilordner jedes Benutzers befindet sich die Datei *NTUSER.DAT*. Standardmäßig ist diese Datei versteckt. Um sie anzuzeigen, wählen Sie im Windows Explorer unter EXTRAS/ORDNEROPTIONEN/ANSICHT die Option ALLE DATEIEN UND ORDNER ANZEIGEN. In dieser Datei werden die Desktop-Einstellungen gespeichert.
2. Um diese Datei mit einem Schreibschutz zu versehen, muss sie umbenannt werden. Geben Sie ihr den neuen Namen *NTUSER.MAN*. Nun kann der Benutzer seine Desktop-Einstellungen nur für die Zeit seiner Arbeit ändern. Bei der nächsten Anmeldung des Benutzers werden die Änderungen nicht übernommen.

18.3.5 Probleme mit lokalen Profilen nach der Migration – SID-History

Nach der Migration von Windows NT-Clients auf Windows 2000 stehen die Benutzer häufig vor dem Problem, dass ihre Einstellungen an den lokalen Benutzerprofilen nicht mehr verfügbar sind. Sie erhalten bei der Anmeldung einen neuen Desktop, so als wären Sie noch nie an dem Computer angemeldet gewesen. Dieses Problem liegt in der Zuweisung der SIDs (Security Identifier) zum alten Windows NT-Benutzerkonto und dem neuen Windows 2000-Konto.

Die SID ist eine eindeutige Kennung für alle Benutzer-, Computer- und Gruppenkonten, die bei der Einrichtung des betreffenden Objekts vergeben wird. Wenn Sie ein Konto löschen und ein gleichnamiges neues erstellen, erhält dieses eine neue SID. Damit müssen Sie für das neue Konto sämtliche Zugriffsrechte etc. neu konfigurieren. Interne Windows-Mechanismen verwenden statt des Kontonamens ausschließlich die SID.

Während der Migration werden von den meisten Migrationstools die SIDs der ursprünglichen NT-Konten in das entsprechende Attribut der SID-History des neuen Windows 2000-Kontos kopiert. Windows 2000 weist den migrierten Konten neue SIDs zu.

Beim Anmelden an einer Windows 2000-Domäne wird für jeden Benutzer ein Zugriffstoken generiert. In diesem Token befinden sich die SIDs des Benutzers, und zwar die SID des ursprünglichen NT-Kontos sowie die SIDs und SID-Histories der Gruppen, zu denen die Benutzer aktuell gehören. Um das Zugriffsrecht auf eine bestimmte Netzwerkressource zu prüfen, vergleicht der Domänencontroller, ob eine der SIDs des Benutzers mit denen in der ACL für das Objekt angegebenen SIDs übereinstimmt. Ist dies nicht der Fall, erhält der Benutzer keinen Zugriff auf das Objekt. Sie sehen also, dass über die SID-History eigentlich immer die ursprünglichen Zugriffsrechte erhalten bleiben.

Eigentlich. Denn leider sind lokale Benutzerprofile nicht in der Lage, mit einer SID-History zu arbeiten. Das lokale Benutzerprofil benutzt ausschließlich die primäre SID eines Benutzerkontos um festzustellen, ob ein Profil vorliegt, das benutzt werden kann, oder ob ein neues Profil erstellt werden muss. Und die primäre SID ist nach der Migration die neu von Windows 2000 zugewiesene SID.

In unserem Beispiel hat ein Benutzer von Windows 2000 die SID 5566778 neu zugewiesen bekommen. Mit dieser hat er sich noch nie lokal angemeldet, also ist auch kein lokales Profil mit dieser SID auf dem Computer vorhanden. Als der Benutzer noch mit Windows

NT gearbeitet hat, besaß sein Konto die SID 1122334. Diese SID wurde in die SID-History des Benutzers kopiert. Für das alte NT-Konto ist nach wie vor ein Profil mit passender SID vorhanden, in dem alle Einstellungen gespeichert sind, außerdem gibt es noch zwei Profile weiterer Benutzer. Da das lokale Profil aber ausschließlich die primäre SID mit den SIDs im Profilpool vergleicht, wird kein passendes Profil gefunden und ein neues erstellt. Ein neues Profil wird erstellt, indem die Einstellungen von \DEFAULT USER kopiert und mit dem neuen Benutzernamen und dessen primärer SID versehen werden. Dieses Profil enthält jedoch nicht die Einstellungen des alten Profils. Diesen Vorgang veranschaulicht Abbildung 18.9.

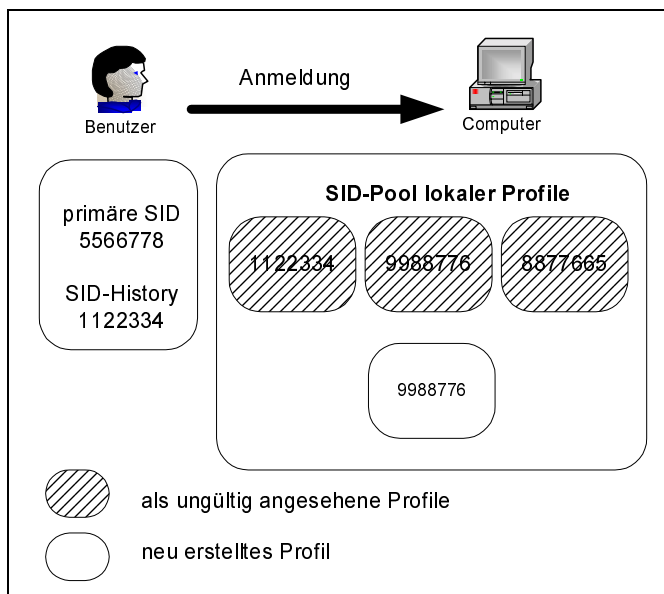


Abbildung 18.9: Verschiedene SIDs lokaler Benutzerprofile nach der Migration

Nun hat der Benutzer bereits zwei lokale Profile, doch dabei ist das aktuell verwendete das Profil mit falschen Einstellungen.

Microsoft entwickelte für die Migration das Programm ADMT (Active Directory Migration Tool, siehe Kapitel 27.5). Doch leider bietet dieses Programm keine Unterstützung zur Lösung des SID-Problems an.

Eine Möglichkeit zur Problemlösung bietet der *Domain Migration Wizard* von Aelita Software. Er enthält die Tools EXPORTPROFILE und CHANGEPROFILE. Beide Programme werden in den Loginskripten der Benutzer ausgeführt. EXPORTPROFILE durchsucht alle SIDs der lokalen Profile, bis das Profil mit einer SID aus der SID-History gefunden wird. Die SID dieses Profils wird auf die der primären SID des Benutzers umgesetzt. Also findet der Benutzer bei der Anmeldung sein altes Profil mit seinen alten Einstellungen mit einer neuen SID vor. CHANGEPROFILE sucht ebenfalls in den lokalen Profilen nach einer SID aus der SID-History des Benutzers und setzt die SID des Profils auf die primäre SID des Benutzers um. Ist bereits ein neues Profil mit der primären SID erstellt, so wird dieses deaktiviert, da nicht zwei Profile mit derselben SID koexistieren können.

Der Benutzer erhält auch auf diese Weise das Profil mit seinen alten Einstellungen zurück. Die beiden Programme müssen so lange in den Loginskripten der Benutzer enthalten bleiben, bis sichergestellt ist, dass sie sich an allen Computern mindestens einmal angemeldet haben, auf denen sie lokale Profile haben.

Um die SIDs in der SID-History sehen zu können, verwenden Sie das Support-Tool *ADSIEDIT* (siehe Kapitel 23.1.2) und öffnen mit diesem die Benutzerobjekte.

18.3.6 Einrichten von Basisverzeichnissen

Ein Basisverzeichnis ist ein alternativer Ordner anstatt *EIGENE DATEIEN* für persönliche Dokumente. Das Basisverzeichnis ist kein Bestandteil eines Benutzerprofils. Auf ein Basisverzeichnis kann ein Benutzer mit jedem beliebigen Microsoft-Betriebssystem von MS-DOS bis zu Windows XP zugreifen. Sie können die Basisverzeichnisse aller Benutzer zentralisiert auf einem Dateiserver anlegen, was die Verwaltung und Sicherung der Daten erleichtert, oder jedem Benutzer lokal ein Basisverzeichnis zuweisen.

Um ein Basisverzeichnis einzurichten, führen Sie die folgenden Schritte aus:

1. Wenn Sie sich für ein serverbasiertes Basisverzeichnis entscheiden, müssen Sie auf einem Dateiserver eine Freigabe erstellen, in der sämtliche Basisverzeichnisse gespeichert werden sollen. Wählen Sie für die Zugriffsberechtigungen der Freigabe nur die Gruppe „Benutzer“ und entfernen die Gruppe „Jeder“.
2. Öffnen Sie nun die Registerkarte *PROFIL* in den Kontoeigenschaften des Benutzers (siehe Abbildung 18.10).



Abbildung 18.10: Das Basisverzeichnis eines Benutzers

3. Da Sie sich für ein servergespeichertes Basisverzeichnis entschieden haben, markieren Sie die Checkbox VERBINDEN VON und wählen einen Laufwerksbuchstaben aus. Sie sollten für alle Benutzer denselben unbelegten Buchstaben, etwa Z, verwenden. Geben Sie dann den Pfad im Format \\SERVERNAME\FREIGABE\BENUTZERNAME an. Anstatt des Benutzernamens können Sie auch hier wieder die Variable %username% verwenden.

Wenn Sie einen lokalen Pfad als Basisverzeichnis verwenden möchten, markieren Sie die Checkbox LOKALER PFAD und geben den Pfad ein. Ein lokaler Pfad ist nur dann sinnvoll, wenn sich der Benutzer nur von einem Computer aus anmeldet. Versucht er die Anmeldung von einem anderen Computer im Netzwerk aus, wird der lokale Pfad selbstverständlich nicht gefunden. Sie müssen in diesem Fall auch auf jedem lokalen Rechner separat für die Datensicherung des Basisverzeichnisses sorgen. In den meisten Fällen ist ein servergespeichertes Basisverzeichnis die bessere Lösung.

18.4 Grundlagen zu Benutzergruppen

In diesem Kapitel lernen Sie nun grundlegende Dinge zum Thema Benutzergruppen. Um sich die Verwaltung der Benutzer zu vereinfachen, können Sie Benutzer, die in einem Unternehmen ähnliche Aufgaben ausführen, zu Benutzergruppen zusammenfassen.

18.4.1 Grundlegendes zu Gruppen

Eine Benutzergruppe ist zunächst einmal nichts anderes als eine Zusammenfassung von mehreren Benutzerkonten. Sie vereinfachen die Benutzerverwaltung durch die Einrichtung von Gruppen enorm, da Sie nun nicht mehr jedem einzelnen Benutzer Zugriffsrechte auf Ressourcen zuweisen, sondern in nur einem Arbeitsschritt einer Gruppe und damit allen darin enthaltenen Benutzern die entsprechenden Rechte geben oder verweigern.

Es ist möglich, dass ein Benutzer Mitglied mehrerer Gruppen oder eine Gruppe Mitglied einer anderen Gruppe ist. Zu einer Gruppe können Sie Benutzerkonten, Computerkonten, andere Gruppen und Kontakte hinzufügen.

18.4.2 Gruppentypen und Gruppenbereiche

Die Gruppen werden in zwei verschiedene Typen und drei Gruppenbereiche unterschieden. Zunächst einmal gibt es die beiden Gruppentypen „Sicherheitsgruppe“ und „Verteilergruppe“. Die wichtigere von beiden ist die Sicherheitsgruppe. In einer Verteilergruppe werden Benutzer ausschließlich für Prozesse zusammengefasst, die nichts mit Zugriffsrechten und Sicherheit zu tun haben. Ein klassisches Beispiel ist eine Verteilerliste zum Massenversand von E-Mails. Nur die Sicherheitsgruppen dienen der Zusammenfassung von Benutzern für die Vereinfachung der Vergabe von Zugriffsrechten. Sie besitzen die Grundfunktionalität der Verteilergruppen, nämlich das Zusammenfassen von mehreren Benutzern für eine bestimmte Funktion sowie zusätzlich die Möglichkeit, den Zugriff auf Ressourcen zu steuern. In unserem Kontext sind ausschließlich die Sicherheitsgruppen relevant. Wenn also künftig von Gruppen die Rede ist, sind damit nur die Sicherheitsgruppen gemeint.

Die Sicherheitsgruppen werden in drei Gruppenbereiche unterteilt. Dies sind globale Gruppen, domänenübergreifende lokale Gruppen sowie universelle Gruppen. Beim

Erstellen einer Gruppe müssen Sie einen dieser drei Bereiche auswählen. Diese Gruppen können Sie für eine Domäne einrichten. Unabhängig von diesen drei Gruppenbereichen gibt es die lokalen Gruppen, die Sie auf Windows 2000/XP Professional-Computern sowie Mitgliedsservern in der Domäne lokale Gruppen einrichten. Diese Gruppen sind lediglich auf dem lokalen Computer verfügbar und dürfen nicht mit domänenübergreifenden lokalen Gruppen verwechselt werden.

Die drei Gruppenbereiche haben bezüglich der Mitgliedschaft ihrer Gruppenmitglieder und des Zugriffs auf die Netzwerkressourcen bestimmte Eigenschaften (siehe Tabelle 18.7).

Gruppenbereich	Mitgliedschaft	Ressourcenzugriff
Global	Mitglieder der lokalen Domäne	auf Ressourcen beliebiger Domänen
Domänenübergreifend lokal	Mitglieder aus einer beliebigen Domäne	auf Ressourcen der lokalen Domäne
Universell	Mitglieder aus einer beliebigen Domäne	auf Ressourcen beliebiger Domänen

Tabelle 18.7: Eigenschaften der Gruppenbereiche



Die universellen Gruppen sind nur im einheitlichen und Windows Server 2003-Betriebsmodus (siehe Kapitel 10.1.2 und 10.1.4) verfügbar.

Sie sehen also, dass die globalen Gruppen hinsichtlich der Gruppenmitgliedschaft eingeschränkt sind, während die domänenübergreifenden lokalen Gruppen hinsichtlich des Ressourcenzugriffs beschränkt sind. Die Nicht-Einschränkung gilt jeweils für die andere Komponente. Nur bei einer universellen Gruppe gibt es keinerlei Einschränkungen.

Diese drei Gruppen bieten umfangreiche und flexible Möglichkeiten für die Konfiguration von Zugriffsberechtigungen. Außerdem wirken sich Änderungen der Mitgliedschaft an den verschiedenen Gruppen auch unterschiedlich im Replikationsverkehr des globalen Katalogs aus. Universelle Gruppen sind im globalen Katalog enthalten. Da diese primär globale Gruppen aus beliebigen Domänen der Gesamtstruktur enthalten, ändern sich die universellen Gruppen nicht allzu häufig. Die globalen Gruppen sind zwar im globalen Katalog enthalten, nicht aber ihre Mitglieder. Ändern sich die Mitglieder der globalen Gruppen, so werden diese Änderungen lediglich in der Domäne repliziert, in der die globale Gruppe definiert ist. Da die domänenübergreifenden lokalen Gruppen nur in der Domäne gültig sind, in der die Gruppe definiert ist, erscheinen diese nicht im globalen Katalog.

18.4.3 Standardmäßig vorhandene Gruppen

Es gibt mehrere standardmäßig vorhandene Gruppen unter Windows 2000. Dabei wird wieder unterschieden in Domänencontroller und Windows-Clients bzw. Mitgliedsserver. Domänencontroller können drei Arten von Gruppen beinhalten, nämlich integrierte, vordefinierte und besondere Gruppen. Auf allen übrigen Windows 2000-Rechnern kön-

nen Sie lediglich vordefinierte lokale Gruppen einrichten. Die folgenden Tabellen geben Ihnen eine Übersicht über die standardmäßigen Mitglieder dieser Gruppen und deren Einsatzmöglichkeiten und Berechtigungen.

Integrierte Gruppen gehören zu dem Gruppenbereich domänenübergreifend lokal. Sie befinden sich im Container BUILTIN der Domäne. Diesen Gruppen sind bereits feste Berechtigungen zugeteilt, die sie für die Arbeit im Active Directory benötigen. Es gibt die folgenden integrierten Gruppen (siehe Tabelle 18.8):

Integrierte Gruppe	Beschreibung	Standardmäßige Mitglieder
Administratoren	Konto, um alle Verwaltungsaufgaben in der Domäne durchzuführen	Domänen-Admins und Organisations-Admins
Benutzer	Benutzer können die Aufgaben durchführen, für die ihnen die Rechte erteilt sind.	Domänenbenutzer und authentifizierte Benutzer
Druck-Operatoren	Konto zum Einrichten und Verwalten von Netzwerkdruckern auf Domänencontrollern	
Gäste	Mitglieder können nur die ihnen erlaubten Aufgaben ausführen	Gast, IWAM_Computername, IUSR_Computername und TsInternetUser
Konten-Operatoren	Konto zum Einrichten und Verwalten von Benutzerkonten und Gruppen	
Prä-Windows 2000-kompatibler Zugriff	Zur Gewährleistung der Abwärtskompatibilität wird allen Benutzern und Gruppen Lesezugriff gewährt.	NT-Systemgruppe „Jeder“
Replikations-Operator	Konto zur Unterstützung der Active Directory-Replikation	
Server-Operatoren	Konto zum Sichern und Wiederherstellen sowie gemeinsamen Zugriff auf Ressourcen des Servers	
Sicherungs-Operatoren	Konto zum Sichern und Wiederherstellen aller Domänencontroller über Windows Backup	

Tabelle 18.8: Integrierte Gruppen

Weiterhin gibt es vordefinierte Gruppen, die dem Gruppenbereich GLOBAL angehören. Diese Gruppen befinden sich im Container USERS der Domäne. Zu diesen Gruppen können neue Mitglieder hinzugefügt werden, und diese globalen Gruppen können zu domänenübergreifenden lokalen Gruppen hinzugefügt werden. Es gibt die folgenden integrierten Gruppen (siehe Tabelle 18.9):

Vordefinierte Gruppe	Beschreibung	Standardmäßige Mitglieder
Domänen-Admins	Sie können auf jedem Computer in der Domäne administrative Aufgaben ausführen.	Administratoren
Domänen-Benutzer	Alle Benutzer werden dieser Gruppe hinzugefügt.	Administrator, Krbtgt, IWAM_Computername, IUSR_Computername und TsInternetUser
Domänen-Gäste	Alle Gäste werden automatisch dieser Gruppe hinzugefügt.	Gast
Organisations-Admins	Konto für Verwaltungsaufgaben im gesamten Netzwerk	Administrator

Tabelle 18.9: Vordefinierte Gruppen

Sofern Sie weitere Dienste installiert haben, sind weitere vordefinierte Gruppen vorhanden, so beispielsweise DHCP-Administratoren und -Benutzer, DNS-Admins, RAS- und IAS-Server, Schema-Admins usw.

Die Gruppen mit besonderer Identität (siehe Tabelle 18.10) befinden sich auf jedem Windows 2000 / 2003-Computer, unabhängig davon, ob es sich um einen Domänencontroller handelt oder nicht. Zu diesen Gruppen können Sie jedoch weder Mitglieder hinzufügen noch diese Gruppen Mitglied anderer Gruppen werden lassen. Es handelt sich um Zweckgruppen, die Benutzer temporär enthalten. Die Gruppen werden nicht durch die Person definiert, die auf einen Computer oder eine Ressource zugreift, sondern dadurch, wie der Zugriff erfolgt.

Besondere Gruppe	Beschreibung
Anonyme Anmeldung	Umfasst alle Benutzer, die nicht von Windows 2000 authentifiziert werden konnten.
Authentifizierte Benutzer	Fasst alle Benutzer zusammen, die über ein gültiges Domänenkonto verfügen. Sie sollten statt der Gruppe „Jeder“ lieber dieser Gruppe Zugriffsrechte erteilen.
Ersteller-Besitzer	Das Benutzerkonto des Benutzers, der die Ressource ursprünglich erstellt oder später in Besitz genommen hat.
Interaktiv	Das Benutzerkonto des Benutzers, der sich an einem Rechner physisch anmeldet.
Jeder	Umfasst alle Benutzer, die auf den Computer zugreifen. Darin ist auch das Gastkonto enthalten. Standardmäßig hat diese Gruppe Vollzugriff auf alle Ressourcen.
Netzwerk	Umfasst alle Benutzer, die aktuell auf eine beliebige freigegebene Ressource zugreifen.
Wählverbindung	Alle aktuellen Benutzer einer DFÜ-Verbindung

Tabelle 18.10: Gruppen mit besonderer Identität

Auf jedem Windows 2000/2003-Computer, der kein Domänencontroller ist, gibt es vordefinierte lokale Gruppen. Die Mitglieder dieser Gruppen können ihre Aufgaben nur auf dem lokalen System ausführen. Diese Gruppenkonten sind nicht in der Domäne gültig. Die folgenden Gruppen sind vordefinierte lokale Gruppen: Administratoren, Benutzer, Gäste, Hauptbenutzer, Replikations-Operator und Sicherungs-Operatoren. Bis auf die Gruppe „Hauptbenutzer“ gelten für diese Konten dieselben Beschreibungen wie in Tabelle 18.8. Lediglich Hauptbenutzer sind nur in lokalen Gruppen vorhanden. Sie können neue lokale Konten erstellen und ändern sowie die Freigabe von Ressourcen vornehmen.

18.5 Planen und Einrichten von Gruppen

In diesem Kapitel lernen Sie nun das Anwenden der verschiedenen Gruppen kennen. Zunächst bekommen Sie eine Übersicht über die planerische Strategie, um bestimmte Benutzer bestimmten Gruppen zuzuweisen. Auch die Simplifizierung der Gruppenverwaltung über Verschachtelung von Gruppen wird Ihnen vorgestellt. Im zweiten Kapitel werden das Einrichten und Konfigurieren von Gruppen erläutert.

18.5.1 Welche Art von Gruppe soll verwendet werden?

Nachdem Sie nun die verschiedenen Arten von Gruppenbereichen kennen gelernt haben, werden Sie erfahren, wie Sie Benutzer den verschiedenen Gruppen sinnvoll zuordnen können. Dabei sollten Sie auch an Aspekte wie Flexibilität und Wachstum denken.

Gruppenzuordnung im gemischten Betriebsmodus

Die erste beschriebene Strategie bezieht sich auf die Verteilung globaler und domänenübergreifender Gruppen im gemischten Betriebsmodus (siehe Kapitel 10.1.1). Beziehen Sie die folgenden Punkte in die Planung mit ein:

- ▶ Untersuchen Sie zunächst, wie Sie allgemeine Tätigkeitsfelder der Benutzer in Ihrem Unternehmen zusammenfassen und benennen können. Sie könnten etwa Gruppen wie „Personalabteilung“, „Buchhaltung“, „Vertrieb“ usw. definieren. Legen Sie diese Gruppen als globale Gruppen fest und weisen Ihnen die Benutzerkonten zu.
- ▶ Prüfen Sie dann, welche Ressourcen von den eben erstellten globalen Gruppen gemeinsam genutzt werden müssen. Hierzu gehören z.B. bestimmte freigegebene Ordner oder Drucker. Erstellen Sie für diese Ressourcen eigene domänenübergreifende Gruppen.
- ▶ Fügen Sie in einem dritten Schritt nun die globalen Benutzergruppen zur domänenübergreifenden lokalen Gruppe hinzu und konfigurieren die Zugriffsrechte für die domänenübergreifende Gruppe. Damit erhalten alle globalen Gruppen automatisch dieselben Zugriffsrechte, da sie Mitglied der domänenübergreifenden Gruppe sind.
- ▶ Durch das Aufteilen der Gruppen in globale und domänenübergreifende Gruppen erzielen Sie eine hohe Flexibilität, da Sie domänenübergreifende Mitgliedschaften und Zugriffe auf Ressourcen miteinander kombinieren. Würden Sie alle Benutzer und Ressourcen nur in globalen Gruppen zusammenfassen, so könnten die Benutzer zwar auf Ressourcen aller Domänen zugreifen, aber Sie müssten bei der Verwendung mehrerer Domänen für jede globale Gruppe separat die Zugriffsrechte einrichten, auch wenn alle globalen Gruppen dieselben Rechte erhalten sollen.

- Richten Sie hingegen ausschließlich domänenübergreifende lokale Gruppen ein, so können Sie den Mitgliedern keine Berechtigungen für Ressourcen zuweisen, die sich außerhalb der Domäne befinden. Sollte sich Ihr Netzwerk vergrößern und die Einrichtung neuer Domänen erfordern, so bleibt den Benutzern der Zugriff auf die Ressourcen der übrigen Domänen verwehrt.

Gruppenzuordnung im einheitlichen Betriebsmodus

Führen Sie Ihre Domäne bereits im einheitlichen Modus aus (siehe Kapitel 10.1.2), sollten Sie die folgende Strategie verwenden. Dies gilt auch für den Betriebsmodus Windows Server 2003 in der Domänen- und Gesamtstrukturfunktionsebene (siehe Kapitel 10.1.4 und 10.1.5).

- Fassen Sie die Benutzer in universellen Gruppen zusammen, die auf Ressourcen in mehreren Domänen zugreifen müssen. Im Gegensatz zu globalen Gruppen sind Sie bei universellen Gruppen nicht mehr darauf beschränkt, dass die Benutzer einer Domäne angehören müssen. Fügen Sie mehrere globale Gruppen als Mitglied einer universellen Gruppe hinzu.
- Wenn Sie die Mitgliedschaft universeller Gruppen ändern, müssen diese Änderungen an alle Domänencontroller repliziert werden, aus deren Domänen Sie Mitglieder in der Gruppe haben bzw. hinzufügen oder entfernen. Um hier die Belastung zu minimieren, fügen Sie nur Mitglieder zu universellen Gruppen hinzu, die diese Mitgliedschaft langfristig behalten sollen.

Tabelle 18.11 gibt Ihnen eine Zusammenfassung der möglichen Mitglieder der drei Gruppenbereiche in den beiden Windows 2000-Betriebsmodi:

Gruppenbereich	Gemischter Modus	Einheitlicher Modus
Global	Alle Benutzer derselben Domäne	Benutzer und globale Gruppen derselben Domäne
Domänen- übergreifend	Benutzer und globale Gruppen aller Domänen	Benutzer, globale und universelle Gruppen aller Domänen, domänenübergreifende Gruppen derselben Domäne
universell	Nicht verfügbar	Benutzer, globale und universelle Gruppen aller Domänen

Tabelle 18.11: Übersicht über die Gruppenmitgliedschaften

Sie sehen also, dass Sie die größte Freiheit bei der Zusammenstellung von Gruppenmitgliedern in der Verwendung von universellen Gruppen haben. Fügen Sie aber nur Mitglieder zu universellen Gruppen hinzu, wenn dieses absolut notwendig ist.

Verschachteln von Gruppen

Auch das Verschachteln von Gruppen, das auch Zusammenführen von Gruppen genannt wird, kann Ihnen die Administration der Gruppen erleichtern. Angenommen, Sie haben in jeder Domäne eine Gruppe „Verkäufer“. Konfigurieren Sie die entsprechenden Eigenschaften für jede Gruppe. Um anschließend nur allen Verkäufern aller Domänen Zugriff auf bestimmte Ressourcen zu ermöglichen, führen Sie die einzelnen Verkäufergruppen zu einer übergeordneten Verkäufergruppe zusammen. Sie müssen dann

ausschließlich für diese übergeordnete Gruppe den Ressourcenzugriff konfigurieren statt für jede einzelne Verkäufergruppe.

18.5.2 Einrichten und Bearbeiten von Gruppen und Gruppeneigenschaften

In diesem Kapitel wird beschrieben, wie Sie eine neue Gruppe auf einem Domänencontroller erstellen und deren Eigenschaften konfigurieren.

Um eine neue Gruppe zu erstellen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER. Wählen Sie aus dem Kontextmenü des Containers, in dem Sie die neue Gruppe erstellen möchten, den Eintrag NEU / GRUPPE.
2. Geben Sie dann im Feld GRUPPENNAME den Namen für die Gruppe an. Dabei wird das Feld GRUPPENNAME (WINDOWS NT3.5X/4.0) automatisch vervollständigt (siehe Abbildung 18.11). Der Gruppenname muss innerhalb der Domäne eindeutig sein. Wählen Sie auch den passenden Gruppenbereich und Gruppentyp. Klicken Sie dann auf OK, und die Gruppe wird erstellt.

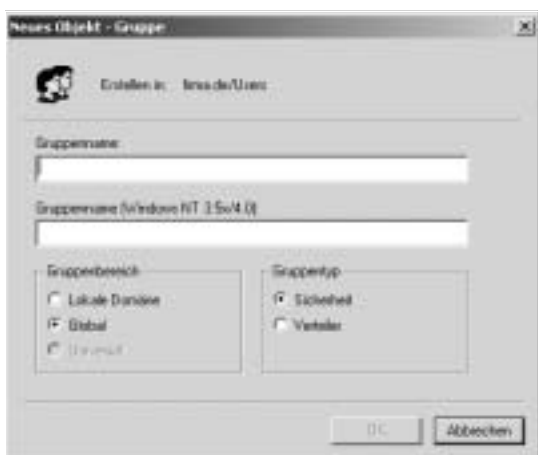


Abbildung 18.11: Erstellen einer neuen Benutzergruppe

Lokale Gruppen erstellen Sie auf dem lokalen Computer über STARTMENÜ / PROGRAMME / VERWALTUNG / COMPUTERVERWALTUNG / LOKALE BENUTZER UND GRUPPEN.

Um zu der neu erstellten Gruppe Mitglieder hinzuzufügen, wählen Sie aus dem Kontextmenü der Gruppe EIGENSCHAFTEN und dort die Registerkarte MITGLIEDER. Klicken Sie auf die Schaltfläche HINZUFÜGEN. Sie können nun Benutzer, Computer, Kontakte oder andere Gruppen auswählen, die Mitglied dieser Gruppe werden sollen. Umgekehrt können Sie auch Benutzer zu Gruppen hinzufügen, indem Sie aus den Benutzereigenschaften die Registerkarte MITGLIED VON wählen.

Um eine Gruppe wieder zu löschen, wählen Sie den entsprechenden Eintrag aus dem Kontextmenü. Eine Gruppe kann nur gelöscht werden, wenn keines der Mitglieder sie als primäre Gruppe definiert hat. Durch das Löschen der Gruppe löschen Sie nicht die

Benutzerkonten der Mitglieder. Da beim Löschen der Gruppe jedoch die SID gelöscht wird, werden auch alle mit der Gruppe verknüpften Berechtigungen entfernt. Das Neu-erstellen einer gleichnamigen Gruppe übernimmt nicht die Einstellungen der alten Gruppe. Eine Gruppe kann erst gelöscht werden, wenn keiner der Mitglieder diese Gruppe mehr als primäre Gruppe definiert hat.

Auch die Eigenschaften des Gruppenbereichs und Gruppentyps können Sie ändern. Sobald Sie z.B. den Betriebsmodus in „einheitlich“ umsetzen, können Sie auch die Gruppen in universelle Gruppen umwandeln. Eine globale Gruppe kann jedoch nicht in eine universelle Gruppe umgewandelt werden, wenn sie noch Mitglied einer anderen globalen Gruppe ist. Auch eine domänenübergreifende Gruppe kann nicht in eine universelle Gruppe umgewandelt werden, solange Sie noch Mitglied einer anderen domänenübergreifenden Gruppe ist. Bei universellen Gruppen kann nicht mehr der Gruppentyp geändert werden. Wird Active Directory im gemischten Modus ausgeführt, ist die Option UNIVERSELLE GRUPPE nicht anwählbar. Sie können auch keine globale Gruppe in eine domänenübergreifende Gruppe und umgekehrt umwandeln.

Um eine der Eigenschaften zu ändern, öffnen Sie die Eigenschaften der Gruppe. Nehmen Sie auf der Registerkarte ALLGEMEIN die gewünschten Änderungen vor.

18.6 Spezielle Optionen für Administratoren

Aus Sicherheitsaspekten sollte der Netzwerk-Administrator nur dann unter dem Benutzerkonto Administrator oder unter einem anderen Konto mit Administratorrechten angemeldet sein, wenn er Aufgaben erledigen muss, für die er die entsprechenden Rechte benötigt. Ansonsten sollte der Administrator sich mit einer Benutzerkennung mit weniger privilegierten Rechten anmelden. Ist der Administrator mit vollen Admin-Rechten angemeldet und holt sich während eines Internet-Besuches einen Virus oder Trojaner, so werden alle Tätigkeiten des Virus ermöglicht, die dem aktuellen Benutzerkonto möglich sind. Bei Administratorrechten können so Daten gelöscht oder Festplatten formatiert werden. Melden Sie sich deshalb über ein Konto an, dem nur minimale Rechte zugewiesen sind.

Sollte es dabei jedoch vorkommen, dass unvorhergesehen das Ausführen einer bestimmten Aufgabe die Administratorrechte verlangt, so kann diese Aktion dennoch unter dem gerade aktuellen Benutzerkonto ausgeführt werden, ohne dass eine Abmeldung und Neu-anmeldung als Administrator am Computer erfolgen muss. Hierzu gibt es die Optionen *Ausführen als* in der grafischen Oberfläche sowie die Kommandozeilenoption *RUNAS*.

18.6.1 Die Option Ausführen als

Sie können jede ausführbare Datei, jede mmc und jedes Element der Systemsteuerung mit der Option *Ausführen als* starten. Dazu müssen Sie lediglich über einen Benutzernamen und ein Passwort verfügen, womit das gewünschte Programm ausgeführt werden darf. Es kann jedoch möglich sein, dass diese Option fehlschlägt, wenn Sie über das Netzwerk ein Programm auf einem anderen Computer ausführen möchten. Dies ist der Fall, wenn das Benutzerkonto, das Sie bei *Ausführen als* angeben, nicht mit dem Konto identisch ist, von dem das Programm ursprünglich gestartet wurde, selbst wenn die Rechte des Ausführen-Kontos ausreichend sind.

Um diese Option zu benutzen, führen Sie die folgenden Schritte aus:

1. Stellen Sie fest, ob unter DIENSTE der Dienst DIENST AUSFÜHREN ALS gestartet ist. Falls dies nicht der Fall ist, starten Sie den Dienst manuell.
2. Markieren Sie die Programmdatei, Verknüpfung, mmc oder das Systemsteuerungselement, das Sie ausführen möchten. Halten Sie die Umschalt-Taste  gedrückt und wählen dann aus dem Kontextmenü AUSFÜHREN ALS.
3. Geben Sie nun an, unter welchem Konto Sie das Programm ausführen möchten. Dazu sind Angaben über Benutzername, Kennwort und Domäne notwendig (siehe Abbildung 18.12).



Abbildung 18.12: Die Option Ausführen als

18.6.2 Verwenden von RUNAS

Das Programm RUNAS wird von der Kommandozeile aus gestartet. Es erfüllt denselben Zweck wie das eben beschriebene *Ausführen als*. Prüfen Sie auch hier zuvor, ob unter Dienste der Dienst DIENST AUSFÜHREN ALS gestartet ist. RUNAS bietet die folgenden Optionen:

```
runas [/profile] [/env] [/netonly] /user:Kontoname Programmpfad
```

Die optionalen Parameter haben folgende Bedeutung:

/profile: Profilpfad des Benutzerkontos, nur nötig, wenn ein Profil geladen werden muss.

/env: wenn die Netzwerkumgebung statt der lokalen Umgebung verwendet werden soll.

/netonly: wenn die Benutzerinformationen nur für den Remote-Zugriff gültig sind.

/user: im Format Computername\Konto bzw. unter 2000 Konto@Computername.

Programmpfad: Pfad zur ausführbaren Datei. Befinden sich Leerzeichen im Programmpfad, müssen die Angaben in Anführungszeichen gesetzt werden.

Eine RUNAS-Befehlszeile könnte folgendermaßen aussehen:

```
runas /user: Administrator@hippokrates.firma.de "mmc %windir%\system32\
Konsole1.msc" 
```

Das Passwort für das Konto können Sie nach Aufforderung eingeben.

19 NTFS-Berechtigungen, Datenträgerkontingente und DFS

In diesem Kapitel werden alle Themen behandelt, die sich auf Zugriffsrechte von Daten und Dateifreigaben beziehen. Zuerst werden Sie die Grundlagen der NTFS-Zugriffsrechte kennen lernen. Der Zugriff auf sämtliche Objekte wird über Zugriffssteuerungslisten (ACLs) gesteuert. Für alle NTFS-Ordner und -Dateien können Sie Berechtigungen vergeben. Sie lernen die standardmäßigen und erweiterten Berechtigungen kennen. Auch das Erstellen von Freigaben und deren Berechtigungen wird erklärt.

19.1 NTFS Ordner- und Dateiberechtigungen

Zunächst werden Sie mit der Grundlage der Zugriffssteuerung auf Objekte, den Zugriffssteuerungslisten (ACLs), in ihrer Funktion vertraut gemacht. Ohne ACLs können die Zugriffsrechte nicht angewendet werden. Danach lernen Sie die verschiedenen Berechtigungsstufen für NTFS-Ordner und -Dateien sowie besondere Berechtigungen kennen. Auch das Zusammenspiel von mehreren Berechtigungen wird Ihnen vorgeführt. Im letzten Kapitel werden die Regeln aufgelistet, wie sich die Zugriffsrechte beim Verschieben oder Kopieren der Objekte ändern können.

Vor der Einrichtung der NTFS-Berechtigungen sollten Sie jedoch die Struktur der Ordner planen, in denen Sie Unterordner und Dateien speichern möchten. Erstellen Sie diese Ordner nach Möglichkeit auf einem separaten Dateiserver und nicht auf einem Domänencontroller. Der Domänencontroller würde durch den Dateizugriff zu stark belastet werden. Weiterhin sollten Sie die Daten auf einer Partition anlegen, auf der sich nicht das Betriebssystem befindet. Um sich die Sicherung der Daten zu erleichtern, können Sie auf dieser Partition auch die Basisverzeichnisse der Benutzer anlegen.

Sie sollten die Benutzer, die eine ähnliche Funktion in dem Unternehmen ausüben und damit ähnliche Zugriffsrechte benötigen, immer zu Gruppen zusammenfassen. Sie müssen dann nur der Gruppe und nicht jedem Benutzer einzeln die Rechte zuweisen. Zum Schutz der Daten durch unbeabsichtigtes oder virenbedingtes Löschen sollten Sie allen Benutzern und Administratoren für diese Verzeichnisse nur das Recht **LESEN / AUSFÜHREN** zuweisen.

19.1.1 Was bedeuten ACL, ACE, DACL und SACL?

Für jede Datei und jeden Ordner, die auf einem mit NTFS formatierten Laufwerk erstellt werden, wird gleichzeitig eine Zugriffssteuerungsliste (= Access Control List, ACL), oder genauer gesagt zwei ACLs, erstellt. Diese beiden ACLs befinden sich im Sicherheitsbeschreiber (Security Identifier, SID) des Objekts. Dabei ist es gleichgültig, ob das Lauf-

werk mit NTFS 4 oder 5 formatiert wurde. Der Zugriff auf bestimmte Ressourcen kann über ACLs für bestimmte Benutzer oder Gruppen eingeschränkt oder sogar ganz verweigert werden. Die ACLs einer Datei oder eines Ordners sehen Sie über die Eigenschaften auf der Registerkarte SICHERHEITSEINSTELLUNGEN.

Die beiden ACLs sind die DACL (Discretionary Access Control List) und die SACL (System Access Control List). Über die DACL werden die Berechtigungen der Benutzer für ein bestimmtes Objekt festgelegt, die im Active Directory hinterlegt sind. Über die SACL werden die Ereignisse bezüglich der Berechtigungen bestimmt, die eine Überwachungs-nachricht bei Erfolg oder Misserfolg generieren. Sind Überwachungsereignisse definiert, können diese auf einem Domänencontroller vom System protokolliert werden. Nähere Informationen zur Zugriffsüberwachung finden Sie in Kapitel 22. Für uns ist im Moment die DACL interessanter.

Für jeden Benutzer und jede Gruppe wird beim Erstellen eine eindeutige SID (Security Identifier) angelegt. Beim Zuweisen der Zugriffsberechtigungen werden die SIDs der Benutzer und Gruppen in die DACLs der Objekte geschrieben. Anhand der SID in der DACL wird geprüft, ob für den Benutzer ein ACE (Access Control Entry) vorliegt. Ist ein ACE vorhanden, kann der Benutzer gemäß der ihm zugewiesenen Rechte auf das Objekt zugreifen. Ist kein ACE vorhanden, wird ihm der Zugriff auf die Ressource verweigert. Dieses Ereignis kann über die SACL protokolliert werden. Ein DACL ist somit die Summe aller vorhandenen ACEs für ein bestimmtes Objekt.

Ein ACE kann sich entweder auf das gesamte Objekt oder auch nur auf einzelne Eigenschaften eines Objekts beziehen. Damit sind die Zugriffsrechte feiner granulierbar. Sie können so z.B. einer Benutzergruppe erlauben, die Eigenschaft E-Mail-Adresse, nicht aber die Eigenschaft Adresse eines Benutzers zu lesen.

Bei den DACLs ist zwischen einer leeren und einer nicht vorhandenen DACL zu unterscheiden. Ist eine DACL leer, so bedeutet dies, dass kein anderer Benutzer außer dem Eigentümer der Datei oder des Ordners Zugriff auf die Ressource besitzt. Ist hingegen für eine Datei oder einen Ordner keine DACL vorhanden, so sind für diese Ressource keinerlei Sicherheitsrestriktionen festgelegt. Auf das Objekt kann also von jedem Benutzer mit der Berechtigung VOLLZUGRIFF zugegriffen werden.

19.1.2 Rechte für NTFS-Ordner und -Dateien

Dieses Kapitel zeigt Ihnen die standardmäßigen Berechtigungen, die Sie NTFS-Ordnern und -Dateien zuweisen können. Sie finden diese Zugriffsrechte unter Windows 2000 in den Eigenschaften eines Ordners oder einer Datei auf der Registerkarte SICHERHEITSEINSTELLUNGEN. Unter Windows Server 2003 und Windows XP finden Sie diese Einstellungen im Kontextmenü FREIGABE UND SICHERHEIT und dort auf der Registerkarte SICHERHEIT. Dazu muss sich die Datei oder der Ordner auf einem NTFS-Laufwerk befinden. Diese Registerkarte mit den Zugriffsrechten wird auch ACL-Editor genannt (siehe Abbildung 19.1).



Abbildung 19.1: Der ACL-Editor



Standardmäßig erhält die Benutzergruppe „Jeder“ für alle Objekte die Berechtigung VOLLZUGRIFF. Diese Standardoption sollte vom Administrator entfernt und durch andere Berechtigungen ersetzt werden. Ansonsten hat jeder Benutzer, einschließlich den Gästen, vollen Zugriff auf alle Daten und kann diese lesen, löschen oder ändern.

Über die Schaltfläche ERWEITERT können Sie eine Reihe von speziellen Berechtigungen konfigurieren (siehe Abbildung 19.2). Diese Zugriffsberechtigungen sind nur auf Laufwerken verfügbar, die mit NTFS formatiert sind, nicht jedoch auf Laufwerken mit FAT16 oder FAT32. Bei FAT-Laufwerken erfolgt die Zugriffssteuerung nur auf Freigabeebene, bei NTFS-Laufwerken basierend auf den Zugriffsrechten für Dateien und Benutzer. FAT-Laufwerke differenzieren nicht die Zugriffsmöglichkeiten für verschiedene Ordner und Dateien in einer Freigabe. Sie kennen nur die Optionen LESEN, SCHREIBEN und VOLLZUGRIFF.

Die NTFS-Ordnerberechtigungen beziehen sich auf Ordner und darin enthaltene Unterordner, die NTFS-Dateiberechtigungen auf einzelne Dateien. Es gibt insgesamt sechs Ordnerberechtigungen und fünf Dateiberechtigungen. Die folgende Tabelle zeigt Ihnen die einzelnen Berechtigungen, ihre Beschreibung sowie die Verfügbarkeit für Ordner und / oder Dateien.

Berechtigung	Verfügbar für: O = Ordner D = Dateien	Beschreibung
Vollzugriff	O, D	Löschen von Ordnern, Dateien und Unterordnern; Ändern von Berechtigungen; Übernehmen des Besitzes; alle Operationen der anderen NTFS-Berechtigungen.
Ändern	O, D	Löschen des Ordners oder der Datei; alle Operationen der Rechte Schreiben und Lesen, Ausführen.
Lesen, Ausführen	O, D	Navigieren in der Ordnerstruktur, um Ordner oder Dateien zu erreichen, für die Zugriff besteht. Für die Ordner, durch die navigiert wird, muss keine Berechtigung vorhanden sein; alle Operationen der Rechte Ordnerinhalt auflisten und Lesen.
Ordnerinhalt auflisten	O	Anzeigen der Namen von Ordnern und Unterordnern
Lesen	O, D	Lesen von Dateien und Ordnern, der Berechtigungen, des Besitzers und der Ordner- bzw. Dateiattribute
Schreiben	O, D	Erstellen neuer Dateien und Ordner bzw. Überschreiben der Datei; Ändern der Ordner- bzw. Dateiattribute; Lesen der Berechtigungen und des Besitzers

Tabelle 19.1: Die NTFS-Ordner- und -Dateiberechtigungen

Um einem Benutzer oder einer Gruppe den Zugriff auf eine Ressource komplett zu verweigern, markieren Sie die Checkbox VERWEIGERN in der Spalte VOLLZUGRIFF.

Wenn ein Benutzer Mitglied in mehreren Gruppen ist, denen Sie verschiedene Berechtigungen zugewiesen haben, oder Sie dem Benutzer und seiner Gruppe verschiedene Berechtigungen zugewiesen haben, sind möglicherweise nicht alle Berechtigungen effektiv gültig, sofern sie sich einander ausschließen.

Haben Sie dem Benutzer und seiner Gruppe verschiedene Rechte zugeteilt, so werden diese addiert. Hat die übergeordnete Gruppe Leserechte an einem Ordner und der Benutzer zusätzlich auch Schreibrechte, so verfügt er über die Rechte Lesen und Schreiben. Bei der Zuweisung von verschiedenen Berechtigungen zu Dateien und Ordnern haben die zugewiesenen Dateiberechtigungen Vorrang. Ist z.B. für einen Benutzer der Zugriff auf einen Ordner verweigert, aber Zugriff auf eine bestimmte Datei darin gestattet, so kann der Benutzer dennoch auf diese Datei zugreifen.

Haben Sie einem Benutzer den Zugriff für eine bestimmte Datei oder einen Ordner verweigert, so wird dieser Verweigerung vor den erlaubten Operationen Vorrang eingeräumt. Haben Sie einem Benutzer für einen Ordner Vollzugriff gewährt, aber für eine darin enthaltene Datei den Zugriff verweigert, so kann er nicht auf diese Datei zugreifen, obwohl er für den übergeordneten Ordner Vollzugriff besitzt. Beim Einrichten der Zugriffsrechte sollten Sie jedoch lieber mit eingeschränkten Berechtigungen als mit Verweigerungen arbeiten.

19.1.3 Spezielle NTFS-Berechtigungen

Sie gelangen an die Konfiguration der speziellen Berechtigungen, wenn Sie im ACL-Editor (siehe Abbildung 19.1) auf die Schaltfläche ERWEITERT klicken. Sie sehen dort die Einträge des ACL-Editors in ausführlicherer Form. Dieses Fenster wird auch als ACS- (Access Control Settings-)Fenster bezeichnet.

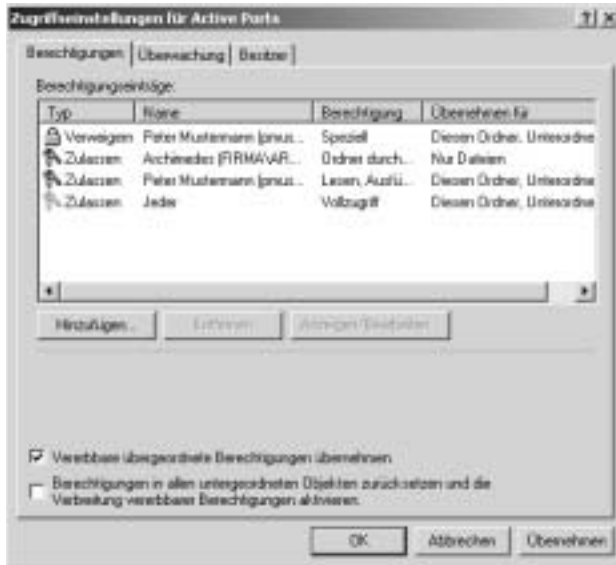


Abbildung 19.2: Das ACS-Fenster

Sie sehen hier sowohl die globalen Berechtigungen, die im vorigen Kapitel beschrieben wurden, als auch die speziellen Berechtigungen. In der Spalte TYP wird angegeben, ob dem Benutzer Berechtigungen zugelassen oder verweigert werden. Sind für einen Benutzer sowohl erlaubte als auch verweigte Berechtigungen konfiguriert, werden zwei Einträge des Benutzers in der Liste angezeigt. Werden für einen Eintrag Berechtigungen geerbt, wird das Symbol ZULASSEN / VERWEIGERN durchsichtig dargestellt. Damit haben Sie einen schnelleren Überblick über die Vererbung. In der letzten Spalte wird angezeigt, wofür diese Berechtigungen übernommen werden, z.B. NUR DATEIEN oder DIESEN ORDNER, UNTERORDNER.

Um für das Objekt spezielle Berechtigungen festzulegen, markieren Sie den Benutzer oder die Gruppe, für die Sie die speziellen Berechtigungen konfigurieren möchten. Klicken Sie dann auf ANZEIGEN / BEARBEITEN. Um einen neuen Benutzer oder eine Gruppe hinzuzufügen, klicken Sie auf HINZUFÜGEN. Sie erhalten in beiden Fällen ein Fenster NAMENS BERECHTIGUNGSEINTRAG FÜR ORDNERNAME / DATEINAME (siehe Abbildung 19.3).



Abbildung 19.3: Die speziellen NTFS-Berechtigungen

Im Feld NAME sehen Sie, für wen die aktuellen Rechte konfiguriert werden. Über ÄNDERN können Sie einen anderen Benutzer auswählen. In der Drop-down-Liste können Sie auswählen, für welche Bereiche des Objekts die Einstellungen übernommen werden sollen. Die Liste Berechtigungen zeigt Ihnen insgesamt 13 verschiedene Berechtigungen an, die Sie zulassen oder verweigern können. Werden die Einstellungen von einem übergeordneten Objekt geerbt, ist die Spalte ZULASSEN grau unterlegt. Sie können in diesem Fall nur Berechtigungen verweigern. Erbt das zu bearbeitende Objekt keine Berechtigungen, können Sie die Einstellungen frei wählen.

Die im letzten Kapitel vorgestellten sechs Standardberechtigungen Vollzugriff, Ändern, Lesen / Ausführen, Ordnerinhalt auflisten, Lesen sowie Schreiben setzen sich aus jeweils mehreren dieser speziellen Berechtigungen zusammen. Im ACS-Fenster sehen Sie in der Spalte BERECHTIGUNG den Typ. Es kann sich entweder um eine der sechs Standardberechtigungen handeln, um den Eintrag SPEZIELL, wenn die Standardberechtigungen abgewandelt sind, oder um den Namen der speziellen Berechtigung, wenn nur eine davon ausgewählt wird.

Tabelle 19.2 gibt Ihnen einen Überblick über die Bedeutung der speziellen Berechtigungen sowie eine Übersicht, mit welchen der sechs Standardberechtigungen die speziellen Rechte verknüpft sind.

Spez. Berechtigung	Beschreibung	V	Ä	L, Ä	O	L	S
Ordner durchsuchen/ Datei ausführen	Ein Ordner, für den keine Rechte bestehen, kann durchsucht werden, um eine Datei zu erreichen. Auch das Ausführen von Dateien kann erlaubt werden.	x	x	x	x		
Ordner auflisten/ Daten lesen	Namen von Unterordnern und Dateien anzeigen, Anzeigen der Daten in allen Dateien	x	x	x	x	x	
Attribute lesen	NTFS-Attribute wie versteckt oder schreibgeschützt lesen	x	x	x	x	x	
Erweiterte Attribute lesen	Erweiterte, von Programmen definierte Attribute lesen	x	x	x	x	x	
Dateien erstellen/ Daten schreiben	Erstellen von Dateien im Ordner und Überschreiben vorhandenen Dateiinhalts	x	x				x
Ordner erstellen/ Daten anhängen	Erstellen neuer Ordner, Änderungen am Dateieinde, kein Ändern, Löschen oder Überschreiben von Dateien	x	x				x
Attribute schreiben	NTFS-Attribute wie versteckt oder schreibgeschützt schreiben	x	x				x
Erweiterte Attribute schreiben	Erweiterte, von Programmen definierte Attribute schreiben	x	x				x
Unterordner und Dateien löschen	Löschen von Unterordnern oder Dateien im Ordner	x					
Löschen	Löschen von Dateien und des Ordners selbst	x	x				
Berechtigungen lesen	Lesen der Berechtigungen wie „Vollzugriff“ etc.	x	x	x	x	x	x
Berechtigungen ändern	Ändern der Berechtigungen wie „Vollzugriff“ etc.	x					
Besitz übernehmen	Den Besitz über eine Datei oder einen Ordner übernehmen. Der Besitzer kann grundsätzlich die Berechtigungen ändern.	x					

Tabelle 19.2: Spezielle NTFS-Berechtigungen

Die verwendeten Abkürzungen bedeuten: V = Vollzugriff, Ä = Ändern, L, Ä = Lesen, Ändern, O = Ordnerinhalt auflisten (nur Ordner), L = Lesen, S = Schreiben



Bei mehreren zugewiesenen Datei- und Ordnerberechtigungen haben die Dateiberechtigungen Vorrang. Eine Ausnahme bildet jedoch die Ordnerberechtigung VOLLZUGRIFF. Da Windows über das POSIX-Teilsystem auch Unix-Applikationen unterstützt und Sie unter Unix mit der Berechtigung VOLLZUGRIFF auch Dateien in einem Verzeichnis löschen können, muss diese Option auch unter Windows bereitgestellt werden. In der Windows-Berechtigung VOLLZUGRIFF ist deshalb die spezielle Berechtigung UNTERORDNER UND DATEIEN LÖSCHEN enthalten. Somit können Sie mit der Ordnerberechtigung auch Dateien in einem Ordner löschen, egal welche Dateiberechtigungen Sie für diese Dateien besitzen. Dies ist der einzige Fall, in dem eine Ordnerberechtigung Vorrang vor einer Dateiberechtigung hat. Um zu verhindern, dass ein Benutzer mit Vollzugriff einzelne Dateien in einem Ordner löscht, deaktivieren Sie in den erweiterten Optionen die Berechtigung UNTERORDNER UND DATEIEN LÖSCHEN.

19.1.4 Verschieben und Kopieren von Ordnern und Dateien

Wenn Sie eine Datei auf ein Laufwerk kopieren oder verschieben, das mit FAT16 oder FAT32 formatiert wurde, gehen dort sämtliche Berechtigungen verloren, da die NTFS-Berechtigungen von FAT nicht unterstützt werden. Die folgenden Ausführungen beziehen sich demnach nur auf NTFS-Datenträger.

Beim Kopieren innerhalb eines Datenträgers übernimmt die Datei oder der Ordner die Zugriffsberechtigungen des Zielverzeichnisses. Beim Verschieben innerhalb eines Datenträgers behält die Datei oder der Ordner seine ursprünglichen Berechtigungen. Beim Verschieben zwischen zwei Datenträgern werden die Berechtigungen des Zielordners übernommen. Das Verschieben zwischen zwei Datenträgern wird als das Kopieren der Datei oder des Ordners auf den anderen Datenträger mit anschließendem Löschen der Quelle angesehen. Also werden analog zu einem Kopiervorgang innerhalb eines Datenträgers die Berechtigungen des Zielverzeichnisses übernommen.

19.1.5 Berechtigungsvererbung

Standardmäßig werden von untergeordneten Ordnern und Dateien die Berechtigungen des übergeordneten Ordners übernommen. Die Berechtigungen werden an alle in ihm enthaltenen Objekte vererbt und gelten auch für die Objekte, die neu in dem Ordner erstellt werden. Wenn Sie für einen Ordner nur Lesezugriff erteilen, darf auch auf alle darin enthaltenen Dateien nur lesend zugegriffen werden.

Sie sehen im ACL-Editor (siehe Abbildung 19.1), dass standardmäßig die Checkbox VERERBBARE ÜBERGEORDNETE BERECHTIGUNGEN ÜBERNEHMEN aktiviert ist. Um die Vererbung zu deaktivieren, müssen Sie diese Checkbox deaktivieren. Beim Deaktivieren werden Sie gefragt, wie die vererbten Einträge behandelt werden sollen. Ihnen stehen dafür drei Optionen zur Verfügung: Kopieren, Entfernen oder Abbrechen. Mit KOPIEREN haben Sie die Möglichkeit, die bis zu diesem Punkt weitervererbten Berechtigungen an das aktuelle Objekt zu kopieren, aber weitere Vererbungen zu verweigern, mit ENTFERNEN werden die übergeordneten Berechtigungen nicht an das Objekt übertragen, sondern nur die von Ihnen konfigurierten angewendet. Mit ABBRECHEN wird die Checkbox nicht deaktiviert.

Damit werden die für den übergeordneten Ordner konfigurierten Rechte nicht an Unterordner und Dateien weitergegeben. An der Stelle, ab der die Berechtigungen nicht weitervererbt werden sollen, wird der entsprechende Unterordner zum neuen übergeordneten Ordner. Alle in ihm erstellten Dateien und Ordner erben die speziell für ihn konfigurierten Zugriffsberechtigungen.

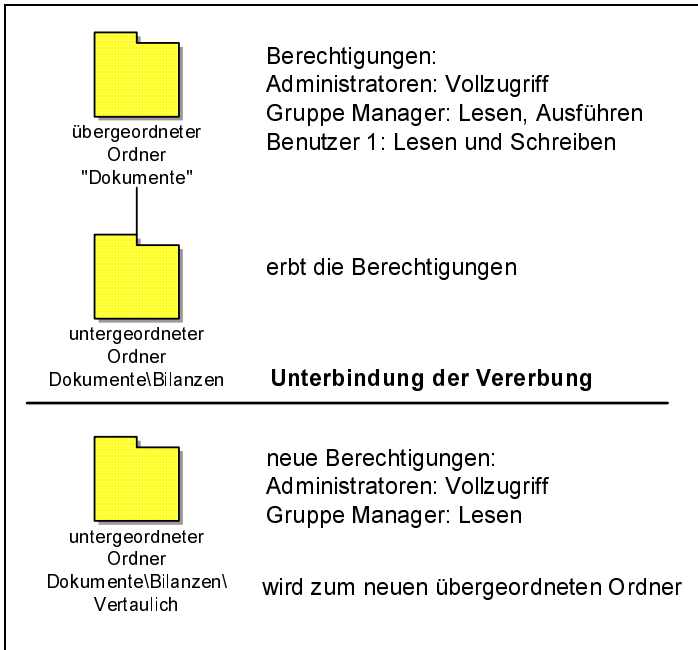


Abbildung 19.4: Die Berechtigungsvererbung

In unserem Beispiel erhält der übergeordnete Ordner *Dokumente* bestimmte Berechtigungen, die vom Unterordner *Dokumente\Bilanzen* geerbt werden. Im Unterordner *Bilanzen* wird der nächste Unterordner *\Vertraulich* erstellt. Für diesen Ordner wird die Vererbung der Berechtigungen deaktiviert. Diesem Ordner werden neue Rechte zugeteilt. Damit wird er zum neuen übergeordneten Ordner und vererbt diese Berechtigungen an alle seine Unterordner und Dateien, bis möglicherweise an einem nächsten Punkt die Vererbung deaktiviert wird.

19.1.6 Ändern der DACLS mit CACLS

Nachdem Sie die Funktionsweise der DACLS und die verschiedenen Zugriffsrechte, die Sie vergeben können, kennen gelernt haben, wird Ihnen nun das Dienstprogramm CACLS vorgestellt. Mit diesem Programm können Sie an der Kommandozeile die DACLS für bestimmte Dateien und Ordner ansehen und ändern. Dieses Programm ist sinnvoll, wenn Sie eine größere Anzahl von DACLS ändern möchten und dafür eine Batchdatei erstellen. Der Funktionsumfang ist identisch mit den Einstellungen, die Sie über den ACL-Editor der grafischen Oberfläche vornehmen können.

Wenn Sie an der Kommandozeile CACLS aufrufen, haben Sie die folgenden Optionen zur Verfügung:

CACLS Dateiname [/T] [/E] [/C] [/G Benutzer:Zugriff] [/R Benutzer [...]]
[/P Benutzer:Zugriff [...]] [/D Benutzer [...]]

Die einzelnen Parameter haben die folgende Bedeutung (siehe Tabelle 19.3):

Parameter	Bedeutung
Dateiname	Zeigt die ACLs für die Datei an, es können im Dateinamen auch Wildcards verwendet werden
/T	Die ACLs von „Dateiname“ im Verzeichnis und allen Unterverzeichnissen bearbeiten
/E	Bearbeiten der ACL, anstatt sie zu ersetzen
/C	Fortsetzen des Änderns, auch wenn eine Zugriffsverletzung auftritt
/G Benutzer:	Zulassen der hinter : angegebenen Zugriffsarten. Diese können sein: R – Lesen, W – Schreiben, C – Ändern, F – Vollzugriff
/R Benutzer	Rechte des Benutzers aufheben, dafür muss /E gesetzt sein
/P Benutzer:	Ersetzen der hinter : angegebenen Zugriffsarten. Diese können sein: R – Lesen, W – Schreiben, C – Ändern, F – Vollzugriff
/D Benutzer	Verweigern des Zugriffs für den Benutzer

Tabelle 19.3: Die Parameter für CACLS

Bei der Variablen Benutzer können Sie in einem Befehl auch mehrere Benutzer angeben, für die die Optionen gelten sollen.

19.2 Planen und Erstellen von Freigaben

Nachdem Sie im vorigen Kapitel die Grundlagen der NTFS-Berechtigungen kennen gelernt haben, werden Ihnen nun die Freigabe von Ordnern im Netzwerk und die Freigabeberechtigungen vorgestellt. Die NTFS-Berechtigungen gelten unabhängig davon, ob auf eine Datei oder einen Ordner lokal oder über das Netzwerk zugegriffen wird.

Die Berechtigungen, die Sie für freigegebene Ordner konfigurieren können, sind nicht so detailliert wie die NTFS-Freigaben. Beide Arten der Freigabe können jedoch miteinander kombiniert werden. Die Freigabeberechtigung ist immer für den gesamten freigegebenen Ordner mit allen seinen Inhalten gültig. Es gibt keine einzeln zuweisbaren Berechtigungen für bestimmte Dateien oder Unterordner. Wie bei den NTFS-Berechtigungen lautet auch bei Freigabeberechtigungen die Standardeinstellung JEDER/VOLLZUGRIFF. Die Freigabeberechtigungen können auch auf FAT16- und FAT32-Datenträgern eingerichtet werden.

Tabelle 19.4 zeigt den Vergleich zwischen Freigabe- und NTFS-Berechtigungen.

Berechtigung für	NTFS-Berechtigung	Freigabeberechtigung
Datenträger	Nur NTFS	NTFS, FAT16, FAT32
Ressourcen	Ordner, Unterordner und Dateien	Nur Ordner
Zugriffsart	Lokal und Netzwerkzugriff	Nur Netzwerkzugriff

Tabelle 19.4: NTFS- und Freigabeberechtigungen im Vergleich

Für die Freigabeberechtigungen gibt es drei verschiedene Berechtigungsoptionen. Dabei handelt es sich um Vollzugriff, Ändern und Lesen. Analog zu den NTFS-Berechtigungen können Sie auch hier Berechtigungen zulassen und verweigern. Sind einem Benutzer über mehrere Gruppenmitgliedschaften mehrere Rechte zugewiesen, werden diese addiert. Das Verweigern hat Vorrang vor Erlauben. Diese drei Optionen erlauben die folgenden Operationen (siehe Tabelle 19.5):

Berechtigung	Beschreibung
Vollzugriff	Alle Operationen der Berechtigungen Ändern und Lesen sowie bei NTFS-Datenträgern Besitzübernahme und Ändern der Berechtigungen.
Ändern	Erstellen und Löschen von Unterordnern und Dateien, Ändern des Dateiinhalts sowie alle Operationen der Berechtigung Lesen.
Lesen	Anzeigen der Namen von Unterordnern und Dateien, Lesen von Dateien, Ausführen von Programmen

Tabelle 19.5: Die Freigabe-Berechtigungen



Auf NTFS-Datenträgern muss für den erfolgreichen Zugriff neben der Freigabeberechtigung auch die entsprechende NTFS-Berechtigung vorliegen. Liegt diese nicht vor, kann der Zugriff allein mit Freigabe-Rechten nicht gewährt werden.

Wenn Sie einen freigegebenen Ordner kopieren, verschieben oder umbenennen, so ist dieser nicht länger freigegeben.

In freigegebene Ordner können Sie alle Unternehmensdaten zentral an einem Ort ablegen, um damit die Sicherung der Daten zu zentralisieren. Die Datenordner können in großen Unternehmen wiederum in öffentliche und gruppenspezifische Daten unterteilt werden. Für öffentliche Daten sollten Sie den Benutzern die Freigabe-Berechtigung **ÄNDERN** zuteilen, sodass sie dort Dateien lesen und speichern können, auf die alle Benutzer Zugriff haben. Weiterhin sollten Sie gruppenspezifische Ordner einrichten, auf die nur Mitglieder bestimmter Arbeitsgruppen Zugriff haben, andere Mitglieder jedoch nicht. Hier können Sie z.B. Freigaben für Dokumente, die nur die Personalabteilung, das Marketing usw. betreffen, einrichten.

Falls Ihr Unternehmen auch Anwendungen zentral verwaltet, sollten Sie in einen freigegebenen Ordner alle Applikationen legen, die auf einem Netzwerkserver installiert werden und auf den die Clients zugreifen, ohne selbst die Anwendung installieren zu müssen.

19.2.1 Erstellen von Freigaben

Um einen Ordner freizugeben, wählen Sie den entsprechenden Eintrag aus dem Kontextmenü. Zum Erstellen einer Freigabe müssen Sie Mitglied der Gruppe „Administrator“, „Hauptbenutzer“ oder „Server-Operator“ sein. Sie erhalten dann folgendes Fenster (siehe Abbildung 19.5):



Abbildung 19.5: Erstellen einer Freigabe

Markieren Sie die Checkbox **DIESEN ORDNER FREIGEBEN**, und geben Sie einen Freigabennamen an. Bei der Vergabe eines Freigabennamens müssen die folgenden Konventionen erfüllt werden: Die Namenslänge für die Freigabe ist auf den Clientbetriebssystemen Windows 9x/NT/2000/XP auf 80 Zeichen begrenzt, die Namenslänge des Ordners darf 255 Zeichen nicht überschreiten. Für Clients mit den Betriebssystemen MS-DOS, Windows 3.1 und Windows for Workgroups muss das 8.3-Format eingehalten werden.

Wenn Sie mehrere Freigaben erstellen, sollten Sie im Feld **KOMMENTAR** eine Beschreibung angeben. Diese wird für die Benutzer zusammen mit dem Namen der Freigabe angezeigt und erleichtert ihnen das Auffinden des gesuchten Ordners.

Standardmäßig ist die Anzahl der gleichzeitigen Benutzerverbindungen nicht begrenzt. Ein Windows 2000-Server kann beliebig viele gleichzeitige Verbindungen verarbeiten, abhängig von der Anzahl der Clientzugriffslicenzen, Windows 2000 Professional zehn gleichzeitige Verbindungen.

Indem Sie auf die Schaltfläche **BERECHTIGUNGEN** klicken, können Sie die Benutzer und Gruppen auswählen, für die Sie die Zugriffsrechte konfigurieren möchten. Standardmäßig findet sich nur der Eintrag **JEDER** mit dem Recht **VOLLZUGRIFF**. Diese Berechtigung sollten Sie entfernen und durch restriktivere Berechtigungen ersetzen.

Über die Schaltfläche ZWISCHENSPEICHERN können Sie bestimmen, wie die Dateien und Programme, auf die vom Netzwerk aus zugegriffen wird, in diesem Ordner zwischengespeichert werden sollen. Dafür stehen Ihnen drei Optionen zur Verfügung. Es können manuelle (Standard) und automatische Zwischenspeicherungen von Dokumenten und automatische Zwischenspeicherungen von Programmen zugelassen werden.

Wenn ein Ordner bereits einmal freigegeben wurde, haben Sie die zusätzliche Schaltfläche NEUE FREIGABE zur Verfügung. Sie können denselben Ordner nun unter einem anderen Namen freigeben. Dies ist sinnvoll, wenn Sie die Freigabenamen umstrukturiert haben, aber den Benutzern dennoch die Freigabe unter dem alten Namen zur Verfügung stellen möchten. Sie können später auch wieder Freigabenamen entfernen, wenn ein Ordner mehrfach freigegeben wurde.

Eine Übersicht über alle erstellten Freigaben sowie die automatischen administrativen Freigaben finden Sie in der Computerverwaltung unter FREIGELEGEBENE ORDNER / FREIGABEN.

19.2.2 Administrative Freigaben

Neben den eben beschriebenen manuell eingerichteten Freigaben werden auf jedem System automatisch administrative Freigaben eingerichtet. Diese administrativen Freigaben sind jedoch nicht für die Benutzer sichtbar, die auf den Computer zugreifen. An alle administrativen Freigaben wird das Zeichen „\$“ angefügt, das diese Art der Freigabe kennzeichnet.

Standardmäßig gibt es die folgenden administrativen Freigaben auf jedem System: C\$, D\$... n\$, Admin\$, IPC\$ und Print\$. Tabelle 19.6 zeigt die Bedeutung der verschiedenen Freigaben.

Administrative Freigabe	Beschreibung
C\$, D\$	Das Rootverzeichnis jeder Partition wird administrativ freigegeben. Über diese Freigabe können Sie auf den Datenträger komplett zugreifen.
Admin\$	Dieses ist die Freigabe von %SYSTEMROOT%. Über diese Freigabe kann Windows verwaltet werden, ohne dass der Pfad von %SYSTEMROOT% bekannt sein muss.
IPC\$	Diese Freigabe wird bei der Anzeige der freigegebenen Ordner sowie der Remote-Verwaltung eines Computers benutzt.
Print\$	Diese Freigabe wird erst erstellt, sobald Sie einen Drucker freigegeben haben. Sie verweist auf den Pfad %SYSTEMROOT%\SYSTEM32\POOL\DRIVERS. Dort werden die Druckertreiber für die Clients hinterlegt.

Tabelle 19.6: Die administrativen Freigaben

Sie können jedoch auch selbst weitere administrative Freigaben erstellen. Dazu müssen Sie einfach das \$-Zeichen an das Ende des Freigabenamens setzen. Damit können nur noch die Benutzer auf den Ordner zugreifen, die den Freigabenamen kennen und die entsprechende Berechtigung für diesen Ordner haben.

19.2.3 Rechte für Freigaben und NTFS-Rechte kombinieren

Wenn Sie für Ihre Freigaben nur Rechte auf Freigabeebene konfigurieren, können Sie nicht Berechtigungen für bestimmte Benutzer und Gruppen für die darin enthaltenen Dateien und Unterordner einrichten. Deshalb haben Sie die Möglichkeit, NTFS-Berechtigungen und Freigabeberechtigungen miteinander zu kombinieren. Dies gilt selbstverständlich nur dann, wenn sich die Freigabe auf einem NTFS-Datenträger befindet. Wenn Sie auf diese Weise verschiedene Berechtigungen miteinander verknüpfen, gilt immer die am weitesten eingeschränkte Berechtigung. Angenommen, ein Benutzer hat für einen freigegebenen Ordner VOLLZUGRIFF, aber für alle darin enthaltenen Dateien nur die NTFS-Berechtigung LESEN, so gilt für diese Dateien die am weitesten eingeschränkte Berechtigung, nämlich LESEN.

Eine Übersicht über alle erstellten Freigaben sowie die automatischen administrativen Freigaben finden Sie in der Computerverwaltung unter FREIGELEGEBENE ORDNER/FREIGABEN. Dort können Sie für jede Freigabe unter den Eigenschaften unter FREIGABEBERECHTIGUNGEN die Freigabe-Berechtigungen und unter SICHERHEITSEINSTELLUNGEN die NTFS-Berechtigungen konfigurieren. Dies dürfte der komfortabelste Weg sein, um die beiden Berechtigungen miteinander zu verknüpfen.

Damit ein Benutzer auf einen Ordner zugreifen kann, für den Sie beide Berechtigungsarten kombiniert haben, muss er auch über die entsprechenden NTFS-Berechtigungen verfügen. Durch die Kombination der beiden Berechtigungsarten erreichen Sie die größtmögliche Flexibilität bei der Zuweisung von Berechtigungen.

19.3 Datenträgerkontingente

Über Datenträgerkontingente können Sie festlegen, wie viel Speicherplatz ein Benutzer auf einem bestimmten Laufwerk belegen darf. Damit können Sie sicherstellen, dass der vorhandene Speicherplatz gleichmäßig zwischen den Benutzern aufgeteilt wird. Da Datenträgerkontingente jedoch nicht das eigentliche Thema von Active Directory, sondern eher von Windows 2000 generell sind, wird das Thema hier auch nur kurz angerissen. Weitere Informationen finden Sie in der Hilfe zu Windows 2000/2003.

Datenträgerkontingente können Sie auf Laufwerken aktivieren, auf denen sich die Benutzerprofile oder Basisverzeichnisse der Benutzer befinden. Sie können eine Maximalgröße des Benutzerordners und Schwellwerte für Warnmeldungen konfigurieren, wenn das Kontingent bald erschöpft ist. Ist das Limit des Kontingents erreicht, kann der Benutzer keine weiteren Daten in seinem Benutzerordner speichern. Damit können Sie sicherstellen, dass ein Benutzer nicht beliebig viele, möglicherweise nie benutzte Daten in seinem Ordner anlegen kann und damit zu viel Festplattenplatz auf dem Dateiserver verschwendet. Er wird so gezwungen, seine Datenbestände regelmäßig zu überprüfen. Bei Datenträgerkontingenten wird die Größe des Benutzerordners nach den Dateien berechnet, für die er der Besitzer ist.

Sie müssen die Datenträgerkontingente einrichten, bevor die Benutzer auf den Datenträger zugreifen. Wenn bereits vor Aktivierung der Datenträgerkontingente Benutzer Daten auf dem Datenträger speichern, greifen die Kontingenteinstellungen nicht mehr für sie, sondern ausschließlich für die Benutzer, die nach der Kontingentaktivierung das erste Mal auf den Datenträger zugreifen.

Datenträgerkontingente können Sie lediglich auf Datenträgern einrichten, die mit NTFS formatiert sind. Um für eine Netzwerkfreigabe die Kontingenteinstellung durchzusetzen, müssen Sie das Rootverzeichnis des Laufwerks freigeben.

Sie finden die Einstellungen zu Datenträgerkontingenten in den Eigenschaften eines Laufwerks auf der Registerkarte KONTINGENT (siehe Abbildung 19.6).

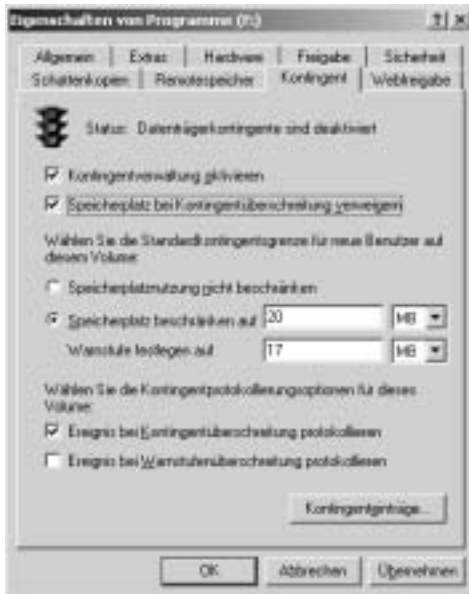


Abbildung 19.6: Einrichten eines Datenträgerkontingents

19.4 Das Distributed File System (DFS)

Über das Distributed File System (DFS) haben die Benutzer die Möglichkeit, auf Daten zuzugreifen, die sich an verschiedenen physischen Standorten im Netzwerk befinden, ohne die genauen Pfade zu diesen Daten kennen zu müssen. Ihnen stellt sich die Menge der Daten als an einem Speicherort befindlich dar. Damit wird für die Benutzer der Zugriff verkürzt und vereinfacht, da er nicht erst nach einem Server suchen muss, auf dem sich die gewünschte Ressource befinden könnte. Er muss lediglich eine Verbindung zum DFS-Stamm herstellen und kann dann auf alle darin befindlichen Ressourcen zugreifen, egal wo sich diese physikalisch befinden.

In einem DFS-Stamm befinden sich DFS-Verknüpfungen. Jeder Stamm kann beliebig viele Verknüpfungen beinhalten. Mit jeder Verknüpfung wird auf eine Freigabe gezeigt, die sich auf einem beliebigen Server befinden kann. Sollte ein Server ausfallen und die Freigabe damit auf einem anderen Server erstellt werden müssen, so brauchen Sie lediglich im DFS-Stamm die Verknüpfung für diese Freigabe durch den Pfad zum neuen Server zu aktualisieren. Durch die Verteilung von freigegebenen Ordnern auf mehrere Server wird zwischen diesen ein Ausgleich der Belastung hergestellt.

Der Zugriff auf DFS-Ressourcen ist für Clients mit den Betriebssystemen Windows 98 / NT / 2000 / XP möglich, für Windows 95 müssen Sie einen DFS-Client von der Microsoft-Webseite downloaden. Die volle Funktionalität von DFS ist für Windows 9x- und NT-Clients jedoch nur verfügbar, wenn auf diesen die ADSI-Services installiert sind (siehe Kapitel 3.8.1).

Der DFS-Stamm kann sowohl auf NTFS- als auch auf FAT-Datenträgern erstellt werden. Aufgrund der effizienteren Sicherheitseinstellungen unter NTFS sollte jedoch ein NTFS-Datenträger für den DFS-Stamm vorgezogen werden.

Eine komplette DFS-Topologie besteht aus einem DFS-Stamm, DFS-Verknüpfungen und freigegebenen DFS-Ordern. Das nächste Kapitel zeigt Ihnen, wie Sie eine vollständige DFS-Topologie einrichten und konfigurieren.

19.4.1 Einrichten eines DFS-Stammes

In diesem Kapitel werden der Reihe nach ein DFS-Stamm, eine DFS-Verknüpfung sowie freigegebene DFS-Ordner angelegt und anschließend die Replikation für die DFS-Ordner konfiguriert.

Erstellen des DFS-Stammes

Um einen DFS-Stamm zu erstellen, führen Sie die folgenden Schritte aus:

1. Wählen Sie aus dem Startmenü PROGRAMME / VERWALTUNG / VERTEILTES DATEISYSTEM (DFS).
2. Klicken Sie in der mmc auf VERTEILTES DATEISYSTEM (DFS) und wählen aus dem Kontextmenü den Eintrag NEUER DFS-STAMM. Damit wird der Assistent zum Erstellen des neuen Stammes gestartet.
3. Wählen Sie im ersten Fenster den Typ des DFS-Stammes (siehe Abbildung 19.7). Sie haben die Möglichkeit, einen Domänen-DFS-Stamm oder einen eigenständigen DFS-Stamm zu erstellen. Klicken Sie dann auf WEITER.



Abbildung 19.7: Auswählen des DFS-Stammtyps

Bei einem Domänen-DFS-Stamm wird die komplette DFS-Topologie im Active Directory gespeichert. Diese Methode bietet Fehlertoleranz, DFS-Verknüpfungen auf meh-

renen Ebenen und DNS-Unterstützung. Ein eigenständiger DFS-Stamm bietet keine Fehlertoleranz, da alle Informationen auf nur einem Computer gespeichert werden. DNS wird nicht unterstützt, und DFS-Verknüpfungen dürfen nur eine Ebene umfassen.

4. Wenn Sie als Typ einen Domänen-DFS-Stamm gewählt haben, müssen Sie nun im Feld DOMÄNENNAME den Namen der Hostdomäne für den Stamm angeben (siehe Abbildung 19.8). Sie sehen eine Liste der aktuellen und aller vertrauenden Domänen. Klicken Sie dann auf WEITER.



Abbildung 19.8: Auswählen der Hostdomäne

5. Als Nächstes geben Sie den Namen des Servers an, auf dem der DFS-Stamm liegen soll (siehe Abbildung 19.9). Dies kann jeder beliebige Server mit dem Betriebssystem Windows 2000/2003 Server sein. Sie können über DURCHSUCHEN den gewünschten Computer angeben. Auf jedem Server kann nur ein DFS-Stamm eingerichtet werden. Klicken Sie dann auf WEITER.

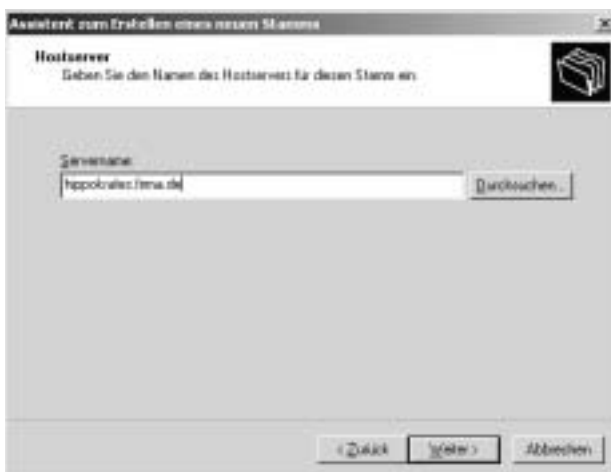


Abbildung 19.9: Den Hostserver für den DFS-Stamm bestimmen

6. Nun müssen Sie einen freigegebenen Ordner als Host für den neuen DFS-Stamm auswählen (siehe Abbildung 19.10). Sie sehen oben eine Drop-down-Liste aller auf dem im letzten Schritt gewählten Computer vorhandenen Freigaben. Sie können eine der bereits bestehenden Freigaben auswählen oder eine neue Freigabe auf dem Computer erstellen. Klicken Sie dann auf WEITER.

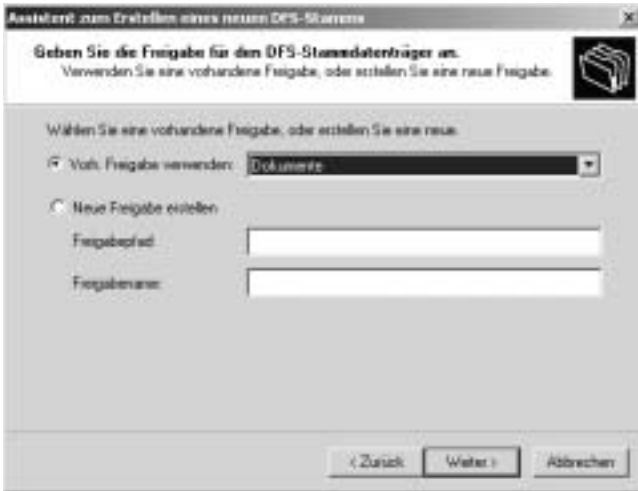


Abbildung 19.10: Festlegen der Freigabe für den DFS-Datenträger

7. Als Letztes müssen Sie einen Namen für den DFS-Stamm angeben (siehe Abbildung 19.11). Standardmäßig wird der Name der Freigabe vorgeschlagen, Sie können aber auch einen anderen Namen vergeben. Zum Abschluss sehen Sie eine Zusammenfassung aller Ihrer Angaben. Klicken Sie dann auf WEITER. Es wird eine Zusammenfassung Ihrer Angaben angezeigt. Klicken Sie hier auf FERTIG STELLEN.

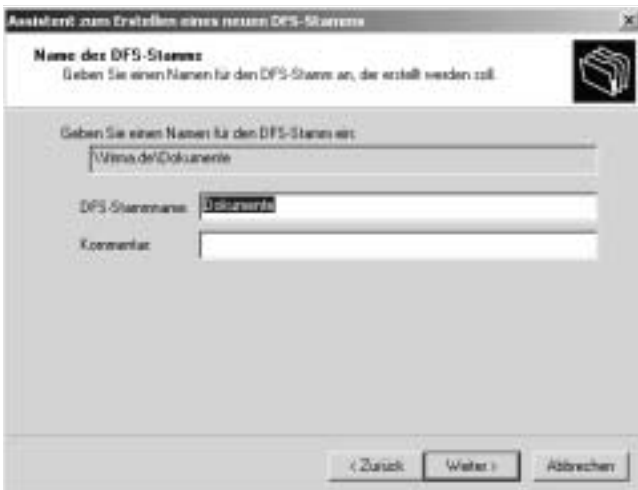


Abbildung 19.11: Einen Namen für den DFS-Stamm vergeben

Nach dem Fertigstellen des DFS-Stammes befindet sich dieser als erster Knoten in der DFS-mmc unter VERTEILTES DATEISYSTEM (DFS). Dieser Stamm kann nun konfiguriert werden.

19.4.2 Einrichten einer DFS-Verknüpfung

Um eine neue DFS-Verknüpfung einzurichten, muss ein DFS-Stamm vorhanden sein. Führen Sie die folgenden Schritte zum Erstellen einer neuen DFS-Verknüpfung durch:

1. Wählen Sie aus dem Kontextmenü des DFS-Stammes den Eintrag **NEUE DFS-VERKNÜPFUNG**. Sie erhalten das Fenster **NEUE DFS-VERKNÜPFUNG ERSTELLEN** (siehe Abbildung 19.12).



Abbildung 19.12: Erstellen einer DFS-Verknüpfung

2. Geben Sie im Feld **VERKNÜPFUNGSNAME** den Namen ein, der den Benutzern für die DFS-Verbindung angezeigt wird. Wählen Sie also einen aussagekräftigen Namen. Im Feld **BENUTZER ZU DIESEM FREIGEgebenEN ORDNER SENDEN** geben Sie den UNC-Pfad zu der Freigabe an, wo sich der Ordner tatsächlich befindet. Im Kommentarfeld können Sie eine Beschreibung des freigegebenen Ordners optional angeben. Schließlich können Sie noch festlegen, wie lange die Clients diese DFS-Verknüpfung zwischenspeichern sollen. Erst nach Ablauf dieses Zeitraums fragt der Client wieder beim DFS-Server nach, ob die Verknüpfung noch aktuell ist. Klicken Sie dann auf **OK**.

Nach Abschluss der Eingabe wird diese Verknüpfung unter dem DFS-Stamm in der DFS-mmc dargestellt. Um zu überprüfen, ob auf den Ordner, auf den die Verknüpfung verweist, zugegriffen werden kann, wählen Sie aus dem Kontextmenü der Verknüpfung **STATUS PRÜFEN**. Sie sollten als Ergebnis ein grünes Häkchen hinter dem Verknüpfungssymbol erhalten.

19.4.3 Einrichten von DFS-Ordnern

Eine DFS-Verknüpfung kann mehr als nur den einen Ordner umfassen, den Sie beim Erstellen der Verknüpfung im letzten Schritt hinzugefügt haben. Sie können zu einer Verknüpfung maximal 32 DFS-Ordner hinzufügen. Die DFS-Ordner werden auch als DFS-Replikate bezeichnet. Um weitere Ordner hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Wählen Sie aus dem Kontextmenü der DFS-Verknüpfung den Eintrag **NEUES REPLIKAT**. Sie erhalten das Fenster **NEUES REPLIKAT HINZUFÜGEN** (siehe Abbildung 19.13).
2. Geben Sie in das Textfeld **BENUTZER AN DIESEN FREIGEgebenEN ORDNER VERWEISEN** den UNC-Pfad zu dem Ordner ein, der in der Verknüpfung enthalten sein soll. Zusätzlich müssen Sie entscheiden, ob der Inhalt des Ordners manuell oder automatisch repliziert werden soll. Diese Option ist nur verfügbar, wenn Sie einen Domänen-DFS-Stamm konfiguriert haben, nicht jedoch bei einem eigenständigen DFS-Stamm. Weitere Informationen zur DFS-Replikation finden Sie im nächsten Kapitel. Klicken Sie dann auf **OK**.

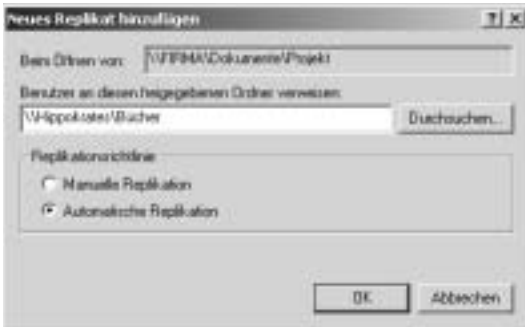


Abbildung 19.13: Hinzufügen weiterer DFS-Ordner

19.4.4 Festlegen der DFS-Replikation

Um die Fehlertoleranz der DFS-Ordner zu erhöhen, können Sie den gesamten DFS-Stamm oder DFS-Ordner auf andere Server replizieren. Damit ist beim Ausfall eines Servers sichergestellt, dass die Benutzer dennoch Zugriff auf die Daten haben.

Wenn Sie einen DFS-Stamm replizieren, stehen für die Benutzer beim Ausfall des ursprünglichen Stammservers dennoch alle DFS-Ordner zur Verfügung. Zur Replikation eines DFS-Stammes führen Sie die folgenden Schritte aus:

1. Wählen Sie aus dem Kontextmenü des DFS-Stammes den Eintrag **NEUES STAMMREPLIKAT**. Damit wird der Assistent gestartet.
2. Wählen Sie zunächst den Hostnamen des Servers aus, der das Replikat des DFS-Stammes erhalten soll. Hierbei muss es sich um einen Windows 2000 / 2003 Server in derselben Domäne handeln.
3. Anschließend wählen Sie einen Freigabenamen oder erstellen eine neue Freigabe für den zu replizierenden DFS-Stamm. Sie finden den neu erstellten DFS-Stamm in der Liste der DFS-Stämme.

Weiterhin können Sie auch die DFS-Ordner replizieren. Wie in Abbildung 19.13 zu sehen ist, müssen Sie beim Hinzufügen eines DFS-Ordners zu einer DFS-Verknüpfung bestimmen, ob dieser automatisch oder manuell repliziert werden soll. Die automatische Replikation ist nur auf einem Domänen-DFS-Stamm verfügbar und für Daten, die sich auf NTFS-Datenträgern befinden. Die Replikation wird über den Dateireplikationsdienst (File Replication Service, FRS) durchgeführt. Der Inhalt des automatisch replizierten Ordners wird dabei den anderen DFS-Ordern des DFS-Verknüpfungssatzes hinzugefügt. Die Clients haben so die Möglichkeit, immer auf den Ordner zuzugreifen, der für sie am besten und schnellsten erreichbar ist. Sobald an einem der DFS-Ordner Änderungen vorgenommen werden, werden diese auch an die anderen Ordner repliziert. Standardmäßig findet die Replikation viertelstündlich statt. Damit werden alle Ordner synchronisiert. Bei einem eigenständigen DFS-Stamm bleibt Ihnen nur die manuelle Replikation. Bei einem Domänen-DFS-Stamm dürfen Sie jedoch nicht für einen Teil der Ordner automatische und für einen anderen Teil die manuelle Replikation zuweisen. Es könnte dadurch zu Fehlern bei der Synchronisierung kommen.

Nachdem Sie sich für ein Replikationsverfahren entschieden haben, müssen Sie für die DFS-Ordner eine Replikationsrichtlinie festlegen, da der Dateireplikationsdienst standardmäßig deaktiviert ist. Führen Sie dazu folgende Schritte aus:

1. Wählen Sie aus dem Kontextmenü der DFS-Verknüpfung, deren Ordner Sie replizieren möchten, den Eintrag REPLIKATIONSRICHTLINIE.
2. In der Liste befinden sich alle DFS-Ordner, die der DFS-Verknüpfung angehören. In der Spalte REPLIKATION sehen Sie, dass noch keiner der Ordner an der automatischen Replikation teilnimmt. Wählen Sie einen der DFS-Ordner als Master-Ordner aus. Der Inhalt dieses Ordners wird in die anderen Ordner des Satzes repliziert. Klicken Sie dazu auf die Schaltfläche MASTER FESTLEGEN. Aktivieren Sie dann die übrigen Ordner, die an der Replikation teilnehmen sollen. Sie können pro Server nur eine Freigabe aktivieren, da eine Replikation innerhalb eines Servers wenig Sinn macht.

19.5 Fehlersuche bei Berechtigungen und DFS

Dieses Kapitel zeigt Ihnen häufige Fehler und Lösungsmöglichkeiten, die im Zusammenhang mit Berechtigungen, Datenkontingenten und DFS auftreten können.

1. Ein Benutzer hat keinen Zugriff auf eine Datei oder einen Ordner
 - ▶ Überprüfen Sie zunächst, ob bei dem Benutzer möglicherweise vergessen wurde, die entsprechende Berechtigung zuzuweisen.
 - ▶ Wenn der Benutzer mehreren Gruppen angehört, prüfen Sie, ob seiner Mitgliedsgruppe der Zugriff verweigert wurde.
 - ▶ Die Berechtigung könnte sich geändert haben, nachdem Sie den Ordner oder die Datei auf einen anderen NTFS-Datenträger verschoben oder innerhalb des NTFS-Datenträgers kopiert haben. Haben Sie die Datei auf einen FAT-Datenträger verschoben oder kopiert, gehen alle NTFS-Berechtigungen verloren.

- ▶ Wenn Sie für den Benutzer gerade die Zugriffsrechte geändert haben und damit die geänderten Zugriffsrechte wirksam werden, muss der Benutzer alle Netzwerkverbindungen zu dem Computer trennen, auf dem sich die Datei befindet, auf die er zugreifen möchte. Alternativ kann sich der Benutzer einmal ab- und dann wieder anmelden. Dadurch werden die Zugriffsberechtigungen aktualisiert.
2. Die DFS-Verknüpfung ist für den Client nicht verfügbar
- ▶ Prüfen Sie, ob für den Benutzer die notwendigen Rechte für die Ordner konfiguriert sind.
 - ▶ Sehen Sie über die Statusprüfung in der mmc nach, ob alle DFS-Ordner verfügbar sind. Möglicherweise kann keine Netzwerkverbindung zu einem Teil der Ordner aufgebaut werden.
 - ▶ Wenn Sie den Namen des Servers oder den Namen des freigegebenen Ordners geändert haben, sehen Sie in der mmc ein Fehlersymbol vor der DFS-Verknüpfung und dem DFS-Ordner. Aktualisieren Sie die Verknüpfungen, wenn Sie Änderungen vorgenommen haben.
 - ▶ Wenn der Client keine Verbindung zum DFS-Stamm und dessen Verknüpfungen herstellen kann, ist möglicherweise der DFS-Dienst auf dem Server angehalten.

20 Gruppenrichtlinien

In diesem Kapitel lernen Sie die Gruppenrichtlinien kennen. Sie sind unter Active Directory das zentrale Werkzeug zur Steuerung der Konfiguration von Benutzern und Computern. Gruppenrichtlinien können auf den Ebenen von Standorten, Domänen und Organisationseinheiten angewendet werden. Ein Gruppenrichtlinienobjekt gibt für einen Benutzer eine Ansammlung von Regeln des Unternehmens in Bezug auf verfügbare Ressourcen, Zugriffsrechte und Konfiguration der Ressourcen wieder. Über eine Gruppenrichtlinie werden die Desktop-Einstellungen eines Benutzers konfiguriert. Sie können ihm über diese Richtlinie beispielsweise Software zuweisen oder bestimmen, welche Objekte er im Startmenü sehen darf und welche nicht. Unter Windows NT stand Ihnen – wenn auch nicht in diesem Umfang – dafür die Systemrichtlinie zur Verfügung. Gruppenrichtlinien sind ein Bestandteil der IntelliMirror-Technologie. IntelliMirror ist der Oberbegriff für die Steuerung der Client-Desktops unter Windows 2000 / XP / 2003. Für jeden Client bestimmen Sie Richtlinien, die auf seiner Funktion, seinem Standort und seinen Gruppenmitgliedschaften basieren. Der Benutzer erhält überall seine in den Gruppenrichtlinien definierten Einstellungen, egal an welchem Computer er sich anmeldet. IntelliMirror umfasst die folgenden Funktionen: Verwaltung von Benutzerdaten und -einstellungen sowie Zuweisung, Installation und Konfiguration von Software. Unter Windows Server 2003 wurde die Administration der Gruppenrichtlinien durch die Bereitstellung der GPMC (Group Policy Management Console) entschieden vereinfacht. Diesem neuen Administrationswerkzeug wird ebenfalls Platz eingeräumt.

20.1 Grundlegendes zu Gruppenrichtlinien

In diesem Kapitel werden Ihnen zunächst die theoretischen Grundlagen für das Verständnis der Gruppenrichtlinien vermittelt. Sie erfahren, welche Vorteile und Verbesserungen die Gruppenrichtlinien gegenüber den Windows NT-Systemrichtlinien bieten, wie eine Gruppenrichtlinie strukturiert ist, welche Einstellungen Sie über Gruppenrichtlinien beeinflussen und wie Gruppenrichtlinien vererbt werden können.

20.1.1 Windows NT-Systemrichtlinie und Windows 2000/2003-Gruppenrichtlinie

Unter Windows NT konnten über den Systemrichtlinien-Editor in der Registry gespeicherte Benutzer- und Computerkonfigurationen festgelegt werden. Sie konnten eine Systemrichtlinie definieren, über die die Arbeitsumgebung eines Benutzers gesteuert werden konnte. Diese Konfigurationseinstellungen konnten dann auf seinen Computer angewendet werden.

In der NT-Systemrichtlinie gab es insgesamt 72 Optionen zur Richtlinieneinstellung. Über die Windows 2000-Gruppenrichtlinie haben Sie hingegen allein für die Sicherheit über 100 Konfigurationsoptionen und zusätzlich ungefähr 450 Registrierungseinstellungen. Der Windows Server 2003 verfügt über mehr als 700 Gruppenrichtlinien. Diese ergeben sich durch erweiterte Features des Betriebssystems wie den Remote Desktop, die Software Restriction Rules oder beziehen sich auf den Windows Media Player bzw. das Startmenü. Über die NT-Systemrichtlinie konnte nur eine Policy von einem Benutzer oder Computer in der Domäne verarbeitet werden, während unter Windows 2000/2003 mehrere Gruppenrichtlinienobjekte in verschiedenen Leveln der Active Directory-Hierarchie mit Containern verbunden werden können. Tabelle 20.1 vergleicht die beiden Richtlinien in ihren entscheidenden Unterschieden miteinander.

Windows NT-Systemrichtlinie	Windows 2000/2003-Gruppenrichtlinie
Die Systemrichtlinie konnte nur über *.adm-Dateien erweitert werden. Dabei handelt es sich um administrative Vorlagen im ASCII-Textformat.	Die Richtlinie kann über *.adm-Dateien oder direkt über die mmc erweitert werden.
Die Richtlinie wird auf Benutzer, Benutzergruppen oder Computer angewendet.	Sie kann auf Benutzer(gruppen) oder Computer in einer Domäne, Organisationseinheit oder einem Standort angewendet werden.
Die Systemrichtlinie ist nicht sicher.	Die Gruppenrichtlinie ist sicher.
Die Richtlinie wird meistens zum Einschränken oder Sperren eines Desktops eingesetzt.	Es kann eine Vielzahl weiterer Sicherheitseinstellungen festgelegt werden.
Die Richtlinie wird im Benutzerprofil gespeichert, bis sie von einer anderen Richtlinie überschrieben wird.	Durch Ändern der geltenden Richtlinie werden die Einstellungen in den Profilen überschrieben.
- . -	Die Richtlinie kann lokal oder für die Domäne definiert werden.
- . -	Die Softwareinstallation und -verwaltung kann über die Gruppenrichtlinie erfolgen.
- . -	Über sie können Ordner (z.B. Eigene Dateien) umgeleitet werden.
- . -	Komponenten wie der Internet Explorer oder Windows Installer können über die Gruppenrichtlinie verwaltet werden.

Tabelle 20.1: Vergleich der NT-Systemrichtlinie und den Gruppenrichtlinien

Insgesamt umfasst die Windows 2000-Gruppenrichtlinie vier administrative Vorlagen. Administrative Vorlagen sind Textdateien, die die entsprechenden Werte für die geänderten Registry-Schlüssel oder auch die Standardwerte enthalten. Für jeden Wert ist auch die entsprechende Stelle der Registry angegeben, an der die Werte stehen. Die beiden Dateien system.adm und inetres.adm werden automatisch in die Gruppenrichtlinie installiert. Sie schreiben die Einstellungen in vier reservierte Bereiche der Registry. Dabei handelt es sich um folgende Schlüssel:

- ▶ HKEY_LOCAL_MACHINE\Software\Policies
- ▶ HKEY_CURRENT_USER\Software\Policies
- ▶ HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies
- ▶ HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

Dabei handelt es sich um die Dateien *Conf.adm* (Einstellungen für NetMeeting), *Inetres.adm* (Internet Explorer), *System.adm* (Systemeinstellungen) und *Wmplayer.adm* (Media Player). Windows XP bringt aktualisierte Versionen dieser administrativen Vorlagen mit.

Sobald eine Gruppenrichtlinie geändert wird, werden die entsprechenden Bereiche in der Registry erst gelöscht und dann komplett neu geschrieben. Änderungen an diesen Bereichen sind nur mit Administratorrechten durchführbar. Diese administrativen Vorlagen des lokalen Gruppenrichtlinienobjekts befinden sich im Verzeichnis %SYSTEM-ROOT%\SYSTEM32\GROUPPOLICY. Sie können manuell editiert werden. Auch das Erstellen eigener *.adm-Dateien ist möglich.

Die drei anderen administrativen Vorlagen können optional in die Gruppenrichtlinien installiert werden. Sie sollten aber besser nur im Systemrichtlinien-Editor (*poledit.exe*) zur Verwaltung älterer Windows-Versionen herangezogen werden. Benutzen Sie diese drei Vorlagen nicht zur Verwaltung von 2000- oder XP-Clients, da die Einstellungen der Systemrichtlinie dauerhaft in der Registry wirksam bleiben können. Es handelt sich um die Dateien *winnt.adm*, *windows.adm* sowie *common.adm*. Über die *winnt.adm* werden Optionen für die Benutzeroberfläche von Windows NT, über die *windows.adm* Optionen für Windows 9x und über *common.adm* gemeinsame Benutzeroberflächen-Optionen für Windows NT und 9x gesteuert.

20.1.2 Update der Windows 2000-Gruppenrichtlinien um XP-Features

Windows XP Professional sowie Windows Server 2003 bringen erweiterte Features der Gruppenrichtlinien gegenüber den Windows 2000-Gruppenrichtlinien. Dabei handelt es sich um erweiterte *.adm-Dateien sowie ein aktualisiertes Gruppenrichtlinien-Snap-In (siehe Abbildung 20.1).

Das ursprüngliche Windows 2000-Gruppenrichtlinienobjekt wird in dem Moment um die neuen *.adm-Dateien mit den XP-Features heraufgestuft, wenn Sie vom XP-Client aus die Benutzer- oder Computereinstellungen des Gruppenrichtlinienobjekts anklicken oder einen der Knoten öffnen. Unter Windows XP können Sie in der mmc zwischen der standardmäßigen und erweiterten Ansicht wählen. Wählen Sie für eine bestimmte Richtlinie die erweiterte Ansicht, erhalten Sie neben der detaillierten Beschreibung der Richtlinie links davon auch einen Hinweis darauf, für welche Windows-Version diese Richtlinie verwendet werden kann. Im folgenden Beispiel sehen Sie, dass die Richtlinie BENUTZER-INSTALLATIONEN NICHT ZULASSEN des Windows Installers als Mindestanforderungen Windows XP oder Windows 2000 mit der Version 1.5 des Windows Installers voraussetzt.



Abbildung 20.1: Die erweiterte GPO-Ansicht unter Windows XP

Wird ein Gruppenrichtlinienobjekt um die neuen XP-Features heraufgestuft, so ignoriert ein Windows 2000-Client alle Einstellungen, die XP-spezifisch sind. Dabei wird jede Einstellung separat abgearbeitet. Wird dabei eine Einstellung gefunden, die von Windows 2000 nicht unterstützt wird, wird diese übergangen. Alle von Windows 2000 unterstützten Einstellungen werden vom aktualisierten Gruppenrichtlinienobjekt übernommen. In unserem eben genannten Beispiel würde ein Windows 2000-Client mit einem Windows Installer der Version 1.2 alle anderen Richtlinien des Windows Installer übernehmen, die als Mindestanforderung nur Windows 2000 voraussetzen, während die eben genannte Richtlinie ignoriert wird.

Ein Windows XP-Gruppenrichtlinienobjekt bietet auch zahlreiche neue Sicherheitseinstellungen. Diese Einstellungen können Sie nur betrachten, wenn das Gruppenrichtlinienobjekt unter Windows XP geöffnet wird. Dabei spielt es keine Rolle, ob Sie für Windows 2000 einige dieser Einstellungen konfiguriert haben oder nicht. Diese sind unter Windows 2000 in keinem Fall einsehbar. Sie sollten sich also einen Windows XP-Client auswählen, von dem aus die Gruppenrichtlinien der Windows 2000-Clients bearbeitet werden.

Um ein Gruppenrichtlinienobjekt eines Windows 2000-Clients um diese XP-Features heraufzustufen, führen Sie eine der folgenden Methoden aus:

1. Öffnen Sie an einem Windows XP-basierten Client der Domäne eine leere mmc.
2. Wählen Sie aus dem Menü KONSOLE den Eintrag SNAP-IN HINZUFÜGEN / ENTFERNEN und klicken im folgenden Fenster auf HINZUFÜGEN.
3. Wählen Sie dann das eigenständige Snap-In GRUPPENRICHTLINIE aus und klicken auf HINZUFÜGEN.
4. In dem Fenster GRUPPENRICHTLINIENOBJEKT AUSWÄHLEN klicken Sie auf DURCHSUCHEN. Wählen Sie dann nicht den lokalen Computer, sondern den Windows 2000-Computer, dessen Gruppenrichtlinienobjekt aktualisiert werden soll. Geben Sie dazu

den Namen oder die IP-Adresse des Computers in die Textbox ein oder klicken auf DURCHSUCHEN. Es erscheint der Eintrag REMOTE-COMPUTER COMPUTERNAME.

5. Beenden Sie den Vorgang über die Schaltflächen FERTIG STELLEN und SCHLIESSEN.
6. Sie können nun die GPO-Einstellungen des ausgewählten Computers von der Gruppenrichtlinien-Konsole des XP-basierten Clients aus vornehmen.

Alternativ dazu können Sie auch folgendes Verfahren für jedes GPO unter Windows 2000 anwenden:

1. Kopieren Sie auf einem Computer mit Windows XP die aktualisierten *.adm-Dateien aus dem Verzeichnis %SYSTEMROOT%\INF in eine beliebige Netzwerkfreigabe.
2. Öffnen Sie dann auf dem Windows 2000-Computer ein GPO in der mmc.
3. Markieren Sie den Knoten ADMINISTRATIVE VORLAGEN und wählen aus dem Kontextmenü VORLAGEN HINZUFÜGEN/ENTFERNEN. Markieren Sie in der folgenden Dialogbox die alten Windows 2000-Versionen und fügen dann die aktualisierten aus der Netzwerkfreigabe hinzu.

Unter Windows XP ist auch das Hilfesystem zu den einzelnen Richtlinien verbessert worden. Sie erhalten nun über F1 die direkte Online-Hilfe zu einem beliebigen Knoten im HTML-Format.

20.1.3 Was bedeuten GPO, GPC und GPT?

Zunächst einmal sollen die drei geheimnisvollen Abkürzungen aufgeschlüsselt werden. GPO bedeutet Gruppenrichtlinienobjekt (Group Policy Object), ein GPC ist ein Gruppenrichtliniencontainer (Group Policy Container), und GPT heißt Gruppenrichtlinienvorlage (Group Policy Template). Nachdem Sie nun die Abkürzungen kennen gelernt haben, sollen diese Begriffe mit Leben gefüllt werden.

Ein GPO besteht aus einer Reihe von einzelnen Gruppenrichtlinien, die Sie einem Benutzer oder Computer zuweisen können. Alle Einstellungen und Daten einer Gruppenrichtlinie werden in einem GPO gespeichert. Sobald Sie ein GPO für einen Benutzer oder Computer implementiert haben, enthält dieses ein GPC und ein GPT. Im GPC befinden sich die GPO-Informationen wie Version oder Status (aktiviert oder deaktiviert). Das GPC enthält Untercontainer für die Richtlinien für Computer und Benutzer. Im GPC werden alle Eigenschaften der Richtlinie gespeichert, die nicht häufigen Änderungen unterworfen sind, also quasi die Beschreibung der Richtlinie. Im GPT werden die Einstellungen für die Richtlinie gespeichert. Dazu zählen z.B. Skripte oder Sicherheitseinstellungen. Diese Daten können sich häufiger ändern. Die Ordnerstruktur des GPT wird beim Erstellen des GPO angelegt. Sie finden die GPT-Daten für domänenbasierte Gruppenrichtlinienobjekte im Verzeichnis %SYSTEMROOT%\SYSVOL\[DOMÄNENNAME]\POLICIES\[GUID DES JEWEILIGEN GPO]. Zusätzlich sind im Verzeichnis \USER\SCRIPTS\ bzw. \MACHINE\SCRIPTS\ von SYSVOL die Anmelde- und Abmeldeskripte für das GPO gespeichert.

Auf jedem Windows 2000/XP-Computer befindet sich auch ein lokales GPO – unabhängig davon, ob der Computer Mitglied einer Domäne ist oder nicht. Dieses finden Sie im Verzeichnis %SYSTEMROOT%\SYSTEM32\GROUPPOLICY. Einige der Funktionen wie Softwareverteilung oder Ordnerumleitung sind in den lokalen GPOs im Gegensatz zu domänenbasierten GPOs nicht verfügbar.

20.1.4 Verarbeiten und Vererben von Gruppenrichtlinien

Auf Domänenebene können GPOs auf Standorte, Domänen und Organisationseinheiten angewendet werden. Wenn sich ein Computer nicht in einer Domäne befindet, ist für ihn nur das lokale GPO gültig. Befindet er sich jedoch in einer Domäne, können die Einstellungen des lokalen GPOs durch die der Domäne überschrieben werden. Gruppenrichtlinien für Computer, die Mitglieder in Active Directory sind, werden in dieser Gültigkeitsreihenfolge abgearbeitet:

1. Lokales GPO
2. GPO des Standorts
3. GPO der Domäne
4. GPO der Organisationseinheit

Als Erstes werden also die Einstellungen des lokalen GPO geprüft. Dann werden die Einstellungen des GPOs für den Standort abgearbeitet. Ist eine Richtlinie nur auf Standortebene definiert, wird sie zu den bestehenden Richtlinieneinstellungen des lokalen GPOs addiert. Ist auf der Standortebene eine vom lokalen GPO abweichende Einstellung getroffen, so überschreibt das GPO des Standorts das lokale GPO. In dieser Weise werden alle GPOs bis zur Ebene der Organisationseinheit abgearbeitet. Wenn Sie eine Hierarchie von OUs und Unter-OUs eingerichtet haben, werden die OU-GPOs bis zu der untersten OU abgearbeitet. Man spricht hierbei auch von der LSDOU-Reihenfolge (Lokal – Standort – Domäne – Organisationseinheit).

Ein einzelnes GPO kann mit mehreren Containern wie Standorten, Domänen und Organisationseinheiten verbunden sein. Andererseits kann aber auch einer dieser Container mehrere GPOs beinhalten. Selbstverständlich kann auch ein GPO in nur einem Container angewendet werden.

In Abbildung 20.2 sehen Sie, dass der Container Domäne mit zwei verschiedenen GPOs, nämlich GPO 1 und 2 verknüpft ist, während andererseits dasselbe GPO, nämlich GPO 3, mit zwei verschiedenen Containern verknüpft ist, nämlich Organisationseinheit 1 und 2. Der einzelne Container-Standort ist mit nur einem GPO, nämlich GPO 4 verbunden.

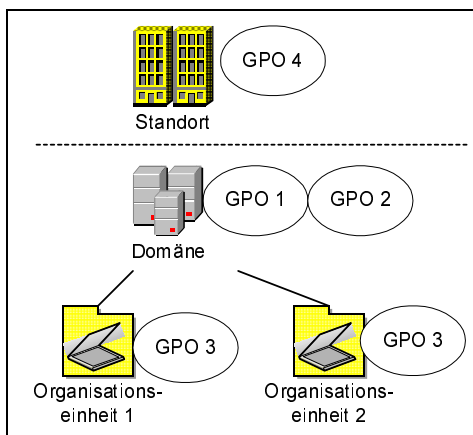


Abbildung 20.2: Die Verteilung von GPOs

Das eben beschriebene Modell geht davon aus, dass pro Hierarchieebene jeweils nur ein Container vorhanden ist, also beispielsweise nur eine Organisationseinheit ohne weitere OU-Untercontainer. Befinden sich aber in einem Container weitere Container (eine OU ist durch weitere OUs strukturiert), so gilt auch für Gruppenrichtlinien der standardmäßige Weg der Vererbung: Der übergeordnete Container vererbt die konfigurierten Richtlinien an alle Benutzer und Computer der untergeordneten Container. Dies gilt jedoch nur für Richtlinien, die entweder aktiviert oder deaktiviert sind. Die nicht konfigurierten Richtlinien werden nicht weiter vererbt.

Haben Sie jedoch in einem untergeordneten Container einige spezielle Richtlinien konfiguriert, so werden diese vorrangig vor den vom übergeordneten Container geerbten behandelt. Sind im über- und untergeordneten Ordner mehrere Richtlinien konfiguriert, die sich nicht widersprechen, so werden diese addiert. Widersprechen sich jedoch die Einträge in der Richtlinie des über- und untergeordneten Containers, so werden die Einstellungen des untergeordneten Containers verwendet, die des übergeordneten Containers werden in diesem Fall nicht vererbt.

Wenn in einem untergeordneten Container eine bestimmte Richtlinie nicht konfiguriert ist, sondern nur in dem übergeordneten Container, so wird daraus die Einstellung übernommen.

20.1.5 Öffnen und Bearbeiten der GPOs

Um an einem GPO Einstellungen und Änderungen vornehmen zu können, müssen Sie zunächst die entsprechende mmc öffnen. Diese befinden sich je nach Hierarchieebene des GPOs an verschiedenen Stellen.

Lokales GPO/lokales GPO eines anderen Computers

1. Öffnen Sie eine leere mmc, wählen aus dem Menü KONSOLE den Eintrag SNAP-IN HINZUFÜGEN/ENTFERNEN und klicken im folgenden Fenster auf HINZUFÜGEN.
2. Wählen Sie dann das eigenständige Snap-In GRUPPENRICHTLINIE aus und klicken auf HINZUFÜGEN.
3. In dem dann folgenden Fenster GRUPPENRICHTLINIENOBJEKT AUSWÄHLEN klicken Sie auf FERTIG STELLEN. Um das GPO eines anderen Computers zu öffnen, klicken Sie auf DURCHSUCHEN. Geben Sie dazu den Namen oder die IP-Adresse des Computers in die Textbox ein oder klicken auf DURCHSUCHEN. Es erscheint der Eintrag REMOTE-COMPUTER COMPUTERNAME. Klicken Sie dann ebenfalls auf FERTIG STELLEN.



Ist die Group Policy Management Console (GPMC, siehe Kapitel 20.3) des Windows Server 2003 installiert, so entfällt das Öffnen verschiedener mmcs für die Bearbeitung der GPOs des Standorts, der Domäne und der OU. Die Bearbeitung dieser GPOs ist über die zentrale Schnittstelle der GPMC möglich. Die folgend beschriebenen Schritte funktionieren dann nicht mehr.

GPO des Standorts

1. Öffnen Sie die mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE.
2. Wählen Sie aus dem Kontextmenü des Standorts EIGENSCHAFTEN und dann die Registerkarte GRUPPENRICHTLINIE.
3. Um ein neues GPO zu erstellen, klicken Sie auf NEU, geben ihm einen Namen und klicken auf BEARBEITEN. Benennen Sie ein neues GPO unbedingt an dieser Stelle, es kann später nicht mehr umbenannt werden. Um ein vorhandenes GPO zu bearbeiten, wählen Sie dieses aus der Liste aus.

GPO der Domäne oder Organisationseinheit

1. Öffnen Sie die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.
2. Wählen Sie aus dem Kontextmenü der Domäne oder der Organisationseinheit EIGENSCHAFTEN und dann die Registerkarte GRUPPENRICHTLINIE.
3. Um ein neues GPO zu erstellen, klicken Sie auf NEU, geben ihm einen Namen und klicken auf BEARBEITEN. Benennen Sie ein neues GPO unbedingt an dieser Stelle, es kann später nicht mehr umbenannt werden. Um ein vorhandenes GPO zu bearbeiten, wählen Sie dieses aus der Liste aus.

Sie erhalten dann die mmc des Gruppenrichtlinien-Editors (siehe Abbildung 20.3). Hier können alle Einstellungen an den Richtlinien vorgenommen werden.

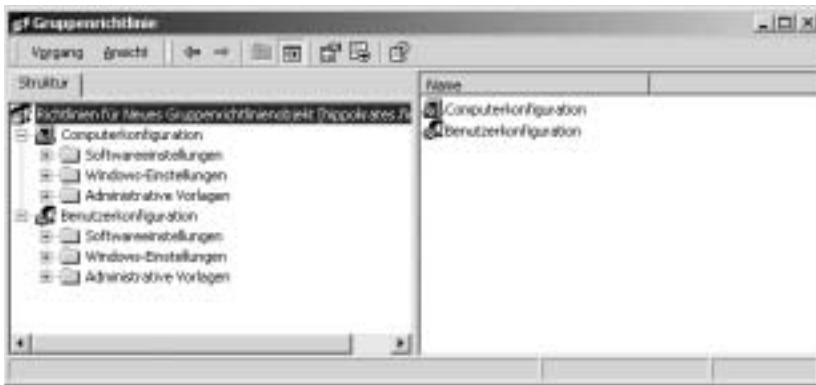


Abbildung 20.3: Der Gruppenrichtlinien-Editor

20.1.6 Inhalte eines GPOs

Jedes GPO ist in die Bereiche Computerkonfiguration und Benutzerkonfiguration unterteilt (siehe Abbildung 20.3). In der Computerkonfiguration werden nur maschinenbezogene Einstellungen getroffen. Sie werden bei jedem Start des Computers angewendet. Dabei ist es gleichgültig, welcher Benutzer sich an dem Computer anmeldet. Umgekehrt bezieht sich die Benutzerkonfiguration nur auf den Benutzer. Dabei spielt es keine Rolle, an welchem Computer sich der Benutzer anmeldet. In beiden Konfigurationsbereichen befinden sich die Untercontainer SOFTWAREEINSTELLUNGEN, WINDOWS-EINSTELLUNGEN und ADMINISTRATIVE VORLAGEN.

Softwareeinstellungen

In beiden Konfigurationen befindet sich standardmäßig nur der Eintrag SOFTWAREINSTALLATION. Über diesen Punkt können neue Pakete für die Softwareverteilung erstellt und konfiguriert werden (siehe Kapitel 20.5).

Windows-Einstellungen

Unter den WINDOWS-EINSTELLUNGEN finden Sie für beide Konfigurationen die Knoten Skripte sowie Sicherheitseinstellungen. Zusätzlich sind in der Benutzerkonfiguration noch Internet Explorer-Wartung, Remote-Installationsdienste sowie Ordnerumleitung vorhanden. Die folgende Tabelle zeigt Ihnen die Bedeutung der einzelnen Knoten.

Knoten	Beschreibung
Skripte	Hier können Sie Skripte für das An- und Abmelden von Benutzern sowie das Starten und Herunterfahren des Rechners definieren. Es sind Skripte in Form von Stapelverarbeitungen (*.cmd/*.bat) oder auch Visual Basic, Java oder Perl-Skripte möglich. Wenn mehrere Skripte eingesetzt werden, kann auch deren Reihenfolge bestimmt werden. Beim Starten eines Rechners wird erst das Startskript und bei der Benutzeranmeldung das Anmeldeskript verarbeitet. Beim Herunterfahren wird zunächst das Abmeldeskript und dann das Skript zum Herunterfahren abgearbeitet. Standardmäßig darf die Verarbeitung der Skripte maximal zehn Minuten in Anspruch nehmen. Dieser Wert kann jedoch bei Bedarf heraufgesetzt werden.
Sicherheits-einstellungen	Hier können Sie detaillierte Sicherheitseinstellungen für die Maschinen oder Benutzer einstellen. Dazu zählen Kontorichtlinien (Kennwort und Kontensperrung), das Zuweisen von Benutzerrechten oder Überwachungsrichtlinien. Die Bedeutungen der einzelnen Überwachungs- und Sicherheitsrichtlinien werden in Kapitel 22.1 und 22.3 vorgestellt. Weiterhin können Sie hier die Startoptionen für Windows-Systemdienste festlegen, für bestimmte Registry-Schlüssel und Dateien Sicherheitseinstellungen konfigurieren sowie die Richtlinien öffentlicher Schlüssel festlegen.
Internet Explorer-Wartung	Hier können Sie den Internet Explorer für die Client-Computer konfigurieren. Dazu zählen beispielsweise ein geändertes Logo, angepasste Symbolleisten, vordefinierte Verbindungen wie Proxy-Einstellungen usw., Links, die automatisch hinzugefügt werden, oder auch das Anpassen des Sicherheitsfilters.
Remote-Installationsdienste	Hier können Sie bestimmen, ob automatische oder benutzerdefinierte Remote-Installationen gestattet werden oder nicht, ob nach der Installation ein Neustart durchgeführt werden soll oder nicht. Die Grundlagen und Konfiguration für die Remote-Installationsdienste finden Sie in Kapitel 13.
Ordnerumleitung	Über die Ordnerumleitung können einige Windows-Ordner wie Eigene Dateien oder Startmenü vom standardmäßigen Benutzerprofil an eine zentrale Stelle im Netzwerk umgeleitet werden. Weitere Hinweise dazu finden Sie in Kapitel 20.4.1.

Tabelle 20.2: Die Windows-Einstellungen in einem GPO



Die mmc-Knoten SOFTWAREEINSTELLUNGEN (Zuweisung, Installation etc.), REMOTE-INSTALLATION sowie ORDNERUMLEITUNG sind nur verfügbar, wenn eine Domäne mit Active Directory eingerichtet worden ist. Die übrigen Optionen sind auch in einer Windows 2000-Domäne verfügbar, die nicht auf Active Directory basiert.

Administrative Vorlagen

Unter der Computer- und Softwarekonfiguration finden Sie jeweils den Knoten ADMINISTRATIVE VORLAGEN. Hier können Sie die Einstellungen konfigurieren, die auf den Bereichen HKEY_LOCAL_MACHINE (Computerkonfiguration) sowie HKEY_CURRENT_USER (Benutzerkonfiguration) der Registry beruhen. Die Computerkonfiguration bezieht sich auf die folgenden Bereiche: Windows-Komponenten, System, Netzwerk und Drucker. Die administrativen Vorlagen der Benutzerkonfiguration umfassen zusätzlich die Bereiche Startmenü und Taskleiste, Desktop sowie Systemsteuerung. Dafür fehlt dort der Bereich Drucker. In den einzelnen Bereichen können Sie folgende Einstellungen vornehmen:

Knoten	Beschreibung
Windows-Komponenten	In der Computerkonfiguration können Sie Einstellungen für die Windows-Komponenten NetMeeting, Internet Explorer, Taskplaner und Windows Installer vornehmen. In der Benutzerkonfiguration sind zusätzlich Einstellungen am Windows Explorer und an der mmc möglich.
System	Für die Computerkonfiguration sind die Bereiche Anmeldung, Datenträgerkontingente, DNS-Client, Gruppenrichtlinien und Windows-Datenschutz verfügbar, für die Benutzerkonfiguration An-/Abmeldung sowie Gruppenrichtlinien.
Netzwerk	Hier legen Sie die Einstellungen für Offline-Dateien und Netzwerk- und DFÜ-Verbindungen fest wie z.B. die Verfügbarkeit des Netzwerkverbindungsassistenten oder das (De-)Aktivieren von LAN-Verbindungen.
Drucker	Hier werden Druckereinstellungen wie z.B. die Veröffentlichung im Active Directory vorgenommen.
Startmenü und Taskleiste	Hier können Sie das Startmenü individuell definieren. Es können bestimmte Programmgruppen oder Menüeinträge entfernt oder auch Kontextmenüs der Taskleiste deaktiviert werden.
Desktop	Es können Einstellungen für den Active Desktop wie z.B. das Hintergrundbild oder das Hinzufügen von Objekten vorgenommen werden. Auch für den Suchdialog des Active Directory können Größe oder Filter gesetzt werden.
Systemsteuerung	Hier können die Menüpunkte Software, Anzeige, Drucker und Ländereinstellungen näher konfiguriert werden. Die übrigen Elemente der Systemsteuerung können wahlweise auch ausgeblendet werden.

Tabelle 20.3: Die administrativen Vorlagen eines GPOs

Jede einzelne Richtlinie der Benutzerkonfiguration (jedoch nicht alle in der Computerkonfiguration) verfügt in den Eigenschaften über zwei Registerkarten. Auf der Karte RICHTLINIE können Sie die richtlinienspezifischen Einstellungen treffen und die Richtlinie aktivieren oder deaktivieren. Auf der Registerkarte ERKLÄRUNG finden Sie die Funktion der jeweiligen Richtlinie sowie die Einstellungen präzise erläutert, die Sie konfigurieren können. Da diese Erklärungen sehr eingängig sind, wird an dieser Stelle darauf verzichtet, alle Richtlinien im Detail zu beschreiben.

Jede Richtlinie kann einen von drei möglichen Werten haben. Entweder ist sie nicht konfiguriert, d.h., es wurde kein Wert festgelegt, oder aber es wurde ein Wert festgelegt, sodass die Richtlinie auf aktiviert oder deaktiviert gesetzt werden kann. Um einen Wert zu setzen oder die Richtlinie zu deaktivieren, wählen Sie die entsprechende Checkbox in den Eigenschaften der Richtlinie.

Wenn Sie eine bestimmte Anzahl von Richtlinien in den administrativen Vorlagen konfiguriert haben und ausschließlich diese im Blickpunkt haben möchten, so sollten Sie eine andere Ansichtsoption wählen. Standardmäßig werden alle Richtlinien angezeigt, egal ob sie konfiguriert sind oder nicht. Markieren Sie den Knoten ADMINISTRATIVE VORLAGEN in der Computer- bzw. Benutzerkonfiguration und wählen aus dem Menü ANSICHT den Punkt NUR KONFIGURIERTE RICHTLINIEN ANZEIGEN. Dadurch werden alle nicht konfigurierten Richtlinien ausgeblendet, und es bleiben nur die aktivierten und deaktivierten übrig.

20.1.7 Abarbeiten der Gruppenrichtlinien für Computer und Benutzer

Sobald ein Computer, für den Gruppenrichtlinien konfiguriert sind, hochgefahren wird und er den RPC-(Remote Procedure Call-) Dienst gestartet hat, werden zunächst die für die Computerkonfiguration definierten Gruppenrichtlinien angefordert. Ist der Computer kein Mitglied der Domäne, wird nur das lokale GPO abgearbeitet. Sind für den Computer mehrere GPOs auf einer Ebene, z.B. Standort, definiert, werden Sie der Reihenfolge der definierten Liste nach abgearbeitet. Dabei wird die Reihenfolge lokal, Standort, Domäne und OU eingehalten. Anschließend werden die Startskripte für den Computer abgearbeitet. Die Abarbeitung der maschinenbezogenen Richtlinien erfolgt, während das Fenster COMPUTEREINSTELLUNGEN WERDEN ÜBERNOMMEN beim Startvorgang angezeigt wird.

Dann erscheint das Fenster für die Benutzeranmeldung. Nachdem sich der Benutzer erfolgreich verifiziert hat, wird zunächst sein Benutzerprofil geladen. Dann werden die Gruppenrichtlinienobjekte in derselben Reihenfolge wie die der Computerkonfiguration abgearbeitet. Schließlich werden noch die Anmeldeskripte für den Benutzer ausgeführt. All dies geschieht im Hintergrund, während das Fenster BENUTZERDEFINIESTE EINSTELLUNGEN WERDEN GELADEN angezeigt wird.

Dies ist die standardmäßige Reihenfolge des Abarbeitens. Jedoch können für diese Reihenfolge auch Ausnahmen definiert werden. Die drei Ausnahmemöglichkeiten lauten KEIN VORRANG, DEAKTIVIERT und LOOPBACK. Die beiden ersten Optionen können Sie aktivieren (siehe Abbildung 20.4), indem Sie auf der Registerkarte GRUPPENRICHTLINIE auf OPTIONEN klicken.

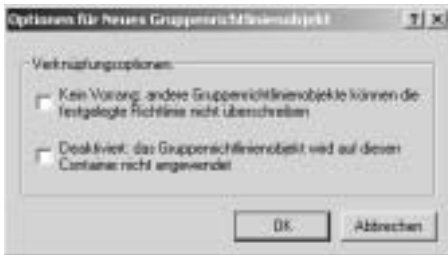


Abbildung 20.4: Verknüpfungsoptionen für ein GPO

Diese beiden Optionen haben folgende Bedeutung:

KEIN VORRANG: Diese Option bewirkt, dass keine Eigenschaft der Richtlinien dieses GPOs überschrieben und damit außer Kraft gesetzt werden kann. Die Durchsetzung der mit KEIN VORRANG markierten Richtlinie wird erzwungen. Sind mehrere GPOs mit dieser Option markiert, so gilt diese Einstellung für das in der Hierarchie höchste Objekt. Sind also ein GPO auf Domänen- und eines auf OU-Ebene auf KEIN VORRANG gesetzt, so gilt die Option für das ranghöhere OU-GPO.

DEAKTIVIERT: Mit der Deaktivierung werden die Einstellungen am GPO am jeweiligen Container nicht durchgesetzt. Das Deaktivieren ist nur wirksam, wenn das GPO nicht auf KEIN VORRANG gesetzt ist.

Eine weitere Option zur Steuerung der GPO-Verarbeitung ist die Option LOOPBACK. Um diese Option anzuwenden, öffnen Sie den folgenden Pfad: GPO / COMPUTERKONFIGURATION / ADMINISTRATIVE VORLAGEN / SYSTEM / GRUPPENRICHTLINIEN. Dort finden Sie die Richtlinie LOOPBACK-VERARBEITUNGSMODUS FÜR BENUTZERGRUPPENRICHTLINIE.

Die Loopback-Funktion ist für Computer sinnvoll, an denen die Benutzerrichtlinie je nach Computer geändert werden muss – unabhängig vom Benutzer. Hierzu zählen etwa Laboratorien oder Unterrichtsräume. Standardmäßig werden alle Benutzereinstellungen aus der GPO-Liste von Standort, Domäne und OU abgerufen, und zwar unter den Vererbungsbedingungen, wie sie vom Administrator konfiguriert sind. Um dieses Verhalten zu ändern, bieten sich beim Aktivieren dieser Richtlinie die Möglichkeiten ERSETZEN und ZUSAMMENFÜHREN.

ERSETZEN: Wenn Sie diese Option wählen, wird statt der GPO-Liste für den Benutzer die GPO-Liste für den Computer verwendet. Die Richtlinieneinträge der Computer ersetzen vollständig die Einträge des Benutzers, die normalerweise verwendet werden würden.

ZUSAMMENFÜHREN: In diesem Fall werden sowohl die GPO-Liste des Computers als auch die GPO-Liste des Benutzers bei der Anmeldung verwendet. Allerdings wird die GPO-Liste des Computers an die Benutzerliste angehängt und somit als zweites bearbeitet. Treten nun Konflikte zwischen den Einstellungen der beiden Listen auf, so überschreiben die Computereinstellungen die des Benutzers, da die Computer GPO-Liste als zweite verarbeitet wird.

20.1.8 Spezielle Optionen für Gruppenrichtlinien

Neben der Reihenfolge des Abarbeitens können Sie auch noch einige spezielle Einstellungen für die Richtlinien der Benutzer- und Computerkonfiguration treffen. Dazu zählen etwa das Aktualisierungsintervall oder synchrone bzw. asynchrone Anwendung des GPOs. Sie erreichen diese Optionen über GRUPPENRICHTLINIE / COMPUTERKONFIGURATION / ADMINISTRATIVE VORLAGEN / SYSTEM / GRUPPENRICHTLINIEN.

Computerkonfiguration

In der Computerkonfiguration stehen Ihnen die folgenden wichtigsten Optionen zur Verfügung:

- ▶ **HINTERGRUNDAKTUALISIERUNG DER GRUPPENRICHTLINIE DEAKTIVIEREN:** Ist diese Richtlinie aktiviert, werden die Richtlinien für die Computer- und Benutzerkonfiguration nicht im laufenden Betrieb des Computers aktualisiert, sondern erst wenn sich der Benutzer abgemeldet hat. Ist die Richtlinie deaktiviert, werden die Richtlinien in einem definierbaren Intervall aktualisiert.
- ▶ **GRUPPENRICHTLINIEN-AKTUALISIERUNGSINTERVALL FÜR COMPUTER:** Sie können das Intervall festlegen, wie oft die Richtlinien für die Computerkonfiguration im Hintergrund während des laufenden Betriebes auf dem Computer aktualisiert werden soll. Es ist ein Wert zwischen 0 bis 64.800 Minuten (= 45 Tage) möglich. Damit nicht alle Clients gleichzeitig ihre Aktualisierung durchführen, ist eine Verzögerung des Intervalls konfigurierbar. Der Standardwert liegt bei 30 Minuten, kann aber bis auf 24 Stunden ausgedehnt werden. Wenn im Hintergrund eine Richtlinie der Computerkonfiguration aktualisiert wird, kann der Benutzer dies u.U. bemerken, wenn sich der Desktop aktualisiert oder geöffnete Menüs geschlossen werden. Über die Richtlinie „Gruppenrichtlinien-Aktualisierungsintervall für Domänencontroller“ können dieselben Einstellungen auch für die Domänencontroller getroffen werden.
- ▶ **GRUPPENRICHTLINIEN FÜR COMPUTER ASYNCHRON BEIM STARTEN ANWENDEN (nur Windows 2000):** Bleibt diese Richtlinie deaktiviert, kann die Benutzeranmeldung erst erfolgen, wenn alle Gruppenrichtlinien der Computerkonfiguration aktualisiert worden sind. Vordem erhalten Sie nicht das Dialogfeld zur Windows-Anmeldung. Dies ist das standardmäßige und sichere Windows 2000-Startverfahren. Ist die Richtlinie aktiviert, kann die Anmeldung bereits erfolgen, wenn noch nicht alle Richtlinien aktualisiert sind.
- ▶ **GRUPPENRICHTLINIEN FÜR BENUTZER ASYNCHRON BEI DER ANMELDUNG ANWENDEN (nur Windows 2000):** Bleibt diese Richtlinie deaktiviert, wird der Desktop für den Benutzer erst verfügbar, wenn alle Gruppenrichtlinien der Benutzerkonfiguration aktualisiert worden sind. Auch dies ist das sichere Windows-Standardverfahren. Wird die Richtlinie aktiviert, ist der Desktop bereits verfügbar, wenn noch nicht alle Richtlinien abgearbeitet sind. Startet der Benutzer bereits in dieser Zeit eine Applikation, an der Änderungen vorgenommen worden sind, so kann dies zu erheblichen Problemen führen.



Die eben beschriebenen Verarbeitungsmethoden werden standardmäßig nur unter Windows 2000 synchron durchgeführt. Windows XP Professional hingegen wartet standardmäßig beim Starten und Anmelden nicht ab, bis das Netzwerk vollständig gestartet ist. Meldet sich ein bekannter Benutzer am System an, werden gecachte Daten benutzt, was den Startvorgang deutlich beschleunigt. Die Gruppenrichtlinien werden somit asynchron verarbeitet, sobald das Netzwerk vollständig verfügbar ist. Nur wenn sich ein Benutzer neu an einem Rechner unter Windows XP anmeldet, werden die GPOs synchron verarbeitet.

Weiterhin können Sie z.B. für Registry, Internet Explorer, Ordnerumleitung, Datenträgerkontingente, Skripte oder Softwareinstallation Optionen wie Hintergrundaktualisierung, Erkennen von langsamen Verbindungen oder die Aktualisierung ohne Änderungen konfigurieren.

20.1.9 Mehrere Anmeldungen unter Windows XP, bis ein GPO wirksam wird

Wie gerade erwähnt, erfolgt die schnelle Benutzeranmeldung unter Windows XP durch das Cachen der letzten Benutzeranmeldung. Sind nun in der Zwischenzeit Änderungen an den Benutzereinstellungen - z.B. eine neue Ordnerumleitung – vorgenommen worden, so können diese Einstellungen bei der asynchronen Richtlinienverarbeitung beim erstmaligen Einloggen des Benutzers nicht übernommen werden. Nachdem aber alle Richtlinien abgearbeitet sind, werden die Änderungen den gecachten Daten hinzugefügt und somit die Login-Einstellungen aktualisiert. Dabei wird für den nächsten Anmeldevorgang die asynchrone Verarbeitung deaktiviert, damit die Änderungen umgesetzt werden können. Der Benutzer erhält also erst bei seiner zweiten Anmeldung nach der Änderung der Richtlinie die entsprechenden Einstellungen.

Ebenso verhält es sich, wenn einem Benutzer über die Softwareinstallation neue Software zugewiesen wurde. Bei der asynchronen Verarbeitung kann die Software nicht installiert werden, wenn für den Benutzer bereits der Desktop verfügbar ist. Stattdessen wird nicht der Benutzer, sondern der Computer darüber informiert, dass eine neue Software zu installieren ist. Bei der nächsten Anmeldung des Benutzers sorgt dann der Computer für die synchrone Richtlinienverarbeitung des Benutzers, sodass die Software installiert werden kann.

Diese Verhaltensweisen gelten selbstverständlich auch für Windows 2000, sofern dort das asynchrone Verarbeiten der Richtlinieneinstellungen aktiviert ist.

Um unter Windows XP wie unter Windows 2000 standardmäßig alle Änderungen bei einem Startvorgang und Einloggen wirksam werden zu lassen, müssen Sie unter COMPUTERKONFIGURATION / ADMINISTRATIVE VORLAGEN / SYSTEM / ANMELDUNG die Richtlinie BEIM NEUSTART DES COMPUTERS UND BEI DER ANMELDUNG IMMER AUF DAS NETZWERK WARTEN aktivieren.

20.1.10 Konflikte von GPO-Einstellungen vorhersagen – RSoP in Windows XP/2003

Wenn Sie Gruppenrichtlinien auf verschiedenen Leveln definieren, z.B. für den Standort und die Domäne, so können die verschiedenen Einstellungen untereinander zu Konflikten führen. Und dann wird es schwierig, das fehlerträchtige GPO zu lokalisieren und anzupassen. Allerdings gibt es auch hierfür Methoden und Programme, die diesem Problem entgegenwirken.

Unter Windows XP und Windows Server 2003 – nicht jedoch unter Windows 2000 – steht Ihnen dazu das Programm RSoP (Resultant Set of Policy – Richtlinienenergebnissatz) zur Verfügung. Der Windows Server 2003 stellt RSoP im Rahmen der neuen Group Policy Management Console (GPMC, siehe Kapitel 20.3) bereit. RSoP ist eine Suchmaschine, die die bestehenden Gruppenrichtlinien abfragt und die Ergebnisse der Abfrage ausgibt. Die Ergebnisse bezieht RSoP aus der CIMOM-Datenbank (Common Information Model Object Manager), die auch als WMI (Windows Management Instrumentation) bezeichnet wird. Damit kann ein Administrator bereits im Vorfeld sämtliche GPOs sowie deren Priorität sehen, die auf einen bestimmten Computer und Benutzer angewendet werden. So können Probleme frühzeitig erkannt werden. RSoP fragt für einen bestimmten Benutzer oder Computer alle auf lokaler, Standort-, Domänen- und OU-Ebene existierenden GPOs ab. Es werden sämtliche Einstellungen angezeigt, die von einem Administrator vorgenommen worden sind. Dazu zählen etwa die administrativen Vorlagen, Ordnerumleitungen oder Skripte. Weiterhin wird auch die Softwareinstallation nach Applikationen durchsucht, die mit einem bestimmten Benutzer oder Computer verbunden sind.

Um RSoP auf Ihrem Windows XP-Computer einzurichten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie eine leere mmc und fügen das Snap-In RICHTLINIENERGEBNISSATZ hinzu. Damit wird ein Assistent gestartet, mit dem Sie sowohl die für bestimmte Computer und Benutzer zugewiesenen Richtlinien anzeigen (Protokollierungsmodus) als auch eine Implementierung zunächst simulieren können (Planungsmodus). Klicken Sie im Begrüßungsbildschirm auf WEITER.
2. Wählen Sie nun den Protokollierungs- oder Planungsmodus aus (siehe Abbildung 20.5). Zur Protokollierung werden die Konfigurationen eines bestimmten Benutzers und/oder Computers ausgewählt. Im Planungsmodus wird die Implementierung von Richtlinien simuliert (und nicht „simuliert“, wie es im Windows-Fenster geschrieben steht). Dabei wird auf die bestehenden Daten des Active Directory zurückgegriffen. Klicken Sie dann auf WEITER.



Abbildung 20.5: Auswahl des RSoP-Modus

3. Sie gelangen nun zur Auswahl des Computers (siehe Abbildung 20.6). Sie können entweder die GPO-Einstellungen für den aktuellen oder einen beliebigen anderen Computer analysieren. Ist die Checkbox KEINE RICHTLINIENEINSTELLUNGEN FÜR DEN AUSGEWÄHLTEN COMPUTER IM ERGEBNIS ANZEIGEN, so werden nur die Einstellungen der Benutzerkonfiguration angezeigt. Klicken Sie dann auf WEITER.



Abbildung 20.6: Auswahl des Computers der RSoP-Anzeige

4. Nun müssen Sie den Benutzer auswählen, für den die GPO-Einstellungen angezeigt werden sollen (siehe Abbildung 20.7). Sie können entweder den aktuellen oder einen anderen Benutzer auswählen. Aktivieren Sie die Checkbox KEINE BENUTZERRICHTLINIENEINSTELLUNGEN IM ERGEBNIS ANZEIGEN, werden keine Einstellungen aus der Benutzerkonfiguration angezeigt, sondern ausschließlich die der Computerkonfiguration. Klicken Sie dann auf WEITER.
5. Sie erhalten nun eine Zusammenfassung Ihrer Auswahl. Klicken Sie hier auf WEITER. Anhand des Statusbalkens wird Ihnen der Fortschritt vermittelt. Schließen Sie dann das Fenster FERTIG STELLEN DES ASSISTENTEN.

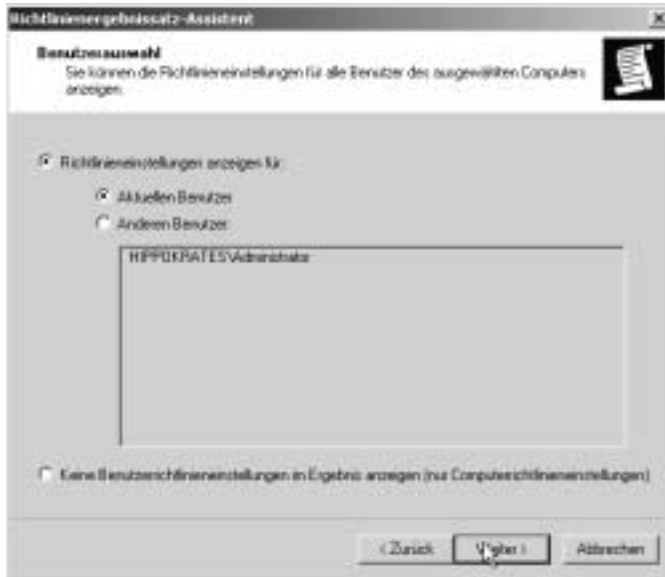


Abbildung 20.7: Benutzerauswahl für die RSoP-Ergebnisse

6. Sie erhalten wieder das Fenster EIGENSTÄNDIGES SNAP-IN HINZUFÜGEN. Klicken Sie hier auf SCHLIESSEN. Klicken Sie dann im Fenster SNAP-IN HINZUFÜGEN/ENTFERNEN auf OK. Sie erhalten dann eine neue mmc, in der das RSoP-Ergebnis angezeigt wird. Öffnen Sie nun den Knoten des Benutzers, und Sie erhalten alle seine Richtlinien, die in den einzelnen GPOs für ihn aktiviert sind.

Um auch den Benutzern die Effekte der ihnen zugewiesenen Richtlinien darzustellen, können sie sich über das Support Center eine benutzerfreundliche Zusammenstellung der verwendeten Richtlinien ausgeben lassen. Um das RSoP-Support Center zu starten, haben die Benutzer zwei Möglichkeiten.

1. Öffnen Sie im Startmenü HILFE UND SUPPORT. Wählen Sie unter der Überschrift EINE AUFGABE AUSWÄHLEN den Link TOOLS ZUM ZEIGEN VON COMPUTERINFORMATIONEN UND ERMITTELN VON FEHLERURSACHEN VERWENDEN.
2. Klicken Sie dann auf ERWEITERTE SYSTEMINFORMATIONEN und dann auf ANGEWENDETE GRUPPENRICHTLINIENEINSTELLUNGEN ANZEIGEN. Sie erhalten einen Statusbalken, während die Informationen ausgelesen werden. Danach erhalten Sie eine Zusammenfassung in Form einer Website (siehe Abbildung 20.8).

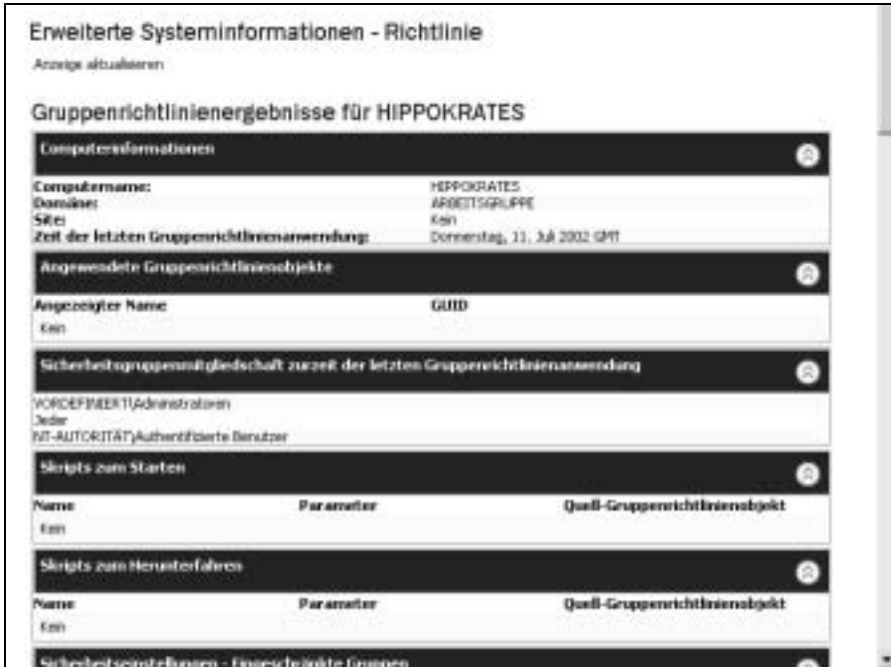


Abbildung 20.8: Ausgabe der RSoP-Ergebnisse

Alternativ dazu können Sie das Support Center auch über folgende Adresse im Webbrowser erreichen: <http://system/sysinfo/RSoP.htm#>.

Den RSoP-Bericht können Sie im html-Format abspeichern. Den entsprechenden Link dazu finden Sie am Ende des Berichts.

20.2 Erstellen von Gruppenrichtlinien

Die Ebene, auf die die Gruppenrichtlinien angewendet werden, ist abhängig von der Struktur des Unternehmens. Sie können einen standardisierten Client für die gesamte Domäne oder nur für Mitglieder bestimmter Gruppen konfigurieren. So können Sie beispielsweise Standards für E-Mail auf Domänenebene festlegen, während z.B. routinemäßige Verwaltungsaufgaben wie die Pflege der Benutzerkonten an Administratoren auf Standort- oder OU-Ebene delegiert werden sollten. Einen Teil dieser Verwaltungsaufgaben, wie etwa die Paßwortbetreuung, können Sie über die Gruppenrichtlinie an Helpdesk-Mitarbeiter delegieren, die ausschließlich diese Aufgabe durchführen können. Für diese Aufgabe wäre der Domänenadministrator an höchster Stelle die falsche Person.

Um einen optimalen Plan zur Verwaltung der clientbezogenen Aufgaben aufzustellen, ermitteln Sie zunächst alle anfallenden Verwaltungsaufgaben. Hierzu zählen Neuinstallation und Konfiguration von Client-Computern, Softwareeinstellungen und -verteilung oder die Arbeit an Benutzerkonten. Analysieren Sie, welche Personen an welchem Punkt des Unternehmens bisher diese Aufgaben ausführen. Legen Sie dann fest, in welcher

Hierarchieebene des Unternehmens diese Aufgaben am effektivsten ausgeführt werden können. Dementsprechend delegieren Sie die Verwaltung.

Sie erfahren nun, wie die Gruppenrichtlinie das Delegieren der Verwaltung auf Standort-, Domänen- und OU-Ebene ermöglicht. Zum Delegieren der Verwaltung über die Gruppenrichtlinie gehören das Verwalten von Gruppenrichtlinienverknüpfungen für Standort, Domäne oder OU sowie das Erstellen und Konfigurieren der GPOs.

Zur Verwaltung der Gruppenrichtlinien sind standardmäßig nur der Domänen- und Organisationsadministrator berechtigt. Sie können über die Eigenschaften der Gruppenrichtlinie auf der Registerkarte GRUPPENRICHTLINIE festlegen, welche GPOs mit einem Standort, einer Domäne oder OU verknüpft werden sollen. Fügen Sie die gewünschten GPOs hinzu. Für jedes der verknüpften GPOs können Sie einem Nicht-Administrator die Berechtigungen Lesen und Schreiben zuweisen. Zum Delegieren der Verwaltung an einen Nicht-Administrator benutzen Sie den Assistenten zur Verwaltungsdelegation, siehe Kapitel 21.5.1.

Das Erstellen neuer GPOs ist standardmäßig auch nur Domänen- und Organisations-Admins sowie den Ersteller-Besitzern der Richtlinie vorbehalten. Um weiteren Personen das Erstellen von neuen GPOs zu ermöglichen, müssen diese Benutzer als Mitglieder der Sicherheitsgruppe Ersteller-Besitzer hinzugefügt werden. Sie haben damit den Vollzugriff auf die von ihnen erstellten GPOs. Dies gilt auch für die GPOs, die explizit an ihn delegiert worden sind.

Die Domänen- und Organisationsadministratoren sowie die Ersteller-Besitzer haben standardmäßig Vollzugriff auf die GPOs. Für Sie ist jedoch nicht die Berechtigung GRUPPENRICHTLINIE ÜBERNEHMEN aktiviert. D.h., sie können das Objekt bearbeiten, ohne dass die Einstellungen auf sie angewendet werden. Authentifizierte Benutzer erhalten Lesezugriff auf alle GPOs, bei denen für sie die Option GRUPPENRICHTLINIE ÜBERNEHMEN aktiviert ist. Für sie gelten damit auch die Einstellungen der Richtlinie. Zum Bearbeiten eines GPO ist der Vollzugriff erforderlich. Es können also nur folgende Personen ein GPO bearbeiten: Domänen- und Organisationsadministratoren, ein Mitglied der Gruppe Ersteller-Besitzer, das das GPO selbst erstellt hat und deshalb Vollzugriff besitzt, oder Personen, an die die Verwaltung des GPOs delegiert wurde.

20.2.1 Implementierungsstrategie für Gruppenrichtlinien

Vor dem Erstellen der Gruppenrichtlinien sollten Sie sich auch einige Gedanken über die Planung der Gruppenrichtlinientypen sowie die Implementierung und Zuweisung machen. Beginnen Sie also nicht damit, planlos GPOs zu erstellen, die auf die Benutzer und Computer losgelassen werden.

Dieses Kapitel zeigt Ihnen einige Entwürfe und Hinweise zur Implementierung der Gruppenrichtlinien. Viele dieser einzelnen Entwürfe sind miteinander kombinierbar.

Anzahl der GPOs pro Benutzer und Computer

Entscheiden Sie, wie viele GPOs insgesamt erstellt und wie diese auf den verschiedenen Hierarchieebenen angewendet werden sollen. Im Modell der dezentralen GPOs wird pro Benutzer bzw. Computer nur ein einziges GPO auf OU-Basis angewendet, das eine Reihe von Richtlinieneinstellungen beinhaltet. Auf Domänen- und Standortbasis wird kein

zentrales GPO definiert. Befinden sich innerhalb einer Organisationseinheit nun Benutzer oder Computer, die nicht dasselbe GPO verwenden können, so werden die Benutzer/Computer mit identischen Sicherheitsanforderungen innerhalb der OU zu einer Unter-OU innerhalb des Containers zusammengefasst. Dieses Modell bietet zwar den Vorteil, dass bei der Anmeldung nur ein GPO abzuarbeiten ist und diese somit schnell erfolgt. Jedoch erhöht sich der Verwaltungsaufwand, da Benutzer / Computer mit identischen Sicherheitsanforderungen in Unter-OUs zusammengefasst werden müssen.

Es ist umgekehrt auch möglich, für eine Domäne oder einen Standort ein zentrales GPO zu erstellen, das die Grundanforderungen an alle Benutzer erfüllt. Denkbar wären hierfür Optionen für die Benutzerkonten und Passwörter. Neben diesem globalen GPO können Sie spezifische GPOs für die einzelnen Organisationseinheiten einrichten. Dieses Verfahren ist sinnvoll, wenn die OUs nach funktionellen Aspekten eingerichtet worden sind. So werden alle Mitglieder einer OU Finanzen innerhalb dieser OU über nahezu identische GPO-Einstellungen verfügen, aber über komplett andere als die Mitglieder der OU Vertrieb. Dabei wird eine bestimmte Richtlinieneinstellung nach Möglichkeit nur in einem GPO vorhanden sein. Sind nun an dieser Richtlinie Änderungen erforderlich, so müssen Sie nur ein einziges GPO bearbeiten und nicht wie im eben beschriebenen Modell alle GPOs, die diese Richtlinie enthalten. Dieses Modell ist sinnvoll, wenn das Unternehmen über verschiedene Organisationseinheiten verfügt, die jeweils andere Sicherheitsaspekte zu bedenken haben. Allerdings können nun auch die Anmeldezeiten der Clients zunehmen, da sie eine Reihe von GPOs mit jeweils nur wenigen Richtlinien abzuarbeiten haben. Dafür ist der Verwaltungsaufwand geringer.

Anzahl der Richtlinien pro GPO

In diesem Zusammenhang ist das Definieren verschiedener Richtlinientypen erforderlich. Sie können GPOs erstellen, in denen entweder nur die Richtlinien der Benutzer- oder Computerkonfiguration enthalten sind. Die Anmeldezeit verlängert sich hierbei ein wenig, da zwei verschiedene GPOs abzuarbeiten sind. Jedoch eignet sich diese Einteilung zur schnellen Fehlersuche. Wird davon ausgegangen, dass der Fehler in dem GPO der Richtlinien der Benutzerkonfiguration liegt, so sollte sich unter einem anderen Benutzerkonto testweise angemeldet werden, dem keine Richtlinien zugewiesen sind. Ist damit der Fehler behoben, liegt er in der Benutzerkonfiguration, andernfalls in der Computerkonfiguration.

Eine weitere Möglichkeit zur Definition von Richtlinientypen besteht darin, den Bereich der Richtlinien festzulegen, die in einem GPO enthalten sein sollen. Sie können beispielsweise ein GPO anlegen, in dem sich nur die Richtlinien zur Softwareinstallation befinden, ein weiteres, das nur Richtlinien zur Anmeldung enthält usw. Selbstverständlich kann ein GPO auch Richtlinien aus verschiedenen Bereichen enthalten. Je mehr Richtlinien in einem GPO enthalten sind, desto geringer wird die Anmeldezeit der Clients, desto höher wird umgekehrt aber auch der administrative Aufwand beim Bearbeiten der Richtlinieneinstellungen.

Verwalten der GPOs

Durch die Delegierung der Verwaltung ist es möglich, dass die Administratoren auf OU-Ebene bestimmte domänenweite GPOs außer Kraft setzen. Bei anderen GPOs kann ihnen diese Möglichkeit auch entzogen werden. Sollen bestimmte Sicherheitseinstellun-

gen eines domänenweiten GPOs nicht die Einstellungen des OU-GPO überschreiben, so sollte das OU-GPO mit der Option KEIN VORRANG versehen werden. Dieses Verfahren kann für unternehmensweite Konto- oder Passwortrichtlinien angewendet werden.

Um einem Administrator die Möglichkeit zu geben, OU-spezifische Einstellungen in seiner OU durchzusetzen und nicht ausschließlich domänenweite Richtlinien zu übernehmen, kann er mit der entsprechenden Berechtigung die Option RICHTLINIENVERERBUNG DEAKTIVIEREN für die gewünschte Organisationseinheit festlegen. Es kann jedoch nur die Vererbung der Gruppenrichtlinien deaktiviert werden, bei denen nicht die Option KEIN VORRANG ausgewählt ist.

20.2.2 Erstellen eines GPO

Um ein neues Gruppenrichtlinienobjekt zu erstellen, führen Sie die folgenden Schritte aus:



Die in diesem Kapitel beschriebenen Schritte beziehen sich lediglich auf Domänencontroller bzw. Verwaltungscomputer, auf denen nicht die Group Policy Management Console (GPMC, siehe Kapitel 20.3) des Windows Server 2003 installiert ist. Über diese ist das Erstellen sämtlicher GPOs über eine zentrale Benutzeroberfläche möglich.

1. Wollen Sie ein GPO auf Domänen- oder OU-Basis erstellen, so öffnen Sie die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER. Soll das GPO für einen Standort erstellt werden, öffnen Sie die mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE.
2. Wählen Sie aus dem Kontextmenü der Domäne, OU oder des Standorts den Eintrag EIGENSCHAFTEN und dann die Registerkarte GRUPPENRICHTLINIE (siehe Abbildung 20.9).



Abbildung 20.9: Erstellen eines neuen GPO

3. Klicken Sie auf die Schaltfläche NEU, um ein neues GPO zu erstellen, und geben Sie dem GPO einen Namen.



Wenn Sie ein oder mehrere GPOs erstellt haben, sollten Sie eine eigene mmc für die Gruppenrichtlinie erstellen, die dann bequem über das STARTMENÜ / PROGRAMME / VERWALTUNG aufgerufen werden kann. In diese mmc können Sie alle erstellten GPOs aufnehmen.

20.2.3 Bearbeiten von GPOs

Nach dem Erstellen eines Gruppenrichtlinienobjekts kann dieses bearbeitet werden. Dazu zählen die Einstellungen an den benötigten Richtlinien, das Deaktivieren nicht benötigter Richtlinien, das Delegieren der Verwaltung sowie auch das Anpassen der GPO-Verarbeitung und das Löschen von GPOs.

Bearbeiten der Richtlinien

Beginnen wir mit den Einstellungen an den Richtlinien eines GPO. Wählen Sie die zu bearbeitende Richtlinie aus und klicken auf BEARBEITEN, oder öffnen Sie die selbst erstellte mmc der Gruppenrichtlinie. Im folgenden Beispiel wird nun die Richtlinie ANZAHL ZWISCHENZUSPEICHERNDER VORHERIGER ANMELDUNGEN konfiguriert. Wie bereits in Kapitel 3.1 beschrieben, kann ein Wert festgelegt werden, wie viele erfolgreiche Domänenanmeldungen lokal gespeichert werden sollen. Wenn für einen Client ein Domänencontroller nicht erreichbar ist, kann er sich dennoch unter Verwendung der gecachten Domänenanmeldung an der Domäne anmelden. Unter Windows NT konnte keine Anmeldung erfolgen, wenn kein PDC verfügbar war. Deshalb wurde auch an sehr kleinen Standorten oftmals ein PDC installiert, da nicht allein auf die Anmeldung via WAN am PDC in der Hauptstelle vertraut werden sollte. Allerdings nützt ein PDC an einem Standort gar nichts, wenn andere Netzwerkkomponenten wie DHCP- oder DNS-Server nur über das WAN zu erreichen sind. Zur Aufrechterhaltung dieser Funktionalitäten an kleinen Standorten, bei denen keine eigenen DHCP-Server etc. installiert werden, sollte über Router nachgedacht werden, die beim Ausfall der WAN-Verbindung redundante ISDN oder andere Wählverbindungen herstellen. Aber nun zurück zu unserem Beispiel.

1. Öffnen Sie im GPO COMPUTERKONFIGURATION / WINDOWS-EINSTELLUNGEN / SICHERHEITSEINSTELLUNGEN / LOKALE RICHTLINIEN / SICHERHEITSOPTIONEN. Sie sehen in der rechten Fensterhälfte eine lange Liste von Richtlinien, die standardmäßig alle die Computereinstellung NICHT DEFINIERT besitzen. Um für die Richtlinie ANZAHL ZWISCHENZUSPEICHERNDER VORHERIGER ANMELDUNGEN einen Wert festzulegen, klicken Sie diese Richtlinie doppelt.

2. Markieren Sie die Checkbox **DIESE RICHTLINIENEINSTELLUNG DEFINIEREN** (siehe Abbildung 20.10) und geben einen Wert für die Anzahl der Zwischenspeicherungen an. Klicken Sie dann auf OK. In der Liste **COMPUTEREINSTELLUNG** wird nun für diese Richtlinie der Wert **5 ANMELDUNGEN** angezeigt.



Abbildung 20.10: Bearbeiten einer Richtlinie im GPO

3. Definieren Sie nun alle weiteren Richtlinien, die das GPO enthalten soll.

Deaktivieren von Richtlinien

Nachdem Sie alle benötigten Richtlinien konfiguriert haben, sehen Sie, dass bei den übrigen der Wert **NICHT DEFINIERT** angegeben ist. **NICHT DEFINIERT** bedeutet jedoch, dass diese Richtlinie dennoch beim Verarbeiten des GPO abgefragt wird, was zu einer unnötigen Verlängerung des Startvorgangs führt. Um dies zu verhindern, müssen die nicht definierten Richtlinien deaktiviert werden.

Um eine Richtlinie zu deaktivieren, wählen Sie deren Eigenschaften. Markieren Sie dort die Checkbox **DIESE RICHTLINIENEINSTELLUNG DEFINIEREN** und dann **DEAKTIVIERT** (siehe Abbildung 20.11).



Abbildung 20.11: Deaktivieren einer Richtlinie im GPO

Delegieren der Verwaltung

Sobald Sie die Richtlinien für ein GPO bearbeitet bzw. deaktiviert haben, kann die Verwaltung dieses GPO an weitere Administratoren delegiert werden. Die Sicherheitseinstellungen eines GPO erreichen Sie auf der Registerkarte **GRUPPENRICHTLINIE** über **EIGENSCHAFTEN** und dort auf der Registerkarte **SICHERHEITSEINSTELLUNGEN** (siehe Abbildung 20.12).



Abbildung 20.12: Die Sicherheitseinstellungen eines GPO

Für jedes GPO haben fünf Sicherheitsgruppen folgende Standardberechtigungen:

1. Authentifizierte Benutzer: Lesen, Gruppenrichtlinie übernehmen, erweiterte Berechtigungen
2. Domänen-Admins: Lesen, Schreiben, alle untergeordneten Objekte erstellen/löschen, erweiterte Berechtigungen
3. Ersteller-Besitzer: erweiterte Berechtigungen
4. Organisations-Admins: Lesen, Schreiben, alle untergeordneten Objekte erstellen/löschen, erweiterte Berechtigungen
5. System: Lesen, Schreiben, alle untergeordneten Objekte erstellen / löschen, erweiterte Berechtigungen

Diese Standardberechtigungen können selbstverständlich geändert werden. Um einen weiteren Benutzer oder eine Benutzergruppe hinzuzufügen, klicken Sie auf HINZUFÜGEN und wählen die gewünschte Person / Gruppe aus. Standardmäßig erhält der neu hinzugefügte Benutzer nur die Berechtigung LESEN. Damit ein Benutzer jedoch das GPO öffnen und alle darin enthaltenen Richtlinien und deren Einstellungen sehen kann, benötigt er zusätzlich die Berechtigung SCHREIBEN. Spezielle Berechtigungen werden über die Schaltfläche ERWEITERT eingestellt.

Besondere Verarbeitungen

Bereits in Kapitel 20.1.7 haben Sie die speziellen Optionen der Richtlinienverarbeitung kennen gelernt. Um die Richtlinienvererbung eines GPO zu deaktivieren, markieren Sie die entsprechende Checkbox auf der Registerkarte GRUPPENRICHTLINIE des GPO. Die Einstellungen werden dann nicht auf höheren Verarbeitungsebenen wirksam. Die Checkbox kann jedoch nur dann markiert werden, wenn für ein GPO nicht die Option

KEIN VORRANG definiert ist (siehe Abbildung 20.4). Um diese Option festzulegen, klicken Sie auf der Registerkarte GRUPPENRICHTLINIE auf OPTIONEN. Die Loopback-Funktion wird in der mmc über COMPUTERKONFIGURATION / ADMINISTRATIVE VORLAGEN / SYSTEM / GRUPPENRICHTLINIEN in der Richtlinie LOOPBACK-VERARBEITUNGSMODUS eingestellt.

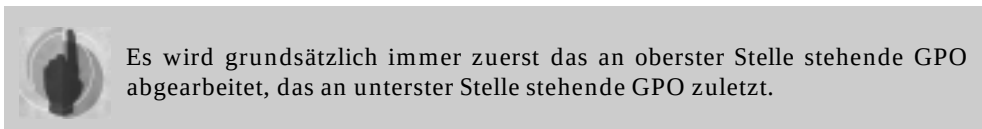


Abbildung 20.13: Mehrere GPOs in einem Container

Über die Schaltfläche EIGENSCHAFTEN können Sie auf der Registerkarte ALLGEMEIN festlegen, die Konfigurationseinstellungen für den Computer und /oder Benutzer zu deaktivieren. Sind im betreffenden GPO keine Benutzer- oder Computerkonfigurationseinstellungen definiert, so sollten Sie die entsprechende Checkbox markieren, um die Abarbeitung des GPO und somit auch den Start- bzw. Anmeldevorgang verkürzen zu können.

Haben Sie für einen Standort oder eine Domäne bzw. Organisationseinheit mehrere GPOs erstellt, so erscheinen diese zunächst in der Reihenfolge des Erstellens auf der Registerkarte GRUPPENRICHTLINIE (siehe Abbildung 20.13).

Über die Schaltflächen NACH OBEN und NACH UNTEN können Sie diese Reihenfolge ändern.



Entfernen und Löschen von GPOs

Das Löschen und Entfernen sind zwei verschiedene Vorgänge. Das Entfernen gilt nur für die Verknüpfungen von GPOs mit einem beliebigen Container. Wird eine Verknüpfung entfernt, so ist damit keineswegs das GPO aus dem Active Directory gelöscht. Um ein

GPO zu entfernen, öffnen Sie die Registerkarte GRUPPENRICHTLINIE des betreffenden Containers (siehe Abbildung 20.9) und wählen LÖSCHEN. Sie erhalten dann eine Dialogbox für den Löschvorgang (siehe Abbildung 20.14).

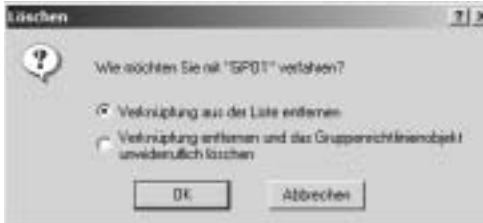
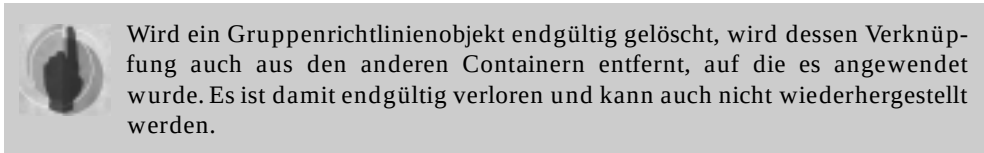


Abbildung 20.14: Löschen oder Entfernen eines GPO

Um lediglich die Verknüpfung des GPO mit dem aktuellen Container aufzuheben, markieren Sie die Checkbox VERKNÜPFUNG AUS DER LISTE ENTFERNEN. Soll das GPO für immer gelöscht werden, wählen Sie die Option VERKNÜPFUNG ENTFERNEN UND DAS GRUPPENRICHTLINIEOBJEKT UNWIDERRUFLICH LÖSCHEN.



20.2.4 Zuweisen von GPOs

Wenn ein GPO erstellt wird, so wird dieses standardmäßig nur für den Container angewendet, in dem es erstellt wurde. So wird also ein GPO, das in der Domäne *firma.de* erstellt wird, nur auf diesen Container angewendet. Dieses GPO kann aber auch einem Standort, einer OU oder einer anderen Domäne der Gesamtstruktur zugewiesen werden. Man spricht dabei auch vom Verknüpfen von GPOs. Um ein GPO einem anderen Container zuzuweisen, führen Sie die folgenden Schritte aus:

1. Wenn Sie ein bestehendes GPO einer Domäne oder OU zuweisen möchten, öffnen Sie die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER; wollen Sie das GPO einem Standort zuweisen, öffnen Sie die mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE.
2. Wählen Sie aus dem Kontextmenü von Standort, Domäne oder OU den Eintrag EIGENSCHAFTEN und dann GRUPPENRICHTLINIEN.
3. Sie sehen eine Liste aller GPOs, die bereits für diesen Container angewendet werden. Um ein zusätzliches GPO hinzuzufügen, klicken Sie auf HINZUFÜGEN.
4. Sie können separat für die Domänen, OUs und Standorte die jeweils vorhandenen GPOs anzeigen lassen (siehe Abbildung 20.15). Auf der Registerkarte ALLE werden sämtliche GPOs aufgelistet, die erstellt worden sind. Wählen Sie nun das gewünschte GPO aus und klicken auf OK.

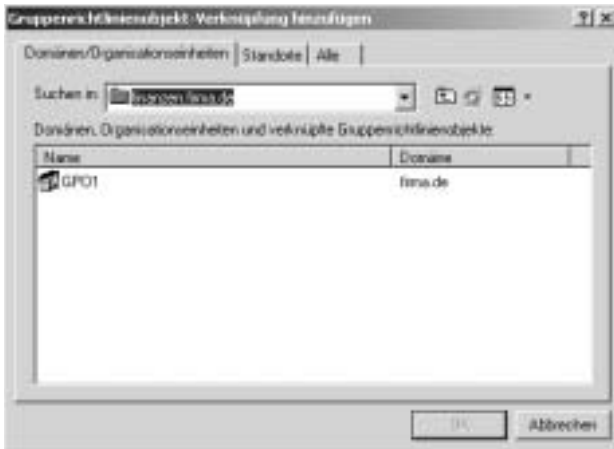


Abbildung 20.15: Verknüpfen von GPOs

Weiterhin können Sie auch ermitteln, von welchen Standorten, Domänen und Organisationseinheiten ein bestimmtes GPO verwendet wird. Wählen Sie dazu aus den Eigenschaften der Gruppenrichtlinie die Registerkarte LINKS (siehe Abbildung 20.16). Sie können nun innerhalb aller Domänen der Gesamtstruktur nach Standorten, Domänen und OUs suchen, die das entsprechende GPO verwenden.

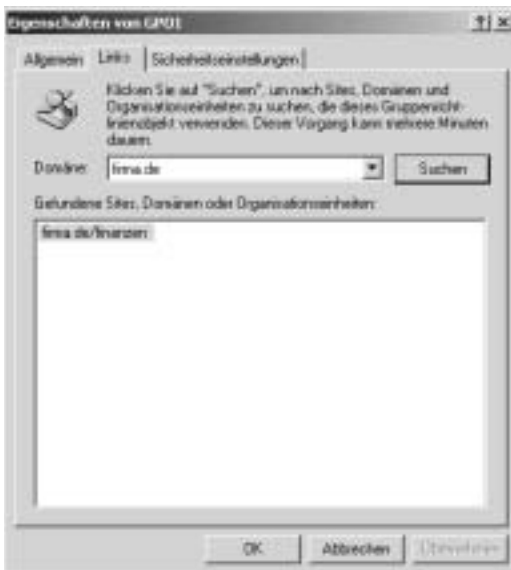


Abbildung 20.16: Suchen eines GPOs innerhalb der Domäne

Nachdem die GPOs konfiguriert und eventuell auch weiteren Standorten, Domänen oder Organisationseinheiten zugewiesen sind, müssen diese den entsprechenden Benutzern, Benutzergruppen und Computern zugewiesen werden. Damit ein GPO für einen

bestimmten Benutzer angewendet wird, müssen diesem die entsprechenden Berechtigungen zugewiesen werden. Dazu zählen die Rechte LESEN sowie GRUPPENRICHTLINIE ÜBERNEHMEN. Die Berechtigungen vergeben Sie über die Registerkarte SICHERHEITSEINSTELLUNGEN (siehe Abbildung 20.12).

Um einer bestimmten Benutzergruppe dieses GPO zuzuweisen, setzen Sie die Berechtigungen LESEN und GRUPPENRICHTLINIE ÜBERNEHMEN auf ZULASSEN. Damit wird das GPO auf alle Mitglieder dieser Gruppe angewendet. Eine Ausnahme bilden nur die Gruppenmitglieder, die einer anderen Gruppe angehören, der eine oder beide Berechtigungen explizit verweigert wurden, bzw. die Gruppenmitglieder, denen als einzelner Benutzer eine oder beide Berechtigungen verweigert wurden.

Wenn für eine bestimmte Gruppe das GPO nicht angewendet werden soll, so setzen Sie LESEN und GRUPPENRICHTLINIE ÜBERNEHMEN auf VERWEIGERN. Da das Verweigern Vorrang vor Zulassen hat, gilt das GPO auch nicht für die Mitglieder, denen über eine andere Gruppenmitgliedschaft eines der Rechte gestattet wurde.

Wenn Sie die Berechtigungen LESEN und GRUPPENRICHTLINIE ÜBERNEHMEN für eine Gruppe weder auf Zulassen noch auf Verweigern setzen, so wird nur auf die Mitglieder das GPO angewendet, die über eine andere Gruppenmitgliedschaft die entsprechende Berechtigung für das GPO erhalten haben.

20.2.5 Spezielle An- und Abmeldeskripte

Über die Gruppenrichtlinie können Sie Computern und Benutzern Skripte zum Starten und Herunterfahren bzw. für die An- und Abmeldung zuweisen. Das Login-Skript für einen Computer wird beim Start des Rechners ausgeführt, das für einen Benutzer, sobald er sich anmeldet. Die An- und Abmeldeskripte befinden sich im Verzeichnis SYSVOL\USER\SCRIPTS.



Diese Skripte können nur für Windows 2000- und XP-Clients ausgeführt werden. Ältere Windows-Clients besitzen nicht die Möglichkeit, diese Skripte aus dem Active Directory auszulesen und auszuführen. Für diese alten Clients müssen Sie die herkömmlichen Start- und Anmeldeskripte verwenden.

Im Gegensatz zu den altbekannten An- und Abmeldeskripten unter Windows NT, die meist als Batchdatei erstellt worden sind, können Sie nun auch Skripte in VBScript oder JScript erstellen. Sie können beispielsweise ein Skript erstellen, das beim Start die Gruppenmitgliedschaft eines Benutzers prüft. Es kann ermitteln, ob der Benutzer z.B. ein Mitglied der Gruppe Buchhalter in der Domäne *firma.de* ist. Mit Hilfe eines solchen Skriptes ist es möglich, Gruppenmitgliedern beim Start bestimmte Laufwerke oder Drucker zuzuweisen. Eine umfangreiche Referenz zu den Skriptsprachen finden Sie unter www.microsoft.com/scripting.

Über ein Skript können Sie das Anmeldeverhalten der Benutzer steuern. Bei der Anmeldung kann über ein Skript der Name des Benutzers abgefragt und geprüft werden, ob es sich um einen gültigen Active Directory-Benutzer handelt. Ist dies der Fall, wird weiter geprüft, ob er Mitglied einer im Skript definierten Benutzergruppe ist. Ist dies der Fall,

werden weitere Optionen wie z.B. das Zumappen bestimmter Laufwerke und Drucker durchgeführt.

Das Skript wird als Textdatei geschrieben und unter der Dateierendung *.vbs bei einem VBScript oder *.js bei einem JavaScript gespeichert. Sie sollten ein Skript jedoch niemals per Doppelklick öffnen, da es automatisch startet und unvorhergesehene Aktionen auslösen könnte. Zum Bearbeiten öffnen Sie das Skript mit einem beliebigen Texteditor.

Ein praktisches Beispiel für den Einsatz eines An- und Abmeldeskripts ergibt sich aus folgender Situation: Wenn sich ein Administrator auch an einem beliebigen Arbeitsplatz unter Windows 2000 oder XP Professional anmelden und von dort aus den Server verwalten möchte, müssen ihm zu diesem Zweck seine Administrationswerkzeuge zur Verfügung stehen, aber nur so lange, wie der Administrator selbst auf dem Rechner angemeldet ist. Wenn sich hinterher ein anderer Benutzer dort anmeldet, dürfen für ihn diese Werkzeuge nicht mehr zur Verfügung stehen. Die Gefahr ist zu groß, dass der nachfolgende unversierte Benutzer diese als Spielzeug missbraucht. Unter Windows NT hätten Sie für sich als Administrator auf jedem Nicht-Server-Arbeitsplatz die Admin-Tools installieren und vor dem Verlassen des Arbeitsplatzes wieder deinstallieren müssen. Dieses zeitaufwändige Verfahren ist unter Windows 2000 nicht mehr notwendig. Bei der Anmeldung als Administrator werden die entsprechenden Programme installiert, über ein Abmeldeskript wird die Deinstallation der Programme durchgeführt.

Die Anzahl der Möglichkeiten für den Einsatz von An- und Abmeldeskripten und auch von Skripten zum Starten / Herunterfahren des Rechners ist vielfältig. Ein entscheidender Vorteil gegenüber Windows NT besteht darin, dass Sie nicht mehr nur ein, sondern eine beliebige Anzahl von Skripten für einen Computer oder Benutzer implementieren können. Angenommen, sämtliche Computer verfügen über ein standardisiertes Startskript. Nun soll jedoch auf allen Rechnern eine neue *.dll oder ein bestimmter Registry-Schlüssel installiert werden. Diese Installation können Sie über ein zweites Startskript steuern. Ist die neue *.dll oder der Schlüssel auf allen Computern installiert, kann dieses zweite Skript wieder entfernt werden.

Skripte eignen sich auch gut, wenn Benutzern nur für einen bestimmten Zeitraum standardmäßig nicht zugewiesene Operationen erlaubt werden sollen. Soll eine Gruppe von Benutzern beispielsweise eine Schulung zum Thema Internet Explorer erhalten, können Sie über ein zweites Anmeldeskript den Benutzern für die Dauer der Schulung erweiterte Berechtigungen zuteilen und ansonsten zugewiesene Einschränkungen wie z.B. Browser-Menüs, Auto-Vervollständigen oder Filtereinstellungen aufheben. Ist die Schulung abgeschlossen, wird das zweite Skript wieder entfernt, und den Benutzern stehen nur noch die eingeschränkten Funktionalitäten zur Verfügung.

20.2.6 Gruppenrichtlinien für Organisationseinheiten sinnvoll planen

In diesem Kapitel wird Ihnen gezeigt, wie Sie Organisationseinheiten sinnvoll planen können, um Gruppenrichtlinien darauf anwenden zu können. Angenommen, Sie haben in Ihrem Unternehmen die Organisationseinheiten nach regionalen Gesichtspunkten Ihrer Filialen erstellt und in jeder dieser OUs dieselbe funktionale Hierarchie etabliert. So könnte beispielsweise Ihre Domäne *firma.de* die drei Organisationseinheiten Dortmund,

Wolfsburg und Oberhausen nach regionalen Aspekten gegliedert umfassen, und in jeder dieser drei OUs haben Sie Unter-OUs nach funktioneller Struktur implementiert, z.B. Werbung und Vertrieb. Sie können so für jede Filiale die Verwaltung von Benutzerkonten usw. an eine Person, nämlich den Administrator der jeweiligen OU delegieren. So weit, so gut.

Nun möchten Sie aber die Gruppenrichtlinie zur Softwareverteilung einsetzen, um allen Mitgliedern der Werbungsorganisationseinheiten aller drei Filialen eine bestimmte Applikation zukommen zu lassen. Dazu müssen Sie dreimal unabhängig für jede übergeordnete Organisationseinheit die Gruppenrichtlinie anwenden. Dies mag ja für drei Standorte noch praktikabel sein, aber wenn Sie über eine sehr große Anzahl von Filialen verfügen, kann die Durchsetzung der Gruppenrichtlinie schnell unübersichtlich werden. Dieses Problem ließe sich auf den ersten Blick lösen, indem Sie die Organisationseinheiten so umstrukturieren, dass sie als Kriterium für die übergeordneten OUs die Funktionalität wählen. Sie hätten dann also die beiden übergeordneten OUs Werbung und Vertrieb, in denen sich jeweils die drei verschiedenen regionalen Zweigstellen befinden. Sie hätten dann zwar kein Problem mehr bei der Anwendung der Gruppenrichtlinie, aber die Verwaltung wird erschwert, da Sie die Verwaltung nun an zwei OUs pro Standort delegieren müssen. Es scheint, als könnte entweder nur die Verwaltung oder nur die Durchsetzung der Gruppenrichtlinie vereinfacht werden, da Sie ja nicht nach Belieben die Struktur der OUs anpassen können, wie Sie diese gerade benötigen.

Abhilfe hierfür schafft wiederum ein Programm von Aelita Software, und zwar der *Enterprise Directory Manager (EDM)*. Dieses Programm arbeitet mit so genannten Managed Units. In einer Managed Unit können Sie nach Ihren Auswahlkriterien Mitglieder festlegen, unabhängig von der Struktur des Active Directory. So können Sie beispielsweise eine Managed Unit für alle Benutzer anlegen, die als Standort Dortmund eingetragen haben. Diese Benutzer können sich in den verschiedensten funktionellen Organisationseinheiten befinden. Sie können dann über EDM die Verwaltung an die Managed Units anstatt an die Organisationseinheiten delegieren. Organisieren Sie also Ihre OUs nach funktionalen Aspekten, und fassen Sie die Benutzer nach regionalen Aspekten in den Managed Units zusammen. In unserem Beispiel würden Sie also eine Managed Unit für Werbung und eine für Vertrieb anlegen. Diesen beiden Units werden die Mitglieder aller drei Filialen hinzugefügt.

Da Sie über EDM zwar alle Verwaltungsaufgaben wie das Anlegen neuer Benutzer etc. durchführen können, jedoch nicht das Zuweisen von Gruppenrichtlinien, sind Sie an das einschränkende Schema gebunden, die OUs nach Funktionalitäten zu ordnen und auf diese Weise die Durchsetzung der Gruppenrichtlinien zu vereinfachen. Sie können nicht OUs nach regionalen Aspekten erstellen und Managed Units nach Funktionalität, da Sie für diese funktionellen Einheiten über EDM keine Gruppenrichtlinien durchsetzen können.

20.3 Die GPMC unter Windows Server 2003

Die Group Policy Management Console (GPMC) ist eine neue mmc, in der sämtliche Einstellungen bezüglich der Gruppenrichtlinien zentral vorgenommen werden können. Dazu zählen Backup und Wiederherstellung an einem beliebigen Ort im Netzwerk sowie Im- und Export von GPOs und Sicherheitseinstellungen. Ferner werden HTML-Reports über die GPO-Einstellungen sowie die Auswirkungen von GPO-Einstellungen ausgegeben. Dieses Feature entspricht dem Resultant Set of Policy der Windows XP-Clients (siehe Kapitel 20.1.10). Auch die Verwaltung der Sicherheitsaspekte wird in der GPMC simplifiziert. Zusätzlich besteht die Möglichkeit, WMI-Filter anzuwenden. Mit Hilfe der WMI-Filter werden Anfragen an eine WMI-Datenbank auf einem Zielcomputer gesendet. Diese Datenbank wertet dies dann als wahr oder falsch aus. Sämtliche Operationen, die Sie über die GUI der GPMC vornehmen können, können auch skriptgesteuert erfolgen. Jedoch kann die Einstellung an den GPOs nicht via Skript vorgenommen werden. Diese Zentralisierung stellt eine deutliche Verbesserung gegenüber Windows 2000 dar. Zum einen war die Verknüpfung eines GPO mit einer Reihe von Benutzergruppen zwar möglich, aber unübersichtlich. Man konnte sehr schnell den Überblick verlieren, an welchen Stellen das GPO verwendet wird. Auch die Anwendung von mehreren GPOs auf den verschiedenen Ebenen Standort, Domäne und OU konnte schnell kompliziert werden. Aufgrund von Vererbung der verschiedenen Richtlinien und Priorisierung von GPOs derselben Ebene war es sicher nicht immer ohne Probleme möglich, die genauen Auswirkungen der GPOs zu erkennen.

Die GPMC ist eine separate freie Komponente des Windows Server 2003. Sie wird u.a. auch in einer deutschen Version angeboten. Diese Version kann unter <https://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=F39E9D60-7E41-4947-82F5-3330F37ADFE8> heruntergeladen werden.

Über die GPMC können sowohl Windows 2000- als auch Windows 2003-Domänen verwaltet werden. Bedenken Sie aber, dass die erweiterten Funktionalitäten der GPMC wie z.B. WMI-Filter in einer reinen Windows 2000-Umgebung nicht verfügbar sind. Der Computer, auf dem die GPMC zur Verwaltung installiert ist, muss entweder ein Windows Server 2003 oder ein Windows XP Professional Client sein. Im Falle von Windows XP müssen zusätzlich die folgenden Komponenten installiert sein:

- ▶ Windows XP SP1 sowie
- ▶ Microsoft .NET Framework

Zusätzlich wird das Post SP1-Hotfix Q326469 benötigt. Dies ist in der GPMC enthalten und wird während der Installation der GPMC mitinstalliert.

Neben den genannten neuen Kern-Features können mit der GPMC auch in weiteren Bereichen Verwaltungsaufgaben durchgeführt und simplifiziert werden. Tabelle 20.4 gibt Ihnen einen Überblick über weitere Features der GPMC.

Feature	Beschreibung
Neue Gruppenrichtlinieneinstellungen	Der Windows Server 2003 enthält über 150 zusätzliche GPO-Einstellungen. Diese beziehen sich u.a. auf die Bereiche Terminal Server, DNS, Fehler-Reporting oder Roaming Profiles.
Webansicht der administrativen Vorlagen	Sobald eine bestimmte Richtlinieneinstellung gewählt wird, zeigt die Webansicht detaillierte Informationen zu den Einstellungen sowie dem Zweck der Einstellungen. Die Webansicht ist auch für die Registerkarte „Erklärung“ jeder Einstellung verfügbar.
GPO-Modeling	Das GPO-Modeling bietet die Möglichkeit, Richtlinieneinstellungen, Sicherheit und Applikationen in einem „Was-Wenn-Szenario“ zu untersuchen. Diese Funktion ist bei einer Umstrukturierung oder Expansion sehr hilfreich. Bevor eine Änderung durchgeführt wird, können zahlreiche Tests ausgeführt werden, um die Konsequenzen für einen Benutzer oder eine Gruppe abzusehen.
DNS-Client	Die DNS-Client-Einstellungen auf einem Windows 2003 Server wie z.B. die dynamische Registrierung der DNS-Records oder die Übernahme des primären DNS-Suffix können vereinfacht über die Gruppenrichtlinie eingestellt werden.
Netzwerkverbindungen	Über die Gruppenrichtlinie kann die GUI zur Einstellung der Netzwerkverbindungen nur bestimmten Benutzern verfügbar bzw. nicht verfügbar gemacht werden.
Softwareinstallation bei der Anmeldung	Bei der Softwareverteilung besteht nun die Möglichkeit, dem Benutzer zugewiesene Software vollständig bei seiner Anmeldung zu installieren und nicht erst bei Bedarf.
Software Support-URL	Für jedes installierte Softwarepaket kann der Benutzer über die Systemsteuerung – Software – Hinzufügen/Entfernen eine URL aufrufen, über die er direkt auf die Supportseite des Herstellers gelangt. Dies entlastet den firmeninternen Support und das Helpdesk.
WMI-Filter	Über WMI (Windows Management Instrumentation) werden Hard- und Software-Inventory-Daten sowie weitere Konfigurationseinstellungen aus der Registry, dem Dateisystem, Treibern, Active Directory, Windows Installer, SNMP, Netzwerk, SQL und Exchange ausgelesen. Beim WMI-Filtering kann festgelegt werden, ob ein GPO auf einem WMI-Filter beruhen soll. Ein WMI-Filter ist eine Abfrage der WMI-Daten. Über diesen Filter können Sie festlegen, auf welche Benutzer und Computer ein GPO angewendet werden soll. Diese Funktion ist sinnvoll, wenn an alle Benutzer einer OU ein bestimmtes Softwarepaket verteilt werden soll, wofür jedoch genügend Festplattenkapazität zur Verfügung stehen muss. Sie können in diesem Fall einen WMI-Filter verwenden, der die Applikation lediglich bei den Benutzern installiert, die über mindestens 500 MB freien Festplattenplatz verfügen.

Tabelle 20.4: Weitere Features der GPMC

Unter Windows 2000 musste ein Administrator eine Reihe von Werkzeugen zur Erstellung und Verwaltung von Gruppenrichtlinien aufrufen. In der GPMC sind jedoch die folgenden Programme enthalten: die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER sowie STANDORTE UND DIENSTE, RSoP (Windows XP), der Delegierungs-Assistent sowie der ACL-Editor. Diese Funktionalitäten sind nun über einen zentralen Aufruf erreichbar. Sobald jedoch die GPMC installiert ist, kann die Administration der GPOs nicht mehr wie bisher gewohnt durchgeführt werden. Wollen Sie den Gruppenrichtlinieneditor beispielsweise über die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER aufrufen, so erhalten Sie die Meldung, dass Sie zur Verwaltung die GPMC benutzen mögen. Die Registerkarte GRUPPENRICHTLINIE in den Eigenschaften von Domänen oder Organisationseinheiten ist nicht länger verfügbar (siehe Abbildung 20.17).



Abbildung 20.17: Die Registerkarte Gruppenrichtlinie ist nach Installation der GPMC nicht länger verfügbar.

Die GPMC verfügt auch über eine Reihe von Skript-Schnittstellen. Skripte oder Anwendungen können auf eigens entwickelte COM-Objekte der GPMC zugreifen und diese verwenden. Eine komplette Dokumentation dieser COM-Objekte befindet sich im GPMC-SDK. Dieses wird künftig wahrscheinlich Bestandteil des Windows Platform SDK werden.

20.3.1 Die Administration über die GPMC

Nach der Installation der GPMC befindet sich im STARTMENÜ/VERWALTUNG der neue Eintrag GRUPPENRICHTLINIENVERWALTUNG. Beim Start dieser mmc werden Sie aufgefordert, sich mit einem gültigen Domänenbenutzerkonto anzumelden, sofern der Verwaltungscomputer lediglich Mitglied einer Arbeitsgruppe ist. Abbildung 20.18 zeigt eine Übersicht über die GPMC.

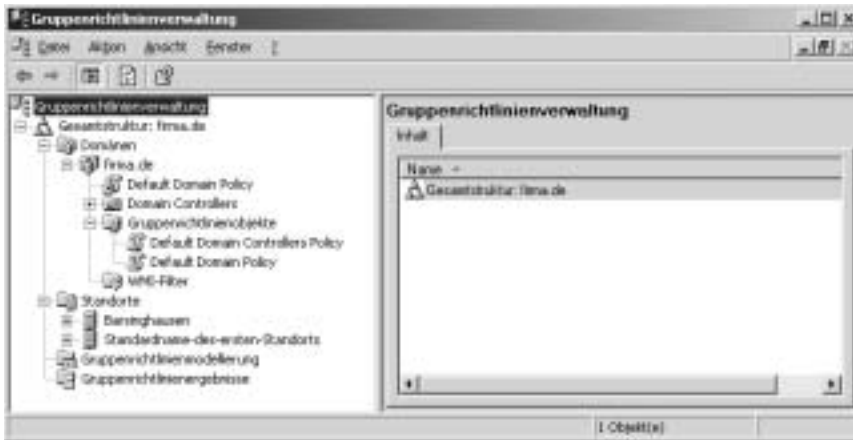


Abbildung 20.18: Die Group Policy Management Console (GPMC)

In der mmc wird die Hierarchie des Netzwerks von der obersten Ebene der Gesamtstruktur über Domänen, Standorte und OUs bis hin zu den einzelnen GPOs abgebildet. Standardmäßig werden dort keine Standorte und weiteren Domänen außer der aktuellen angezeigt. Um weitere Objekte der mmc hinzuzufügen, wählen Sie aus dem Kontextmenü von DOMÄNEN bzw. STANDORTE den Eintrag DOMÄNEN ANZEIGEN bzw. STANDORTE ANZEIGEN. Aus der Liste wählen Sie die Standorte bzw. Domänen aus, die in der mmc angezeigt werden sollen. Mehrere Gesamtstrukturen können nur dann angezeigt werden, wenn Vertrauensstellungen zwischen Gesamtstrukturen aktiviert sind. Hierzu müssen jedoch alle Domänencontroller unter Windows Server 2003 im Gesamtstrukturfunktionsmodus Windows Server 2003 betrieben werden (siehe Kapitel 10.1.5).

20.3.2 Erstellen, Löschen und Verknüpfen von GPOs

Um in der GPMC ein neues GPO zu erstellen, wählen Sie eine Domäne und klicken dort auf GRUPPENRICHTLINIENOBJEKTE. Aus dem Kontextmenü wählen Sie NEU und vergeben einen Namen für das neue GPO. Soll das neue GPO zugleich mit der Domäne verknüpft werden, so wählen Sie GRUPPENRICHTLINIENOBJEKT HIER ERSTELLEN UND VERKNÜPFEN. Soll ein bestehendes GPO mit einer Domäne, einem Standort oder einer OU verknüpft werden, so wählen Sie aus dem jeweiligen Kontextmenü den Eintrag VORHANDENES GRUPPENRICHTLINIENOBJEKT VERKNÜPFEN.

Nachdem das Objekt erstellt ist, wählen Sie aus dessen Kontextmenü BEARBEITEN. Es öffnet sich der Gruppenrichtlinienobjekt-Editor, mit dem Sie alle Einstellungen bearbeiten können, wie in Kapitel 20.1.6 beschrieben. Bedenken Sie, dass sich die Änderungen an einem bestehenden GPO auf sämtliche Container auswirken, mit denen das GPO verknüpft ist. Bei Änderungen gibt die GPMC jeweils eine Warnmeldung aus, die Sie an diese Tatsache erinnert.

Jedes GPO verfügt über insgesamt vier Registerkarten. Unter BEREICH (siehe Abbildung 20.19) sehen Sie, mit welchen Standorten, Domänen und OUs das GPO verknüpft ist, für welche Benutzergruppen das GPO angewendet wird und mit welchen WMI-Filtern es verknüpft ist.

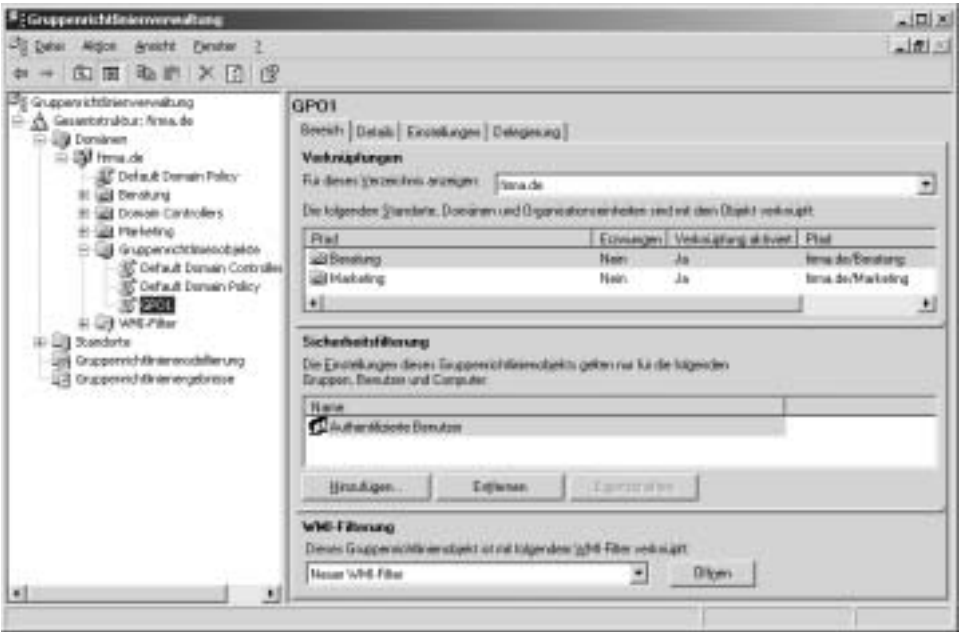


Abbildung 20.19: Die Registerkarte Bereich eines GPO

Die Registerkarte DETAILS (siehe Abbildung 20.20) gibt Auskunft über Erst- und Änderungsdatum, die GUID, den Besitzer, die Domäne sowie den Objektstatus.

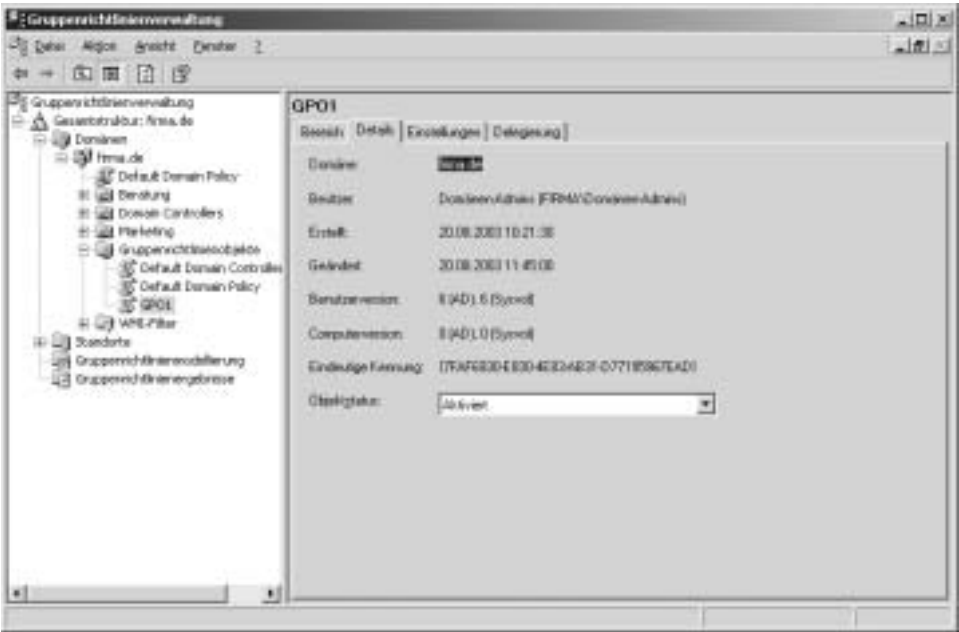


Abbildung 20.20: Die Registerkarte Details eines GPO

Die Registerkarte EINSTELLUNGEN (siehe Abbildung 20.21) zeigt, welche Bereiche des GPO konfiguriert worden sind. Für die Computer- und Benutzerkonfiguration finden Sie eine übersichtliche Auflistung der Richtlinien, die aktiviert oder deaktiviert sind. Nicht konfigurierte Einstellungen werden nicht angezeigt.

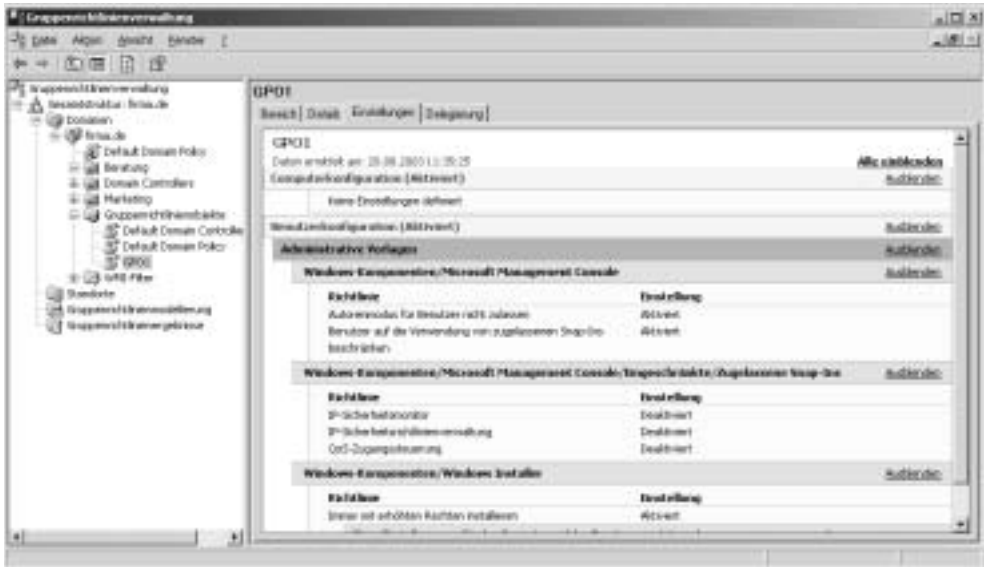


Abbildung 20.21: Die Registerkarte Einstellungen eines GPO

Die vierte Registerkarte DELEGIERUNG (siehe Abbildung 20.22) zeigt an, welche Benutzer und Gruppen welche Berechtigungen für das GPO besitzen. Über die Einträge im Kontextmenü der Gruppen und Benutzer können die Berechtigungen auch modifiziert werden.

Bevor Sie ein GPO löschen, sollten Sie auf dessen Registerkarte BEREICH prüfen, ob noch domänenübergreifende Verknüpfungen bestehen. Wählen Sie dazu aus der Drop-down-Liste VERKNÜPFUNGEN FÜR DIESES VERZEICHNIS ANZEIGEN DEN EINTRAG [GESAMTSTRUKTUR]. Nun können Sie alle bestehenden Verknüpfungen löschen, bevor das GPO selbst endgültig gelöscht wird. Die beiden GPOs *Default Domain Controllers Policy* und *Default Domain Policy* können nicht gelöscht werden.

Über den Kontextmenüeintrag STATUS DER GRUPPENRICHTLINIE jedes GPO können Sie den Status der Richtlinien festlegen. Sie können das GPO aktivieren, separat die Einstellungen der Benutzerkonfiguration oder Computerkonfiguration oder das gesamte GPO deaktivieren.

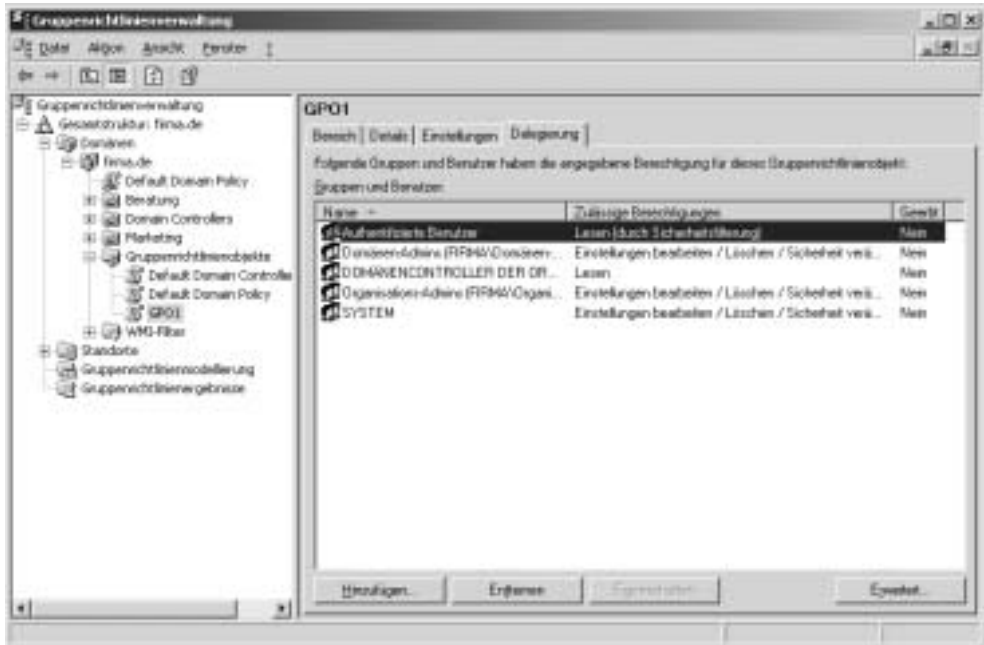


Abbildung 20.22: Die Registerkarte Delegation eines GPO

20.3.3 Backup von GPOs

Beim Backup eines GPO werden sämtliche Bestandteile des GPO gesichert, die im Active Directory selbst sowie der Dateistruktur im Ordner SYSVOL enthalten sind. Dazu zählen die GUID des GPO sowie die Domäne, die Einstellungen des GPO, die Zugriffsberechtigungen für das GPO sowie der Verweis auf möglicherweise verknüpfte WMI-Filter. Die WMI-Filter selbst werden beim Backup eines GPO jedoch nicht gesichert. Dasselbe gilt auch für IPSec-Richtlinien, die auf eine GPO angewendet werden können. Dies liegt darin begründet, dass beispielsweise für einen WMI-Filter andere Berechtigungen gelten als für das GPO selbst. Es wäre also möglich, dass einem Administrator beim Backup oder Wiederherstellen eines GPO nicht die erforderlichen Berechtigungen für einen WMI-Filter oder eine IPSec-Richtlinie zur Verfügung stehen. Zusätzlich würde es unnötig sein, WMI-Filter oder IPSec-Richtlinien zusammen mit jedem GPO zu speichern, wenn diese mit mehreren GPOs verknüpft sind. Für das Backup der WMI-Filter selbst verwenden Sie in der GPMC die Export- und Importfunktion des WMI-Filters selbst (siehe Kapitel 20.3.11). Ein Backup der IPSec-Richtlinien führen Sie über die Import- und Exportfunktion des Snap-In IP-SICHERHEITSRICHTLINIEN IN DEM JEWEILIGEN GPO SELBST DURCH.

Beim Backup eines GPO wird ein XML-basierter Bericht erstellt. Dieser Bericht enthält einen Zeitstempel, optional eine Beschreibung sowie die GPO-Einstellungen. Jeder Backup-Vorgang wird durch eine eindeutige Nummer gekennzeichnet. So ist es möglich, mehrere Sicherungen desselben GPO an demselben Speicherort abzulegen. Die XML-basierten Backup-Berichte können über die GPMC als HTML betrachtet werden.

Damit ein Backup durchgeführt werden kann, muss für das GPO die Berechtigung Lesen bestehen. Für den Speicherort des Backups muss Schreibzugriff vorhanden sein. Um ein Backup eines GPO anzulegen, führen Sie die folgenden Schritte durch:

1. Wählen Sie aus dem Kontextmenü des gewünschten GPO den Eintrag Sichern.
2. Sie erhalten das Fenster GRUPPENRICHTLINIENOBJEKT SICHERN (siehe Abbildung 20.23). Über die Schaltfläche DURCHSUCHEN legen Sie den Speicherort fest. In das Textfeld BESCHREIBUNG können Sie optional einen Kommentar angeben. Klicken Sie dann auf SICHERN.



Abbildung 20.23: Sichern eines GPO

Während des Sicherungsvorgangs werden Sie über den Status sowie den Erfolg oder Misserfolg informiert.

Wollen Sie mehrere GPOs gleichzeitig sichern, so klicken Sie in der GPMC auf den Knoten GRUPPENRICHTLINIENOBJEKTE. Auf der Registerkarte INHALT markieren Sie nun ein GPO oder mehrere. Wollen Sie mehrere GPOs markieren, halten Sie dabei die Taste **Strg** gedrückt. Sie erhalten dasselbe Dialogfeld wie in Abbildung 20.23 dargestellt. Es werden dann alle gewählten GPOs gesichert.

Wollen Sie sämtliche vorhandenen GPOs sichern, so wählen Sie aus dem Kontextmenü des Knotens GRUPPENRICHTLINIENOBJEKTE den Eintrag ALLE SICHERN. Sie erhalten dasselbe Dialogfeld wie in Abbildung 20.23 dargestellt. Es werden dann alle vorhandenen GPOs gesichert.

Für die Sicherung der GPOs können Sie auch Skripte verwenden. Sie können entweder eigene Skripte schreiben oder ein vordefiniertes Skript benutzen. Die vordefinierten Skripte befinden sich im Verzeichnis GPMC\SCRIPTS. Mit Hilfe des Skripts *BackupGPO.wsf* können Sie die Sicherung eines GPO durchführen, das Skript *BackupAllGPO.wsf* führt eine Sicherung sämtlicher GPOs durch.

Verwalten mehrerer Backups

Außer der Erstellung von Sicherungen ist über die GPMC auch die Verwaltung der Backups möglich. Um das Dialogfenster zur Backup-Verwaltung aufzurufen, wählen Sie entweder aus dem Kontextmenü des DOMÄNEN-Containers oder des Containers GRUPPENRICHTLINIENOBJEKTE den Eintrag SICHERUNGEN VERWALTEN. Im ersten Fall werden alle gesicherten GPOs der kompletten Gesamtstruktur angezeigt, im zweiten Fall lediglich die GPOs der aktuellen Domäne. Die Verwaltungsmöglichkeiten sind in beiden Fällen dieselben (siehe Abbildung 20.24).

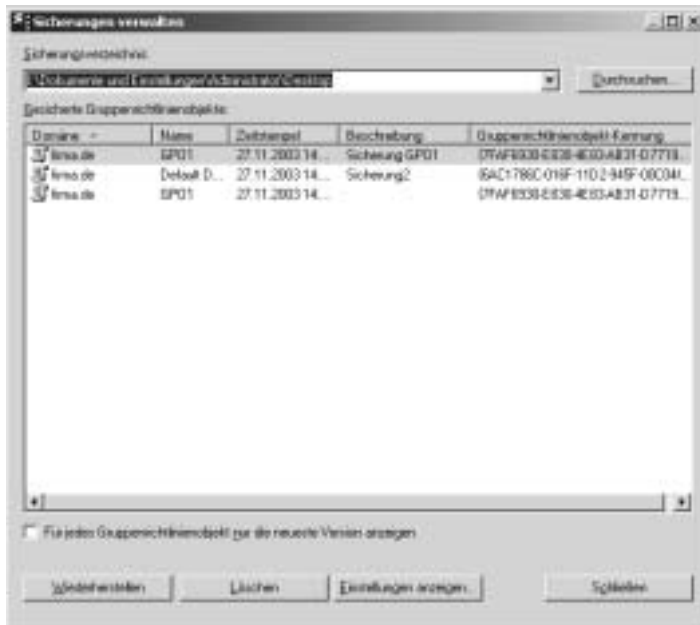


Abbildung 20.24: Die Verwaltung der gesicherten GPOs

Im Fenster SICHERUNGEN VERWALTEN sehen Sie unter SICHERUNGSVERZEICHNIS den Pfad zu der Lokation, in der sich die angezeigten Sicherungen der GPOs befinden. Zu jedem gesicherten Objekt wird der Name der Domäne, der Name des GPO, der Zeitpunkt des Backups, eine optionale Beschreibung sowie die eindeutige GUID des GPO angegeben. Sofern Sie die Checkbox FÜR JEDES GRUPPENRICHTLINIENOBJEKT NUR DIE NEUESTE VERSION ANZEIGEN aktivieren, wird für ein GPO, das mehrmals gesichert wurde, lediglich der Eintrag angezeigt, der den neuesten Zeitstempel trägt.

Im unteren Bereich befinden sich drei Schaltflächen, über die Sie ein gesichertes GPO wieder herstellen oder löschen können. Jede dieser beiden Aktionen muss vor ihrer Durchführung separat bestätigt werden. Auch das Anzeigen der GPO-Einstellungen ist möglich. Hierzu öffnet sich der standardmäßige Webbrowser des Benutzers und zeigt die Einstellungen als html-Seite an.

Die Verwaltung mehrerer Sicherungen kann auch skriptgesteuert erfolgen. Verwenden Sie hierzu das Beispielskript *QueryBackupLocation.wsf*, das sich im Verzeichnis GPMC\SCRIPTS befindet.

20.3.4 Wiederherstellung von GPOs

Die Wiederherstellung eines GPOs darf nicht mit dem Import oder Kopieren eines GPOs (siehe Kapitel 20.3.5) verwechselt werden. Beim Wiederherstellen wird das GPO auf einen früheren Status zurückgesetzt. Dies kann erforderlich werden, wenn ein GPO wieder auf einen funktionierenden älteren Status gebracht werden soll (Rollback) oder wenn ein GPO versehentlich gelöscht worden ist. Bei der Wiederherstellung behält das GPO seine ursprüngliche GUID. Ersetzt werden die Einstellungen des GPO, seine Berechtigungen sowie die verknüpften WMI-Filter. Sind beim Löschen eines GPOs auch seine Verknüpfungen gelöscht worden, so müssen diese manuell wiederhergestellt werden. Dieser Prozess ist nicht Bestandteil der GPO-Wiederherstellung. Um die Verknüpfungen schneller wiederherstellen zu können, sehen Sie sich den Sicherungsbericht des GPOs an, in dem alle Verknüpfungen des GPOs innerhalb der Domäne aufgeführt sind.



Ein gesichertes GPO kann nicht wiederhergestellt werden, wenn zwischenzeitlich die Domäne umbenannt worden ist. Sie sollten also grundsätzlich sämtliche GPOs sichern, sobald eine Domäne umbenannt worden ist.

Wiederherstellen vorhandener GPOs

Um ein vorhandenes GPO mit seinen ursprünglichen Einstellungen wiederherzustellen, führen Sie die folgenden Schritte aus:

1. Wählen Sie aus dem Kontextmenü des GPOs den Eintrag VON SICHERUNG WIEDER HERSTELLEN. Damit wird der Wiederherstellungsassistent gestartet.
2. Geben Sie zunächst den Ordner an, in dem sich die Sicherungen der GPOs befinden (siehe Abbildung 20.25). Sie können auch über die Schaltfläche DURCHSUCHEN nach einem Ordner suchen. Klicken Sie dann auf WEITER.

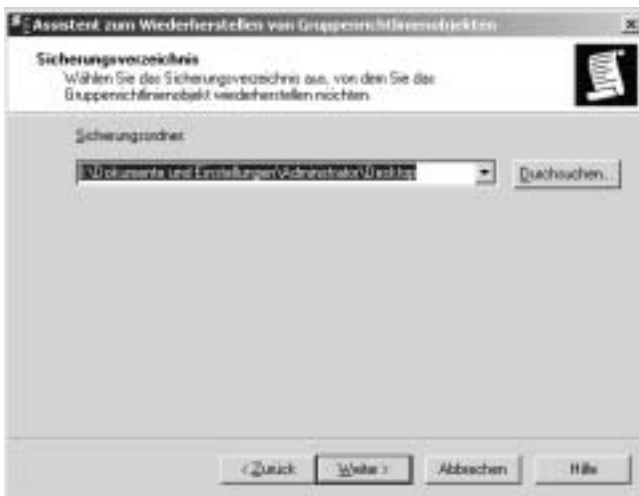


Abbildung 20.25: Auswählen des Sicherungsverzeichnisses zum Wiederherstellen des GPO

3. Nachdem Sie einen Sicherungsordner ausgewählt haben, werden nun alle Sicherungen des GPO angezeigt, die sich in diesem Ordner befinden (siehe Abbildung 20.26). Zur besseren Orientierung wird für jede Sicherung der Zeitstempel sowie die optionale Beschreibung angezeigt. Über die Schaltfläche EINSTELLUNGEN ANZEIGEN können Sie die Details des GPO betrachten. Markieren Sie dann die gewünschte Sicherung und klicken auf WEITER.

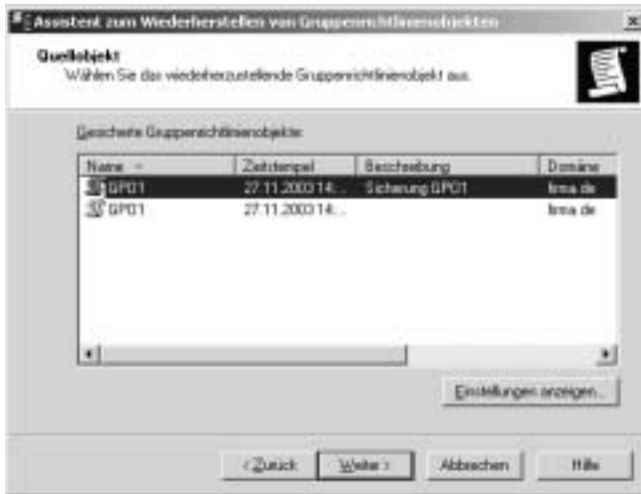


Abbildung 20.26: Auswahl des wiederherzustellenden GPO

4. Sie erhalten eine Zusammenfassung über die gewählten Schritte. Klicken Sie hier auf FERTIG STELLEN. Damit wird das gesicherte GPO mit seinen Einstellungen wiederhergestellt und überschreibt die aktuellen Werte des GPO. Die Versionsnummer des GPO wird dabei um einen Wert erhöht. Dies ist erforderlich, damit die Clients, auf die das GPO angewendet wird, das wiederhergestellte GPO übernehmen.
5. Um ein GPO wiederherstellen zu können, müssen Sie über Berechtigungen verfügen, die ein Löschen, Ändern der Sicherheitseinstellungen sowie Bearbeiten der Einstellungen zulassen. Zudem müssen Sie über Lesezugriff auf das Quellverzeichnis des gesicherten GPOs verfügen. Es ist jedoch nicht die Berechtigung zum Erstellen von GPOs erforderlich.

Wiederherstellen bereits gelöschter GPOs

Um ein versehentlich gelöscht GPO wiederherzustellen, öffnen Sie das Fenster SICHERUNGEN VERWALTEN (siehe Abbildung 20.24). Markieren Sie dort den gewünschten Eintrag und klicken auf die Schaltfläche WIEDERHERSTELLEN. Wenn Sie ein bereits gelöscht GPO wiederherstellen, wird die Versionsnummer des gesicherten GPOs beibehalten. Das wiederhergestellte GPO trägt also dieselbe Versionsnummer wie das gesicherte GPO. Um ein gelöscht GPO wiederherstellen zu können, müssen Sie über die Berechtigung verfügen, GPOs in der Domäne erstellen zu dürfen. Die Person, die das GPO wiederherstellt, wird zudem zum neuen Ersteller-Besitzer des GPO.

Skriptgesteuerte Wiederherstellung von GPOs

Um ein GPO skriptgesteuert wiederherzustellen, können Sie entweder ein eigenes Skript schreiben oder auf die vordefinierten Skripte im Verzeichnis GPMC\SCRIPTS zugreifen. Verwenden Sie das Skript *RestoreGPO.wsf*, um ein einzelnes GPO wiederherzustellen, und das Skript *RestoreAllGPOs.wsf*, um sämtliche GPOs wiederherzustellen.

Wiederherstellen von GPOs mit Einstellungen zur Softwareinstallation

Beim Wiederherstellen von GPOs ist besondere Beachtung den GPOs zu schenken, die Einstellungen zur Softwareinstallation (siehe Kapitel 20.5) enthalten. Dies gilt, wenn ein solches GPO gelöscht wurde und wieder hergestellt werden soll. Dabei können zwei verschiedene Probleme auftreten.

1. Sofern GPO-übergreifende Beziehungen bestehen, die eine Applikation in dem wiederhergestellten GPO updaten, werden diese nach der Wiederherstellung nicht beibehalten. Die Applikation des wiederhergestellten GPOs verliert also ihr Update. In diesen GPO-übergreifenden Beziehungen ist festgelegt, dass eine Applikation eine andere updaten soll, wobei die beiden Applikationen nicht über dasselbe GPO verteilt werden. Die Beziehungen bleiben jedoch bestehen, wenn die Applikationen im wiederhergestellten GPO ihrerseits Applikationen anderer GPOs updaten soll.
2. Sofern der Client-Computer noch nicht darüber informiert ist, dass ein GPO gelöscht wurde – dies ist der Fall, wenn seit dem Löschen noch kein Neustart des Computers oder keine neue Anmeldung des Benutzers erfolgt ist – und an ihn Applikationen verteilt wurden, die die Option ANWENDUNGEN DEINSTALLIEREN, WENN SIE AUSSERHALB DES VERWALTUNGSBEREICHS LIEGEN besitzen, so werden veröffentlichte Applikationen (siehe Kapitel 20.5.4), die bereits installiert sind, beim nächsten Einloggen gelöscht, und zugewiesene Applikationen werden vor einer Neuinstallation zunächst deinstalliert.



Normalerweise wird bei der Option ANWENDUNGEN DEINSTALLIEREN, WENN SIE AUSSERHALB DES VERWALTUNGSBEREICHS LIEGEN die Anwendung deinstalliert, wenn das betreffende GPO nicht mehr auf den Computer oder Benutzer angewendet wird.

Dieses ungewünschte Verhalten liegt darin begründet, dass bei der Wiederherstellung dem Active Directory-Objekt, das die entsprechende Applikation repräsentiert, eine neue GUID zugewiesen wird. Da sich die GUID der bereits vorhandenen Applikation von der neu zugewiesenen GUID unterscheidet, wird die Applikation von Windows als zwei verschiedene Applikationen angesehen. Eine Lösung dieses Problems kann nur darin bestehen, bei der Wiederherstellung des GPOs die ursprüngliche GUID der Applikation zu benutzen. Da jedoch die GUIDs vom Active Directory vergeben werden, kommt hier ein neues Feature des Windows Server 2003 zum Tragen. Hierbei handelt es sich um die sog. Tombstone-Reanimierung (Tombstone re-animation). Tombstones sind Objekte im Active Directory, die zwar gelöscht sind, aber noch nicht endgültig aus dem Verzeichnis entfernt worden sind. Standardmäßig werden alle gelöschten Objekte erst nach 60 Tagen endgültig entfernt. Weitere Hinweise zum Thema Tombstoning finden Sie in Kapitel 21.4.

Die Tombstone-Reanimierung wird beim Wiederherstellen von GPOs automatisch von der GPMC ausgeführt. Diese Reanimierung kann erfolgreich durchgeführt werden, wenn die folgenden drei Punkte erfüllt sind:

- ▶ Die GPMC arbeitet mit einem Domänencontroller, auf dem Windows Server 2003 ausgeführt wird.
- ▶ Der Zeitraum zwischen dem Löschen und Wiederherstellen des GPO darf nicht das definierte Tombstone-Intervall überschreiten. Standardmäßig liegt dieser Zeitraum bei 60 Tagen.
- ▶ Der Benutzer, der die Wiederherstellung durchführt, muss über die Berechtigung zur Tombstone-Reanimierung verfügen. Standardmäßig besitzen nur die Domänen- und Organisationsadministratoren diese Berechtigung. Sie kann jedoch über den ACL-Editor (siehe Abbildung 19.1) jeder anderen Person zugewiesen werden.

Schlägt die Tombstone-Reanimierung fehl, wird der Applikation eine neue GUID zugewiesen und sie somit als neue Applikation identifiziert, sodass die oben beschriebenen Probleme auftreten.

20.3.5 Kopieren von GPOs

Ob GPOs zwischen zwei Domänen kopiert werden sollen oder ein Import des GPOs von einer Domäne in die andere durchgeführt werden soll, ist davon abhängig, ob zwischen den Domänen eine Vertrauensstellung besteht oder nicht. Ist dies der Fall, können die GPOs kopiert werden, andernfalls ist ein Import durchzuführen (siehe Kapitel 20.3.6). Man spricht im zweiten Fall auch von Migration der GPOs.

Über die GPMC ist es möglich, GPOs zwischen Domänen und sogar Gesamtstrukturen auszutauschen. Im letzten Fall müssen jedoch alle Domänencontroller der Gesamtstrukturen unter Windows Server 2003 im Gesamtstrukturmodus 2003 ausgeführt werden. Ist dies nicht der Fall, besteht die Möglichkeit, GPOs aus einer Domäne zu exportieren und in eine Domäne derselben oder einer anderen Gesamtstruktur zu importieren. So können beispielsweise GPOs, die in einer Testdomäne erstellt, getestet und validiert worden sind, in die produktive Umgebung übernommen werden. Allerdings sollten GPOs immer nur innerhalb einer lokalen Domäne benutzt werden, da das Abarbeiten von GPO-Verknüpfungen über Domänengrenzen hinweg kompliziert ist und zusätzlich die Anmeldedauer eines Benutzers erhöht werden kann. In diesem Fall sollten Sie besser lediglich sämtliche Einstellungen eines GPO in ein anderes importieren, sodass keine Verknüpfung zwischen den beiden Objekten besteht.

Beim Kopieren eines GPO werden dessen sämtliche Einstellungen in ein neues GPO am Zielort geschrieben. Dieser Zielort kann sich entweder in derselben Domäne, in einer anderen Domäne derselben Gesamtstruktur oder sogar in einer anderen Domäne einer anderen Gesamtstruktur befinden. Zwischen der Quell- und der Zieldomäne muss lediglich eine Vertrauensstellung bestehen. Zudem müssen Sie in der Zieldomäne über die Berechtigung verfügen, GPOs erstellen zu dürfen; für die Quelldomäne muss Lesezugriff bestehen. Besteht keine Vertrauensstellung, müssen Sie das Programm *Gespeicherte Benutzernamen und Kennwörter* benutzen.

Das Programm *Gespeicherte Benutzernamen und Kennwörter*

Wollen Sie das GPO in eine Domäne kopieren, zu der keine Vertrauensstellung besteht, so müssen Sie die Anmeldeinformationen für diese Domäne mithilfe des Programms *Gespeicherte Benutzernamen und Kennwörter* hinzufügen. Dieses Programm finden Sie auf einem Windows Server 2003 unter SYSTEMSTEUERUNG/GESPEICHERTE BENUTZER-NAMEN UND KENNWÖRTER.

Um dort die Domäne hinzuzufügen, klicken Sie auf HINZUFÜGEN und geben den Namen der Domäne sowie ein gültiges Benutzerkonto an.

Öffnen Sie dann die GPMC-mmc und deaktivieren unter den Optionen auf der Registerkarte ALLGEMEIN die Möglichkeit, Vertrauensstellungen automatisch zu erkennen.

Fügen Sie dann die Gesamtstruktur hinzu (Kontextmenüeintrag GESAMTSTRUKTUR HINZUFÜGEN des Knotens GRUPPENRICHTLINIENVERWALTUNG).

Um ein GPO zu kopieren, wählen Sie aus dem Kontextmenü den Eintrag KOPIEREN. Markieren Sie dann die Zieldomäne und wählen aus deren Kontextmenü den Eintrag EINFÜGEN. Sie werden dann gefragt, ob Sie das GPO mit der Domäne verknüpfen möchten. Sobald Sie die Meldung bestätigt haben, ist das GPO an die neue Lokation kopiert. Die neue Verknüpfung wird auf der Registerkarte BEREICH des GPOs angezeigt.

Sie können das GPO auch kopieren, indem Sie das Objekt per Drag&Drop an die neue Zieldomäne verschieben. Auch ein skriptgesteuerter Kopiervorgang ist möglich. Hierzu finden Sie im Ordner GPMC\SCRIPTS das Skript CopyGPO.wsf.

Je nachdem, ob Sie ein GPO innerhalb derselben Domäne oder zwischen zwei verschiedenen Domänen kopieren, gibt es einige Unterschiede. Beim Kopieren eines GPO innerhalb derselben Domäne bleiben die Verknüpfungen mit WMI-Filtern sowie IPsec-Richtlinien bestehen. Wird das GPO in eine andere Domäne kopiert, werden die Verknüpfungen mit dem WMI-Filter gelöscht, da diese Filter nur mit GPOs innerhalb der eigenen Domäne verknüpft werden können. Auch die Verknüpfungen mit IPsec-Richtlinien werden beim Kopieren in eine andere Domäne nicht beibehalten, weil nicht sichergestellt werden kann, dass sich eine übereinstimmende Richtlinie in der Zieldomäne befindet. Auch das Festlegen der Zugriffsberechtigungen gestaltet sich in beiden Fällen unterschiedlich. Befinden sich Quelle und Ziel innerhalb derselben Domäne, werden die Berechtigungen beibehalten. Andernfalls wird ein Assistent gestartet, mit dem die Einstellungen vorgenommen werden können. Zudem können auch Migrationstabellen (siehe Kapitel 20.3.7) spezifiziert werden.

20.3.6 Import und Export von GPOs

Der Importvorgang von GPOs wird auch als Migration bezeichnet. Beim Migrieren von GPOs sind verschiedene Dinge zu bedenken, da die Daten sehr komplex sind, an verschiedenen Stellen gespeichert werden und einige dieser Daten domänenspezifisch sind. Damit diese domänenspezifischen Daten ebenfalls korrekt migriert werden können, verwendet die GPMC Migrationstabellen (siehe Kapitel 20.3.7). In diesen Tabellen können die domänenbezogenen Daten mit den neuen Werten für das GPO eingetragen werden.

Bei dem Import werden die Einstellungen eines GPO in ein vorhandenes GPO transferiert. Als Quelle dient die Sicherung des GPOs. Wie beim Kopieren kann sich das Ziel-GPO entweder in derselben Domäne, in einer anderen Domäne derselben Gesamtstruktur oder sogar in einer anderen Domäne einer anderen Gesamtstruktur befinden. Allerdings muss in diesem Fall keine Vertrauensstellung zwischen den Domänen bestehen. Es muss lediglich von der Zieldomäne aus Zugriff auf den Speicherort der GPOs in der Quelldomäne bestehen. Das Ziel-GPO, in das die Einstellungen transferiert werden, behält seine Sicherheitseinstellungen sowie Verknüpfungen mit seinen WMI-Filtern.

Um ein GPO zu importieren, führen Sie die folgenden Schritte durch:

1. Wählen Sie aus dem Kontextmenü des GPO den Eintrag **EINSTELLUNGEN IMPORTIEREN**. Damit wird ein Assistent gestartet.
2. Da die aktuellen Einstellungen des GPO beim Import überschrieben werden, können Sie diese sichern (siehe Abbildung 20.27). Wollen Sie eine Sicherung durchführen, klicken Sie auf die Schaltfläche **SICHERN**. Sie können dann einen Speicherort angeben. Klicken Sie danach auf **WEITER**.



Abbildung 20.27: Sichern der GPO-Einstellungen vor einem Import

3. Als Nächstes wählen Sie den Sicherungsordner (siehe Abbildung 20.25) aus, in dem sich das zu importierende GPO befindet. Sind dort mehrere GPOs vorhanden, so wählen Sie das gewünschte aus (siehe Abbildung 20.26). Klicken Sie dann auf **WEITER**.
4. Nun wird die ausgewählte Sicherung überprüft, ob sich in dieser UNC-Pfade oder Sicherheitsprincipals befinden, die übertragen werden müssen (siehe Abbildung 20.28). Ist dies der Fall, kommen die Migrationstabellen zum Zuge. Andernfalls klicken Sie auf **WEITER**. Sie erhalten eine Zusammenfassung. Klicken Sie hier auf **FERTIG STELLEN**.

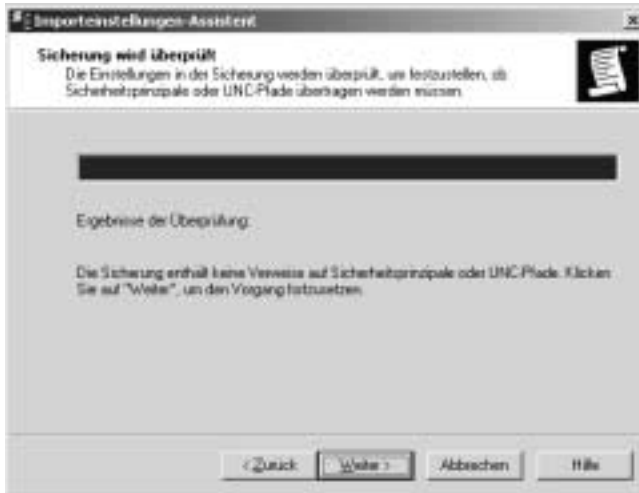


Abbildung 20.28: Überprüfen der GPO-Sicherung auf Sicherheitsprincipals und UNC-Pfade

Auch ein skriptgesteuerter Import ist möglich. Hierzu finden Sie im Ordner GPMC\SCRIPTS das Skript ImportGPO.wsf, um ein GPO zu importieren, sowie das Skript ImportAllGPOs.wsf, um sämtliche GPOs zu importieren.

20.3.7 Migrationstabellen

Migrationstabellen werden beim Kopieren und Importieren von GPOs zwischen zwei verschiedenen Domänen benutzt. In diesen Tabellen sind die domänenspezifischen Daten der GPOs eingetragen. Zu verschiedenen Datentypen wie z.B. UNC-Pfaden oder globalen Gruppen ist jeweils der Wert der Quelle und des Ziels eingetragen. Mit Hilfe dieser Tabellen können die Werte des Quell-GPOs während des Kopier- oder Importvorgangs so konvertiert werden, dass sie für das Ziel-GPO nutzbar sind. Der Aufbau einer Migrationstabelle sieht folgendermaßen aus:

Datentyp	Wert der Quelle	Wert des Ziels
UNC-Pfad	\\Server1\Freigabe1	\\Server2\Freigabe2
Globale Gruppe	Domäne1\Gruppe1	Domäne2\Gruppe2

Tabelle 20.5: Aufbau einer Migrationstabelle

Angenommen, Sie möchten ein GPO von Domäne1 nach Domäne2 migrieren. In Domäne1 befindet sich die Sicherheitsgruppe Gruppe1. In Domäne2 gibt es hingegen nur die Gruppe2. Für diese Gruppe sind jedoch identische Sicherheitseinstellungen konfiguriert, sodass auch Gruppe2 das GPO benutzen soll. Wird für den Kopiervorgang keine Migrationstabelle verwendet, so beziehen sich die Sicherheitseinstellungen in Domäne2 auf Gruppe1, obwohl diese Gruppe in der Domäne nicht vorhanden ist. Die Sicherheitseinstellungen können also für Gruppe2 nicht greifen. Dieses Problem lässt sich auch dann nicht lösen, wenn in Domäne2 ebenfalls eine Gruppe1 vorhanden wäre. Der Grund dafür

liegt darin, dass neben dem Namen der Gruppe auch deren eindeutige SID gespeichert wird – und die SIDs für eine Gruppe 1 in Domäne1 und Domäne2 können nicht identisch sein. Bei lokalen Domänengruppen besitzt die Gruppe ohnehin nur Gültigkeit in der Quelldomäne und in keiner externen Domäne. Für Verweise auf die folgenden Bereiche von Sicherheitseinstellungen können die Migrationstabellen angepasst werden:

- ▶ Zuweisen von Benutzerrechten
- ▶ Eingeschränkte Gruppen
- ▶ Systemdienste
- ▶ Dateisystem
- ▶ Registry

Auch im GPO vorhandene UNC-Pfade bereiten Probleme, wenn die Werte nicht in einer Migrationstabelle angepasst werden. Dies gilt, wenn UNC-Pfade – z.B. Pfade zu den persönlichen Ordnern von Benutzern – nur in Domäne1 verfügbar sind, da sich Domäne2 in einem anderen Netzwerksegment befindet. Diese umgeleiteten Ordner sind für die Benutzer in der Domäne2 nicht mehr erreichbar. UNC-Pfade können für die folgenden Bereiche über die Migrationstabellen angepasst werden:

- ▶ Einstellungen für die Ordnerumleitung (siehe Kapitel 20.4.1)
- ▶ Einstellungen für die Softwareinstallation, z.B. Softwareverteilungspunkte (siehe Kapitel 20.5)
- ▶ Verweise auf Skripte (z.B. An- und Abmeldeskripte), die außerhalb des GPO gespeichert sind. Die Skripte selbst werden nur dann zusammen mit dem GPO kopiert, wenn sie innerhalb des Quell-GPO gespeichert sind.

Mit dem Einsatz von Migrationstabellen werden die eben beschriebenen Probleme bereits während des Import- oder Kopiervorgangs behoben. Es wird automatisch im GPO nach Einstellungen gesucht, die z.B. den Wert \\Domäne1\Freigabe1 oder Domäne1\Gruppe1 enthalten. Diese Werte werden automatisch durch die Einträge \\Domäne2\Freigabe2 oder Domäne2\Gruppe2 ersetzt. Somit ist die Funktionsfähigkeit des GPO in der Zieldomäne gewährleistet.

Anwenden von Migrationstabellen

Sobald beim Kopieren oder Importieren (siehe Abbildung 20.28) eines GPO festgestellt wird, dass sich in diesem Verweise auf UNC-Pfade oder Bereiche der genannten Sicherheitseinstellungen befinden, wird eine Migrationstabelle verwendet. Für deren Einsatz gibt es drei verschiedene Optionen:

1. KEINE MIGRATIONSTABELLE VERWENDEN: In diesem Fall werden sämtliche Verweise – so wie sie sind – in das Ziel-GPO kopiert. In diesem Fall kann eine Funktionsfähigkeit des GPO in der Zieldomäne nicht gewährleistet werden.
2. EINE MIGRATIONSTABELLE VERWENDEN: Mit dieser Option werden alle Verweise des Quell-GPO auf die Werte umgesetzt, die für das Ziel-GPO in der Migrationstabelle festgelegt sind. Sind für einige Einträge keine Werte für die Zieldomäne angegeben, so werden die Werte des Quell-GPO übernommen.

3. EINE MIGRATIONSTABELLE EXKLUSIV VERWENDEN: Um diese Option nutzen zu können, müssen für alle Verweise des Quell-GPO Werte für das Ziel-GPO in der Migrationstabelle eingetragen sein. Ist dies nicht der Fall, wird der Kopier- bzw. Importvorgang nicht fortgesetzt. Mit dieser Option können Sie also immer sicherstellen, dass für alle Verweise der Wert umgesetzt wird.

Aufbau der Migrationstabellen

Bei den Migrationstabellen handelt es sich um XML-Dateien. Sie tragen die Dateierweiterung *.migtable*. In der GPMC ist der Migrationstabellen-Editor integriert. Die Anpassungen müssen also nicht in der XML-Datei vorgenommen werden. Um den Migrationstabellen-Editor zu öffnen, verwenden Sie eine der folgenden Möglichkeiten:

- ▶ Wählen Sie aus dem Kontextmenü des Containers GRUPPENRICHTLINIENOBJEKTE den Eintrag MIGRATIONSTABELLEN-EDITOR ÖFFNEN.
- ▶ Wählen Sie aus dem Kontextmenü des Containers DOMÄNEN den Eintrag MIGRATIONSTABELLEN-EDITOR ÖFFNEN.
- ▶ STARTEN SIE DAS PROGRAMM *mtedit.exe* IM GPMC-INSTALLATIONSVERZEICHNIS.
- ▶ Doppelklicken Sie eine bestehende *.migtable*-Datei.

Im Verzeichnis GPMC\Script befindet sich eine Beispieldatei einer Migrationstabelle. Öffnen Sie die Datei *SampleMigrationTable.migtable* mit dem Migrationstabellen-Editor (siehe Abbildung 20.29) oder einem Texteditor wie Notepad, um den XML-Code zu betrachten (siehe Abbildung 20.1).



Quelle	Quelltyp	Ziel
Group1@testdomain1.com	Universelle Gruppe	<Identisch mit Quelle>
testdomain3\Group3	Lokale Gruppe (in D=)	Group4@testdomain4.com
testdomain1\Group02	Globale Gruppe (in D=)	<Zuordnung mit relativem Namen>
testdomain1.com\Group1	Globale Gruppe (in D=)	testdomain2.com\Group2
testdomain3.com\Computer35	Computer	testdomain4.com\Computer45
Group5@testdomain5.com	Universelle Gruppe	Group6@testdomain6.com
Group01@testdomain1.com	Globale Gruppe (in D=)	<Kein>
testdomain1\User1	Benutzer	testdomain2\User2
S-1-5-11-111111111-111111111-111111111-11	Freier Text oder SID	testdomain1\Group02
Group05	Freier Text oder SID	Group06
EVERYONE	Freier Text oder SID	<Kein>
User5@testdomain5.com	Benutzer	User6@testdomain6.com
Computer51@testdomain5.com	Computer	Computer15@testdomain6.com
testdomain1\Computer15	Computer	testdomain2\Computer25
S-1-5-11-111111111-111111111-111111111-11	Freier Text oder SID	<Identisch mit Quelle>
testdomain3.com\User3	Benutzer	testdomain4.com\User4
V\domain01\share1\Script1.bat	UNC Pfad	V\domain02\share2\Script2.bat
V\domain01.test.com\share1\olde\redirect1	UNC Pfad	V\domain02.test.com\share2\olde\redirect2
V\domain01\deploy0	UNC Pfad	V\domain02\deploy2

Abbildung 20.29: Der Aufbau einer Migrationstabelle

Das folgende Listing zeigt den XML-Code einer Migrationstabelle. Als Beispiel wurde der Code für die Tabelle 20.5 verwendet.

```
<?xml version="1.0" encoding="utf-16"?>
<MigrationTable xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns=
"http://www.microsoft.com/GroupPolicy/GPOOperations/MigrationTable">
  <Mapping>
    <Type>GlobalGroup</Type>
    <Source>Domäne1\Gruppe1</Source>
    <Destination>Domäne2\Gruppe2</Destination>
  </Mapping>
  <Mapping>
    <Type>UNCPath</Type>
    <Source>\\Server1\Freigabe1</Source>
    <Destination>\\Server2\Freigabe2</Destination>
  </Mapping>
</MigrationTable>
```

Listing 20.1: XML-Code einer Migrationstabelle

In jeder Migrationstabelle befindet sich mindestens ein Eintrag. Für jeden dieser Einträge sind drei Angaben in den jeweiligen Spalten vorhanden: Quelle, Quelltyp und Ziel (siehe Abbildung 20.29).

Die Spalte QUELLE gibt den Namen der Quelle an, z.B. einen Gruppennamen oder UNC-Pfad, auf den im Quell-GPO verwiesen wird. Der Namenstyp, z.B. Benutzername, muss im Quell-GPO und mit dem in der Migrationstabelle angegebenen Ziel-GPO identisch sein. Die Namen können in einem der folgenden Formate angegeben werden:

- ▶ User Principal Name (UPN), z.B. user1@domäne.de
- ▶ DNS-Name, z.B. domäne.de\user1
- ▶ SAM, z.B. Domäne\user1
- ▶ Freier Text, z.B. user1. Unter QUELLTYP muss FREIER TEXT ODER SID eingetragen werden.
- ▶ SID, z.B. S-1-11-11111111-11111111-11111111-1112. Unter QUELLTYP muss FREIER TEXT ODER SID eingetragen werden.

Der QUELLTYP bezeichnet die domänenspezifische Information des Quell-GPOs. In die Migrationstabelle können die folgenden Quelltypen eingetragen werden:

- ▶ Benutzer
- ▶ Computer
- ▶ Lokale Domänengruppe
- ▶ Globale Domänengruppe
- ▶ Universelle Gruppe
- ▶ UNC-Pfad
- ▶ Freier Text oder SID (Diese Kategorie wird nur für Sicherheitsprincipals benutzt, die als pure SID oder Text vorliegen.)

In der Spalte ZIEL wird angegeben, wie der Name des Benutzers, der Gruppe, der UNC-Pfad usw. bei der Transferierung in das Ziel-GPO behandelt werden soll. Hierzu stehen vier Optionen zur Verfügung:

- ▶ Der Zielname entspricht dem Quellnamen: In diesem Fall wird im Ziel-GPO derselbe Verweis wie im Quell-GPO verwendet. Denselben Effekt erreichen Sie, wenn Sie gar keinen Wert angeben.
- ▶ <KEINS>: Hiermit wird der Benutzer, Computer oder die Gruppe aus dem GPO gelöscht. Diese Option kann jedoch nicht für UNC-Pfade benutzt werden.
- ▶ <ZUORDNUNG MIT RELATIVEM NAMEN>: Hierdurch wird z.B. aus dem Verweis Domäne1\Gruppe1 automatisch der Verweis Domäne2\Gruppe1. Anstelle der Domäne des Quell-GPO wird der Domänenname des Ziel-GPO gesetzt. Der Name des Benutzers, der Gruppe oder des Computers bleibt erhalten. Diese Option kann jedoch nicht für UNC-Pfade benutzt werden.
- ▶ Der Zielname wird explizit angegeben: In diesem Fall wird der Name des Quell-GPO durch den angegebenen Namen im Ziel-GPO ersetzt.

Erstellen einer Migrationstabelle

Für die Erstellung einer Migrationstabelle bietet Ihnen der Editor die Möglichkeit, die Tabelle automatisch mit den Werten eines GPO oder einer GPO-Sicherung auszufüllen.

1. Öffnen Sie zunächst eine leere Migrationstabelle, indem Sie aus dem Kontextmenü des Containers DOMÄNE oder GRUPPENRICHTLINIENOBJEKTE den Eintrag MIGRATIONSTABELLEN-EDITOR ÖFFNEN wählen.
2. Sie erhalten eine leere Tabelle mit den drei beschriebenen Spalten Quelle, Quelltyp und Ziel. Wählen Sie aus dem Menü EXTRAS den Eintrag VON GRUPPENRICHTLINIENOBJEKT AUFFÜLLEN oder VON SICHERUNG AUFFÜLLEN.
3. Wählen Sie dann das GPO oder die Sicherung des GPO aus, deren Verweise auf Sicherheitsprincipals und UNC-Pfade automatisch in die Tabelle in die Spalte QUELLE und QUELLTYP geschrieben werden sollen.
4. Für die Spalte ZIEL können Sie nun die gewünschten Einträge vornehmen.
5. Nachdem Sie eine Migrationstabelle bearbeitet haben, sollten Sie die eingetragenen Werte überprüfen. Öffnen Sie dazu im Migrationstabellen-Editor das Menü EXTRAS/TABELLE VALIDIEREN. Das Fenster VALIDIERUNGSERGEBNISSE (siehe Abbildung 20.30) gibt Ihnen eine Zusammenfassung. Unter den Details sehen Sie Hinweise und Warnungen, bei welchen Tabelleneinträgen Probleme bei der Validierung aufgetreten sind.

Eine Migrationstabelle kann auch skriptgesteuert erstellt werden. Verwenden Sie hierzu das Skript *CreateMigrationTable.wsf*. Dabei wird die automatische Auffüllfunktion des Migrationstabellen-Editors benutzt. Die Werte für die neuen Pfade müssen danach manuell eingetragen werden.

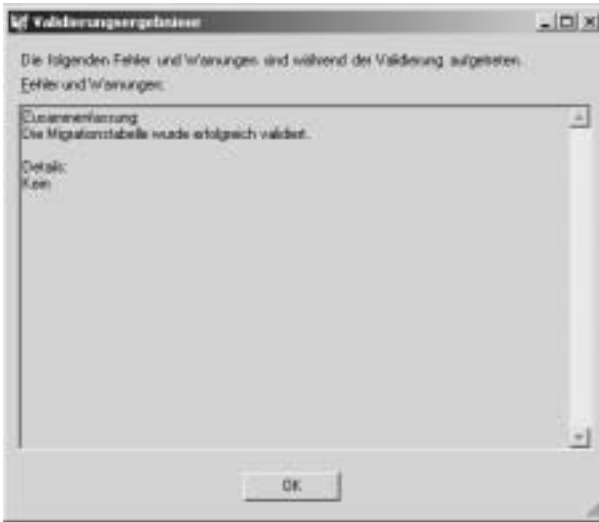


Abbildung 20.30: Validierung einer Migrationstabelle

20.3.8 Erstellen von HTML-Berichten

Um einen HTML-Bericht für ein GPO zu erstellen, wählen Sie zunächst aus der OU oder der Domäne das gewünschte GPO. Im Detailbereich klicken Sie nun auf die Registerkarte EINSTELLUNGEN (siehe Abbildung 20.21).

Aus dem Kontextmenü des Einstellungsberichts wählen Sie nun DRUCKEN oder BERICHT SPEICHERN. Berichte werden im HTML-Format gespeichert und können im Internet Explorer angezeigt werden. Hierzu ist entweder der Internet Explorer in der Version 6 oder der Netscape Navigator in der Version 7 erforderlich. Über EIN- / AUSBLENDEN können Sie auswählen, welche Informationen über die GPO der Bericht enthalten soll. Ist im Internet Explorer eine erhöhte Sicherheitskonfiguration aktiviert, so müssen Sie beim Anzeigen der Berichte jeweils eine Bestätigung ausführen, da ein Skript ausgeführt wird. Um diese Bestätigung zu umgehen, fügen Sie zur Liste vertrauenswürdiger Sites im Internet Explorer den Eintrag `about:security_mmc.exe` hinzu.

20.3.9 Gruppenrichtlinienmodellierung und -ergebnisse

Über die Gruppenrichtlinienmodellierung der GPMC können Sie wie bereits bei Windows XP-Clients (über RSoP, siehe Kapitel 20.1.10) die Verteilung von Gruppenrichtlinien simulieren und die Ergebnisse der Gruppenrichtlinieneinstellungen ausgeben lassen. Um dieses Feature nutzen zu können, muss mindestens ein Domänencontroller in der Gesamtstruktur unter Windows Server 2003 ausgeführt werden. Andernfalls ist in der GPMC der Knoten GRUPPENRICHTLINIENMODELLIERUNG nicht verfügbar.

Um die Verteilung einer Gruppenrichtlinie und deren Auswirkungen zu simulieren, führen Sie die folgenden Schritte durch:

1. Wählen Sie aus dem Kontextmenü des Knotens GRUPPENRICHTLINIENMODELLIERUNG den Eintrag GRUPPENRICHTLINIENMODELLIERUNGS-ASSISTENT.
2. Nach der Willkommensmeldung wählen Sie einen Domänencontroller aus, auf dem die Simulation durchgeführt werden soll (siehe Abbildung 20.31). Hierbei muss es sich um einen Domänencontroller handeln, auf dem Windows Server 2003 ausgeführt wird. Sie können einen beliebigen oder einen speziellen Domänencontroller auswählen. Klicken Sie dann auf WEITER.



Abbildung 20.31: Auswahl des Domänencontrollers für die Simulation

3. Als Nächstes wählen Sie, ob die Richtlinien für einen bestimmten Benutzer und / oder Computer simuliert werden sollen oder für einen Container, in dem sich Benutzer-/Computerinformationen befinden (siehe Abbildung 20.32). Markieren Sie die gewünschte Checkbox und wählen dann den Container, den Benutzer oder den Computer aus. Klicken Sie dann auf WEITER.

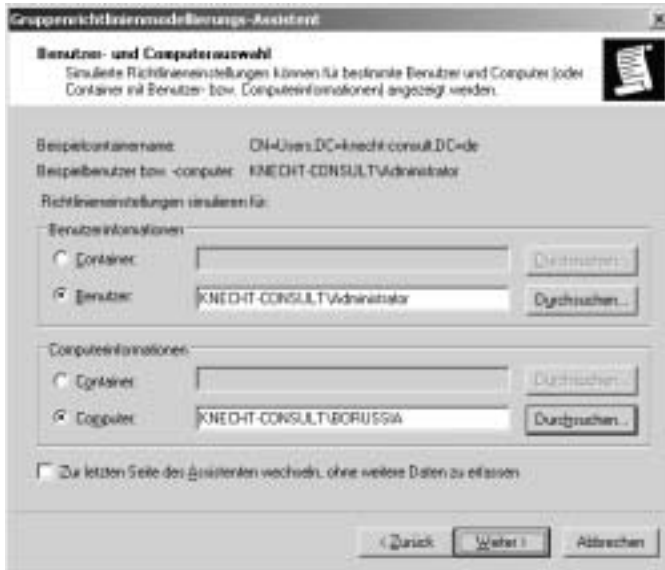


Abbildung 20.32: Auswahl des Benutzers oder Computers, für den die Richtlinie simuliert werden soll

4. Dann können Sie optional zusätzliche Simulationsparameter angeben (siehe Abbildung 20.33). Sie können eine langsame Netzwerkverbindung (DFÜ-Verbindung) simulieren. Auch die Loopback-Verarbeitung mit ihren Optionen ERSETZEN und ZUSAMMENFÜHREN (siehe Kapitel 20.1.8) ist wählbar. Weiterhin können Sie einen bestimmten Standort für die Simulation wählen. Klicken Sie dann auf WEITER.

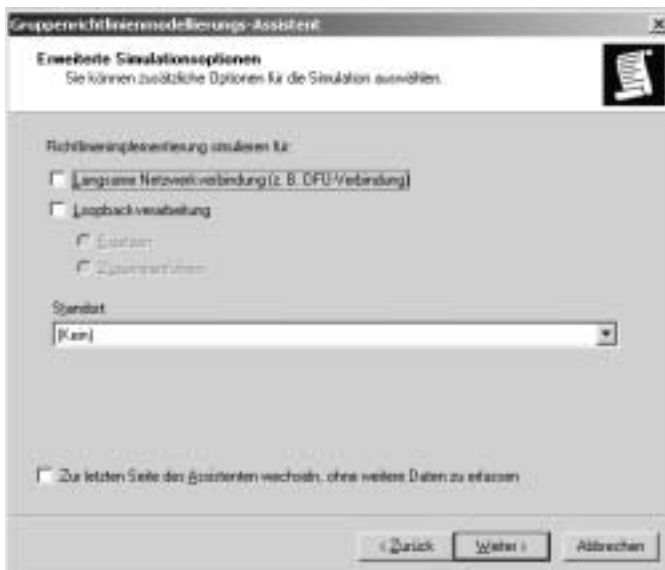


Abbildung 20.33: Angabe optionaler Simulationsparameter

5. Weiterhin können Sie alternative Active Directory-Pfade für den Benutzerstandort sowie den Computerstandort angeben (siehe Abbildung 20.34). Für diese Einstellungen werden die Richtlinien simuliert. Klicken Sie dann auf WEITER.

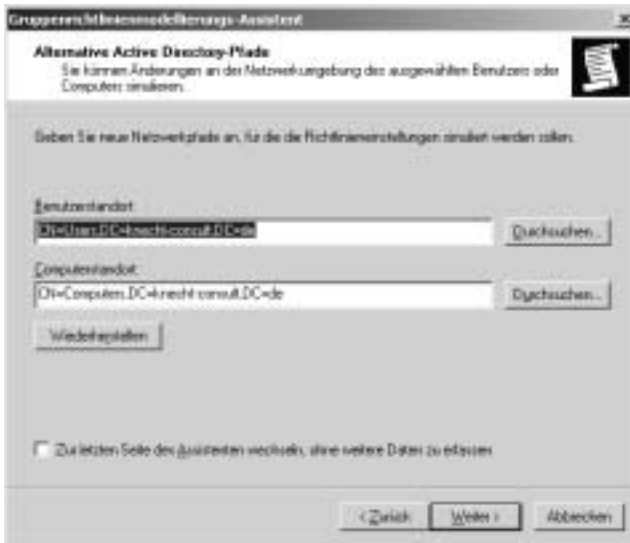


Abbildung 20.34: Auswahl alternativer Benutzer- und Computerstandorte

6. Als Nächstes können Sie die Zugehörigkeit des gewählten Benutzers zu den Sicherheitsgruppen bestimmen (siehe Abbildung 20.35). In der Liste SICHERHEITSGRUPPEN werden die aktuellen Zugehörigkeiten angezeigt. Über die Schaltflächen HINZUFÜGEN und ENTFERNEN können Sie die Mitgliedschaften modifizieren. Klicken Sie dann auf WEITER.

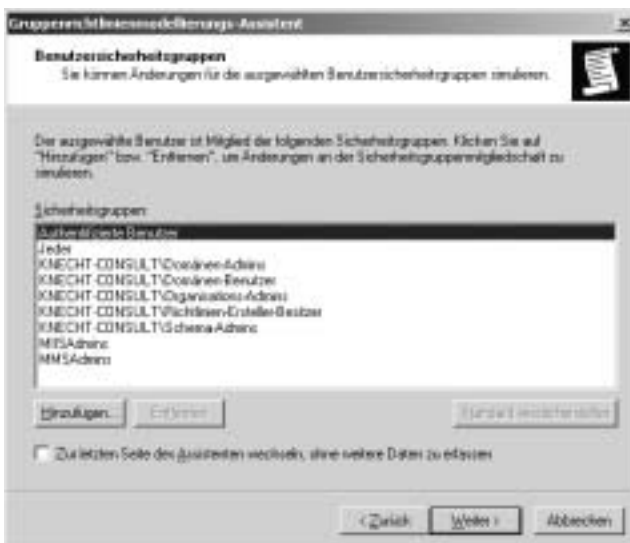


Abbildung 20.35: Die Gruppenmitgliedschaften des Benutzers modifizieren

7. Wie im letzten Fenster für den Benutzer kann auch für den Computer die Gruppenzugehörigkeit bearbeitet werden (siehe Abbildung 20.36). Klicken Sie dann auf WEITER.

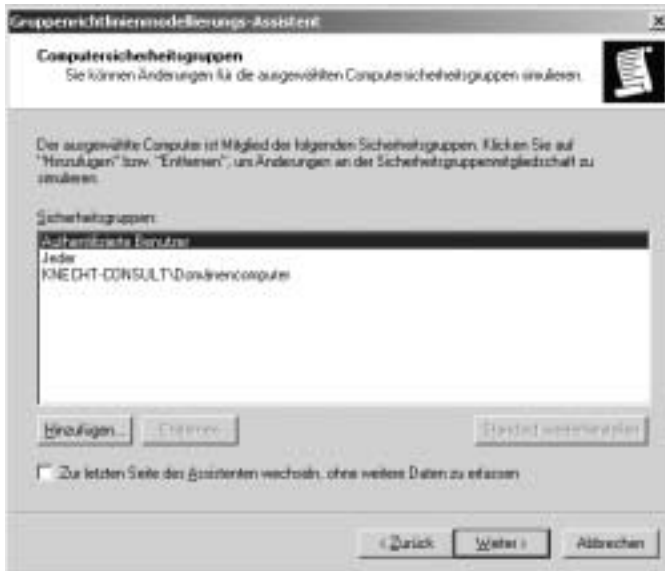


Abbildung 20.36: Die Gruppenmitgliedschaften des Computers modifizieren

8. Weiterhin können Sie WMI-Filter für die Benutzer auswählen, die mit dem GPO verknüpft werden sollen (siehe Abbildung 20.37). Sie haben die Möglichkeit, alle mit dem GPO verknüpften oder nur einzelne WMI-Filter zu wählen. Klicken Sie dann auf WEITER.

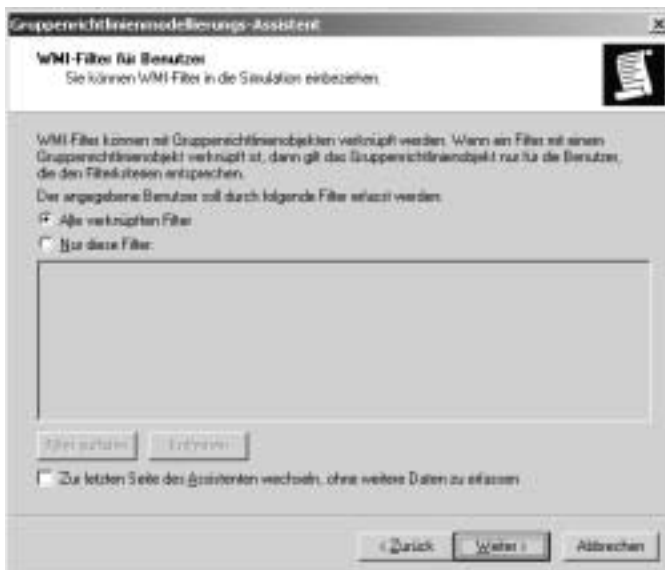


Abbildung 20.37: Auswahl von WMI-Filtern für die Benutzer

9. Auch für die Computer können WMI-Filter ausgewählt werden (siehe Abbildung 20.38). Die Auswahl funktioniert genauso wie im letzten Schritt beschrieben. Klicken Sie dann auf WEITER.

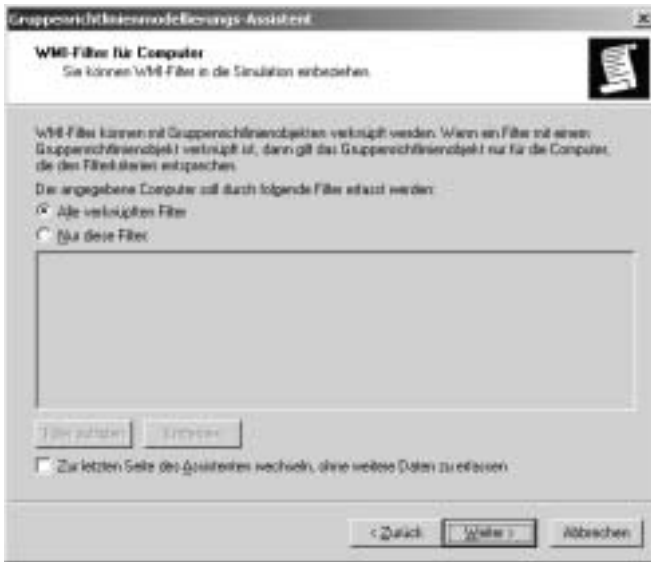


Abbildung 20.38: Auswahl von WMI-Filtern für die Computer

10. Sie erhalten nun eine Zusammenfassung Ihrer Auswahl (siehe Abbildung 20.39). Um die Gruppenrichtlinienmodellierung zu starten, klicken Sie hier auf WEITER und im folgenden Fenster auf FERTIG STELLEN.



Abbildung 20.39: Zusammenfassung des Gruppenrichtlinienmodellierungs-Assistenten

Nachdem Sie den Modellierungs-Assistenten beendet haben, befindet sich unter dem Knoten GRUPPENRICHTLINIENMODELLIERUNG ein neuer Eintrag. Der Knoten selbst zeigt auf der Registerkarte INHALT für alle vorhandenen Objekte Informationen über den verwendeten Domänencontroller, den gewählten Benutzer und Computer sowie das Durchführungsdatum an. Markieren Sie eines der Objekte, erhalten Sie die spezifischen Angaben zu diesem Objekt (siehe Abbildung 20.40). Die Registerkarte ZUSAMMENFASSUNG enthält einen HTML-basierten Bericht für die Benutzer- und Computerkonfiguration über die Gruppenmitgliedschaften, GPOs sowie WMI-Filter. Auf der Registerkarte EINSTELLUNGEN finden Sie einen HTML-Bericht über die simulierten Richtlinieneinstellungen. Die Registerkarte ABFRAGE enthält die Parameter, die Sie für die Generierung der Simulation eingegeben haben.

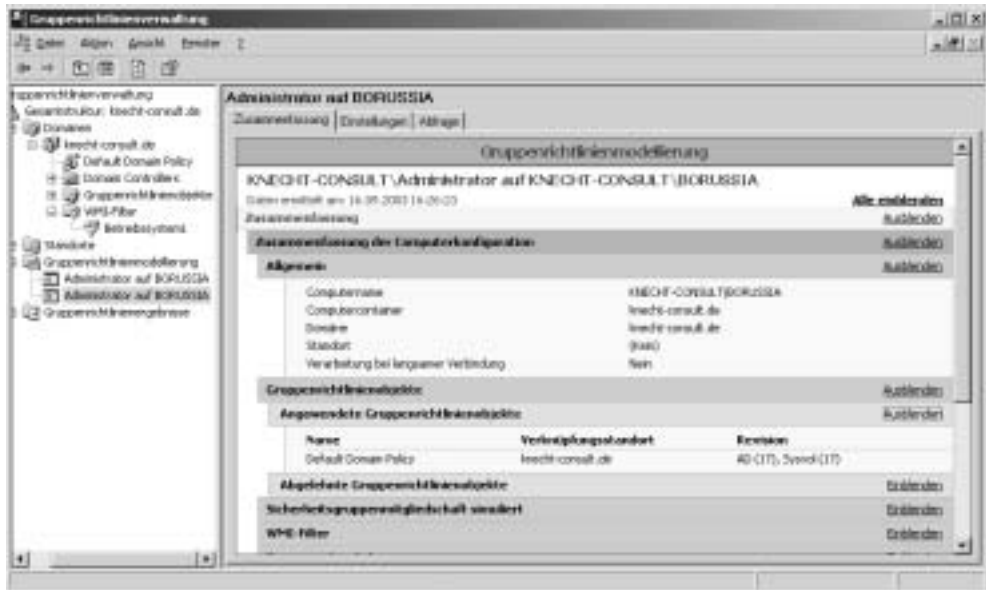


Abbildung 20.40: Die Gruppenrichtlinienmodellierung in der GPMC

Über das Kontextmenü des modellierten Objekts können Sie dieselbe Abfrage erneut ausführen, eine neue Abfrage erstellen, die auf dieser basiert, sowie einen Bericht erstellen.

Wählen Sie aus dem Kontextmenü den Eintrag ERWEITERTE ANSICHT, wird die mmc RICHTLINIENERGEBNISSATZ (RSOP) geöffnet (siehe Abbildung 20.41). In dieser mmc sind dieselben Daten enthalten wie in dem HTML-Bericht.



Abbildung 20.41: Die mmc Richtlinienergebnissatz

Allerdings zeigt der HTML-Bericht nur den aktuellen Wert einer Richtlinie sowie das GPO, das diesen Wert setzt. Sind mehrere GPOs zugewiesen, so wird nur in der mmc RICHTLINIENERGEBNISSATZ die Liste aller GPOs sowie deren Verarbeitungsreihenfolge angezeigt.

Gruppenrichtlinienergebnisse

Die Gruppenrichtlinienergebnisse können nicht nur für Benutzer und Computer angezeigt werden, für die eine Gruppenrichtlinienmodellierung durchgeführt wurde, sondern auch für reale Benutzer und Computer. Es handelt sich hier also um reale Daten, die von einem vorhandenen Computer gesammelt werden. Es erfolgt keine Simulation auf einem Domänencontroller. Der Zielcomputer muss dafür unter Windows XP oder Windows Server 2003 betrieben werden. Von Computern mit dem Betriebssystem Windows 2000 können keine Gruppenrichtlinienergebnisse bezogen werden.

Um Gruppenrichtlinienergebnisse vom Zielcomputer beziehen zu können, muss der Benutzer über lokale Administratorrechte für diesen Computer verfügen. Diese Berechtigung kann an weitere Benutzer delegiert werden. Für die Delegierung von Richtlinienergebnisdaten ist es jedoch erforderlich, dass in der Gesamtstruktur das Windows 2003-Schema vorhanden ist. Benutzen Sie hierfür das Programm *ADPREP* (siehe Kapitel 9.5). Ein Domänencontroller unter Windows Server 2003 ist nicht erforderlich.

Um Gruppenrichtlinienergebnisse anzuzeigen, führen Sie die folgenden Schritte durch:

1. Wählen Sie aus dem Kontextmenü des Knotens GRUPPENRICHTLINIENERGEBNISSE den Eintrag GRUPPENRICHTLINIENERGEBNIS-ASSISTENT.
2. Klicken Sie bei der Willkommensmeldung auf WEITER. Danach wählen Sie den Computer aus, für den die Gruppenrichtlinienergebnisse angezeigt werden sollen (siehe Abbildung 20.42). Sie können den aktuellen Computer oder einen beliebigen anderen auswählen. Wollen Sie für den Computer keine Richtlinienergebnisse anzeigen, so aktivieren Sie die Checkbox KEINE RICHTLINIENEINSTELLUNGEN FÜR DEN AUSGEWÄHLTEN COMPUTER IM ERGEBNIS ANZEIGEN. Klicken Sie dann auf WEITER.

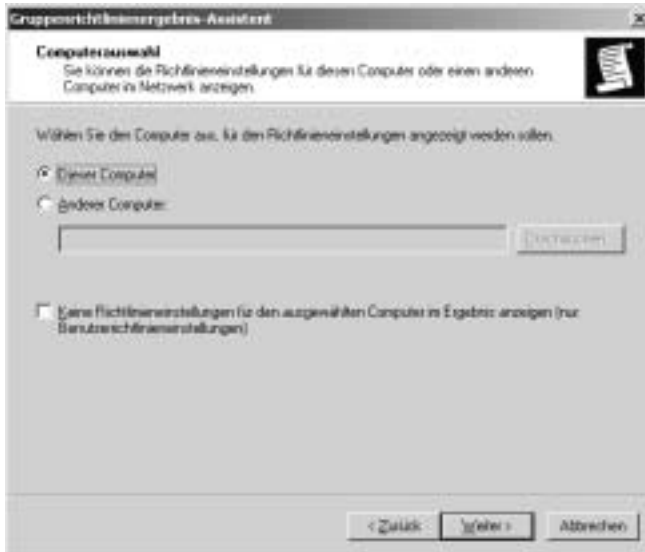


Abbildung 20.42: Auswahl des Computers für die Gruppenrichtlinienergebnisse

3. Wählen Sie nun den Benutzer aus (siehe Abbildung 20.43). Sie können den aktuellen oder einen anderen Benutzer wählen. Wollen Sie für den Benutzer keine Richtlinienergebnisse anzeigen, so aktivieren Sie die Checkbox KEINE BENUTZERRICHTLINIENEINSTELLUNGEN IM ERGEBNIS ANZEIGEN. Klicken Sie dann auf WEITER.



Abbildung 20.43: Auswahl des Benutzers für die Gruppenrichtlinienergebnisse

4. Sie erhalten eine Zusammenfassung Ihrer Einstellungen. Klicken Sie hier auf WEITER und dann auf FERTIG STELLEN.

5. Der neu erstellte Richtlinienresultatsatz ist als neuer Knoten unter Gruppenrichtlinienergebnisse vorhanden. Standardmäßig trägt dieser Ergebnissatz den Namen im Format BENUTZERNAME AUF COMPUTERNAMEN. Er verfügt über die drei Registerkarten ZUSAMMENFASSUNG, EINSTELLUNGEN und RICHTLINIENEREIGNISSE. Die beiden Karten ZUSAMMENFASSUNG und EINSTELLUNGEN enthalten dieselben Informationen wie unter der Gruppenrichtlinienmodellierung. Die Registerkarte RICHTLINIENEREIGNISSE (siehe Abbildung 20.44) enthält alle sicherheitsbezogenen Ereignisse (Informationen, Warnungen und Fehlermeldungen) des Ereignisprotokolls vom Zielcomputer. Hierzu muss der Benutzer über die Berechtigung verfügen, per Remote-Zugriff das Ereignisprotokoll lesen zu können. Unter Windows XP besitzen alle Benutzer diese Berechtigung, nicht jedoch unter Windows Server 2003.

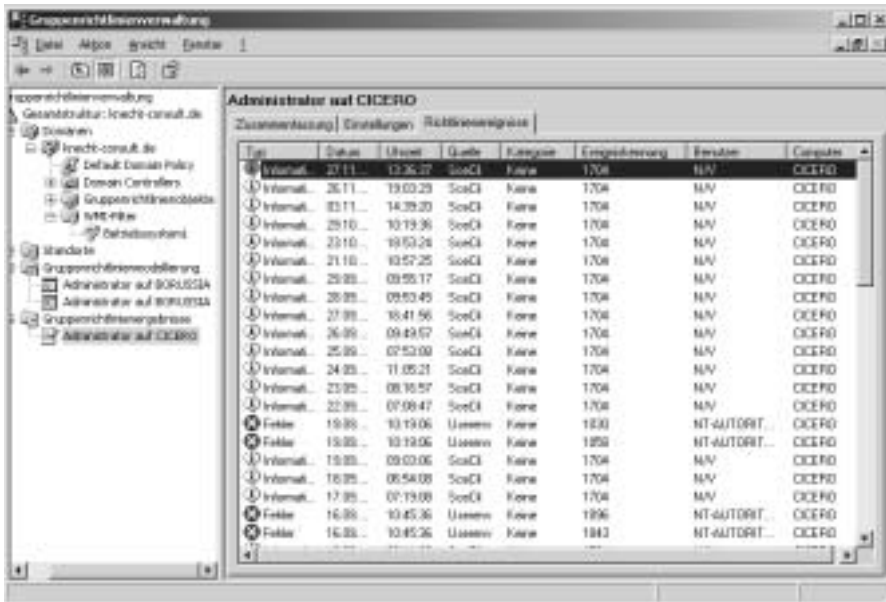


Abbildung 20.44: Die Richtlinienereignisse der Richtlinienereignisse

20.3.10 Aufgabendelegierung

Da die Verwaltung der Gruppenrichtlinien ein sehr weites Feld ist, die nicht von einer einzelnen Person allein durchgeführt werden muss, kann die Delegation einzelner Teilaufgaben an weitere Personen erfolgen. So können Sie beispielsweise die Erstellung von GPOs, deren Verknüpfung und Bearbeitung oder die Gruppenrichtlinienmodellierung an bestimmte Personen delegieren. Die folgenden Abschnitte zeigen, wie die Delegation für die wichtigsten Verwaltungsaufgaben durchgeführt wird.

Erstellen von GPOs

Standardmäßig können alle Mitglieder der Sicherheitsgruppe Richtlinien-Ersteller-Besitzer GPOs erstellen. Sie können entweder weitere Benutzer zu dieser Gruppe hinzufügen oder direkt über die GPMC Benutzern und Gruppen diese Berechtigung erteilen. Da es

sich bei der Gruppe Richtlinien-Ersteller-Besitzer um eine globale Domänengruppe handelt, konnten keine Benutzer hinzugefügt werden, die nicht der Domäne angehören. Sofern Sie die Benutzer über die GPMC hinzufügen, besteht dieses Problem nicht mehr. Öffnen Sie dazu in der GPMC die Registerkarte DELEGIERUNG des Knotens GRUPPEN-RICHTLINIENOBJEKTE und fügen neue Benutzer hinzu (siehe Abbildung 20.45).

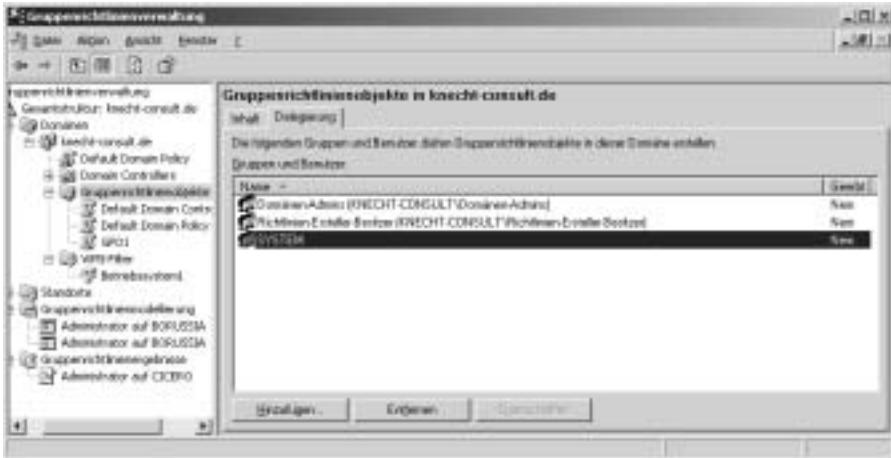


Abbildung 20.45: Benutzerdelegation zum Erstellen neuer GPOs

Sobald ein Benutzer die Berechtigung zum Erstellen von GPOs besitzt, ist er dennoch nicht in der Lage, bestehende GPOs zu bearbeiten oder löschen. Lediglich die von ihm erstellten können geändert und gelöscht werden.

Zugriff auf einzelne GPOs

Für jedes einzelne GPO können Sie Benutzern bestimmte Berechtigungen zuweisen. Öffnen Sie dazu die Registerkarte DELEGIERUNG des gewünschten GPO.

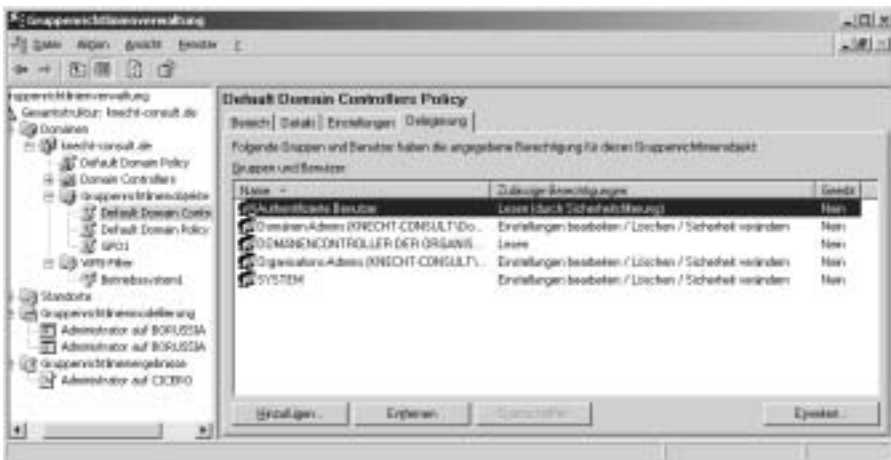


Abbildung 20.46: Berechtigungen für den Zugriff auf einzelne GPOs

Tabelle 20.6 zeigt die verschiedenen Berechtigungen.

Berechtigung	Auswirkung
Lesen	Auf das GPO kann nur lesend zugegriffen werden.
Einstellungen bearbeiten	Erlaubt sind Lesen, Schreiben sowie das Erstellen und Löschen von untergeordneten Objekten.
Einstellungen bearbeiten, Löschen, Sicherheit verändern	Erlaubt sind Lesen, Schreiben, Löschen, Verändern der Berechtigungen, Übernahme des Besitzes sowie das Erstellen und Löschen von untergeordneten Objekten. Diese Berechtigung ermöglicht Vollzugriff auf das GPO.
Lesen (durch Sicherheitsfilterung)	Diese Berechtigung kann nicht direkt gesetzt werden. Sie wird lediglich für alle Benutzer angezeigt, die über die Leseberechtigung verfügen sowie in der Liste SICHERHEITSFILTERUNG auf der Registerkarte BEREICH des GPO angezeigt werden.
Benutzerdefiniert	Beliebige Kombinationen von Berechtigungen können zugewiesen werden. Über die Schaltfläche ERWEITERT wird der ACL-Editor gestartet.

Tabelle 20.6: Berechtigungen, die einem Benutzer für ein GPO zugewiesen werden können

Verknüpfen von GPOs

Damit die Einstellungen eines GPO wirksam werden, muss dieses mit einer Domäne, einem Standort oder einer OU verknüpft werden. Sie können Benutzern die Berechtigung erteilen, GPOs zu verknüpfen, die Verknüpfungsreihenfolge zu bearbeiten und die Vererbung von GPO-Einstellungen zu unterbrechen. Öffnen Sie dazu die Registerkarte DELEGIERUNG der gewünschten Domäne oder OU.

Gruppenrichtlinienmodellierung und Gruppenrichtlinienergebnisse

Die Berechtigung zur Gruppenrichtlinienmodellierung besitzen standardmäßig nur Domänenadministratoren, die Berechtigung zum Lesen der Gruppenrichtlinienergebnisse nur Benutzer mit lokalen Administratorrechten und Remote-Zugriff auf die Gruppenrichtlinienergebnisse.

Um diese Einstellungen zu ändern, öffnen Sie die Registerkarte DELEGIERUNG der gewünschten Domäne oder OU. Aus der Listbox BERECHTIGUNG wählen Sie entweder den Eintrag GRUPPENRICHTLINIENERGEBNISSE LESEN oder ANALYSEN ZUR GRUPPENRICHTLINIENMODELLIERUNG DURCHFÜHREN. Über die Schaltfläche HINZUFÜGEN können Sie weiteren Benutzern die gewünschte Berechtigung erteilen.



Alternativ können Sie die Berechtigungen auch über die Schaltfläche ERWEITERT direkt über den ACL-Editor zuweisen. Die Option GRUPPENRICHTLINIENERGEBNISSE LESEN entspricht der Berechtigung RICHTLINIENERGEBNISSE ERSTELLEN (PLANUNG) im ACL-Editor, die zweite Option der Berechtigung RICHTLINIENERGEBNISSE ERSTELLEN (PROTOKOLLIERUNG). Für den Planungsmodus muss auf allen Domänencontrollern der Gesamtstruktur das Windows 2003-Schema ausgeführt werden. Verwenden Sie hierzu das Programm ADPREP (siehe Kapitel 9.5).

20.3.11 WMI-Filter

Über die GPMC können GPOs mit WMI-(Windows Management Instrumentation-) Filtern verknüpft werden. Über den WMI-Filter werden bestimmte Attribute vorgegeben, die der Zielcomputer erfüllen muss, damit das GPO angewendet wird. Treffen die Attribute nicht zu, wird das GPO nicht angewendet. Über WMI können Sie umfangreiche Inventarisierungsdaten zu Hard- und Software abfragen wie z.B. Angaben zu RAM, CPU, freiem Speicherplatz, installierten Treibern, Softwarekonfiguration usw. So ist es möglich, über eine Gruppenrichtlinie eine bestimmte Software nur an Clients zu verteilen, die z.B. mindestens über 128 MB RAM und 400 MB freien Speicherplatz verfügen.



WMI-Filter können lediglich für Windows XP sowie 2003 angewendet werden. Für Windows 2000 ist keine WMI-Filterung möglich, und das GPO wird grundsätzlich angewendet. Weiterhin muss in einer Domäne mindestens ein Domänencontroller unter Windows Server 2003 vorhanden sein. Andernfalls wird in der GPMC der Knoten WMI-FILTER nicht angezeigt.

Jeder WMI-Filter beinhaltet mindestens eine Abfrage der Hard- bzw. Softwaredaten. Als Sprache für die Abfragen wird WQL (WMI Query Language) verwendet. Diese Sprache ist sehr eng mit SQL verwandt. Eine Abfrage wird immer für einen bestimmten WMI-Namensraum ausgeführt, der bei der Erstellung anzugeben ist. Standardmäßig handelt es sich um den Namensraum root\CIMv2. Ausführliche Hinweise zu WQL finden Sie unter http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wmisdk/wmi/wql_operators.asp.

Die Abfrage wird gegenüber dem Zielclient entweder als true oder false ausgewertet. Im Falle von true treffen die im Filter definierten Attribute zu, und das mit dem Filter verknüpfte GPO wird angewendet. Sie können pro GPO nur einen WMI-Filter anwenden. Ein WMI-Filter kann jedoch mit mehreren GPOs verknüpft werden. Die WMI-Filter werden domänenbasiert gespeichert. Ein GPO muss sich also immer in derselben Domäne befinden wie der WMI-Filter, mit dem es verknüpft werden soll.

Um einen neuen WMI-Filter zu erstellen, führen Sie die folgenden Schritte aus:

1. Klicken Sie im Kontextmenü von WMI-FILTER auf NEU (siehe Abbildung 20.47) und dort auf die Schaltfläche HINZUFÜGEN. Soll ein GPO mit einem Filter verknüpft werden, so wählen Sie auf der Registerkarte BEREICH des GPO WMI-FILTERUNG. Dort wählen Sie den gewünschten Filter aus.

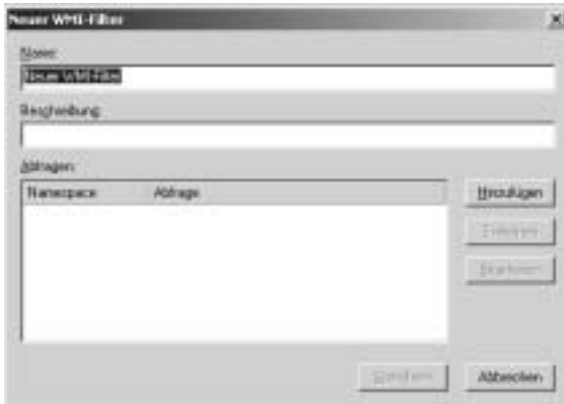


Abbildung 20.47: Erstellen eines neuen WMI-Filters

2. Angenommen, Sie möchten einen WMI-Filter für ein GPO erstellen, das nur bei Windows XP Professional angewendet wird, so verwenden Sie folgende Syntax (der Namensraum `root\CimV2` ist bereits im Feld `Namespace` vorgegeben, siehe Abbildung 20.48):

```
Select * from Win32_OperatingSystem where Caption = "Microsoft Windows XP Professional"
```

Soll eine Softwareinstallation nur dann durchgeführt werden, wenn mindestens eine von zwei Applikationen bereits installiert ist, so verwenden Sie die folgende Syntax und bestätigen mit OK und klicken dann auf **SPEICHERN**.

```
Select * from Win32_Product where name = "MSIApplikation1" OR "MSIApplikation2"
```

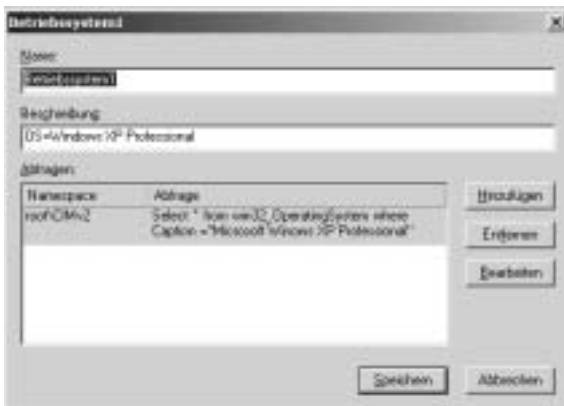


Abbildung 20.48: Erstellen einer Abfrage für einen WMI-Filter

Um den erstellten WMI-Filter mit einem GPO zu verknüpfen, öffnen Sie die Registerkarte **BEREICH** des GPO. Dort wählen Sie unten in der Sektion **WMI-FILTER** den gewünschten Filter aus (siehe Abbildung 20.19). Bedenken Sie, dass jedes GPO mit nur einem WMI-Filter verknüpft sein kann.

Delegieren der WMI-Filter

Auch für WMI-Filter ist eine Delegierung der Verwaltung möglich. Es gibt zwei Typen von Zugriffsberechtigungen für WMI-Filter, nämlich Vollzugriff und Bearbeiten. Die Berechtigung Vollzugriff ist standardmäßig nur Domänen- und Unternehmens-Admins zugewiesen, die Berechtigung Bearbeiten den Erstellern des Filters. Mit dieser Berechtigung kann ein Benutzer neue WMI-Filter erstellen sowie die von ihm erstellten modifizieren und löschen. WMI-Filter, die von anderen Personen erstellt sind, können nicht geändert werden.

Um die Berechtigungen an weitere Personen zu delegieren, öffnen Sie die Registerkarte DELEGIERUNG des WMI-Filters. Über die Schaltfläche HINZUFÜGEN können Sie weitere Benutzer und Gruppen hinzufügen. Nachdem Sie den Benutzer ausgewählt haben, wählen Sie aus der Listbox BERECHTIGUNGEN die Option VOLLZUGRIFF oder BEARBEITEN aus.

20.4 Ordnerverwaltung über Gruppenrichtlinien

Über die Gruppenrichtlinien haben Sie die Möglichkeit, Ordner, die zum Benutzerprofil gehören, an eine zentrale Stelle im Netzwerk umzuleiten. Dazu zählen die Ordner Eigene Dateien, Eigene Bilder, Desktop, Startmenü und Anwendungsdaten, die sich standardmäßig auf der SYSTEMPARTITION \DOKUMENTE UND EINSTELLUNGEN\%BENUTZERNAME% befinden (bei einer Neuinstallation von Windows 2000/XP). Bei einer Aktualisierung von Windows NT befinden sie sich in %SYSTEMROOT%\PROFILE, bei einer Aktualisierung von Windows 9x in %SYSTEMROOT%\SYSTEM\PROFILE.

Insbesondere der Ordner Eigene Dateien kann im Laufe der Zeit sehr groß werden. Deshalb ist es sinnvoll, bei der Verwendung von servergespeicherten Profilen vor allem diesen Ordner umzuleiten. Wird dieser Ordner nicht umgeleitet, wird er als Teil des Profils bei jeder Benutzeranmeldung zwischen Client und Server hin- und herkopiert. Ist der Ordner umgeleitet, enthält das Profil lediglich den Verweis auf den umgeleiteten Speicherort des Ordners im Netzwerk. Werden alle Ordner sämtlicher Benutzer an einen zentralen Dateiserver weitergeleitet, wird damit auch die Sicherung der Daten vereinfacht, da nur ein einzelner Speicherort zu sichern ist. Auch wenn Sie kein servergespeichertes Benutzerprofil anwenden, können die Daten lokal von der Systempartition an eine andere lokale Festplatte weitergeleitet werden. Somit sind die Daten auch dann noch vorhanden, wenn eine Neuinstallation des Betriebssystems erforderlich wird.

20.4.1 Ordnerumleitung

Dieses Kapitel beschreibt, wie Sie die Umleitung der benutzerspezifischen Ordner einrichten und konfigurieren. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie das GPO des Standorts, der Domäne oder OU. Dieses GPO muss dem Benutzer zugewiesen sein, für den Sie die Ordnerumleitung konfigurieren möchten.
2. Öffnen Sie in der mmc des GPO den Knoten BENUTZERKONFIGURATION / WINDOWS-EINSTELLUNGEN / ORDNERUMLEITUNG. Dort sehen Sie die vier Ordner ANWENDUNGSDATEN, DESKTOP, EIGENE DATEIEN (mit dem Unterordner EIGENE BILDER) sowie STARTMENÜ. Wählen Sie aus dem Kontextmenü des umzuleitenden Ordners EIGENSCHAFTEN. In unserem Beispiel wählen wir den Ordner EIGENE DATEIEN. Die Konfiguration der anderen Ordner erfolgt analog dazu.

3. Auf der Registerkarte ZIEL der Eigenschaften stehen Ihnen mehrere Einstellungsoptionen zur Verfügung. Sind bisher noch keine Einstellungen vorgenommen, befindet sich in der Listbox EINSTELLUNG die Angabe ES WURDEN KEINE ADMINISTRATORRICHTLINIEN ANGEZEIGT. Sie haben zu den Einstellungen die Wahl zwischen den Optionen STANDARD – LEITET ALLE ORDNER AUF DEN GLEICHEN PFAD UM und ERWEITERT – GIBT PFADE FÜR VERSCHIEDENE BENUTZERGRUPPEN AN. Beide Optionen werden verschieden konfiguriert und deshalb getrennt beschrieben.

Standard – leitet alle Ordner auf den gleichen Pfad um

Bei diesem Verfahren werden für jeden Benutzer an einem Standort, einer Domäne oder OU die gewählten Ordner in einer bestimmten Freigabe auf einem Dateiserver gespeichert.

1. Wenn Sie sich für die Standardvariante entschieden haben, erhalten Sie folgendes Fenster (siehe Abbildung 20.49):
2. Wählen Sie über DURCHSUCHEN den Pfad des Ordners, an den der gewählte Ordner umgeleitet werden soll. Sie sollten dabei in jedem Fall mit der Variablen %username% arbeiten. Geben Sie beispielsweise den Pfad \\ARCHIMEDES\DATEN\%USERNAME%\EIGENE DATEIEN an, erhält jeder Benutzer seinen eigenen Ordner mit Unterordnern innerhalb der Freigabe auf dem Dateiserver. Der Pfad muss immer als UNC-Pfad angegeben werden.



Abbildung 20.49: Standardeinstellung für die Ordnerumleitung

3. Wechseln Sie dann auf die Registerkarte EINSTELLUNGEN. Standardmäßig sind dort bereits die Optionen DEM BENUTZER EXKLUSIVE ZUGRIFFSRECHTE FÜR EIGENE DATEIEN ERTEILEN sowie DEN INHALT VON EIGENE DATEIEN AN DEN NEUEN ORT VERSCHIEBEN aktiviert (siehe Abbildung 20.50). Sind die exklusiven Zugriffsrechte aktiviert, erhält lediglich der Benutzer selbst sowie das lokale System Vollzugriff auf den Ordner. Nicht einmal ein Administrator oder ein anderer Benutzer kann Änderungen an diesem Ordner vornehmen. Die zweite Option bewirkt, dass die Inhalte des ausgewählten Ordners

in den umgeleiteten Zielordner verschoben und nicht mehr am ursprünglichen Speicherort vorgehalten werden.



Abbildung 20.50: Einstellungen zur Ordnerumleitung

4. Weiterhin können Sie bestimmen, was mit dem umgeleiteten Ordner nach dem Entfernen der Richtlinie geschehen soll. Er kann dann entweder an seinem neuen Ort bleiben oder aber wieder lokal umgeleitet werden. Das Ergebnis dieser Einstellung ist abhängig von der Einstellung **DEN INHALT VON EIGENE DATEIEN AN DEN NEUEN ORT VERSCHIEBEN** auf dieser Registerkarte. Tabelle 20.7 gibt einen Überblick über die Effekte der Einstellungen.

Status der Einstellung DEN INHALT ... VERSCHIEBEN	Status von ENTFERNEN DER RICHTLINIE	Nach Entfernen der Richtlinie
Aktiviert oder deaktiviert	Ordner belassen	Der Ordner bleibt am umgeleiteten Ort; der Benutzer hat weiterhin Zugriff.
Aktiviert	Ordner umleiten	Der Ordner wird mit seinen Inhalten an den lokalen Ort des Benutzers kopiert, bleibt aber auch auf dem Server noch bestehen. Der Zugriff des Benutzers erfolgt aber nur noch auf die lokalen Dateien, nicht mehr auf die im Netzwerk.
Deaktiviert	Ordner umleiten	Der Ordner wird <i>ohne</i> seine Inhalte an den lokalen Speicherort kopiert. Werden die Inhalte nicht gesondert dorthin kopiert oder verschoben, hat der Benutzer keinen Zugriff mehr auf die Daten.

Tabelle 20.7: Einstellungen zum Entfernen einer Richtlinie

5. Lediglich für den Ordner EIGENE DATEIEN finden Sie die Option für den Umgang mit dem Ordner EIGENE BILDER. Dabei wird der Ordner EIGENE BILDER dem Ordner EIGENE DATEIEN untergeordnet. Vergeben Sie keine Richtlinie, wird EIGENE BILDER nicht als Unterordner von EIGENE DATEIEN umgeleitet. Damit EIGENE BILDER der Umleitung von EIGENE DATEIEN folgen kann, öffnen Sie im GPO den Pfad BENUTZERKONFIGURATION / WINDOWS-EINSTELLUNGEN / ORDNERUMLEITUNG / EIGENE BILDER. Wählen Sie aus den Eigenschaften den Eintrag DEM ORDNER EIGENE DATEIEN FOLGEN.

Erweitert – gibt Pfade für verschiedene Benutzergruppen an

Bei diesem Verfahren werden für jeden Benutzer die gewählten Ordner in einer bestimmten Freigabe auf einem Dateiserver gespeichert. Die Ordnerumleitung basiert dabei auf der Gruppenmitgliedschaft der Benutzer.

1. Wenn Sie sich für die erweiterte Variante entschieden haben, erhalten Sie folgendes Fenster (siehe Abbildung 20.51):

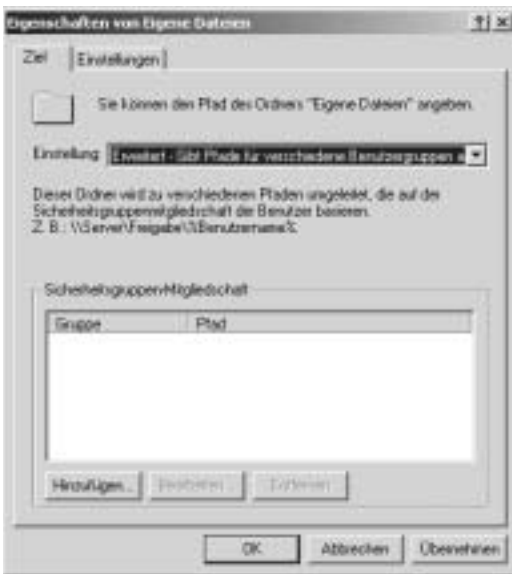


Abbildung 20.51: Erweiterte Einstellungen für die Ordnerumleitung

2. Klicken Sie auf HINZUFÜGEN. In der dann folgenden Dialogbox GRUPPE UND PFAD ANGEBEN wählen Sie die Sicherheitsgruppe aus, für die Sie einen bestimmten Zielordner einrichten möchten. Alternativ können Sie die Gruppe auch über DURCHSUCHEN auswählen. Geben Sie dann den Pfad zu der Freigabe ein, in die die Ordner umgeleitet werden sollen. Arbeiten Sie mit der Variablen %username%, um für jeden Benutzer einen Ordner mit seinem Benutzernamen anzulegen. Der Pfad zur Freigabe sollte als UNC-Pfad angegeben werden.
3. Wechseln Sie dann auf die Registerkarte EINSTELLUNGEN des gewählten Ordners (siehe Abbildung 20.50). Die hier vorzunehmenden Einstellungen sind identisch mit den bereits dort beschriebenen.

20.4.2 Probleme bei der Ordnerumleitung unter Windows XP

Wenn Sie die eben beschriebene Ordnerumleitung auf einen Benutzer anwenden, der Windows XP Professional verwendet, kann das Problem auftreten, dass der Benutzer eine Warnmeldung über unzureichenden Speicherplatz erhält oder zumindest nur noch sehr wenig Speicherplatz verfügbar ist.

Dieses Problem liegt darin begründet, dass Windows XP Professional standardmäßig alle Inhalte der umgeleiteten Ordner lokal zwischenspeichert. Ist dabei der Inhalt der umgeleiteten Ordner größer als der lokal verfügbare Platz, kommt es zur Fehlermeldung. Ansonsten wird lokal die Größe der Freigabe belegt.

Um dieses Problem zu beheben, muss die standardmäßig nicht definierte Gruppenrichtlinie **UMGELEITETE ORDNER NICHT AUTOMATISCH OFFLINE VERFÜGBAR MACHEN** aktiviert werden. Weitere Hinweise zu Offline-Inhalten von Ordnern finden Sie in Kapitel 20.4.3. Um diese Richtlinie zu aktivieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie das GPO, das auf den Benutzer angewendet wird, und wählen den Knoten **BENUTZERKONFIGURATION / ADMINISTRATIVE VORLAGEN / NETZWERK / OFFLINE-DATEIEN**.
2. Aktivieren Sie dort die Richtlinie **UMGELEITETE ORDNER NICHT AUTOMATISCH OFFLINE VERFÜGBAR MACHEN**.

20.4.3 Offline-Inhalte von Ordnern

Wie eben in der Problembeschreibung für Windows XP gesehen, können die Inhalte von Netzwerkordnern auch lokal zwischengespeichert werden. Dabei spricht man von Offline-Inhalten der Ordner. Sie können nicht nur die Benutzerordner wie **Eigene Dateien** offline verfügbar machen, sondern auch jeden anderen im Netzwerk freigegebenen Ordner. Offline-Ordner und deren Inhalte sind auch dann für den Benutzer verfügbar, wenn er vorübergehend keine Verbindung zum Netzwerk hat. Auch bei der Verwendung eines Laptops in einer Docking-Station ist die Konfiguration von Offline-Ordnern sinnvoll.

In der Zwischenzeit kann der Benutzer mit seinen Dateien weiterarbeiten, als würde die Netzwerkverbindung auch weiterhin bestehen. Wenn er sich dann wieder mit dem Netzwerk bzw. der Docking-Station verbindet, können Sie festlegen, wie die Synchronisierung zwischen seinen in der Zwischenzeit bearbeiteten und den im Netzwerk vorhandenen Dateien geschehen soll.

Um einen Computer für die Verwendung von Offline-Ordnern vorzubereiten, führen Sie die folgenden Schritte aus:

1. Öffnen Sie den Arbeitsplatz und wählen aus dem Menü **EXTRAS** den Eintrag **ORDNER-OPTIONEN**.
2. Aktivieren Sie auf der Registerkarte **OFFLINE-DATEIEN** den Eintrag **OFFLINE-DATEIEN AKTIVIEREN**. Sie können hier auch eine Maximalgröße auf dem lokalen Computer für die zwischenzuspeichernden Dateien angeben.

Führen Sie danach die folgenden Schritte aus, um ein Laufwerk, einen Ordner oder eine Datei offline verfügbar zu machen:

1. Öffnen Sie die Netzwerkumgebung oder den Arbeitsplatz und markieren dort die freigegebene Ressource. Markieren Sie entweder die gesamte Freigabe, einen Ordner

oder eine Datei daraus und wählen aus dem Menü DATEI den Eintrag OFFLINE VERFÜGBAR MACHEN. Es erscheint ein Assistent, der Sie durch den Vorgang leitet.

2. Klicken Sie auf WEITER. Sie können festlegen, ob die ausgewählten Dateien beim An- und Abmelden synchronisiert werden sollen (siehe Abbildung 20.52). Die Synchronisierung kann auch manuell erfolgen oder zeitgesteuert. Weitere Hinweise dazu finden Sie im Abschnitt Synchronisation in diesem Kapitel. Außerdem wird Ihnen das Symbol gezeigt, das alle Dateien und Ordner erhalten, die offline verfügbar sind. Sie können so im Windows Explorer leicht die offline verfügbar gemachten Dateien innerhalb einer Netzwerkfreigabe erkennen. Klicken Sie dann auf WEITER.



Abbildung 20.52: Synchronisationseinstellungen für Offline-Dateien

3. Sie können nun festlegen, ob Sie im Statusbereich der Taskleiste ein Symbol erhalten möchten, wenn die Verbindung zur Netzwerkressource getrennt ist (siehe Abbildung 20.53). Wünschen Sie dieses Symbol, aktivieren Sie die Checkbox ERINNERUNGEN AKTIVIEREN. Zusätzlich können Sie auf dem Desktop eine Verknüpfung zum lokalen Ordner der Offline-Dateien anlegen. Über diese Verknüpfung sehen Sie alle Dateien, die offline verfügbar sind. Sie werden jedoch in einer Liste aufgeführt und nicht nach ihrem tatsächlichen Speicherort in Unterordnern in der eigentlichen Freigabe. Klicken Sie dann auf FERTIG STELLEN.



Abbildung 20.53: Erinnerungssymbol für Offlinedateien aktivieren

4. Im letzten Schritt müssen Sie angeben, welche Inhalte offline zur Verfügung stehen sollen (siehe Abbildung 20.54). Standardmäßig wird der gewählte Ordner mit allen Unterordnern offline verfügbar (OPTION JA, DEN ORDNER UND ALLE UNTERORDNER OFFLINE VERFÜGBAR MACHEN). Sie können aber auch nur den gewählten Ordner auswählen (Option NEIN, NUR DEN ORDNER OFFLINE VERFÜGBAR MACHEN). Bestätigen Sie Ihre Auswahl mit OK.



Abbildung 20.54: Auswahl des Verfügbarkeitsbereiches für Offlinedateien



Machen Sie eine Verknüpfung zu einer Datei offline verfügbar, so wird auch die Datei selbst verfügbar. Machen Sie hingegen eine Ordnerverknüpfung verfügbar, wird nur der Ordner, nicht jedoch sein Inhalt verfügbar.

5. Nachdem Sie mit OK Ihre Auswahl bestätigt haben, wird der Synchronisierungsvorgang durchgeführt. Rechts unten sehen Sie die Schaltfläche SETUP. Über diese können Sie weitere Optionen zur Synchronisierung einstellen. Dies wird im nächsten Kapitel beschrieben. Sie erhalten Statusmeldungen über den Fortschritt sowie über Dateien, die standardmäßig nicht synchronisiert werden können wie etwa .pst-Dateien von MS Outlook oder andere Sicherungsdateien (.mdb, .ldb, .mdw, .mde, .db???? und .slm). Weitere Hinweise dazu finden Sie unter <http://support.microsoft.com/default.aspx?scid=kb;en-us;q252509>

Um die Offline-Inhalte nicht länger verfügbar zu machen, markieren Sie den gewünschten Ordner oder die Datei im Arbeitsplatz oder der Netzwerkumgebung und deaktivieren im Menü DATEI die Checkbox OFFLINE VERFÜGBAR MACHEN.

Synchronisieren der Offline-Inhalte

Wie in Abbildung 20.52 gezeigt, werden die Offline-Inhalte standardmäßig beim An- und Abmelden mit den Netzwerkinhalten synchronisiert.

Um ein einzelnes Objekt zu einem beliebigen Zeitpunkt zu synchronisieren, markieren Sie dieses in der Desktop-Verknüpfung zum Offline-Ordner oder in der Netzwerkumgebung bzw. dem Arbeitsplatz und wählen aus dem Kontextmenü SYNCHRONISIEREN.

Am komfortabelsten geschieht die Synchronisierung jedoch über die Synchronisationsverwaltung. Diese ist ein Bestandteil von IntelliMirror zur Verwaltung der Benutzerdaten.

1. Die Synchronisationsverwaltung rufen Sie über die Schaltfläche SETUP im Fenster des Synchronisierungsfortschritts auf. Wenn Sie neue Offline-Inhalte hinzufügen, können Sie für diese auch gleich die entsprechenden Optionen bestimmen.
2. Sie erhalten das Fenster SYNCHRONISATIONSEINSTELLUNGEN (siehe Abbildung 20.55). Unter BEI VERWENDUNG DIESER NETZWERKVERBINDUNG legen Sie die Netzwerkverbindung fest, über die die Synchronisation erfolgen soll. Die Konfiguration unterschiedlicher Netzwerkverbindungen ist sinnvoll, wenn diese unterschiedlich schnell sind. Konfigurieren Sie die Offline-Synchronisierung beispielsweise nicht für eine langsame redundante Wählverbindung.

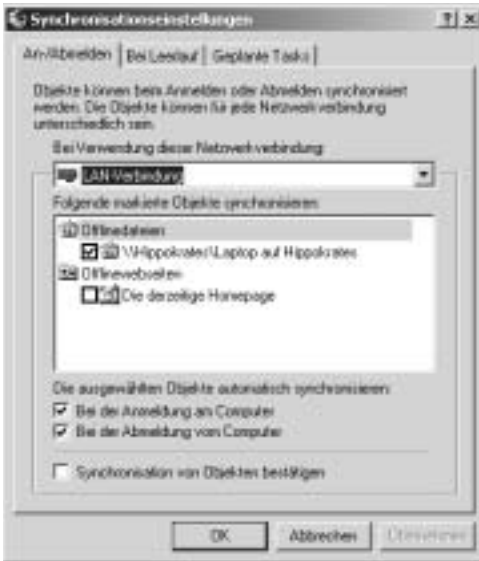


Abbildung 20.55: Auswahl der Netzwerkverbindung für die Synchronisation

3. Sie sehen unter OFFLINEDATEIEN eine Liste aller Verzeichnisse, die auf dem lokalen Rechner offline verfügbar sind. Sie können für die Verzeichnisse festlegen, ob diese bei der Anmeldung und/oder Abmeldung synchronisiert werden sollen. Hier wird die Synchronisation bei An- und/oder Abmeldung eingestellt sowie ob diese vom Benutzer bestätigt werden soll. Bestätigen Sie Ihre Wahl mit OK.
4. Auf der Registerkarte BEI LEERLAUF können Sie festlegen, welche Dateien im Leerlauf synchronisiert werden sollen (siehe Abbildung 20.56). Über die Schaltfläche ERWEITERT kann zusätzlich eingestellt werden, wie lange sich der Computer im Leerlauf befinden muss, wie hoch das Wiederholungsintervall ist und ob eine Synchronisierung stattfinden darf, wenn der Computer im Akkubetrieb ist.

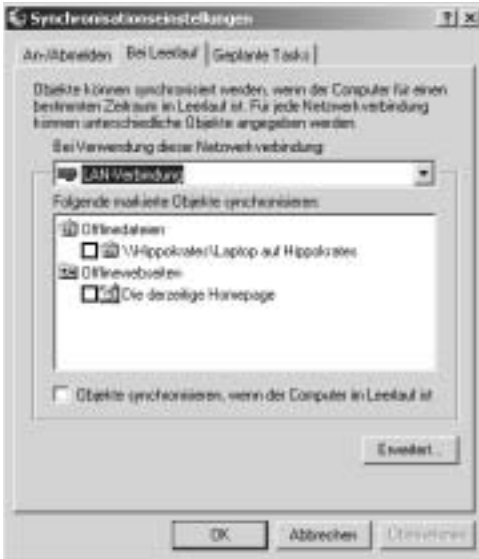


Abbildung 20.56: Synchronisationseinstellungen für Leerlaufphasen konfigurieren

5. Auf der Registerkarte GEPLANTE TASKS können Sie über einen Assistenten konfigurieren, zu welchen festen Zeiten die Synchronisation erfolgen soll. Bereits konfigurierte Tasks können hier auch bearbeitet oder wieder gelöscht werden.

20.5 Softwareverwaltung und -verteilung über Gruppenrichtlinien

Über die Gruppenrichtlinie können Sie nicht nur die Desktop-Umgebung Ihrer Clients verwalten, sondern den Benutzern auch Software zur Installation zuweisen. Diese Möglichkeit der Gruppenrichtlinien sollten Sie anwenden, sofern Ihr Unternehmen nicht bereits ein anderes Tool eines Drittanbieters zur Softwareverteilung einsetzt. Dieses Kapitel gibt Ihnen eine Übersicht über den theoretischen Planungsablauf. In den folgenden Kapiteln wird die praktische Umsetzung beschrieben.

20.5.1 Der Prozess der Softwareverteilung

Vor der Softwareverteilung sind verschiedene Punkte zu bedenken und zu klären. Den gesamten Prozess der Softwareverteilung kann man in vier große Abschnitte gliedern:

1. Vorbereitung
2. Quelle der Installation
3. Empfänger der Software
4. Installation

Vorbereitung

In der Vorbereitungsphase legen Sie allgemeine Punkte fest, die für jede Methode der Softwareverteilung gültig sind.

- ▶ Untersuchen Sie zunächst, welche Software momentan eingesetzt wird und welche davon an die Benutzer auch weiterhin verteilt werden soll.
- ▶ Unterteilen Sie diese Software in verbindliche und optionale Programme. Standardisieren Sie dadurch die Arbeitsplätze im Unternehmen.
- ▶ Ermitteln Sie weiter, bei welcher der Softwares es sich um reine Windows Installer-Pakete handelt, die direkt über die Gruppenrichtlinie zugewiesen werden können. Die Programme, die eine herkömmliche Setup-Routine bereitstellen, müssen für die Verteilung repaketiert werden. Im Lieferumfang von Windows 2000 Server befindet sich dafür das Programm *WinInstall LE* der Firma Veritas Software. Dieses Programm ist jedoch nicht mehr im Lieferumfang von Windows Server 2003 enthalten. Weiterhin stehen Ihnen z.B. folgende Produkte von Drittanbietern zur Verfügung:
 - ▶ *Wise Package Studio* (<http://www.wise.com/wps.asp>) oder
 - ▶ *Installshield AdminStudio* (<http://www.installshield.com/isas/>)
- ▶ Legen Sie außerdem fest, ob bestimmte Anpassungen und Konfigurationen der Software für bestimmte Benutzer erforderlich sind. Ist es erforderlich, dass z.B. verschiedene Office-Versionen mit unterschiedlichen Features über Transform Files gebildet werden? Weitere Hinweise dazu finden Sie in Kapitel 20.7.

Quelle der Installation

Als Nächstes müssen Sie festlegen, welche Computer die Softwareverteilungspunkte sein sollen, von denen aus die Softwarepakete auf den Clients installiert werden können. Bestimmen Sie außerdem, ob Sie die Gruppenrichtlinie zur Softwareverteilung auf Standort- oder OU-Ebene anwenden wollen.

Empfänger der Software

Entscheiden Sie dann, ob die Software an einen Benutzer oder einen Computer verteilt werden soll. Bestimmen Sie dann die Benutzer und Computer, die die Software erhalten sollen.



Die Softwareverteilung kann nicht bei Terminalserver-Clients durchgeführt werden.

Installation

Einem Benutzer können Sie Software zuweisen oder veröffentlichen / ankündigen, einem Computer nur zuweisen. Beim Zuweisen von Software wird diese bei der Benutzeranmeldung angekündigt. Die Installation erfolgt, wenn der Benutzer ein Dokument öffnet, das die Applikation erfordert, oder wenn er das entsprechende Icon im Startmenü oder auf dem Desktop anklickt. Die einem Benutzer zugewiesene Software wird auf jedem Arbeitsplatz installiert, unabhängig davon, an welchem Computer er sich anmeldet.

Wird die Software einem Computer zugewiesen, wird die Installation beim Start des Computers durchgeführt. Mit Windows Server 2003 haben Sie auch die Möglichkeit, die komplette einem Benutzer zugewiesene Software bei dessen Anmeldung installieren zu lassen und nicht erst, wenn die Applikation das erste Mal benötigt wird. Dies bringt den Vorteil einer konsistenten Umgebung, da ab dem Zeitpunkt der Anmeldung alle Softwarepakete bereits vorhanden sind.

Das Veröffentlichen von Software funktioniert nur für Benutzer. Dabei werden jedoch keine Verknüpfungen auf dem Desktop oder im Startmenü angezeigt. Die bereitgestellte Software speichert ihre Informationen zur Veröffentlichung im Active Directory und nicht in der lokalen Registry des Computers. Die Applikation wird erst installiert, wenn der Benutzer eine Datei öffnet, die die Applikation erfordert, oder wenn er unter SYSTEM-STEUERUNG/SOFTWARE die veröffentlichten Applikationen zur Installation auswählt.

Zur Installation der Softwarepakete verwendet die Softwareinstallation die systemimmanente Windows Installer-Technik. Sie können über den Windows Installer Pakete zur Verteilung bringen, die über die folgenden Dateiendungen verfügen:

- ▶ **.msi:** Die msi-Datei ist die zentrale Steuerungsdatei für das gesamte Setup einer Applikation, die den Windows Installer benutzt. Die Datei beinhaltet in einer Datenbankstruktur alle Features sowie entweder direkt die cab-Dateien, Kopieranweisungen etc. oder Verweise auf diese. Das Setup ruft intern den Befehl `msiexec /i` auf, wodurch das MSI-File gestartet wird. Eine Applikation kann auch mehrere MSI-Files enthalten, die sich während der Installation gegenseitig aufrufen. Diese Dateien können für ein Programm nativ vorliegen oder durch Repaketierung erzeugt worden sein.
- ▶ **.mst:** Die mst-Datei wird auch Transform-File genannt. Hierbei handelt es sich um eine Datei, die ein bearbeitetes Feature-Set für eine Applikation enthält. Eine solche Datei wird z.B. für Office 2000 über das Office Resource Kit erstellt. Das Erstellen eines MST-Files ist optional. Wenn Sie einer msi-Datei kein Transform-File hinzufügen, werden auf dem Client die Features installiert, die bei einer Standardinstallation von Hand auch ausgewählt werden.
- ▶ **.msp:** Hierbei handelt es sich um Patch-Dateien oder Service Pack-Dateien für eine Applikation, die den Windows Installer benutzt. Ein Beispiel hierfür ist das Office 2000 SR-1A oder SP2.
- ▶ **.ass:** Application Assignment Scripts. Diese Skripte enthalten spezielle Befehle für die Veröffentlichung oder Zuweisung eines bestimmten Softwarepakets.

Weitergehende Details zur Funktionsweise der Windows Installer-Technologie und den speziellen Pakettypen finden Sie in Kapitel 20.6.

Außerdem müssen Sie sich eine Strategie überlegen, wie die Software auf dem Arbeitsplatz aktualisiert oder deinstalliert werden kann. Testen Sie danach die Verteilung der Pakete daraufhin, ob alle Ihre Anforderungen erfüllt werden konnten.

In den folgenden Kapiteln wird Schritt für Schritt die Bereitstellung und Konfiguration eines Softwarepakets beschrieben. Zunächst gehen wir davon aus, dass die zu verteilende Applikation bereits als Windows Installer-Paket vorliegt und Sie keine weiteren Änderungen und Anpassungen an der Software vornehmen. Spezielle Beschreibungen für derartige Operationen finden Sie in den Kapiteln 20.6 und 20.7.

20.5.2 Einrichten des Softwareverteilungspunktes und administratives Setup

Zunächst muss für die Applikation ein Softwareverteilungspunkt (SDP = Software Deployment Point) definiert werden.

1. Erstellen Sie auf einem Dateiserver eine Freigabe, in der sämtliche Unterordner für die zu installierenden Applikationen angelegt werden. Für die Freigabe des SDP müssen Sie für die Benutzer die Berechtigung Lesen vergeben, die von dort aus die Software installieren sollen. Administratoren erhalten Lese- und Schreibrechte, damit diese auch Änderungen an den Softwarepaketen vornehmen können.
2. Für jede Applikation müssen Sie einen separaten Ordner anlegen, der alle notwendigen Installationsdateien, also die .msi-Datei sowie optionale .mst- oder .msp-Dateien enthält.
3. Kopieren Sie nun in diesen Ordner alle Komponenten, die zur Applikation gehören.

Administratives Setup

Einige Applikationen können auch über das administrative Setup direkt in den SDP installiert werden. Im folgenden Beispiel wird das administrative Setup für Office 2000 beschrieben. Der Vorgang des administrativen Setups besteht im Wesentlichen aus dem Kopieren des CD-Inhalts in den SDP. Dabei haben Sie die Möglichkeit, das Paket mit dem CD-Schlüssel und dem Firmennamen zu personalisieren. Beim administrativen Setup sind die folgenden Schritte auszuführen:

1. Legen Sie die Office 2000-CD ins Laufwerk. Die CD sollte automatisch starten. Es erscheint die Willkommenseite. Brechen Sie hier den Installationsprozess ab und wechseln zur Eingabeaufforderung.
2. Wechseln Sie dort als aktuelles Laufwerk zum CD-Laufwerk und geben folgenden Befehl ein:

```
Setup.exe /a data1.msi shortfilenames=true
```



Es könnten bei anderen Applikationen noch weitere MSI-Files auf der CD vorhanden sein, die data2.msi, data3.msi usw. heißen. Wenn Sie ein administratives Setup für eines dieser MSI-Files erstellen, ersetzen Sie den Namen für data1.msi in der Kommandozeile entsprechend.

Der Parameter `/a` fordert den Windows Installer auf, das administrative Setup anstatt einer normalen Installation durchzuführen.

Der Parameter `shortfilenames=true` zwingt den Windows Installer dazu, kurze Dateinamen zu speichern. Damit ist die Kompatibilität zu verschiedenen Plattformen sichergestellt.



Einige CDs des MSDN unterstützen nicht den o.g. Befehl für das administrative Setup. Verwenden Sie stattdessen folgenden Befehl:

```
msiexec /a data1.msi shortfilenames=true
```

3. Nach der Eingabe dieses Befehls erscheint die grafische Oberfläche des administrativen Setups (siehe Abbildung 20.57).
4. Geben Sie hier den CD-Schlüssel sowie den Namen der Organisation an. Klicken Sie auf WEITER.
5. Sie sehen nun das Fenster mit dem Endbenutzer-Lizenzvertrag. Sie müssen hier die Checkbox zum Einverständnis aktivieren. Ansonsten können Sie die Installation nicht fortsetzen. Klicken Sie dann auf WEITER.



Abbildung 20.57: Administratives Setup für MS Office 2000

6. Sie müssen nun den Pfad zur Freigabe des SDP als Zielort des administrativen Setups angeben. Klicken Sie danach auf JETZT INSTALLIEREN. Dieser Vorgang kann eine Weile dauern, da fast der gesamte CD-Inhalt (ca. 500 MB) auf die Platte kopiert werden muss. Eine Statusanzeige informiert Sie über den Fortschritt.



Nach Beendigung des administrativen Setups müssen Sie die Datei **OFFICE1.CAB** von der Office 2000 CD-ROM manuell in das Root-Verzeichnis des Ordners im SDP kopieren. Andernfalls werden alle weiteren Schritte fehlschlagen. Hierbei handelt es sich um einen Fehler des administrativen Setups von Office 2000. Diese Aktion ist nur bei Office 2000 nötig, andere Applikationen sind nicht von diesem Fehler betroffen.

7. Markieren Sie nun alle Objekte und heben über das Kontextmenü EIGENSCHAFTEN den Schreibschutz auf.

Damit ist das administrative Setup abgeschlossen. Es befinden sich im SDP alle Dateien der Office 2000-CD. Wird nun eine Installation ausgeführt, erfolgt diese mit den Einstellungen des standardmäßigen Setups. Sollen benutzerdefinierte Setup-Einstellungen benutzt werden, so ist zusätzlich das Erstellen einer **.mst**-Datei erforderlich. Dieses Verfahren wird in Kapitel 20.7 beschrieben.

20.5.3 Festlegen der Installationsoptionen

Nachdem Sie serverseitig die Applikation bereitgestellt haben, beginnen nun die Einstellungen am GPO. Öffnen Sie dazu das GPO und in der Benutzer- oder Computerkonfiguration den Knoten SOFTWAREEINSTELLUNGEN / SOFTWAREINSTALLATION und wählen aus dem Kontextmenü EIGENSCHAFTEN. Auf der Registerkarte ALLGEMEIN (siehe Abbildung 20.58) legen Sie Optionen für die Pakete fest.



Abbildung 20.58: Optionen der Softwareinstallation

Im Feld STANDARDPFAD FÜR PAKETE geben Sie den Pfad zu den Ordnern der jeweiligen .msi-Datei der Applikation an. Im Abschnitt NEUE PAKETE stehen Ihnen vier Möglichkeiten für das Hinzufügen neuer Pakete zu den Benutzereinstellungen zur Wahl.

1. **BEREITSTELLUNGSDIALOG ANZEIGEN** bewirkt, dass das Dialogfeld SOFTWARE BEREITSTELLEN angezeigt wird, wenn ein neues Paket zu den Benutzereinstellungen hinzugefügt wird (siehe Abbildung 20.59). Dadurch können Sie die Eigenschaften des Pakets bearbeiten oder es zuweisen bzw. veröffentlichen.
2. **VERÖFFENTLICHEN:** Diese Option ist nicht verfügbar, wenn die Softwareeinstellungen der Computerkonfiguration geöffnet sind. Ein Softwarepaket wird nur mit den standardmäßigen Eigenschaften des Pakets veröffentlicht.
3. **ZUWEISEN** bedeutet, dass das Paket mit seinen standardmäßigen Eigenschaften einem Benutzer oder Computer zugewiesen wird.
4. **ERWEITERT VERÖFFENTLICHT ODER ZUGEWIESEN** bewirkt, dass beim Zuweisen oder Veröffentlichen eines Pakets das Dialogfeld PAKETEIGENSCHAFTEN KONFIGURIEREN angezeigt wird.

Im Bereich BENUTZERBEREICHENOPTIONEN FÜR DIE INSTALLATION können Sie festlegen, ob der Benutzer bei der Installation nur die standardmäßigen (Option EINFACH) oder alle

Installationsfenster (Option MAXIMUM) erhalten soll. Eine Installation im Hintergrund (Silent Installation) von Software ist hier nicht vorgesehen.

Aktivieren Sie die Checkbox ANWENDUNGEN DEINSTALLIEREN, WENN SIE AUSSERHALB DES VERWALTUNGSBEREICHS LIEGEN, so wird die Anwendung deinstalliert, wenn das betreffende GPO nicht mehr auf den Computer oder Benutzer angewendet wird.

20.5.4 Zuweisen und Veröffentlichen von Paketen

Um eine Applikation zuzuweisen oder zu veröffentlichen, führen Sie die folgenden Schritte durch:

1. Öffnen Sie im GPO in der Benutzer- oder Computerkonfiguration den Knoten SOFTWAREEINSTELLUNGEN / SOFTWAREINSTALLATION. Wählen Sie aus dem Kontextmenü NEU / PAKET.
2. Im Dialogfeld ÖFFNEN sehen Sie den Inhalt des Ordners, den Sie als Standardpfad zu den Applikationen ausgewählt haben (siehe Abbildung 20.58). Öffnen Sie den Ordner der gewünschten Applikation und wählen die gewünschte .msi-Datei aus. In unserem Beispiel handelt es sich um die Data1.msi der Applikation Office 2000.
3. Da Sie als Standardmethode für die Bereitstellung neuer Pakete den Bereitstellungsdialog (siehe Abbildung 20.58) gewählt haben, erhalten Sie nun das Dialogfeld SOFTWARE BEREITSTELLEN (siehe Abbildung 20.59).



Abbildung 20.59: Das Dialogfeld Software bereitstellen

4. Sie haben hier die Auswahlmöglichkeiten VERÖFFENTLICHT (nicht in der Computerkonfiguration), ZUGEWIESEN und ERWEITERTE METHODE VON „VERÖFFENTLICHT“ UND „ZUGEWIESEN“. Wählen Sie eine der beiden ersten Optionen, wenn Sie die Anwendung ohne weitere Änderungen in der Standardkonfiguration zuweisen möchten. Wählen Sie die dritte Methode, erhalten Sie das Dialogfenster EIGENSCHAFTEN VON (NAME DER APPLIKATION) (siehe Abbildung 20.60). Hier können Sie beispielsweise auf der Registerkarte ÄNDERUNGEN Transform Files auf die Standardkonfiguration anwenden.



Diese Änderungen müssen sofort an dem Paket vorgenommen werden, bevor es erstmalig veröffentlicht oder zugewiesen wird, da bei der erstmaligen Installation die Transform Files abgearbeitet werden und nicht mehr nachträglich. Bevor nicht alle .mst-Dateien zugeordnet sind, dürfen Sie nicht auf OK klicken. Ansonsten müssen Sie später entsprechende Aktualisierungen zuweisen.

Die folgende Tabelle gibt eine kurze Zusammenfassung über die Unterschiede zwischen veröffentlichten und zugewiesenen Applikationen in Bezug auf Verfügbarkeit, Installation usw.

Kriterium	An Computer zugewiesene Applikation	An Benutzer zugewiesene Applikation	Veröffentlichte Applikation
Verfügbarkeitszeitpunkt des Pakets	Nächster Start des Computers	Nächste Anmeldung des Benutzers	Nächste Anmeldung des Benutzers
Installationsmethode	Automatische Installation	Installation über Verknüpfung in Startmenü oder Desktop	Applikation kann über SYSTEMSTEUERUNG/SOFTWARE gewählt werden
Deinstallationsmöglichkeit für den Benutzer	Keine; nur mit lokalen Administratorrechten	Deinstallation und Neuinstallation möglich	Deinstallation möglich; kann über SYSTEMSTEUERUNG/SOFTWARE jederzeit neu installiert werden

Tabelle 20.8: Unterschiede zwischen zugewiesener und veröffentlichter Software

- Nachdem Sie die gewünschte *.msi*-Datei ausgesucht haben, wird das Paket erstellt. Sie sehen nun die Eigenschaftsseite des Pakets. Bestätigen (oder ändern) Sie dann den vorgegebenen Namen des Pakets. Für Office 2000 lautet dieser *Microsoft Office 2000 Professional*.



Abbildung 20.60: Die Eigenschaften eines Installationspakets

20.5.5 Allgemeine Einstellungen an den Applikationspaketen

Als Nächstes legen Sie nun noch einige allgemeine Einstellungen für die Pakete fest. Dazu zählen die mit den einzelnen Applikationen verknüpften Dateitypen sowie das Zusammenfassen der Applikationen in bestimmte Anwendungskategorien. Um diese beiden Einstellungen vorzunehmen, öffnen Sie den Knoten SOFTWAREEINSTELLUNGEN / SOFTWAREINSTALLATION in der Benutzer- bzw. Computerkonfiguration und öffnen über das Kontextmenü dessen EIGENSCHAFTEN.

Registerkarte Dateierweiterungen

Sie haben die Möglichkeit, bestimmten Dateitypen Anwendungen zuzuweisen, die innerhalb des GPO bereitgestellt sind, die automatisch installiert werden, wenn der Benutzer eine Datei mit einer derartigen Endung anklickt. Werden über ein GPO mehrere Applikationen bereitgestellt, die den jeweiligen Dateityp öffnen können, so können Sie auch die Priorität für die Installation dieser Applikationen treffen.

Auf der Registerkarte DATEIERWEITERUNGEN sehen Sie eine Liste aller vorhandenen Pakete (siehe Abbildung 20.61). Wählen Sie nun aus der Listbox DATEIERWEITERUNG AUSWÄHLEN die gewünschte Dateiendung aus. Sobald der Benutzer ein Dokument mit der gewählten Dateiendung öffnet, wird die gewählte Applikation ausgeführt.

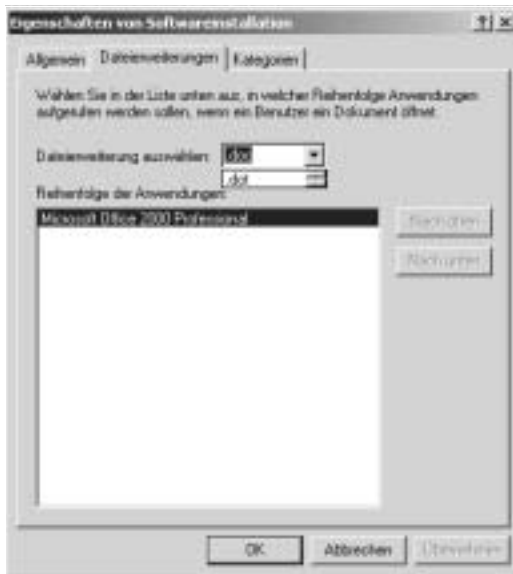


Abbildung 20.61: Die Dateierweiterungen bestimmen, die mit einer Applikation verknüpft sind

Sind mehrere Pakete in dem GPO vorhanden, können Sie über die Schaltflächen NACH OBEN und NACH UNTEN festlegen, welche Applikation automatisch installiert werden soll.

Sie müssen zwar diese Einstellungen nicht treffen, es ist aber in jedem Fall sinnvoll, dies zu tun, da der Benutzer sonst beim Öffnen eines unbekannten Dateityps das Dialogfeld ÖFFNEN MIT erhält. Dabei müsste er dann aus den auf dem Computer bereits vorhande-

nen Programmen eines auswählen, mit dem die Datei geöffnet werden soll. Dies kann jedoch schnell zu Problemen führen, wenn er nicht weiß, welches Programm für welche Dateien geeignet ist, oder noch kein kompatibles Programm installiert ist.



Diesen ÖFFNEN MIT-Dialog erhalten alle Benutzer, denen Applikationen nur veröffentlicht, aber nicht zugewiesen sind, sofern nicht für diese eine automatische Installation festgelegt ist.

Registerkarte Kategorien

Auf der Registerkarte KATEGORIEN können Sie für die Applikationspakete Kategorien anlegen, in denen sie zusammengefasst werden. Unter diesen Oberkategorien finden die Benutzer ihre veröffentlichten Applikationen unter SYSTEMSTEUERUNG/SOFTWARE. Sie können zur Übersichtlichkeit Kategorien wie Office-Pakete, Grafiksuiten oder Utilities einrichten.

Um eine neue Kategorie einzurichten, klicken Sie auf HINZUFÜGEN und geben einen Namen ein. Über ENTFERNEN können nicht mehr benötigte Kategorien wieder gelöscht werden.

Die hier erstellten Kategorien gelten für die gesamte Domäne und nicht nur für das aktuelle GPO. Somit müssen diese Oberkategorien nur ein einziges Mal festgelegt werden.

20.5.6 Bearbeiten und Entfernen von Applikationspaketen

Nachdem Sie ein Paket für die Verteilung bereitgestellt und die allgemeinen Paketoptionen konfiguriert haben, können Sie nun zu jedem einzelnen Paket spezielle Eigenschaften einstellen. Dazu zählen etwa das Zuweisen zu Kategorien, Aktualisierungs- und Deinstallationseinstellungen oder die Sicherheitseinstellungen.

Wenn Sie die Eigenschaften eines vorhandenen Applikationspaketes öffnen, finden Sie die sechs Registerkarten ALLGEMEIN, BEREITSTELLUNG VON SOFTWARE, AKTUALISIERUNGEN, KATEGORIEN, ÄNDERUNGEN und SICHERHEITSEINSTELLUNGEN.

Registerkarte Allgemein

Hier sehen Sie die allgemeine Zusammenfassung (siehe Abbildung 20.60) mit Informationen wie Versionsnummer, Herausgeber oder Sprache des Applikationspaketes.

Registerkarte Bereitstellung von Software

Hier können Sie die Optionen für die Bereitstellung von Software einstellen oder Änderungen gegenüber der Standardeinstellung (siehe Abbildung 20.59) vornehmen. Sie können hier zwischen VERÖFFENTLICHT und ZUGEWIESEN umschalten.

Im Bereich BEREITSTELLUNGSOPTIONEN können Sie Eigenschaften der Installation und Bereitstellung festlegen. Dabei ist die erste Option AUTOMATISCH INSTALLIEREN, WENN DIE DATEIERWEITERUNG AKTIVIERT WIRD bereits aktiviert (und kann auch nicht deaktiviert werden), wenn Sie, wie in Kapitel 20.5.5 beschrieben, bestimmte Dateierweiterungen mit festen Applikationen verknüpft haben.

Mit der Option DIESE ANWENDUNG DEINSTALLIEREN, WENN SIE AUSSERHALB DES VERWALTUNGSBEREICHES LIEGT bestimmen Sie, ob eine Applikation deinstalliert werden soll, wenn sich der Computer bzw. Benutzer an einem Standort oder einer Domäne bzw. OU befindet, für die das GPO mit dieser Applikation nicht zugewiesen wurde. Die Deinstallation erfolgt in diesem Fall beim Computerstart oder bei der Benutzeranmeldung.

Über DIESES PAKET IN DER SYSTEMSTEUERUNG UNTER SOFTWARE NICHT ANZEIGEN können Sie dort ein Paket verbergen, das der Benutzer nicht selbstständig installieren soll.

Im Bereich BENUTZERBEREICHEN FÜR DIE INSTALLATION geben Sie an, ob der Benutzer nur die standardmäßigen (z.B. Zielpfad) oder alle Fenster und Dialoge während der Installation sehen darf.

Über die Schaltfläche ERWEITERT können Sie festlegen, ob die Spracheinstellungen ignoriert werden sollen oder nicht. Wenn Sie beispielsweise ein deutsches Windows-Betriebssystem verwenden, können Sie für ein englischsprachiges Applikationspaket bestimmen, ob dieses trotz der Sprachdiskrepanz bereitgestellt werden soll oder nicht. Ferner können Sie angeben, was mit einer Applikation geschehen soll, die bereits auf dem Computer installiert ist, aber nicht durch die Gruppenrichtlinie zugewiesen wurden. Diese Applikationen können deinstalliert werden.



Diese Einstellung gilt jedoch nur, wenn Sie z.B. Office 2000 bereits früher per Hand installiert haben und dasselbe Produkt nun zuweisen. Sie haben nicht die Möglichkeit, andere bereits vorhandene unerwünschte Software zu deinstallieren wie z.B. Moorhühner.

Registerkarte Aktualisierungen

In dieser Sektion konfigurieren Sie die Optionen für die Aktualisierung oder Deinstallation des Applikationspaketes. Bei einem Aktualisierungspaket handelt es sich entweder um eine neuere Version der Applikation oder um eine Applikation, die die bisher verwendete ersetzen soll. So kann Office 2000 durch die neuere Version von Office XP ersetzt werden. Das Aktualisierungspaket wird, wie in Kapitel 20.5.2 und Kapitel 20.5.3 beschrieben, im Active Directory bereitgestellt. Um ein Aktualisierungspaket hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Wählen Sie aus der Liste der Pakete unter Softwareinstallation in der mmc das Paket aus, das zur Aktualisierung dienen soll – *nicht das zu aktualisierende Paket*. Wählen Sie aus dessen Eigenschaften die Registerkarte AKTUALISIERUNGEN.
2. Klicken Sie nun auf HINZUFÜGEN, um das Aktualisierungspaket dem ursprünglichen Paket hinzuzufügen. Sie erhalten das Fenster AKTUALISIERUNGSPAKET HINZUFÜGEN. Wählen Sie hier aus, ob sich das zu aktualisierende Paket im aktuellen oder in einem anderen GPO befindet. Befindet es sich in einem anderen GPO, wird dieses über DURCHSUCHEN ermittelt. Sie sehen in der Liste ZU AKTUALISIERENDES PAKET alle im GPO vorhandenen Applikationspakete.
3. Markieren Sie das gewünschte Paket. Entscheiden Sie dann, was bei der Installation der Aktualisierung mit dem ursprünglichen Paket geschehen soll. Aktivieren Sie dazu die Checkbox BESTEHENDES PAKET DEINSTALLIEREN, AKTUALISIERUNGSPAKET INSTALLIEREN oder PAKET KANN ÜBER DAS BESTEHENDE PAKET AKTUALISIEREN. Die

erste Option ist zu wählen, wenn Sie ein komplett neues Programmpaket eines anderen Herstellers installieren möchten. Diese Option wäre zu wählen, wenn Sie alle Microsoft Office-Anwendungen etwa durch eine Version von Star Office ersetzen möchten. Die zweite Option ist zu wählen, wenn das vorhandene Paket durch eine neuere Version derselben Anwendung ersetzt werden soll. Sie können so Office 2000 durch Office XP aktualisieren. Es bleiben dabei alle Einstellungen der Anwendung erhalten. Klicken Sie dann auf OK.

4. Aktivieren Sie dann auf der Registerkarte AKTUALISIERUNGEN die Checkbox BESTEHENDE PAKETE AKTUALISIEREN. Damit ist der Aktualisierungsvorgang verbindlich und wird ab sofort für alle Benutzer und Computer angewendet.

Registerkarte Kategorien

Wie bereits in Kapitel 20.5.5 beschrieben, sollten Sie aus Gründen der Übersichtlichkeit Kategorien für die Applikationen einrichten. Sie können hier nun aus der Liste VERFÜGBARE KATEGORIEN die passende auswählen und der Applikation über AUSWÄHLEN zuweisen. Sie können zwar mehrere Kategorien zu einer Applikation zuweisen, aber dadurch könnte die Einteilung wieder undurchsichtig werden, wenn der Benutzer dieselbe Applikation in verschiedenen Kategorien findet.

Registerkarte Änderungen

Diese Registerkarte wird bereits geöffnet, wenn Sie bei der Bereitstellung der Software die Option ERWEITERTE METHODE VON „VERÖFFENTLICHT“ ODER „ZUGEWIESEN“ wählen (siehe Abbildung 20.59). Hier weisen Sie den standardmäßigen Einstellungen der Windows Installer-Pakete Konfigurationsänderungen über .mst-Dateien (Transform Files) zu. Weitere Hinweise zu *.mst-Dateien sowie ein Beispiel für deren Erstellung finden Sie in Kapitel 20.7.



Die Änderungen, die über die .mst-Dateien vorgenommen werden, müssen bereits bei der Bereitstellung des Pakets konfiguriert werden. Sie müssen konfiguriert sein, bevor das Paket zugewiesen oder veröffentlicht wird.

1. Um Änderungen für ein standardmäßiges Paket zu erstellen, wählen Sie aus dem Kontextmenü aus der Softwareinstallation den Menüpunkt NEU / PAKET. Wählen Sie aus der Liste der vorhandenen Windows Installer-Pakete die gewünschte .msi-Datei aus und klicken auf ÖFFNEN.
2. Wählen Sie im Dialogfeld SOFTWARE BEREITSTELLEN die dritte Option aus. Wählen Sie dann im Dialogfeld EIGENSCHAFTEN VON (APPLIKATIONSNAME) die Registerkarte ÄNDERUNGEN.
3. Klicken Sie auf HINZUFÜGEN, um eine .mst-Datei zum vorhandenen Installer-Paket hinzuzufügen. Falls Sie mehrere .mst-Dateien hinzufügen möchten, wiederholen Sie diesen Schritt. Über ENTFERNEN können bereits gewählte .mst-Dateien auch wieder gelöscht werden.

4. Haben Sie mehrere .mst-Dateien ausgewählt, so können Sie deren Reihenfolge zum Installieren der Änderungen über die Schaltflächen NACH OBEN und NACH UNTEN festlegen. Klicken Sie dann auf OK.

Registerkarte Sicherheitseinstellungen

Damit die Applikationspakete den Benutzern korrekt zugewiesen werden können, müssen Sie die geeigneten Sicherheitseinstellungen treffen. Sie müssen allen Benutzern, denen diese Applikation zugewiesen oder veröffentlicht werden soll, die Berechtigung Lesen zuweisen. Damit die Pakete von Administratoren bearbeitet werden können, müssen diese über die Berechtigung Vollzugriff verfügen.

Entfernen von Applikationspaketen

Wenn bestimmte Applikationspakete nicht mehr benötigt werden, sollten Sie diese entfernen. Um ein Paket zu entfernen, öffnen Sie in der Benutzer- oder Computerkonfiguration den Knoten SOFTWAREEINSTELLUNGEN / SOFTWAREINSTALLATION. Wählen Sie dort das zu entfernende Paket aus und aus dessen Kontextmenü ALLE TASKS / ENTFERNEN.

Sie erhalten das Dialogfeld SOFTWARE ENTFERNEN. Hier können Sie zwei verschiedene Arten der Deinstallation festlegen:

1. SOFTWARE SOFORT VON BENUTZERN UND COMPUTERN DEINSTALLIEREN: Hiermit wird die Applikation endgültig vom Computer deinstalliert. Die Deinstallation wird beim nächsten Start des Computers bzw. der nächsten Benutzeranmeldung vorgenommen. Die Applikation kann dann nicht mehr verwendet werden und steht dem Benutzer auch nicht mehr zur erneuten Installation bereit. Auch wenn er eine Datei mit der zugeordneten Dateiendung öffnet, wird die Applikation nicht mehr automatisch installiert. Sie sollten eine Applikation erst auf diese Weise entfernen, wenn Sie eine neue Applikation an die Benutzer / Computer verteilt haben, die dem Funktionsumfang der alten Applikation entspricht.
2. BENUTZER DÜRFEN DIE SOFTWARE WEITERHIN VERWENDEN, ABER NEUINSTALLATIONEN SIND NICHT ZUGELASSEN: Wenn Sie diese Option wählen, wird die Applikation selbst nicht vom Computer entfernt, sondern lediglich der Eintrag unter SYSTEMSTEUERUNG / SOFTWARE, damit der Benutzer sie nicht erneut installieren kann. Eine erneute Installation ist auch nicht über das Öffnen von Dateien mit der jeweiligen Dateiendung möglich. Damit ist die Benutzung sichergestellt, bis eine endgültige Deinstallation erfolgt.

Erneutes Bereitstellen einer Applikation

Im Kontextmenü jeder Applikation können Sie über ALLE TASKS / ANWENDUNG ERNEUT BEREITSTELLEN diese nochmals bereitstellen. Dabei wird die Applikation auf allen Computern, auf denen sie bereits vorhanden ist, neu installiert. Dieser Vorgang kann erforderlich werden, wenn Sie einer Applikation nicht alle oder nicht die korrekten .mst-Dateien zugewiesen und sie somit zu früh bereitgestellt haben, sodass sie bereits auf einigen Computern installiert wurde.

20.5.7 Strategie zur Konfiguration der Softwareinstallation

Dieses Kapitel beschreibt einige allgemein gültige Strategien zur Implementierung und Konfiguration der Richtlinie Softwareinstallation.

Grundsätzlich sollten Sie die Software, die Sie bereits in der Designphase (siehe Kapitel 6) zu Standards erklärt haben, für die Benutzer- und Computerkonfiguration zuteilen. Sind im Unternehmen fast ausschließlich die Benutzer an festen Arbeitsplätzen tätig, so sollten Sie die Software den entsprechenden Computern zuweisen. Auf diese Weise wird die Software automatisch installiert, und die Benutzer können keinen Einfluss darauf nehmen.

Sie sollten andernfalls den Benutzern alle Softwarepakete zuweisen, die sie für ihre Arbeit benötigen. Damit wird sichergestellt, dass die Applikation entweder aus einer Desktop-Verknüpfung oder beim Öffnen einer Datei des festgelegten Dateityps installiert wird. Veröffentlichen sollten Sie nur solche Applikationen, die der Benutzer nicht zwingend für seine Arbeit benötigt, die aber unter Umständen nützlich sind und dann schnell zur Hand sein sollten. Informieren Sie die Benutzer darüber, wie sie über Systemsteuerung – Software optionale Software installieren können. Dies sollte zahlreichen Anfragen an den Support vorbeugen. Zur besseren Auffindbarkeit von Applikationen unter SOFTWARE sollten Sie die Applikationen in Kategorien unterteilen.

Weiterhin sollten Sie ein Windows Installer-Paket in einem GPO nur ein einziges Mal zuweisen oder veröffentlichen. Es macht wenig Sinn, dieselbe Applikation einmal in der Computerkonfiguration den Computern und einmal in der Benutzerkonfiguration den Benutzern zuzuweisen. Sie erhalten zwar keine Fehlermeldung, aber dadurch wird der Anmeldevorgang der Benutzer an dem Computer unnötig verlangsamt.

Wenn Sie sich für den Einsatz einer neuen Software entscheiden, sollten Sie immer zuerst prüfen, ob die Applikation bereits als Windows Installer-Paket vorliegt oder nicht. Unter Umständen kann die Repaketierung sehr aufwändig werden. Auch die Bereitstellung von Resource Kits zu Applikationen zur Erstellung von .mst-Dateien kann ein wichtiger Faktor für den Erwerb einer Applikation sein.

20.6 Windows Installer-Technologie und Repaketierung

In diesem Kapitel werden die Grundlagen der Windows Installer-Technologie sowie der Repaketierung beschrieben. Diese beiden Themen sind als Grundlagenwissen zur Softwareverteilung nahezu unentbehrlich.

20.6.1 Windows Installer-Technologie

Mit Office 2000 wurde von Microsoft die erste Applikation veröffentlicht, die den Windows Installer als standardmäßiges Setup-Programm benutzt. Damit das Setup ordnungsgemäß ausgeführt werden kann, muss auf den Zielcomputern der Windows Installer vorhanden sein und als Dienst laufen. Den Windows Installer gibt es in verschiedenen Versionen. Folgende Betriebssysteme enthalten bereits nativ den Installer bzw. müssen eine entsprechende Version nachinstallieren:

Betriebssystem	Nativ vorhandene Version des Windows Installers	Folgende Versionen können nachinstalliert werden
Windows XP/ Windows Server 2003	2.0	–
Windows 2000	1.1	kann nicht die Version 1.2 nachinstallieren, nur Version 2.0
Windows ME	1.2	2.0
Windows NT SP3	–	1.x
Windows NT SP6	–	1.x, 2.0
Windows 98	–	1.x, 2.0
Windows 95	–	1.x, 2.0

Tabelle 20.9: Übersicht über die Windows Installer-Versionen

Installationspakete für den Windows Installer in der Version 2.0 finden Sie unter folgenden Adressen:

Für Windows NT 4, SP6 und Windows 2000:

<http://www.microsoft.com/downloads/release.asp?releaseid=32832>

Für Windows 95, Windows 98 und Windows Me:

<http://www.microsoft.com/downloads/release.asp?releaseid=32831>

Die Installationspakete des Windows Installers enthalten die Executables *INSTMSI.EXE* sowie *INSTMSIW.EXE*. *INSTMSI.EXE* installiert den Windows Installer-Dienst unter Windows 9x, *INSTMSIW.EXE* unter Windows NT. Der laufende Installer-Dienst auf den Clients wird von der *msiexec.exe* ausgeführt.

Die Installation erfolgt auf der Basis von *msi*-Dateien. Die Dateierendung *.msi* bedeutet Managed Software Installation. Jede *msi*-Datei entspricht dabei einer kleinen relationalen Datenbank. In ihr ist der Zielzustand enthalten, wie er nach der Installation auf dem Client vorliegen soll. Dies ist der sog. Post-Install-State. Dieser Zustand wird nicht wie bei herkömmlichen Setup-Programmen durch ein Installationsskript erreicht, sondern durch die Anwendung von bestimmten Regeln. Dieser definierte Zielzustand wird dann auf dem entsprechenden Computer gespeichert. Treten aufseiten des Computers Änderungen am ursprünglich definierten Zielzustand auf, z.B. durch das versehentliche Löschen von Dateien, so wird der Post-Install-State durch den Windows Installer wiederhergestellt. Dieser automatische Reparaturmechanismus ist bei einem herkömmlichen Setup nicht gegeben.

Wird eine Windows Installer-Installation nicht erfolgreich abgeschlossen, erfolgt ein automatisches Rollback auf den Zustand vor der Installation des missglückten *msi*-Paketes. Ein weiteres Feature der Windows Installer-Technologie ist die Installation der Software bei Bedarf. Das heißt, dass bestimmte weniger häufig benutzte Features erst dann installiert werden, wenn der Benutzer sie tatsächlich das erste Mal benötigt.

Auch für die Definition von verschiedenen *msi*-Paketen bietet die Windows Installer-Technologie eine Möglichkeit: Sie können ein *msi*-Paket, z.B. Office 2000, durch den Ein-

satz von mst-Dateien mit speziellen Features konfigurieren. Die mst-Dateien werden auch als Transform Files bezeichnet. Das Transform wird einmalig bei der ersten Installation des msi-Pakets angewendet. Nach der Installation des Basis-msi-Pakets können Sie keine weiteren Transform Files zur Aktualisierung nachinstallieren. Sie können für ein msi-Paket beliebig viele Transform Files erstellen. Das Erstellen von mst-Dateien ist zwar optional, wird aber sicherlich in den meisten Fällen durchgeführt werden.

Um ein msi-Paket verteilen zu können, muss zunächst ein administratives Setup der entsprechenden Applikation durchgeführt werden. Dies geschieht mit dem Parameter /a in der Setup-Anweisung (siehe Kapitel 20.5.2). Dabei wird quasi der Inhalt der Applikations-CD an einen bestimmten Ort im Netzwerk kopiert, von dem aus später die Installation auf die Clients erfolgt. Das Standard-msi-Paket enthält dabei alle Features, die bei einer standardmäßigen Installation auch enthalten sind. Wollen Sie auf das Basispaket Änderungen anwenden, erstellen Sie mithilfe eines Resource Kits ein oder mehrere Transform Files. Diese werden über die Gruppenrichtlinie dem msi-Paket zugewiesen und bei der ersten Installation auf dem Client angewendet.

20.6.2 Repaketierung

Die Repaketierung von Applikationen kann aus verschiedenen Gründen erfolgen. Der häufigste Grund dürfte wohl die Anpassung des Setups sein. Standardmäßig erhält der Benutzer bei der Installation eine Reihe von Dialogboxen, in denen er den Installationspfad oder Features festlegen kann. Diese Möglichkeit soll dem Benutzer jedoch in den meisten Fällen genommen werden. Idealerweise läuft der Installationsprozess im Hintergrund ab, wobei der Benutzer nicht eine einzige Dialogbox sieht. Er hat bei dieser Silent Installation keine Möglichkeit einzugreifen. Auch das Bereitstellen einer Applikation, deren Installationsinformationen in einer Setup.exe, nicht aber in einer msi-Datei enthalten sind, erfordert die Repaketierung.

Zur Repaketierung gibt es eine Reihe von Programmen von Drittanbietern. Im Lieferumfang von Windows 2000 Server befindet sich das Programm WinInstall LE der Firma Veritas Software. Sie finden dieses Programm auf der CD im Verzeichnis \VALUEADD\3RDPARTY\MGMT\WINSTLE. Für WinInstall LE wurde von Veritas ein Patch herausgegeben, der einige Programmfehler behebt. Den Patch finden Sie zum Download unter folgender Adresse:

<http://seer.support.veritas.com/docs/229403.htm>

Allerdings gehört WinInstall LE nicht mehr zum Lieferumfang des Windows Servers 2003.

Beim Repaketieren einer Applikation wird ein neues Windows Installer-Paket aus den Änderungen gebildet, die während der Installation auf dem Computer durchgeführt werden, wie etwa das Hinzufügen oder Modifizieren von Dateien, Pfaden, Registry-Einträgen usw. Die meisten Programme verwenden dazu einen Mechanismus, bei dem der Zustand des Computers vor und nach der Installation miteinander verglichen wird. Aus den sich dabei ergebenden Differenzen wird das neue Paket gebildet. Also darf die zu repaketierende Applikation nicht bereits auf dem Rechner vorhanden sein. Ansonsten würden die Änderungen nicht erkannt und damit das Paket fehlerhaft werden.

20.7 Erstellen einer .mst-Datei (Transform-File)

In diesem Kapitel wird Ihnen das Erstellen eines Transform Files am Beispiel von Office 2000 vorgeführt. Wie bereits mehrfach erwähnt, ist dieser Arbeitsschritt zwar optional, wird aber sicherlich in den meisten Fällen umgesetzt werden. Um bei unserem Beispiel Office 2000 zu bleiben, würden alle Benutzer ohne angepasste Transform Files die standardmäßige Installation des Office-Paketes erhalten. So ist es aber möglich, dass ein Teil der Benutzer unnötig viele Programmteile auf seinem Rechner installiert hat, während anderen Anwendern bestimmte Features nicht standardmäßig zur Verfügung stehen, sondern erst bei Bedarf nachinstalliert werden müssten. Für Benutzer, die lediglich für Korrespondenz zuständig sind, wären z.B. Word und Excel ausreichend, während z.B. den Benutzern der Marketingabteilung zusätzlich PowerPoint zur Verfügung stehen sollte.

Sie erzeugen ein MST-File für Office 2000, indem Sie den *Custom Installation Wizard* starten. Dieser ist eine Komponente des Office 2000 Resource Kit. Dieses ist ausschließlich in englischer Sprache verfügbar. Das Office 2000 Resource Kit können Sie unter folgender Adresse downloaden: <http://www.microsoft.com/office/ork/2000/appndx/toolbox.htm>.

Resource Kits können für eine Reihe von Applikationen bezogen werden. Steht für eine bestimmte Anwendung kein Resource Kit zur Verfügung, so können verschiedene Pakete mit unterschiedlichen Feature-Sets durch Repaketierung erzeugt werden.

Wenn Sie den Wizard starten, können bis zu 17 Fenster erscheinen, die Ihre Daten zur Änderung der Default-Einstellungen abfragen. Die gesammelten Daten werden in dem Transform-File gespeichert, dessen Namen Sie in dem Wizard festlegen. Diese Datei hat die Erweiterung .MST. Sie können ein .MST-File neu erstellen oder ein existierendes .MST-File editieren.



Alle Optionen der individuellen Anpassung im Custom Installation Wizard sind in dem Handbuch zum Office Resource Kit ausführlich beschrieben.

20.8 Verteilen von mmcs

Außer Softwarepaketen können auch mmcs über die Gruppenrichtlinie bestimmten Benutzern oder Gruppen zugewiesen werden, die dann per Remote-Zugriff auf den Domänencontroller zugreifen können. Auch bei diesem Verfahren haben Sie die Möglichkeit, die mmcs zu veröffentlichen oder zuzuweisen.

Um eine mmc veröffentlichen oder zuweisen zu können, muss diese zunächst repaketiert werden, damit sie als msi-Paket über die Softwareinstallation des GPOs verteilt werden kann. Dieses Paket wird wie gewohnt einem Benutzer oder einer Gruppe zugewiesen.

Sofern Sie eine benutzerdefinierte Konsole packen und verteilen möchten, müssen Sie prüfen, ob auf dem Zielrechner, an den die Konsole verteilt werden soll, alle erforderlichen Snap-Ins zur Verfügung stehen oder nicht. Ist ein bestimmtes Snap-In dort nicht verfügbar, so muss auch diese Datei inklusive ihrer Registrierung gepackt und mitverteilt werden. Dabei ist es egal, ob Sie zwei separate Pakete erstellen und verteilen oder das Snap-In mitsamt seiner Registrierung in das mmc-Paket integrieren.

20.9 Fehlersuche bei Gruppenrichtlinien

Dieses Kapitel gibt Ihnen eine Übersicht über häufig auftretende Probleme im Zusammenhang mit den Gruppenrichtlinien. Dazu erhalten Sie zunächst eine Auflistung von Problemen mit Lösungsansätzen. Am Ende dieses Kapitels erhalten Sie Hinweise auf mögliche Fehlfunktionen von Gruppenrichtlinien nach der Migration von Windows NT.

1. Ein GPO-Snap-In kann nicht geöffnet und / oder bearbeitet werden.
 - ▶ Um ein GPO bearbeiten zu können, muss der Benutzer nicht nur über die Berechtigung Lesen, sondern über Vollzugriff auf das entsprechende Objekt verfügen. Lokale Administratoren können nur die lokalen GPOs bearbeiten, während standardmäßig ein Domänen-Admin auch die Active Directory-basierten GPOs bearbeiten kann.
 - ▶ Erhalten Sie die Fehlermeldung, dass das Objekt nicht geöffnet werden konnte, prüfen Sie die Netzwerkverbindung zum Objekt. Es kann auch ein Fehler in der DNS-Konfiguration vorliegen.
2. Die lokalen Richtlinieneinstellungen zeigen keinen Effekt.
 - ▶ Sind weitere Richtlinien auf Standort-, Domänen- oder OU-Ebene definiert, so überschreiben diese die lokalen Einstellungen, sofern sie nicht miteinander kompatibel sind.
3. Die Richtlinieneinstellungen im Active Directory zeigen keinen Effekt.
 - ▶ Wenn ein Benutzer oder Computer nicht die Einstellungen der Richtlinien erhält, kann dies verschiedene Ursachen haben. Prüfen Sie zunächst, ob die gewünschten Einstellungen auch tatsächlich eingestellt sind und die Richtlinie nicht mehr standardmäßig deaktiviert ist.
 - ▶ Bedenken Sie, dass die GPOs in der Reihenfolge lokal, Standort, Domäne und OU abgearbeitet werden. Widersprechen sich dabei Konfigurationen, so wird die ranghöhere Einstellung die darunter liegende überschreiben.
 - ▶ Die Benutzer bzw. Computer müssen sich in einem der Container Standort, Domäne oder OU befinden. Nur auf diese drei Container können Richtlinien angewendet werden.
 - ▶ Prüfen Sie dann, ob das GPO auch auf die OU angewendet wird, in der der Benutzer oder Computer Mitglied ist. Alternativ dazu können Sie das GPO auch auf eine übergeordnete OU oder die Domäne anwenden, sofern die Einstellungen weitervererbt werden.
 - ▶ Prüfen Sie, ob innerhalb einer OU mehrere GPOs definiert worden sind und dabei möglicherweise eines mit der Option „Kein Vorrang“ versehen worden ist. Dieses GPO vererbt seine Einstellungen zwingend. Ansonsten werden die Einstellungen des GPO übernommen, das als letztes abgearbeitet wird. Wenn die Optionen KEIN VORRANG sowie RICHTLINIENVERERBUNG DEAKTIVIEREN beide ausgewählt sind, so wird die Option KEIN VORRANG vorrangig behandelt.
 - ▶ Auch wenn die Gruppenrichtlinien nicht auf der Zugehörigkeit von Benutzern und Computern zu bestimmten Sicherheitsgruppen basieren, so müssen Sie trotzdem sicherstellen, dass ein Benutzer nicht Mitglied einer Gruppe ist, deren Berechtigung GRUPPENRICHTLINIE ÜBERNEHMEN auf Verweigern gesetzt ist. Stattdessen muss für mindestens eine Gruppe das Übernehmen der Gruppenrichtlinie gestattet und Leseberechtigung dafür gegeben sein.

- ▶ Überprüfen Sie, ob der DNS-Server korrekt eingetragen ist. Es muss unbedingt der DNS-Server eingetragen sein, der die gesamten Ressourceneinträge (siehe Kapitel 16.2.5) enthält. Dies ist der DNS-Server, der als erster in der Domäne eingerichtet worden ist. Verwenden Sie keinen DNS-Server unter einem Windows-Betriebssystem, so müssen Sie den Server angeben, auf dem Sie die Ressourceneinträge manuell vorgenommen haben.
4. Spezielle Probleme bei der Softwareinstallation
- ▶ Wenn eine veröffentlichte Anwendung dem Benutzer nicht unter Systemsteuerung/ Software zur Verfügung steht, prüfen Sie, ob die entsprechende Gruppenrichtlinie auf ihn angewendet wurde (siehe vorherige Problemstellung). Stehen in den angewendeten GPOs überhaupt veröffentlichte Applikationen bereit? Außerdem darf es sich bei dem Client um keinen Terminalserver-Client handeln.
 - ▶ Erhält der Benutzer bei der Installation die Fehlermeldung, dass die Applikation nicht im Quellverzeichnis auffindbar ist, so prüfen Sie seine Berechtigungen für die Freigabe des Quellverzeichnisses. Der Benutzer muss über die Berechtigung Lesen für dieses Verzeichnis verfügen. Prüfen Sie auch die Netzwerkverbindung zum Quellverzeichnis.
 - ▶ Erhält der Benutzer die Meldung, dass die Bereitstellung des Pakets vom Active Directory nicht zugelassen wird oder das Paket nicht zur Bereitstellung vorbereitet werden kann, so liegt eine Beschädigung am Installationspaket vor. Prüfen Sie auch die Netzwerkverbindung zum Quellverzeichnis.
 - ▶ Nach der Installation des Pakets finden Sie im Ereignisprotokoll eine Fehlermeldung mit einer der folgenden IDs: 102, 108, 303 oder 1000, und das Paket ist nicht korrekt installiert. Dies deutet darauf hin, dass für den Computer nicht die entsprechenden Berechtigungen für die Freigabe vorliegen, von der aus das Paket installiert werden soll. Das Abarbeiten einer Gruppenrichtlinie für einen Computer geschieht immer im Kontext des System Accounts der Maschine. Stellen Sie also sicher, dass auch der Computer über die Leseberechtigung für die Freigabe verfügt. Vergeben Sie z.B. diese Berechtigung an die Sicherheitsgruppe Domänencomputer.
 - ▶ Treten Fehler bei der Installation auf, wenn sich das Quellpaket in einer DFS-Freigabe befindet, so müssen Sie überprüfen, ob die Berechtigungen sowohl auf Freigabe- als auch auf NTFS-Ebene ausreichend sind. Dies gilt für alle Repliken des DFS-Root-Verzeichnisses und die Freigaben des DFS-Links.
 - ▶ Befindet sich der Server, der die Freigabe für das Installationspaket enthält, in einer anderen Gesamtstruktur als der Client, der das Paket erhalten soll, so ist es möglich, dass Sie im Ereignisprotokoll eine Fehlermeldung mit der ID 1612 (evtl. auch 102) erhalten. Die Berechtigungen für die Freigabe und dem darin enthaltenen Installationspaket sind dem Computer zugewiesen. Allerdings kann sich ein Computer an einem Rechner in einer anderen Gesamtstruktur nur über NTLM, nicht jedoch über Kerberos identifizieren. Dabei findet jedoch keine Überprüfung des Computerkontos statt. Computerkonten benötigen jedoch Kerberos für die Authentifizierung, also kann auf das Installationspaket nicht zugegriffen werden. Um dieses Problem zu beheben, müssen Sie die Berechtigungen den entsprechenden Benutzern zuweisen. Dasselbe Phänomen tritt auch auf, wenn sich die Ressource auf einem Cluster-Server (NT oder 2000) befindet. Dieser unterstützt ebenfalls nur die NTLM-Authentifizierung.

- ▶ Wird die Software nicht automatisch installiert, sobald sie für das Öffnen eines bestimmten Dokuments benötigt wird, so sind die Optionen für die Softwareinstallation nicht auf AUTOMATISCH INSTALLIEREN gesetzt.
5. Spezielle Probleme bei der Softwaredeinstallation
- ▶ Wird eine Applikation wieder deinstalliert und entfernt dabei nicht alle Bestandteile, so etwa Verknüpfungen auf dem Desktop oder in der Taskleiste, so sind diese nach der Installation vom Benutzer selbst angelegt worden. Mit der Deinstallation werden nur die zur Applikation gehörenden Komponenten wieder entfernt, die bei der Installation eingespielt worden sind.

Ein sehr nützliches Programm zur Analyse der einzelnen Gruppenrichtlinieneinstellungen ist das Support-Tool GPResult.exe. Mit GPResult haben Sie die Möglichkeit, die Effekte der GPO-Einstellungen für einen Computer und /oder angemeldeten Benutzer zu sehen. Das Programm GPResult können Sie unter folgender Adresse downloaden:

<http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp>

Weitere Hinweise zur Funktion dieses Support-Tools finden Sie in Kapitel 23.1.12.

20.9.1 Inkonsistenz bei Gruppenrichtlinien nach der Migration

Möglicherweise werden Sie auf Inkonsistenzen bei der Durchsetzung von Gruppenrichtlinien bei Windows 2000-Clients stoßen, nachdem Sie die Domänencontroller von Windows NT migriert haben. Das im Folgenden beschriebene Problem tritt nur auf, wenn Sie zunächst alle Clients auf den Stand von Windows 2000 gebracht haben, die Domänencontroller zunächst aber noch unter Windows NT betrieben wurden.

Da die Windows NT-Domänencontroller noch keine Gruppenrichtlinien unterstützen, können die Windows 2000-Clients zunächst auch keine Richtlinien empfangen und verarbeiten. Die Domänencontroller unter Windows NT werden lediglich zur Authentifizierung benutzt. Sobald Sie aber nun den Windows NT-PDC auf Windows 2000 migrieren, verwenden die Windows 2000-Clients nur noch diesen zur Authentifizierung und nicht mehr die vorhandenen NT-BDCs. Da die Windows 2000-Clients mit diesem Verhalten jedoch schnell den einzigen Windows 2000-Domänencontroller in die Knie zwingen würden, wurde im Servicepack 2 für Windows 2000 ein entsprechendes Fix eingebaut. Sobald die Clients mit dem Servicepack versorgt sind, wird ihnen durch das Servicepack vorgespielt, dass der Windows 2000-Domänencontroller in Wirklichkeit immer noch ein NT-Domänencontroller sei. Damit wird die Last wieder gleichmäßig auf alle Domänencontroller umgelegt.

Allerdings bringt dieses Fix eine Tücke mit sich: Da die Windows NT-Domänencontroller nicht über Features wie Lastenausgleich verfügen, melden sich die Clients bei einem beliebigen Domänencontroller an. Dies geschieht nach dem Zufallsprinzip und nicht wie bei einem Windows 2000-Controller, dass sich ein Client zunächst bei einem Domänencontroller an seinem eigenen Standort verifiziert. Da nun den Clients vorgespielt wird, alle Domänencontroller seien noch Windows NT-Domänencontroller, so führen sie selbstverständlich auch ihre Anmeldung nach dem Zufallsprinzip aus. Und da ihnen für die Anmeldung ein in Wirklichkeit realer Windows 2000-Domänencontroller sowie der Rest an NT-BDCs zur Verfügung steht, kann ein Client einmal seine Gruppenrichtlinieneinstel-

lungen erhalten, wenn er sich zufällig bei dem Windows 2000-Domänencontroller anmeldet, ein anderes Mal aber nicht, wenn er die Anmeldung an einem NT-BDC vornimmt. Dies führt selbstverständlich zu Inkonsistenzen in den GPOs auf den Clients.

Um dieses Problem zu beheben, stehen Ihnen bis zur Migration aller Domänencontroller zwei Möglichkeiten offen. Wenn bereits der PDC auf Windows 2000 aktualisiert wurde, bleibt Ihnen nichts anderes übrig, als sämtliche Windows 2000-Clients aus der Domäne zu entfernen und dann wieder hinzuzufügen. Diesen Arbeitsschritt können Sie sich mit dem Support-Tool NETDOM vereinfachen (siehe Kapitel 23.1.17). Damit identifizieren sie sich nur an den Windows 2000-Domänencontrollern und ignorieren die bestehenden NT-BDCs, führen also genau wieder das aus, was sie vor dem Einspielen des SP2 bereits getan haben. Allerdings sollten Sie diesen Schritt erst ausführen, wenn Sie genügend Windows 2000-Domänencontroller bereitgestellt haben.

Sofern Sie den PDC noch nicht auf Windows 2000 aktualisiert haben, sollten Sie auf diesem vor der Aktualisierung einen Registry-Schlüssel hinzufügen.

Im **Zweig** `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters` fügen Sie einen neuen Schlüssel vom Typ **DWORD-Wert** mit dem Namen `NT4Emulator` und dem Wert `1` ein. Wiederholen Sie diesen Schritt auch an jedem BDC, bevor er auf Windows 2000 aktualisiert wird. Durch das Hinzufügen dieses Schlüssels behandeln die Clients den aktualisierten Domänencontroller auch weiterhin wie einen NT-PDC. Da sie auf diese Art und Weise keine Gruppenrichtlinien beziehen, können auch diesbezüglich keine Inkonsistenzen entstehen. Haben Sie alle Domänencontroller aktualisiert, können Sie den Schlüssel löschen oder den Wert auf `1` setzen und den Domänencontroller neu starten. Sobald sich die Clients nun identifizieren, sehen sie ihn als Windows 2000-Domänencontroller an und beziehen von diesem auch in korrekter Weise die Gruppenrichtlinien. Dieser Weg ist weniger arbeitsaufwändig als das Entfernen und erneute Hinzufügen aller Clients aus bzw. zur Domäne.

21 Administrative Aufgaben am Active Directory

In diesem Kapitel wird Ihnen eine Reihe von Aufgaben und Verwaltungstätigkeiten vorgestellt, die Sie bei Ihrer täglichen Arbeit mit Active Directory durchzuführen haben. Dazu zählen das Veröffentlichen, Verschieben, Löschen und Suchen von Objekten, die Delegierung der Verwaltung, das Sichern und Wiederherstellen von Active Directory sowie die Defragmentierung der Active Directory-Datenbank.

21.1 Veröffentlichen von Objekten und Netzwerkdiensten

Eine wichtige Aufgabe bei der Arbeit mit Active Directory ist das Veröffentlichen von Objekten und Ressourcen, damit die Benutzer auf die entsprechenden Informationen zugreifen können. Objekte wie Benutzer, Computer, Drucker und freigegebene Ordner werden über die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER hinzugefügt. Markieren Sie dazu den Knoten der Domäne und wählen aus dem Kontextmenü NEU / DRUCKER oder NEU / FREIGELEGEBENER ORDNER. Geben Sie dann den UNC-Pfad zum freigegebenen Ordner bzw. Drucker an. Ein Drucker kann jedoch erst im Active Directory veröffentlicht werden, wenn er zuvor installiert wurde. Ein Netzwerkdrucker unter Windows 2000 wird bei seiner Installation automatisch im Active Directory veröffentlicht. Beim Veröffentlichen dieser Objekte werden alle konfigurierten Sicherheitseinstellungen übernommen.

Neben den eben genannten Ressourcen können im Active Directory auch Netzwerkdienste veröffentlicht werden. Hierzu wird die mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE verwendet. Ein gutes Beispiel für die Veröffentlichung sind die Zertifikatsdienste. Wählen Sie in der mmc im Menü ANSICHT den Punkt DIENSTKNOTEN ANZEIGEN. Sie erhalten das Fenster, wie Abbildung 21.1 zeigt. Unter dem Knoten SERVICES finden Sie alle verfügbaren Netzwerkdienste. Um den Zertifikatsdienst zuzuweisen, öffnen Sie den Knoten PUBLIC KEY SERVICES und darunter CERTIFICATE TEMPLATES. Markieren Sie dann die gewünschten Vorlagen und wählen über die Eigenschaften des Kontextmenüs die Sicherheitseinstellungen aus. Die Einstellungen werden für die gewählten Zertifikatsvorlagen in der Domäne gültig.

Sind in das Active Directory zusätzliche Dienste, wie etwa Microsoft Exchange, integriert, so können auch diese ihre Einstellungen im Verzeichnis veröffentlichen.

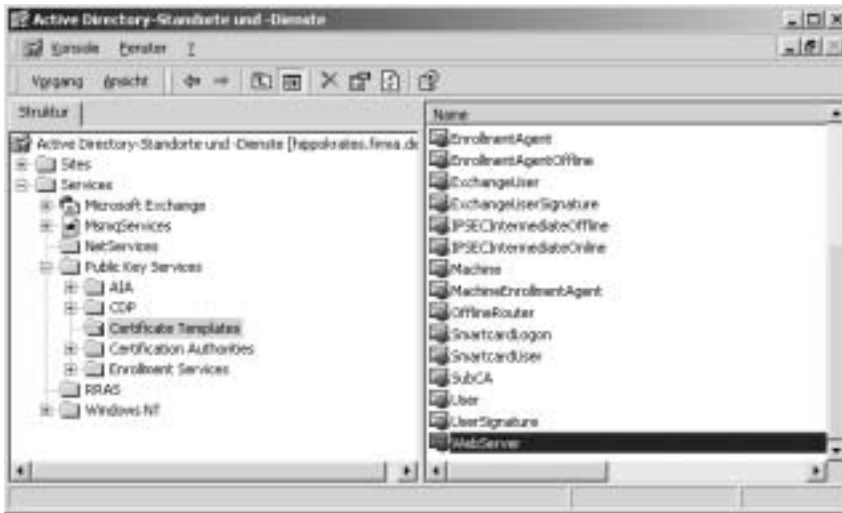


Abbildung 21.1: Veröffentlichen von Netzwerkdiensten im Active Directory

Bevor Sie einen Netzwerkdienst im Active Directory veröffentlichen, sollten Sie die folgenden Überlegungen durchführen:

- ▶ Wird der Dienst von einer größeren Anzahl von Clients in der Domäne genutzt? Ist die Anzahl zu gering oder nur auf einen bestimmten Bereich beschränkt, lohnt sich die Veröffentlichung nicht, da durch den intensiven Anspruch an die Domänenressourcen keine Verhältnismäßigkeit gegenüber dem Nutzen für die Clients gegeben ist.
- ▶ Weiterhin sollten Sie nur Dienste veröffentlichen, die nicht allzu häufig ihre Informationen ändern. Beim Start des Dienstes werden bestimmte Informationen an das Active Directory übergeben. Ändern sich diese Informationen, müssen diese zunächst repliziert werden, bevor die Clients die neuen gültigen Werte empfangen können. Aus diesem Grund sollte das Änderungsintervall der Dienste mindestens zwei Replikationsintervalle des Active Directory umfassen oder idealerweise noch höher liegen.

21.2 Die Suchfunktion im Active Directory

Da im Active Directory eine sehr große Anzahl von Informationen gespeichert werden kann, ist auch die Suchfunktion nach Objekten anhand dieser Informationen sehr komplex. Voraussetzung für eine effektive Suche ist jedoch, dass beim Erstellen von Objekten möglichst viele Angaben zu den einzelnen Objekten hinzugefügt werden. In diesem Kapitel werden die umfangreichen Suchfunktionen im Active Directory vorgestellt.

Jeder Benutzer hat die Möglichkeit, über STARTMENÜ/SUCHEN nach Druckern bzw. nach Personen innerhalb des Active Directory zu suchen. Bei der Suche nach Personen kann der Benutzer entweder den Namen oder die E-Mail-Adresse angeben. In der erweiterten Suche kann eine komplexere Abfrage gestartet werden. Es kann in den Kriterien Name, E-Mail, Vorname, Nachname und Organisation mit Abfragen wie *enthält*, *beginnt mit* oder *ist ähnlich mit* nach bestimmten Kriterien gesucht werden.

Auch nach Druckern kann in der gesamten Domäne gesucht werden. Zur Suche können bekannte Kriterien wie Druckernamen oder Modell verwendet werden. Auch funktionelle Komponenten wie Farbdruck, minimale Auflösung oder Duplexfähigkeit können als Suchkriterien benutzt werden. Zusätzlich kann eine benutzerdefinierte erweiterte Suche gestartet werden.

In der mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER kann der Administrator eine komplexe Suche anstoßen. Markieren Sie dazu die Domäne oder einen beliebigen Container und wählen aus dem Kontextmenü SUCHEN. Es kann wahlweise innerhalb jeder Domäne der Gesamtstruktur oder im gesamten Verzeichnis nach Benutzer, Namen, Kontakten, Computern, Druckern, Freigegebenen Ordnern, Organisationseinheiten oder in einer benutzerdefinierten Abfrage gesucht werden. Mit der Suchanfrage wird eine verzeichnisweite LDAP-Suche gestartet.

Bei der Suche über dieses Dialogfeld wird der globale Katalog nach entsprechenden Active Directory-Objekten durchsucht. Über das darin enthaltene Teilreplikat des gesamten Verzeichnisses können Informationen zu Objekten aus allen Domänen der Gesamtstruktur bezogen werden.

Je nach Wahl des zu suchenden Objekts erhalten Sie eine andere Suchmaske mit speziell angepassten Optionen. Für jedes Suchobjekt kann auf der Registerkarte WEITERE zusätzlich eine benutzerdefinierte Suche gestartet werden. Wählen Sie dazu aus der Liste unter FELD das gewünschte Kriterium aus und verbinden es mit einer Bedingung, die erfüllt sein muss, sowie dem zu suchenden Wert. Bei der Eingabe des Wertes kann auch mit Wildcards gearbeitet werden. Unser Beispiel zeigt das Ergebnis der Suchabfrage nach Computern, deren Betriebssystem mit dem Wert Windows beginnt (siehe Abbildung 21.2).

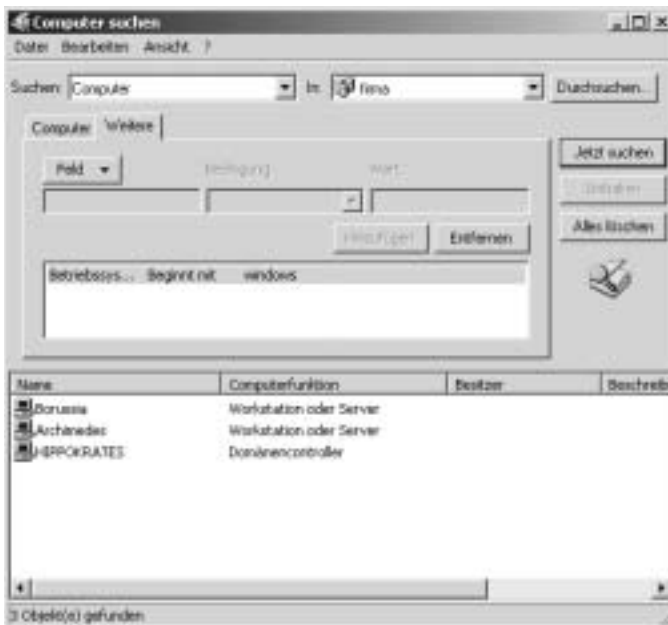


Abbildung 21.2: Die Suchfunktion im Active Directory

21.3 Verschieben von Objekten

Das Verschieben und Löschen von Objekten wird notwendig, wenn sich innerhalb des Unternehmens Änderungen ergeben, z.B. wenn ein Benutzer an einen anderen Standort wechselt oder das Unternehmen verlässt.

Beim Verschieben von Objekten liegt der Hauptunterschied darin, ob das oder die Objekte innerhalb einer Domäne oder zwischen zwei Domänen verschoben werden.

Verschieben innerhalb der Domäne

Um Objekte innerhalb einer Domäne zu verschieben, öffnen Sie die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER.

1. Öffnen Sie den Container, aus dem Sie ein Objekt verschieben möchten. Sie können alle vorhandenen Objekte verschieben. Markieren Sie ein oder mehrere Objekte und wählen aus dem Kontextmenü VERSCHIEBEN. Sie erhalten dann ein neues Fenster mit der Containerstruktur der aktuellen Domäne (siehe Abbildung 21.3).



Abbildung 21.3: Verschieben von Objekten innerhalb einer Domäne

2. Wählen Sie hier den Zielcontainer und klicken auf OK. Die Objekte werden in den neuen Container eingefügt. Nach dem Verschieben erhalten die Objekte die Berechtigungen, die für den neuen Container konfiguriert sind. Die Berechtigungen, die bisher von übergeordneten Containern geerbt wurden, sind nun außer Kraft gesetzt. Es bleiben nur die Sicherheitseinstellungen gültig, die den verschobenen Objekten direkt zugewiesen worden sind.

Verschieben von Objekten zwischen zwei Domänen

Das Verschieben von Objekten zwischen Domänen wird mit den Active Directory-Support-Tools *MOVETREE* (siehe Kapitel 23.1.15) und *NETDOM* (siehe Kapitel 23.1.17) durchgeführt. Mit dem Support-Tool *NETDOM* können Sie jedoch nur Mitgliedsserver und Computer zwischen zwei Domänen verschieben. Diese Methode des Verschiebens kann notwendig werden, wenn Sie die Anzahl der bestehenden Domänen reduzieren möchten, z.B. beim Auflösen von überflüssigen NT-Ressourcendomänen nach der Migration.

Beim domänenübergreifenden Verschieben bleibt die GUID des Objekts bestehen, allerdings ändert sich die SID. Da Windows 2000 – allerdings nur im einheitlichen Betriebsmodus – jedoch eine SID-History pflegt (siehe Kapitel 18.3.5), ist dieser Umstand kein Problem. Beim Verschieben müssen Sie bedenken, dass Sie ein bereits bestehendes Objekt nur unter ein übergeordnetes Objekt in der Zieldomäne verschieben können. Wird eine Organisationseinheit zwischen zwei Domänen verschoben, so bleiben dennoch die damit verknüpften GPOs bestehen und sind weiterhin funktionstüchtig, auch wenn sich die GPOs selbst in einer anderen Domäne befinden als die damit verknüpften OUs.

Mit *MOVETREE* können Sie zwischen Domänen Objekte sowie Container mit Objekten verschieben. Das Verschieben von leeren Containern wird nicht unterstützt. Bei Sicherheitsgruppen gelten die folgenden Regeln beim Verschieben: Lokale und globale Gruppen mit den dazugehörigen Mitgliedern können nur innerhalb einer Domäne verschoben werden, die Gruppen ohne Mitglieder zwischen Domänen. Universelle Gruppen können mitsamt ihren Mitgliedern sowohl innerhalb einer als auch zwischen zwei Domänen verschoben werden. Für alle eben beschriebenen Möglichkeiten besteht die Bedingung, dass sich die Domänen innerhalb derselben Struktur befinden müssen. Alle Objekte, die nicht verschoben werden können, werden in dem Container *LOSTAND-FOUND* abgelegt. Diesen finden Sie über die erweiterten Ansichtsoptionen in der *mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER*.

Um Domänencontroller oder Mitgliedsserver zwischen Standorten zu verschieben, öffnen Sie die *mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE*. Wählen Sie hier den gewünschten Standort und öffnen den Knoten *SERVERS*. Wählen Sie aus dem Kontextmenü des Domänencontrollers oder Mitgliedsservers den Eintrag *VERSCHIEBEN*. Sie erhalten ein neues Fenster mit den verfügbaren Standorten. Wählen Sie den neuen Standort und bestätigen mit *OK*.

21.4 Löschen von Objekten – Tombstoning

Wenn Sie Objekte im Active Directory nicht mehr benötigen, sollten Sie diese löschen. Löschen Sie jedoch nur solche Objekte, die definitiv nicht mehr benötigt werden, z.B. Benutzerobjekte von Mitarbeitern, die nicht mehr der Firma angehören. Haben Sie ein Objekt gelöscht, verliert dieses dabei seine SID. Diese kann auch nicht wiederhergestellt werden, wenn Sie ein gleichnamiges Objekt neu erstellen. Mit dem Löschvorgang werden alle konfigurierten Sicherheitseinstellungen des Objekts ebenfalls entfernt.

In diesem Zusammenhang soll nun auch der Vorgang beschrieben werden, der quasi hinter den Kulissen beim Löschen eines Objekts abläuft. Sobald das Objekt gelöscht ist, haben Sie keine Möglichkeit mehr, das Objekt wiederherzustellen. Allerdings wird es zunächst noch nicht endgültig aus der Active Directory-Datenbank entfernt. Die gelöschten Objekte werden zunächst mit einem sog. *Tombstone* versehen. Dabei handelt es sich um ein Flag, das dem Active Directory anzeigt, dass dieses Objekt gelöscht ist. Dieses Tombstone-Flag wird an alle anderen Domänencontroller repliziert, sodass das Objekt auch auf diesen nicht mehr erscheint.

Die mit einem Tombstone markierten Objekte bleiben standardmäßig 60 Tage in der Active Directory-Datenbank enthalten. Die Datenbank wird alle 12 Stunden dahingehend untersucht, ob sich mit einem Tombstone gekennzeichnete Objekte darin befinden, die älter als

60 Tage sind. Ist dies der Fall, werden diese endgültig gelöscht. Dieser Vorgang wird auch als *Garbage Collection* bezeichnet – quasi die Müllabfuhr für die Active Directory-Datenbank. Das endgültige Löschen der Tombstones wird auch als Online-Defragmentierung der Active Directory-Datenbank bezeichnet. Weitere Hinweise zur Defragmentierung finden Sie in Kapitel 21.8.1. Dabei wird der belegte Platz für neue Objekte in der Datenbank freigegeben, aber die Datenbankdatei wird dadurch nicht kleiner.

Den Standardwert von 60 Tagen für die Lebensdauer des Tombstones können Sie anpassen. Öffnen Sie dazu beispielsweise mit *ADSIEDIT* (siehe Kapitel 23.1.2) das entsprechende Objekt. Auf dem Server Hippokrates in der Domäne *firma.de* lautet der vollständige Pfad: CN=DIRECTORY SERVICE,CN=WINDOWS NT,CN=SERVICES,CN=CONFIGURATION,DC=HIPPOKRATES,DC=FIRMA,DC=DE. Hier können Sie das Attribut *TOMBSTONELIFETIME* anpassen.

Das Tombstoning von gelöschten Objekten ist wichtig für den Wiederherstellungsprozess. Angenommen, Sie führen auf Domänencontroller A ein vollständiges Backup durch. Danach löschen Sie eine Organisationseinheit auf DC A. Diese Änderung wird auch ordnungsgemäß an den Domänencontroller B repliziert. Doch dann bemerken Sie, dass Sie das Objekt nur versehentlich gelöscht haben. Allerdings ist es auf beiden Domänencontrollern nicht mehr aktiv verfügbar. Um das Objekt wiederherzustellen, müssen Sie dann auf dem Domänencontroller A eine autorisierende Wiederherstellung durchführen. Dabei wird die Versionsnummer der im Backup noch vorhandenen OU um 100.000 erhöht. Damit ist die Versionsnummer höher und aktueller als das auf DC B vorhandene OU-Objekt mit dem Tombstone-Flag. Das gelöschte Objekt wird auf DC B durch die Version des ungelöschten Objekts ersetzt.

Bei einer nicht autorisierenden Wiederherstellung wird die Versionsnummer des OU-Objekts auf DC A nicht heraufgesetzt. Da sich das gelöschte Objekt mit dem Tombstone-Flag noch auf DC B befindet und die höhere Versionsnummer trägt – das Löschen wurde ja nach dem Backup durchgeführt –, wird das Objekt auf DC A repliziert und damit automatisch auch auf DC A gelöscht. Weitere Hinweise zur autorisierenden und nicht autorisierenden Wiederherstellung der Active Directory-Datenbank finden Sie in Kapitel 21.7.

21.5 Delegieren der Active Directory-Verwaltung

In diesem Kapitel lernen Sie die Delegierung der Active Directory-Verwaltung kennen. Zunächst wird Ihnen der Delegierungs-Assistent vorgestellt, mit dem Sie die Verwaltung von Objekten komfortabel an andere Benutzer übergeben und somit die Administration dezentralisieren können. Allerdings gibt es auch einige Hürden zu nehmen, wenn die Vergabe der Benutzerrechte nicht wie gewünscht an alle untergeordneten Objekte weitervererbt wird. Weiterhin erhalten Sie Hinweise, wie Sie Berechtigungen für große Mengen an Objekten schnell und effektiv umsetzen können.

21.5.1 Der Assistent zur Verwaltungsdelegierung

Bevor Sie den Assistenten zur Delegierung der Verwaltung starten, sollten Sie sich einen Plan erstellen, welchen Mitarbeitern welche Berechtigungen zum Durchführen welcher Verwaltungsaufgaben zugeteilt werden sollen. Sie können den Benutzern das Erstellen,

Löschen und Bearbeiten von Objekten innerhalb einer OU oder eines anderen Containers zuweisen sowie das Bearbeiten von Objekteigenschaften in einer OU oder einem Container.

Beim Planen sollten Sie die entsprechenden Mitarbeiter zu globalen Gruppen zusammenfassen. So können Sie flexibler Benutzer zu dieser Gruppe hinzufügen oder wieder entfernen als bei der Verwendung von Einzelbenutzern.

1. Sie starten den Delegierungs-Assistenten, indem Sie die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER öffnen und dort aus dem Kontextmenü einer OU oder eines anderen Containers, dessen Verwaltung delegiert werden soll, OBJEKTVERWALTUNG ZUWEISEN auswählen.
2. Nach dem Begrüßungsbildschirm wählen Sie über die Schaltfläche HINZUFÜGEN die Benutzer oder Gruppen aus, denen die Verwaltung übertragen werden soll. Klicken Sie auf WEITER.
3. Dann müssen Sie entscheiden, ob dem Benutzer allgemeine oder benutzerdefinierte Aufgaben zugewiesen werden sollen. Als allgemeine Aufgaben können Sie eine oder mehrere der folgenden Optionen wählen:
 - ▶ Erstellen, Entfernen und Verwalten von Benutzerkonten
 - ▶ Zurücksetzen von Kennwörtern
 - ▶ Lesen aller Benutzerinformationen
 - ▶ Erstellen, Löschen und Verwalten von Gruppen
 - ▶ Ändern der Gruppenmitgliedschaft
 - ▶ Verwalten von Gruppenrichtlinien-Verknüpfungen
4. Haben Sie die allgemeinen Aufgaben ausgewählt, erscheint eine Zusammenfassung, und der Assistent wird beendet. Wurden jedoch die benutzerdefinierten Aufgaben gewählt, müssen Sie weitere Angaben treffen (siehe Abbildung 21.4):

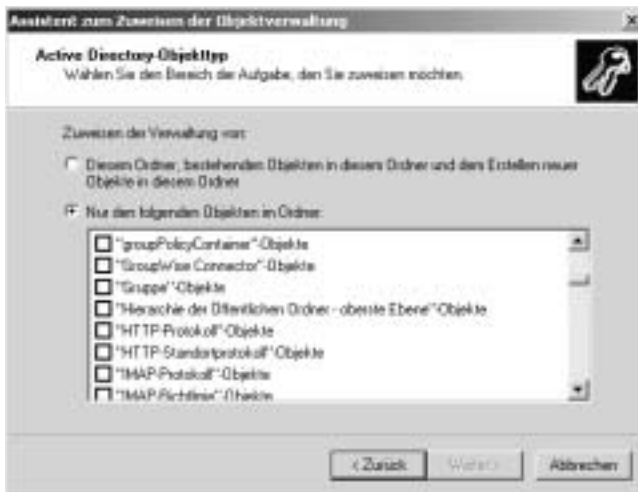


Abbildung 21.4: Zuweisen benutzerdefinierter Aufgaben

5. Sie müssen festlegen, ob die Verwaltungsaufgaben für den aktuellen Ordner mit allen vorhandenen und neu zu erstellenden Objekten gelten sollen oder nur für bestimmte

Objekte im Container. Bei Wahl der zweiten Option können Sie aus allen verfügbaren Active Directory-Objekten die gewünschten wählen. Klicken Sie dann auf WEITER.

6. Im nächsten Schritt werden nun die zu delegierenden Aufgaben ausgewählt. Die Aufgaben sind in folgende drei Bereiche unterteilt:

Berechtigungsart	Beschreibung
Allgemein	Die häufigsten Berechtigungen wie Vollzugriff, Lesen, Schreiben usw.
Eigenschaftsspezifisch	Berechtigungen, die den Attributeigenschaften zugewiesen werden können, Lesen/Schreiben von Attributen.
Erstellen/Löschen der Berechtigungen von bestimmten untergeordneten Objekten	Berechtigungen, die das Erstellen und Löschen von allen verfügbaren Active Directory-Objekten gestatten.

Tabelle 21.1: Die Berechtigungsarten für die Verwaltungsdelegation

Nach Auswahl der Berechtigungen zeigt der Assistent eine Zusammenfassung Ihrer Auswahl an. Sie können noch Änderungen vornehmen oder den Vorgang abschließen. Klicken Sie dazu auf FERTIG STELLEN.

Damit einem bestimmten Benutzer die Delegation der Verwaltung übertragen werden kann, darf in seinem Benutzerkonto nicht die Option KONTO KANN NICHT DELEGIERT WERDEN aktiviert sein. Standardmäßig ist diese Option bei keinem Konto aktiviert. Sie sollten aber die Delegation an Konten unterbinden, deren Benutzer diese Aufgabe nicht erfüllen können. Sollten Sie ansonsten versehentlich ein falsches Konto zur Verwaltung angeben, kann der unversierte Benutzer schnell ein großes Chaos anrichten. Haben Sie bei einem Benutzerkonto die Option KONTO WIRD FÜR DELEGIERUNGSZWECKE VERTRAUT aktiviert (dies ist standardmäßig auch bei keinem Konto der Fall), so kann außer dem Administrator auch der betreffende Benutzer die Verwaltung delegieren. Die Optionen eines Benutzerkontos wurden in Kapitel 18.2.2 besprochen.

Nachdem mit dem Delegierungs-Assistenten die Berechtigungen vergeben worden sind, können Sie diese betrachten, indem Sie folgende Schritte ausführen:

1. Öffnen Sie die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER und aktivieren in dem Menü ANSICHT den Menüpunkt ERWEITERTE OPTIONEN.
2. Wählen Sie die gewünschte OU oder einen anderen Container und wählen aus dem Kontextmenü die Eigenschaften und dort die Registerkarte SICHERHEITSEINSTELLUNGEN. Haben Sie nur standardmäßige Berechtigungen vergeben, werden diese hier angezeigt. Wurden jedoch erweiterte Sicherheitseinstellungen vergeben, so erhalten Sie lediglich einen Hinweis darauf neben der Schaltfläche ERWEITERT. Erst wenn Sie diese Schaltfläche anklicken, werden die speziellen Berechtigungen sichtbar.

21.5.2 Die Berechtigungsvererbung funktioniert nicht immer

Wie Sie im letzten Kapitel erfahren haben, können Sie die Verwaltung komfortabel über den Delegierungs-Assistenten einrichten. In diesem Fall wird es auch zu keinerlei Problemen bei der Vererbung von Berechtigungen kommen. Allerdings kann dieses Phänomen

auftreten, wenn Sie manuell die Sicherheitseinstellungen an einem Active Directory-Container, z.B. einer OU, ändern.



An dieser Stelle sei ausdrücklich darauf hingewiesen, dass Sie beim manuellen Ändern der Sicherheitseinstellungen möglicherweise so tief ins Active Directory eingreifen, dass danach seine Funktion nicht mehr sichergestellt werden kann. Sie sollten also in jedem Fall den Delegierungs-Assistenten benutzen, außer ein besonderer Grund zwingt Sie dazu, manuelle Änderungen vorzunehmen. In diesem Fall sollten Sie zunächst ein Backup der Active Directory-Datenbank vornehmen.

Zum besseren Verständnis nehmen wir den folgenden Fall an: Sie verfügen über eine OU namens Vertrieb. Dieser OU sind die beiden OUs Personalwesen und Bestellabteilung untergeordnet. Für die übergeordnete OU Vertrieb haben Sie dem Benutzer Peter Mustermann die Berechtigungen Lesen und Schreiben erteilt. Diese Berechtigungen wurden manuell zugeordnet und nicht über den Delegierungs-Assistenten zugewiesen. Auf der Registerkarte SICHERHEITSEINSTELLUNGEN für die untergeordnete OU Bestellabteilung ist zwar die Checkbox VERERBBARE ÜBERGEORDNETE BERECHTIGUNGEN ÜBERNEHMEN aktiviert, aber die Berechtigungen für den Benutzer Peter Mustermann wurden dennoch nicht übernommen. Auf der Registerkarte SICHERHEITSEINSTELLUNGEN der OU Bestellabteilung befindet sich der Benutzer Peter Mustermann nicht in der Liste der Benutzer und Gruppen, denen Berechtigungen für dieses Objekt zugewiesen worden sind.

Dieses Verhalten wird bei allen Berechtigungen auftreten, die nicht mit dem Delegierungs-Assistenten zugewiesen worden sind. Aber auch wenn Sie jetzt den Umkehrschluss ziehen, dass Active Directory manuell editierte Berechtigungen generell nicht weitervererbt, wäre dies falsch.

Um dieses Problem zu beheben, müssen Sie auf der Registerkarte SICHERHEITSEINSTELLUNGEN der übergeordneten OU Vertrieb die erweiterten Optionen anklicken. Dort sehen Sie die für den Benutzer zugewiesenen Berechtigungen. Allerdings steht in der Spalte ANWENDEN AUF der Eintrag NUR DIESES OBJEKT. Damit wird die Vererbung verhindert. Klicken Sie auf die Schaltfläche BEARBEITEN und wählen aus, für welche Objekte die Berechtigungen gelten sollen. In unserem Beispiel wäre der Eintrag DIESES OBJEKT UND angemessen. Sobald Sie diesen Schritt durchgeführt haben, erscheint der Benutzer Peter Mustermann in der Liste in den Sicherheitseinstellungen der OU Bestellabteilung. Deaktivieren Sie hier die Checkbox VERERBBARE ÜBERGEORDNETE BERECHTIGUNGEN ÜBERNEHMEN, so verliert der Benutzer wieder alle geerbten Berechtigungen für diese untergeordnete OU.

Normalerweise wird die Registerkarte für die erweiterten Sicherheitseinstellungen nicht in den Eigenschaften eines Objekts eingeblendet. Damit soll sichergestellt werden, dass Sie den Assistenten zur Delegierung benutzen, der für eine Durchsetzung der Vererbung sorgt. Die standardmäßige Berechtigungsvererbung im Active Directory ist also nur auf die standardmäßig zuweisbaren Berechtigungen der Registerkarte SICHERHEITSEINSTELLUNGEN beschränkt.

Weiterhin unterstützt das Active Directory die Berechtigungsvererbung für Gruppenrichtlinien. Weisen Sie einer OU ein bestimmtes GPO zu, so wird dieses an alle untergeordneten OUs vererbt. Es sein denn, für eine spezielle untergeordnete OU ist die Berechtigungsvererbung für das GPO explizit unterbunden.

21.5.3 Objektberechtigungen mit DSACLs bearbeiten

Bei *DSACLs* handelt es sich um ein Befehlszeilenprogramm aus dem Windows 2000 Resource Kit. Sie können damit für eine große Anzahl von Objekten im Active Directory gleichzeitig die Berechtigungen überprüfen oder auch neue Berechtigungen auf die ACLs der Active Directory-Objekte anwenden.

Für jedes Objekt ist der vollständige DN anzugeben, also im Format CN=Benutzername, OU=Organisationseinheit,DC=Domäne, DC=TLD, z.B. CN=PeterMustermann,OU=Vertrieb,DC=Firma,DC=de. Geben Sie keine weiteren Parameter an, werden die aktuellen Berechtigungen des Objekts angezeigt.

Tabelle 21.2 gibt Ihnen einen Überblick über weitere DSACLs-Parameter:

Parameter	Beschreibung
/a	Zeigt alle Sicherheitsinformationen des Objekts an, z.B. Berechtigungen oder Besitz von Objekten.
/g Benutzer:Berechtigung	Erteilt dem Benutzer oder einer Gruppe Berechtigungen. Geben Sie den Benutzernamen im Format Benutzer@Domäne bzw. Gruppe@Domäne an. Die Parameter für die Berechtigungen zeigt .
/d Benutzer:Berechtigung	Verweigert dem Benutzer oder einer Gruppe Berechtigungen. Geben Sie den Benutzernamen im Format Benutzer@Domäne bzw. Gruppe@Domäne an. Die Parameter für die Berechtigungen zeigt .
/i:Option	Konfiguriert die Vererbung. Folgende Optionen sind möglich: p = Berechtigungen nur für einen Level, s = nur für untergeordnete Objekte oder t = für das Objekt mit allen untergeordneten Objekten zur Vererbung zulassen.
/n	Die bestehenden Berechtigungen des Objekts werden durch die neu definierten ersetzt.
/r Benutzer	Entfernt alle Berechtigungen für den Benutzer oder die Gruppe. Das Format muss lauten Benutzer@Domäne. Benutzen Sie diesen Parameter nur in Zusammenhang mit /g, um eine neue Berechtigung zuzuweisen. Ansonsten kann es schnell passieren, dass kein Benutzer mehr über Zugriff auf das Objekt verfügt.
/s	Setzt die Sicherheitseinstellungen für das Objekt auf die im Schema definierten Standardeinstellungen zurück.
/t	Zusammen mit dem Parameter /s können Sie für einen ganzen Zweig, z.B. für eine OU mit allen untergeordneten Objekten, die Standardeinstellungen des Schemas wiederherstellen.

Tabelle 21.2: Die Parameter für das Programm DSACLs

Tabelle 21.3 zeigt Ihnen die Parameter für die Berechtigungen, die Sie im Zusammenhang mit dem /g- und /d-Parameter verwenden können.

Parameter	Beschreibung
GR	Leseberechtigung
GW	Schreibberechtigung
GE	Ausführberechtigung
GA	Vollzugriff
SD	Löschen
DT	Löschen des Objekts mit untergeordneten Objekten
RC	Lesen von Sicherheitsinformationen
WD	Ändern der Sicherheitseinstellungen
LC	Auflisten der untergeordneten Objekte
CC	Erzeugen untergeordneter Objekte
DC	Löschen untergeordneter Objekte
WP	Schreiben von Eigenschaften
RP	Lesen von Eigenschaften

Tabelle 21.3: Beschreibung der DSACLs-Parameter für verschiedene Berechtigungen

DSACLs sollten Sie verwenden, wenn Sie in großen Mengen Berechtigungen editieren müssen, z.B. für eine OU, die sehr viele Benutzer enthält. Weiterhin ist DSACLs auch sehr gut geeignet, um standardmäßige Berechtigungen schnell wiederherzustellen. Bevor Sie das Programm ausführen, überlegen Sie sich gut, was Sie erreichen möchten. DSACLs liefert Ihnen keinerlei Warnmeldungen für Ihre Schritte.

21.6 Backup des Active Directory

In diesem Kapitel wird die Sicherung von Active Directory beschrieben. Zunächst erhalten Sie einige Vorschläge für ein generelles Sicherungskonzept des Active Directory. Daran anschließend wird Ihnen das Windows 2000-eigene Backup-Programm kurz erläutert und mit seinen Schwächen gegenüber einigen Backup-Programmen von Drittanbietern gemessen. Zusätzlich erhalten Sie Hinweise zum Wiederherstellen eines Teil-Backups und zum Sichern der Gruppenrichtlinien.

Das Backup des Active Directory ist ein komplexer Vorgang. Es ist nicht damit getan, in regelmäßigen Abständen den SYSVOL-Ordner wegzusichern und bei Bedarf wiederherzustellen. Über den Windows-Sicherungsassistenten werden bei einem Domänencontroller die Systemstatusdaten der Registrierung und der COM+-Klassenregistrierung, die Startdateien sowie der SYSVOL-Ordner gesichert. Der SYSVOL-Ordner enthält den freigegebenen Ordner NETLOGON, die Login-Skripte der Clients, sämtliche GPOs, die Junction Points sowie die Staging-Verzeichnisse des FRS (File Replication Service). Aus dem Active Directory selbst werden die folgenden Dateien gesichert: Die Datenbankdatei *NTDS.DIT*, die Checkpoint-Datei *edb.chk*, sämtliche *edb*.log*-Transaktionslogs (jede

dieser Dateien ist 10 MB groß) sowie die beiden Transaktionslogs *Res1.log* und *Res2.log*. Verwenden Sie Active Directory-integrierte DNS-Zonen, so werden diese als Bestandteil der Datenbankdatei gesichert. Verwenden Sie keine Active Directory-integrierten DNS-Zonen, so müssen Sie die Zonendatenbankdateien separat sichern. Erfüllt der Domänencontroller zusätzlich noch die Rolle eines Zertifikatsservers, so wird auch die Datenbank der Zertifikatsdienste mit dem Systemstatus gesichert. Dasselbe gilt auch für Cluster-Dienste, die auf dem Domänencontroller ausgeführt werden. Das Backup des Active Directory ist im Verhältnis zu den Sicherungen von einem Dateiserver sehr klein.

Auch wenn Sie die Active Directory-Datenbank und die Logdateien aus Gründen der Performance auf zwei verschiedenen Partitionen angelegt haben, müssen Sie die unterschiedlichen Lokationen dem Windows-Backup nicht explizit mitteilen, da die entsprechenden Pfade automatisch erkannt werden.

Das Backup eines Domänencontrollers kann nur auf dem Domänencontroller wiederhergestellt werden, auf dem das Backup durchgeführt wurde. Dies liegt darin begründet, dass Active Directory Passwörter nicht im Klartext, sondern in irreversibler Verschlüsselung (Hash) speichert. Diese Hashes werden abermals mit dem Verschlüsselungsschlüssel des Domänencontrollers verschlüsselt. Damit das Backup wieder entschlüsselt werden kann, muss es wieder auf den Domänencontroller mit dem zugehörigen Schlüssel zurückgespielt werden. Selbst wenn die Sicherungsmedien in falsche Hände geraten, kann keiner etwas mit diesen Daten anfangen. Ein Backup kann nur im Zeitraum von 60 Tagen wieder eingespielt werden. Dieser Zeitraum ist identisch mit der Lebensdauer gelöschter Objekte mit dem Tombstoning-Flag (siehe Kapitel 21.4). Danach verweigert das Betriebssystem die Wiedereinspielung. Das heißt also, dass Sie die archivierten Backup-Medien nach maximal 60 Tagen mit einer neueren Version überspielen können.



Um ein in jedem Fall funktionsfähiges Backup mit dem Windows-Sicherungs-Assistenten herzustellen, müssen Sie unter Windows 2000 unbedingt mindestens das SP2 einsetzen. Mit dem SP2 wurde ein Fehler an der Windows-Backup-API beseitigt.

21.6.1 Planen einer Backup-Strategie

Ein weiterer wichtiger Punkt ist die Planung eines Backups. Serveranwendungen und Datenbanken werden über ein Backup-Verfahren gesichert, bei dem beispielsweise einmal wöchentlich ein Komplet-Backup durchgeführt wird und an den anderen Tagen ein inkrementelles Backup. Bei dieser herkömmlichen Methode müssen Sie für ein Active Directory jedoch einige Punkte bedenken. Aufgrund der Komplexität der Informationen auf den Servern für die Replikation können Sie schnell eine inkonsistente, nicht mehr aktuelle Umgebung haben.

Ein gutes Backup umfasst neben der Sicherung des Systemstatus auch die Sicherung der Systempartition. Damit ist sichergestellt, dass alle erforderliche Systemdateien und -ordner des Betriebssystems vorhanden sind und dieses wiederhergestellt werden kann.

Auch der Einsatz von Images zum Backup kann diese Problematik nicht aus der Welt schaffen. Sie müssten theoretisch nach jeder Replikation ein Image jedes Domänencontrollers erstellen. Dies ist jedoch ein nicht vertretbarer Arbeitsaufwand.

Das Backup des Active Directory kann im laufenden Betrieb durchgeführt werden. Eine Wiederherstellung ist jedoch nur beim Startvorgang im Wiederherstellungsmodus möglich.

Obwohl sich auf jedem Domänencontroller eine identische Kopie der Active Directory-Datenbank befindet, sollten Sie dennoch immer auf mindestens zwei, wenn nicht sogar auf allen Domänencontrollern gleichzeitig das Backup durchführen. Dabei sollten Sie darauf achten, dass einer dieser Domänencontroller auch Inhaber der Betriebsmasterrolle ist. Hat ein Domänencontroller so großen Schaden, z.B. physikalisch, genommen, dass das Backup nicht wiederhergestellt werden kann, so verfügen Sie immer noch über einen alternativen Domänencontroller, von dem aus Informationen wiederhergestellt werden können. Diese beiden Domänencontroller sollten sich zudem an einem Standort befinden und über eine gute Netzwerkanbindung untereinander verfügen. Damit ist sichergestellt, dass sie über die Replikation immer auf demselben Stand sind.

Weiterhin sollten Sie sich überlegen, ob Sie das Backup auf einem Band oder auf einer zweiten Festplatte des Domänencontrollers anlegen möchten. Das Medium Festplatte gestattet ein schnelleres Erstellen und Einspielen von Backups. Diese Backup-Dateien können ihrerseits redundant auf ein Bandlaufwerk gesichert werden.

Entscheidend ist auch das Alter des Backups. Standardmäßig kann ein Backup nur innerhalb von 60 Tagen zurückgespielt werden. Dieser Zeitraum entspricht dem für das Active Directory festgelegten Tombstoning-Intervall. Hierbei handelt es sich um einen Schutzmechanismus, da das Zurückspielen stark veralteter Daten zu Inkonsistenzen oder anderen unvorhersehbaren Fehlern führen kann. Nach Ablauf der 60 Tage wird das aus dem Active Directory gelöschte Objekt endgültig gelöscht.

Sollte ein Fehler nicht in dem Ausfall eines Domänencontrollers begründet sein, so kann auch das Active Directory mit falschen Einstellungen an alle Domänencontroller repliziert worden sein. Auch eine Änderung, die sich nicht mehr rückgängig machen lässt, wie etwa das Löschen von Benutzern, kann bereits an alle Domänencontroller repliziert worden sein. In diesen Fällen müssen Sie auf ein Backup des Active Directory zurückgreifen können. Und wo wir gerade beim Thema Backup sind: Ein Backup können Sie nur einspielen, wenn dieses auch in regelmäßigen Abständen angelegt wird. An dieser Stelle soll nun keine Entscheidung darüber getroffen werden, was regelmäßig zu bedeuten hat. Sie sollten aber nach jeder größeren Aktion am Active Directory ein Backup durchführen, z.B. nach Änderungen des Schemas oder Hinzufügen vieler neuer Objekte. Außerdem sollten Sie auch regelmäßig Backups wieder einspielen, um zu testen, ob Sie auch funktionieren. Um die Funktionalität des Backups an einem Domänencontroller zu testen, führen Sie die folgenden Schritte aus:

1. Entfernen Sie einen Domänencontroller aus dem Netzwerk und führen Sie an diesem eine autorisierende Wiederherstellung mit einem Backup durch, und prüfen Sie, ob alles korrekt wiederhergestellt wurde.
2. Bevor Sie diesen Server wieder ins Netzwerk integrieren, müssen Sie eine nicht autorisierende Wiederherstellung (siehe Kapitel 21.7.1) durchführen. Andernfalls würde er die Einträge aller anderen Domänencontroller überschreiben.
3. Sie können den Domänencontroller nun wieder online schalten. Die gültigen Einträge seiner Active Directory-Datenbank bezieht er nun aus der regelmäßigen Replikation mit seinen Replikationspartnern.

21.6.2 Backup-Programme von Drittanbietern

Sie können das Backup mit dem Windows 2000-eigenen Backup-Programm oder einem Backup-Programm eines Drittanbieters durchführen. Stellen Sie beim Einsatz eines solchen Drittanbieter-Programms unbedingt sicher, dass dieses auch Active Directory-kompatibel ist. Möglicherweise werden unternehmensweit bereits Backup-Suiten wie *Veritas Backup Exec* oder *BrightStor ARCserve Backup* von Computer Associates eingesetzt. Dies dürfte allein schon aus Kostengründen nur in großen Unternehmen der Fall sein. Diese Suiten bieten komplette Backup-Möglichkeiten, beispielsweise auch für SQL- oder Exchange-Server. Für kleinere Unternehmen ist das Programm *ERDisk* von Aelita Software interessant. Das Windows-eigene Backup-Programm ist leider insofern eingeschränkt, dass Sie nicht den Systemstatus eines Domänencontrollers im Netzwerk sichern können, sondern nur den Status des lokalen Servers. *ERDisk* hingegen bietet Ihnen die Möglichkeit, das Backup auch auf Remote-Servern durchzuführen. Somit haben Sie die Möglichkeit, domänenweite Backups von einem zentralen Punkt aus durchzuführen. Über das Windows-Backup können Sie jedes Gerät zum Backup verwenden, das sich auf der Hardware Compatibility List (HCL) befindet. Mit *ERDisk* können Sie ein Backup lediglich auf der Festplatte des Rechners ablegen, auf dem *ERDisk* aufgeführt wird. Bandlaufwerke werden nicht unterstützt. Zunächst mag dieses als Nachteil gegenüber dem Windows-Backup erscheinen. Allerdings sind die Sicherungen auf einer Festplatte schneller herzustellen und zurückzuspielen als auf einem Bandlaufwerk. Sollen die Backups der Festplatte archiviert werden, so können diese Dateien über den Sicherungs-Assistenten immer noch auf ein Bandlaufwerk gesichert werden. Die letzten Backups sind aber immer schnell von der Festplatte verfügbar. Weiterhin kann bei *ERDisk* ausgewählt werden, ob alle oder nur ein Teil der Systemstatusdateien gesichert werden sollen. Zusätzlich können Sie mit *ERDisk* einzelne Active Directory-Objekte wiederherstellen, ohne den Domänencontroller offline schalten zu müssen.

Sie müssen theoretisch nur an einem Domänencontroller ein Backup durchführen, um alle Informationen des Verzeichnisses zu sichern. Um aber auf der sicheren Seite zu sein, sollten Sie alle Ihre Domänencontroller sichern. Den Systemstatus des Domänencontrollers sollten Sie so häufig wie möglich sichern. Da diese Sicherungen nicht viel Platz in Anspruch nehmen, sollten Sie diese täglich, bei umfangreichen Änderungen sogar mehrmals täglich durchführen. Halten Sie nach Möglichkeit auch die Sicherungen eines längeren Zeitraums bereit. So können Sie schnell einen ganz bestimmten Status wiederherstellen. Bei größeren Änderungen, wie z.B. dem Ändern des Schemas, sollten Sie ein Backup direkt davor und ein zweites direkt danach anlegen. Legen Sie Ihren Backups eine Dokumentation über die Änderungen gegenüber dem letzten Backup bei. So werden Sie schneller das geeignete Backup wiederfinden, das Sie einspielen möchten. Bei Backups, die mit dem Windows-Backup-Tool erstellt worden sind, haben Sie keine andere Möglichkeit, als durch Ihre Dokumentation festzustellen, welche Inhalte sich im Backup befinden.

21.6.3 Wiederherstellen eines Teil-Backups

Nachdem Sie nun Ihr Backup angelegt haben, könnte es passieren, dass Sie in Ihrem Active Directory versehentlich eine große Gruppe von Benutzern löschen. Sie könnten nun zwar Ihr Backup komplett einspielen, um auf diese Weise wieder die verlorenen Objekte verfügbar zu machen. Das komplette Einspielen kann jedoch eine langwierige

und für die meisten Objekte auch unnötige Aufgabe sein. Deshalb sollte es auch möglich sein, beim Backup nur die fehlenden Objekte anstelle des Komplett-Backups in der autorisierenden Wiederherstellung zurückzuspielen.

Microsoft bietet Ihnen dafür eine – wenn auch etwas umständliche – Methode an. Starten Sie dazu über das Kommandozeilenprogramm *NTDSUTIL* (siehe Kapitel 23.1.18) die autorisierende Wiederherstellung einzelner Objekte. Um beispielsweise den Benutzer Peter Mustermann aus der Organisationseinheit Marketing in der Domäne *firma.de* wiederherzustellen, müssten Sie den folgenden Befehl eingeben:

```
Authoritative restore: restore subtree „cn=Peter Mustermann,ou=Marketing,  
dc=firma,dc=de“ 
```

Wenn Sie eine Benutzergruppe mit ihren ursprünglichen Mitgliedschaften wiederherstellen müssen, wird die Angelegenheit noch komplizierter. Sie müssen in diesem Fall zuerst sämtliche Mitglieder der Gruppe wiederherstellen. Dann muss der Domänencontroller neu gestartet werden, damit die Benutzerinformationen in der Domäne repliziert werden können. Anschließend müssen Sie erneut die autorisierende Wiederherstellung starten, um das Gruppenobjekt selbst wiederherzustellen. Diese Methode ist praktikabel, wenn Sie nicht große Mengen von Objekten wiederherstellen müssen. Selbst wenn Sie sich eine Batchdatei erstellen, um eine große Anzahl verlorener Objekte wiederherzustellen, müssen Sie dennoch viel Zeit für die Wiederherstellung aufwenden. Außerdem muss der Domänencontroller für die Zeit der autorisierenden Wiederherstellung offline geschaltet werden.

Es gibt jedoch auch Programme von Drittanbietern, die dieselbe Funktionalität in einer grafischen Oberfläche bieten. Hierzu zählen beispielsweise *Veritas Backup Exec*, *Directory and Resource Manager* von NetIQ oder *ERDisk* von Aelita Software. Mit diesen Programmen haben Sie die Möglichkeit, von einem Nicht-Domänencontroller aus über das Netzwerk Active Directory wiederherzustellen. *ERDisk* ist in der Lage, einzelne Objekte aus einem Backup wiederherzustellen, und zwar nicht nur aus seinem eigenen Backup, sondern auch aus einem mit Windows-Backup erstellten. Ihnen wird eine GUI in Form des Online Restore Wizard geboten, mit dem Sie komfortabel die wiederherzustellenden Objekte auswählen können. Sie können hier bei der Wiederherstellung eines Gruppenobjekts auswählen, ob Sie nur die Gruppe oder die Gruppe mit allen Mitgliedern wiederherstellen möchten. Außerdem müssen die Domänencontroller nicht vom Netzwerk getrennt werden, wenn Sie eine autorisierende Wiederherstellung mit einem dieser Programme durchführen.

21.6.4 Backup der Active Directory-Gruppenrichtlinien

Beim Backup des Active Directory werden zwar alle Objekte gesichert, nicht jedoch die Gruppenrichtlinien. Active Directory selbst enthält nur Verknüpfungen mit den einzelnen Richtlinien. Diese Verknüpfungen beinhalten den Verweis auf das GPO sowie die Angabe, ob dieses GPO auf die Domäne, die OU usw. angewendet werden soll. Die GPOs an sich befinden sich jedoch im SYSVOL-Verzeichnis des Domänencontrollers. Dort befindet sich in einem Ordner, der den Namen der Domäne trägt, ein Unterordner „Policies“. Dieser ist der Speicherort der GPOs. Jedes GPO ist dort in einem Ordner mit dem Namen seiner GUID abgelegt. Führen Sie also das Backup des Active Directory

durch, so sind zwar die Verweise auf die GPOs noch erhalten, aber dies nützt Ihnen nichts, wenn sich die GPOs nicht mehr an ihrem ursprünglichen Speicherort befinden.

Sie sollten deshalb bei jedem Backup-Vorgang des Active Directory auch den SYSVOL-Ordner eines Domänencontrollers sichern. Im Gegensatz zum für den Domänencontroller spezifischen Active Directory-Backup genügt eine einzige Sicherung eines beliebigen SYSVOL-Ordners. Der Inhalt des SYSVOL-Ordners wird über den File Replication Service (FRS) von einem Domänencontroller auf den anderen kopiert. FRS benutzt dabei dasselbe Interface wie der Windows Explorer bei einem Kopiervorgang. Der FRS-Replikationsmechanismus benutzt im Gegensatz zur Active Directory-Replikation keine Versionsnummern für die Änderungen an Dateien. Eine GPO-Datei wird über FRS nur dann kopiert und somit an alle Domänencontroller repliziert, sobald an ihr die Eigenschaft „Geändert am“ modifiziert worden ist.

21.7 Wiederherstellen des Active Directory

Dieses Kapitel beschäftigt sich mit dem Wiederherstellen des Active Directory. Sofern ein Domänencontroller nicht mehr funktionstüchtig ist, muss auf ihm die Active Directory wiederhergestellt werden. Zur Wiederherstellung des Domänencontrollers gibt es neben einer Neuinstallation auch noch die Möglichkeiten der autorisierenden und nicht autorisierenden Wiederherstellung. Ist lediglich ein einziger Domänencontroller nicht mehr funktionsfähig, ist in den meisten Fällen die nicht autorisierende Wiederherstellung ausreichend. Selbstverständlich benötigen Sie ein Backup des Computers, um diesen wiederherstellen zu können.

Bevor wir uns den beiden Wiederherstellungsarten zuwenden, sollte nicht unerwähnt bleiben, dass in einigen Fällen eine Neuinstallation des Active Directory auf dem betreffenden Domänencontroller der schnellere Weg sein kann. Eine Scratch-Installation ist in jedem Fall nötig, wenn das Problem des Domänencontrollers aufseiten des Betriebssystems zu suchen ist. Liegt das Problem doch im Active Directory, so können Sie die Datenbank auch reparieren, indem Sie auf dem Domänencontroller zunächst DCPROMO an der Eingabeaufforderung ausführen, um den Domänencontroller zu einem Mitgliedsserver herabzustufen. Nach der Herabstufung geben Sie erneut DCPROMO ein. Damit wird er wieder zum Domänencontroller heraufgestuft und erhält eine funktionierende Kopie der Active Directory-Datenbank über die Replikation. Je nach Standort des nächsten Replikationspartners kann es in diesem Fall dauern, bis der Domänencontroller die aktuelle Kopie erhalten hat. Dieser Replikationsprozess kann einmalig einen großen Teil der Netzwerkbandbreite einnehmen.

Der Windows Server 2003 bietet eine zusätzliche Möglichkeit, die Inhalte der Active Directory-Datenbank auf einen beliebigen Domänencontroller zu überspielen. Sie können auf einem Domänencontroller oder globalen Katalogserver, der auf einem möglichst aktuellen Stand ist, ein Backup mit einem beliebigen Backup-Programm durchführen. Diese Backup-Daten können auf einem beliebigen Medium wie CD, DVD oder Bandlaufwerk direkt auf dem Zieldomänencontroller eingespielt werden. Damit entfällt die Replikation der kompletten Datenbankkopie über das Netzwerk. Dieses Verfahren wurde ausführlich in Kapitel 9.4.1 beschrieben.

21.7.1 Die nicht autorisierende Wiederherstellung

Im Zuge der nicht autorisierenden Wiederherstellung wird ein Domänencontroller wieder auf den Stand des letzten Backups seiner Systemstatusdaten gebracht. Nach der autorisierenden Wiederherstellung empfängt der Domänencontroller bei der nächsten Replikation von seinen Replikationspartnern alle Änderungen, die seit seinem letzten Sicherungsstatus durchgeführt worden sind. Damit wird die Active Directory-Datenbank wieder auf den aktuellen Stand gebracht. Diese Methode wird in den meisten Fällen angewendet, wenn die Active Directory-Daten fehlerhaft sind. Sie sehen, dass hierbei dasselbe Ergebnis erzielt wird wie beim Herunter- und anschließenden Heraufstufen des Domänencontrollers. Allerdings ist der Vorgang der autorisierenden Wiederherstellung aufwändiger als das Ausführen von DCPROMO.

1. Zum Ausführen der nicht autorisierenden Wiederherstellung müssen der Computer neu gestartet und mit der Taste **F8** die erweiterten Startoptionen ausgewählt werden. Wählen Sie dort den Menüpunkt VERZEICHNISDIENSTWIEDERHERSTELLUNG. Ab diesem Zeitpunkt ist sichergestellt, dass der Computer beim Starten offline geschaltet ist. Beim Start des Servers im abgesicherten Modus müssen Sie das Administratorkonto mit dem zugehörigen Kennwort angeben, das Sie bei der Installation des Active Directory angegeben haben. Das normale Administratorkennwort kann in diesem Moment nicht geprüft werden, da der Domänencontroller offline und nicht mit dem Active Directory verbunden ist.
2. Nach dem Start wählen Sie aus dem STARTMENÜ/PROGRAMME/ZUBEHÖR/SYSTEMPROGRAMME den Eintrag SICHERUNG. Auf der Willkommenseite wählen Sie den Wiederherstellungs-Assistenten aus. Wählen Sie hier das Medium mit dem wiederherzustellenden Datensatz aus. Sie können entweder den kompletten Datensatz oder nur einzelne Objekte daraus wiederherstellen. Klicken Sie dann auf WEITER. Wählen Sie dann FERTIG STELLEN, wird die nicht autorisierende Wiederherstellung gestartet. Sie können aber auch über die Schaltfläche ERWEITERT spezielle Einstellungen zum Zielort und Optionen zur Wiederherstellung treffen.

Beim Zielort der Wiederherstellung können Sie angeben, ob die Dateien an ihrem ursprünglichen Speicherort wiederhergestellt werden sollen. Damit werden schadhafte Dateien überschrieben. Die Dateien können aber auch an einem alternativen Ort wiederhergestellt werden. Damit wird eine ältere Dateiversion in einem zu spezifizierenden Ordner wiederhergestellt. Die Dateien können auch in einem ebenfalls anzugebenden einzelnen Ordner wiederhergestellt werden – außerhalb der ursprünglichen Baumstruktur.

Bei den Optionen der Wiederherstellung wird gewählt, was beim Wiederherstellen geschehen soll. Mit der Standardeinstellung DATEI NICHT ERSETZEN wird die bestehende Datei nicht durch die des Backups ersetzt. Mit der gegenteiligen Option DATEI IMMER ERSETZEN wird immer die Datei aus dem Backup wiederhergestellt. Die Option NUR ERSETZEN, WENN SIE ÄLTER IST überschreibt die bestehende Datei nur, wenn die des Backups neuer ist. Mit dieser Einstellung haben Sie die aktuellsten Dateiversionen zur Verfügung.

Als Letztes können Sie noch erweiterte Wiederherstellungsoptionen für Sicherheits- und Systemdateien angeben. Mit der Option SICHERHEITSDATEN WIEDERHERSTELLEN werden alle ursprünglichen Sicherheitseinstellungen wie Berechtigungen oder Besitz

wiederhergestellt. Weiterhin können Sie Einstellungen zur Konfigurationsdatenbank für Removable Storage-Geräte (RSM) und zur Wiederherstellung von Daten unter Abzweigungspunkten angeben.

3. Haben Sie alle Einstellungen getroffen, müssen Sie nochmals das Quellmedium bestätigen. Dann beginnt die Wiederherstellung. Dabei wird eine Reihe von Statusmeldungen ausgegeben.

Die nicht autorisierende Wiederherstellung von SYSVOL

Auch für den Ordner SYSVOL kann eine nicht autorisierende Wiederherstellung durchgeführt werden. Dabei wird die lokale SYSVOL-Kopie mit dem SYSVOL-Verzeichnis der Replikationspartner verglichen. Bei Bedarf aktualisiert der Domänencontroller seine SYSVOL-Daten. Die nicht autorisierende Wiederherstellung von SYSVOL sollten Sie durchführen, solange noch mindestens ein weiterer Domänencontroller in der Domäne funktionstüchtig ist. Befindet sich kein weiterer Domänencontroller in der Domäne, wird eine primäre Wiederherstellung von SYSVOL durchgeführt. Bei einer primären Wiederherstellung werden die aktuellen SYSVOL-Daten geladen und daraus eine neue FRS-Datenbank angelegt. Dieses Verfahren ähnelt der normalen nicht autorisierenden Wiederherstellung; der Unterschied besteht darin, dass hier SYSVOL als primär gekennzeichnet wird.

21.7.2 Die autorisierende Wiederherstellung

Die autorisierende Wiederherstellung ist eine Erweiterung der nicht autorisierenden Wiederherstellung, die vor einer autorisierenden Wiederherstellung durchgeführt werden muss. Bei diesem Verfahren werden bei der Wiederherstellung die Versionsnummern (USN) der Attribute aller Objekte des gesamten Verzeichnisses, eines bestimmten Subtrees oder eines einzelnen Objekts heraufgesetzt, sodass diese Objekte als autorisierend im Verzeichnis gelten. Je nachdem, welche Daten wiederhergestellt werden müssen, sollten Sie immer darauf achten, die kleinste mögliche Dateneinheit wiederherzustellen. Bei der autorisierenden Wiederherstellung können lediglich Objekte der beiden Verzeichnispartitionen Konfigurationsinformationen sowie Domänendaten (siehe Kapitel 3.7.2) wiederhergestellt werden. Objekte der Verzeichnispartition Schemainformationen können nicht wiederhergestellt werden.

Die autorisierende Wiederherstellung müssen Sie anwenden, wenn Sie nach einem Backup Änderungen am Active Directory durchgeführt haben, die nun wieder rückgängig gemacht werden sollen. Dies kann z.B. der Fall sein, wenn Sie versehentlich eine größere Anzahl von Objekten gelöscht haben, deren manuelle Wiederherstellung zu aufwändig wäre. Wie bereits in Kapitel 17.3.1 erwähnt, kann die autorisierende Wiederherstellung auch die letzte Lösung von bestehenden Replikationsproblemen sein.

Die autorisierende Wiederherstellung wird durchgeführt, nachdem auf einem Domänencontroller erfolgreich die nicht autorisierende Wiederherstellung abgeschlossen, aber dieser noch nicht wieder online geschaltet wurde. Es kann auch ein Domänencontroller ausgewählt werden, der die fehlerhaften Informationen noch nicht über die Replikation erhalten hat. Auf diesem werden die Daten mit dem Programm *NTDSUTIL* (siehe Kapitel 23.1.18) als autorisierend gekennzeichnet. Dies geschieht durch eine Heraufsetzung

jeder USN auf den höchsten Wert im gesamten Verzeichnis. Er wird damit zum neuen Master der Domäne, und alle übrigen Domänencontroller beziehen bei der nächsten Replikation seine Daten, die als die aktuell gültigen markiert werden. Bedenken Sie aber auch, wie viel Netzwerkverkehr danach stattfinden wird, wenn sich sämtliche Domänencontroller eine große Menge an Daten von einem Domänencontroller holen müssen. Aber dennoch kann dies unter Umständen Ihre letzte Chance sein, um das Verzeichnis wieder ordnungsgemäß lauffähig zu machen.

Um die autorisierende Wiederherstellung durchzuführen, sind folgende Schritte erforderlich:

1. Starten Sie den Domänencontroller, an dem Sie die nicht autorisierende Wiederherstellung durchgeführt haben, wieder neu.



Dieser Domänencontroller darf zwischenzeitlich noch nicht wieder neu gestartet worden sein.

2. Fahren Sie den Computer hoch und wählen mit der Taste **[F8]** die erweiterten Startoptionen. Wählen Sie dort den Menüpunkt VERZEICHNISDIENSTWIEDERHERSTELLUNG.
3. Öffnen Sie die Eingabeaufforderung. Geben Sie dort den Befehl `NTDSUTIL authoritative restore` **[↵]** ein. Sie haben nun die Möglichkeit, die gesamte Datenbank oder nur einen bestimmten Zweig daraus wiederherzustellen. Haben Sie beispielsweise nur innerhalb einer OU eine Reihe von Objekten gelöscht, so ist es ausreichend, diesen Zweig wiederherzustellen. Geben Sie dazu entweder `restore database` oder `restore subtree <DN des Objekts>` ein. Um die OU Finanzen in der Domäne *firma.de* wiederherzustellen, wäre folgende Eingabe nötig: `restore subtree OU=Finanzen,DC=Firma,DC=de` **[↵]**

Besonders in Umgebungen mit mehreren Domänencontrollern und Domänen müssen Sie darauf achten, ob die gesamte Datenbank oder nur eine Teilstruktur daraus wiederhergestellt werden soll. Stellen Sie die gesamte Datenbank wieder her, werden auch Passwörter von Computern sowie Passwörter für Vertrauensstellungen auf den Stand des Backups gebracht. Haben sich diese nachträglich geändert, besteht für Clients kein Zugriff mehr auf die Server oder Domänencontroller. Im Fall der Passwörter müssen Sie diese alle zurücksetzen. Funktionieren NTLM-Vertrauensstellungen zu Windows NT- oder 2000-Domänen nicht mehr, so müssen Sie die Vertrauensstellung zunächst aufheben und dann wieder neu einrichten. Diese Aufgabe kann Ihnen das Support-Tool *NETDOM* (siehe Kapitel 23.1.17) erleichtern. Sie sollten also immer nur den Bereich der Datenbank wiederherstellen, an dem Probleme aufgetreten sind. Andernfalls würden Sie sich viel unnötige Arbeit machen.

Wollen Sie die automatische Erhöhung der USNs bei der Wiederherstellung verhindern, so geben Sie zusätzlich den Parameter `verinc` ein. `Verinc` steht für Version increase. *NTDSUTIL* öffnet die Datenbankdatei *NTDS.DIT* und setzt die USN entweder automatisch oder um einen eingegebenen Wert herauf. Dann wird die Anzahl der zu aktualisierenden Datensätze ausgerechnet. Vor der Fertigstellung wird diese Anzahl nochmals geprüft.

4. Wurde die autorisierende Wiederherstellung abgeschlossen, beenden Sie *NTDSUTIL* mit quit  und starten den Domänencontroller im normalen Modus neu.

Der autorisierend wiederhergestellte Domänencontroller repliziert dann seine Daten an alle anderen Domänencontroller. Die Objekte, deren USNs heraufgesetzt worden sind, werden verbindlich an die übrigen Domänencontroller repliziert. Dies sind z.B. die versehentlich gelöschten Objekte. Die wiederhergestellten Objekte behalten ihre GUID sowie SID. Damit ergeben sich keinerlei Probleme bei Berechtigungen und anderen Sicherheitseinstellungen. Änderungen, die an den anderen Domänencontrollern durchgeführt worden und dem wiederhergestellten noch nicht bekannt sind, werden an ihn übertragen.

Sobald Sie die autorisierende Wiederherstellung durchgeführt haben, müssen Sie bei einer vollständigen Wiederherstellung den Ordner SYSVOL, bei der Wiederherstellung von Teilen der Datenbank den Ordner der Gruppenrichtlinien über den vorhandenen SYSVOL- bzw. Gruppenrichtlinienordner kopieren. Den Ordner mit der entsprechenden Richtlinie müssen Sie über die zugehörige GUID ermitteln. Dieser Schritt ist zur Wahrung der Gruppenrichtlinien-Identität auf dem wiederhergestellten Domänencontroller erforderlich. Der SYSVOL-Ordner wird dann bei der Replikation mit den übrigen Domänencontrollern abgeglichen. Allerdings sollten Sie nicht gleichzeitig alle Domänencontroller mit der autorisierenden Methode wiederherstellen. Führen Sie dieses Verfahren an einem DC durch, die restlichen können über die nicht autorisierende Methode wiederhergestellt werden.

Im Rahmen der autorisierenden Wiederherstellung können jedoch auch zwei Probleme auftreten. Zum einen kann es zu Problemen mit Gruppenmitgliedschaften kommen, zum anderen zu Problemen mit Kennwörtern für Computerkonten und Vertrauensstellungen.

Probleme mit der Gruppenmitgliedschaft

Bei der autorisierenden Wiederherstellung besteht das Problem, dass möglicherweise die Informationen über Gruppenmitgliedschaften verloren gehen können. Das Attribut der Gruppenmitgliedschaft ist ein Attribut mit mehreren Werten. Je nachdem, ob nach der autorisierenden Wiederherstellung zuerst Benutzer- oder Gruppenobjekte repliziert werden, ergeben sich unterschiedliche Resultate für die Gruppenmitgliedschaft. Die Reihenfolge der zu replizierenden Objekte kann jedoch nicht festgelegt werden. Fehler ergeben sich lediglich in der Konstellation, wenn zuerst das versehentlich gelöschte Gruppenobjekt wiederhergestellt und vor dem Benutzerobjekt repliziert wird. Die Replikationspartner streichen in diesem Fall das gelöschte – und zu diesem Zeitpunkt noch nicht replizierte – Benutzerobjekt aus der Liste der Gruppenmitglieder. Auch wenn das Benutzerobjekt danach repliziert wird, ist dieses nicht mehr Mitglied der Gruppe. Lediglich die primäre Gruppe des Benutzers wird stets korrekt angezeigt. Alle Mitglieder dieser Gruppe werden korrekt angezeigt, und die Mitglieder dieser Gruppe besitzen auch die Information über die Mitgliedschaft darin.

Wird hingegen das versehentlich gelöschte Benutzerobjekt bei der autorisierenden Wiederherstellung ersetzt und dieses vor dem Gruppenobjekt repliziert, so ist sowohl die Information über die Mitglieder der Gruppe als auch die Information über die Gruppenmitgliedschaften des Benutzers korrekt auf allen Replikationspartnern vorhanden.

Sobald nach der autorisierenden Wiederherstellung dieses Problem aufgetreten ist, müssen Sie das Attribut der Gruppenmitgliedschaft für die betroffenen Gruppen anpassen. Diese Anpassung geschieht auf dem Domänencontroller, auf dem die Wiederherstellung vollzogen wurde.

Um wieder korrekte Gruppenangaben zu erhalten, erstellen Sie einen fiktiven Benutzer. Fügen Sie diesen Benutzer zu jeder Gruppe hinzu, die von der autorisierenden Wiederherstellung betroffen war (die also entweder selbst wiederhergestellt wurde oder einige ihrer Mitglieder, für die diese Gruppe nicht als primäre Gruppe definiert ist) und löschen ihn dann wieder aus den Gruppen. Dabei werden die korrekten Informationen von dem Domänencontroller aus repliziert, auf dem die autorisierende Wiederherstellung durchgeführt wurde. Die falschen Informationen der Replikationspartner werden dabei überschrieben. Bei diesem Verfahren müssen Sie jedoch sicherstellen, dass auf keinem anderen Domänencontroller Änderungen an den Gruppenmitgliedschaften der betroffenen Benutzer und Gruppen vorgenommen werden, bis die eben beschriebenen Schritte abgeschlossen sind. Andernfalls kann auf dem Domänencontroller, auf dem die autorisierende Wiederherstellung durchgeführt wurde, die korrekte Versionsnummer der Mitgliedschaftsinformationen geändert werden. In diesem Fall bleibt nur noch ein manuelles Bearbeiten der Informationen oder eine erneute autorisierende Wiederherstellung, bei der Sie die Option „verinc“ verwenden müssen, um die korrekte ursprüngliche Versionsnummer als autorisierend zu setzen.

Probleme mit Kennwörtern für Computerkonten und Vertrauensstellungen

Bei der autorisierenden Wiederherstellung kann es passieren, dass Passwörter für Computerkonten und Vertrauensstellungen wiederhergestellt werden, die zum aktuellen Zeitpunkt bereits ungültig sind. Dies liegt darin begründet, dass ab Windows 2000 standardmäßig Kennwörter nach maximal 30 Tagen geändert werden sollen. Sind Passwörter zwischen dem Zeitpunkt des Backups und dem Wiederherstellen geändert worden, ergibt sich logischerweise ein Problem.

Im Falle der Computerkonten können Sie entweder den Benutzern mitteilen, sie mögen die Anmeldung mit ihrem bisherigen Passwort versuchen. Oder aber – sofern dieses nicht mehr möglich ist, müssen Sie die Kennwörter manuell zurücksetzen. Sind die Vertrauensstellungen zwischen zwei Domänen betroffen, so müssen Sie die Vertrauensstellung manuell entfernen und wieder neu einrichten.

21.7.3 Ein allgemeiner Disaster Recovery-Plan

Die Frage zur Planung eines Disaster Recovery sollte sich nicht erst in dem Moment stellen, wenn der einzige oder letzte Domänencontroller Ihrer Domäne seinen Dienst verweigert. In diesem Satz ist bereits ein wichtiger Punkt angesprochen. Domänencontroller sind zwar fehlertolerant, da sie alle dieselben Informationen der Active Directory-Datenbank besitzen. Aber zur Wahrung der Fehlertoleranz müssen Sie mindestens zwei Domänencontroller eingerichtet haben. Um nach Möglichkeit die Verfügbarkeit eines dieser beiden Server zu gewährleisten, sollten Sie bei der Einrichtung einige standort- und netzwerktechnische Punkte bedenken:

- ▶ Achten Sie idealerweise auf verschiedene physikalische Standorte der beiden Domänencontroller, z.B. zwei verschiedene Räume. Damit könnte einer der Domänencontroller im Falle eines Feuers, Wasserschadens etc. möglicherweise erhalten bleiben. Weiterhin sollten Sie auch separate Switches verwenden, sodass auch bei netzwerkbedingten Problemen zumindest einer der Domänencontroller noch erreichbar ist.
- ▶ Sie sollten auf dem Domänencontroller auch keine DHCP oder WINS-Dienste laufen lassen. Falls Ihr Domänencontroller ausfällt, wären somit nicht gleichzeitig auch die anderen Netzwerkdienste betroffen. Wenn Sie DHCP und WINS auf dem Domänencontroller ausführen, sollten Sie für diese Dienste einen alternativen Server konfiguriert haben, der im Ernstfall die beiden Dienste ausführen kann.
- ▶ Benutzen Sie Active Directory-integrierte DNS-Zonen anstelle von herkömmlichen primären und sekundären DNS-Zonen (siehe Kapitel 16.2), die in Textdateien gespeichert werden. Bei der Verwendung von Active Directory-integrierten Zonen kann jeder beliebige Domänencontroller zum DNS-Server werden, indem Sie den DNS-Serverdienst auf dem Computer installieren und ausführen. Die Zoneninformationen können direkt aus dem Active Directory abgerufen werden.
- ▶ Sie sollten immer zumindest einen Domänencontroller zur Verfügung haben, auf dem sich kein globaler Katalog (siehe Kapitel 15) befindet und der auch keine der Betriebsmasterrollen (siehe Kapitel 11) ausführt. Dieser Domänencontroller kann bei Ausfall eines anderen Servers den globalen Katalog oder eine Betriebsmasterrolle übernehmen.

Nachdem ein Domänencontroller ausgefallen ist, müssen Sie seine Grundfunktionen an einen anderen Domänencontroller übertragen. Wenn der Server auch als DNS-Server konfiguriert war, installieren und starten Sie den DNS-Dienst auf dem zweiten Server. Falls auch noch der globale Katalog ausgefallen ist, so machen Sie den zweiten Server auch noch zum globalen Katalogserver. Sobald der erste Domänencontroller wieder online geschaltet wird, werden alle Änderungen, die während seines Ausfalls vorgenommen wurden, automatisch an ihn repliziert. Weisen Sie dem zweiten Server auch die ausgefallenen Betriebsmasterrollen zu.



Wenn Sie die Rolle des Schemamasters, RID-Masters oder Domännennamen-Masters übertragen haben, dürfen Sie den alten Server erst wieder online schalten, wenn er formatiert und das Betriebssystem neu installiert wurde. Alternativ dazu können Sie an dem alten Server den Befehl DCPROMO zur Deinstallation des Active Directory (siehe Kapitel 9.3) ausführen, bevor Sie ihn wieder ins Netzwerk integrieren. Dadurch wird er zu einem allein stehenden Server herabgestuft, auf dem alle Einträge bezüglich Active Directory gelöscht werden. Sobald Sie ihn wieder online geschaltet haben, führen Sie erneut DCPROMO aus, um ihn wieder zum Domänencontroller heraufzustufen.

21.7.4 Domänencontroller-Wiederherstellung via Neuinstallation und Backup

Dieses Kapitel beschreibt, in welchen Fällen die Wiederherstellung eines Domänencontrollers via Neuinstallation oder Neuinstallation und Backup angewendet werden sollte. Auch die Wiederherstellung der globalen Katalogserver sowie der Betriebsmaster wird besprochen. Zusätzlich erhalten Sie Hinweise zur Wiederherstellung eines Domänencontrollers auf geänderter Hardware.

Domänencontroller-Wiederherstellung durch Neuinstallation

Bei einer Wiederherstellung eines Domänencontrollers durch Neuinstallation wird nicht sein ursprünglicher Systemstatus per Backup eingespielt. Nach der Neuinstallation des Betriebssystems wird das Active Directory neu installiert, und die Datenbankinformationen werden von den Replikationspartnern empfangen. Dieses Verfahren können Sie in den folgenden Fällen anwenden:

- ▶ Der Verzeichnisdienst-Wiederherstellungsmodus kann nicht gestartet werden.
- ▶ In der Domäne ist noch mindestens ein Replikationspartner vorhanden.
- ▶ Auf dem Domänencontroller werden keine weiteren Dienste wie DNS, DHCP oder Exchange ausgeführt.
- ▶ Ein Fehler liegt in der Hardwarekonfiguration vor, z.B. die Konfiguration der Festplatten.

Domänencontroller-Wiederherstellung durch Neuinstallation und Backup

Bei diesem Verfahren installieren Sie das Betriebssystem neu und starten dann die Verzeichnisdienstwiederherstellung mit einer nicht autorisierenden Wiederherstellung des Systemstatus und des Active Directory. Führen Sie diese Methode in folgenden Fällen aus:

- ▶ Der Verzeichnisdienst-Wiederherstellungsmodus kann nicht gestartet werden.
- ▶ Es ist liegt ein Hardware-Fehler vor, z.B. die Konfiguration der Festplatten.
- ▶ Auf dem Domänencontroller werden keine weiteren Dienste wie DNS, DHCP oder Exchange ausgeführt.
- ▶ Das Backup des Domänencontrollers ist nicht älter als 60 Tage (Tombstoning-Intervall, siehe Kapitel 21.4). Andernfalls kann das Backup nicht eingespielt werden.
- ▶ Über den Domänencontroller müssen die folgenden Informationen bekannt sein:
 - ▶ Der Name des Domänencontrollers. Dieser muss identisch sein, wenn Sie nicht entsprechende Änderungen an sämtlichen Client-Konfigurationen durchführen möchten.
 - ▶ Die Mitgliedschaft in der Domäne, da u.U. ein neues Computerkonto erstellt werden muss.
 - ▶ Das lokale Administratorpasswort, das zum Zeitpunkt des Backups benutzt wurde. Ist dieses nicht verfügbar, können Sie sich nicht einloggen, um ein Domänen-Computerkonto zu erstellen. Das Passwort des Domänenadministrators können Sie in diesem Moment noch nicht verwenden, da der Computer noch nicht Mitglied der Domäne ist. Außerdem benötigen Sie das lokale Administratorpasswort, um den

Systemstatus des Domänencontrollers wiederherzustellen. Auch in diesem Moment können Sie das Kennwort des Domänenadministrators nicht verwenden, da der Domänencontroller bei der Wiederherstellung offline geschaltet ist.

- Bei einem Festplatten-Fehler müssen Sie zusätzlich die alten Partitionierungsdaten kennen. Um den alten Systemstatus wiederherstellen zu können, muss eine identische Festplattenkonfiguration vorliegen. Ansonsten kann der Domänencontroller nach der Systemwiederherstellung möglicherweise nicht neu gestartet werden.

Wiederherstellen globaler Katalogserver

Zur Wiederherstellung eines globalen Katalogservers können Sie entweder auf dem ursprünglichen Server das Backup einspielen oder einen neuen globalen Katalogserver auf einem anderen Domänencontroller einrichten (siehe Kapitel 15). Bedenken Sie beim Zurückspielen des Backups jedoch, dass besonders in einer Umgebung mit mehreren Domänen das Zurückspielen des Backups eines globalen Katalogservers mehr Zeit in Anspruch nimmt als das Backup eines Domänencontrollers.

Verzögert sich das Rückspielen des Backups, so müssen Sie zumindest vorübergehend einen neuen globalen Katalogserver einrichten, wenn für die Benutzer kein weiterer Server zur Verfügung steht oder Exchange 2000 eingesetzt wird, wofür ein globaler Katalogserver zwingend ist. Ist der ursprüngliche Katalogserver wiederhergestellt, können Sie den vorübergehend konfigurierten Server theoretisch wieder entfernen.

Je mehr globale Katalogserver in einer Gesamtstruktur vorhanden sind, desto höher liegt zwar die Redundanz und Ausfallsicherheit. Gleichzeitig erhöht sich aber auch der Replikationsverkehr sowie die Größe der Datenbank auf den Servern.

Wiederherstellen von Betriebsmastern

Ausgefallene Betriebsmaster können via Backup wiederhergestellt werden. Lässt sich ein Betriebsmaster nicht wiederherstellen, müssen Sie dessen Rolle(n) an einen anderen Domänencontroller übertragen. Dieses Verfahren ist in Kapitel 11.1.4 beschrieben. Beim Ausfall des RID-Masters und Schemamasters ist jedoch vom Einspielen des Backups abzuraten. Das Wiederherstellen des Schemamasters kann verwaiste Objekte als Konsequenz haben, das des RID-Masters kann die Active Directory-Daten korrumpieren.

Wiederherstellungen auf geänderter Hardware

Der Systemstatus eines Domänencontrollers kann auch dann wiederhergestellt werden, wenn dieser auf geänderter Hardware ausgeführt werden soll. Dies kann entweder der Fall sein, wenn ein Hardwaredefekt den Austausch notwendig gemacht hat oder wenn der Domänencontroller aus Performance-Gründen auf einem anderen Server installiert wird. Allerdings müssen Sie dabei die folgenden Punkte bedenken:

- Die Partitionierungsdaten auf dem neuen Domänencontroller müssen mit denen des alten Domänencontrollers übereinstimmen. Dies gilt für die Laufwerksbuchstaben und Größen der einzelnen Partitionen. Ist diese Voraussetzung nicht erfüllt, kann der Domänencontroller nach der Wiederherstellung des Systemstatus möglicherweise nicht neu gestartet werden.

- ▶ Ein weiteres Problem tritt auf, wenn das alte und neue System unterschiedliche Hardware Abstraction Layer (HAL) verwenden. Dies ist der Fall, wenn der neue Domänencontroller auf einem Multi-Prozessor-System betrieben wird, der alte jedoch nicht. Da bei der Sicherung des Systemstatus zwar die Datei *kernel32.dll* gesichert wird, nicht jedoch die *hal.dll*, kann das System nicht wiederhergestellt werden. Sie haben dann lediglich die Möglichkeit, die alte *hal.dll* manuell auf dem neuen System zu installieren. Allerdings wird das neue System dann nur als Ein-Prozessor-System angesehen. Dies ist aber die einzige Möglichkeit der Wiederherstellung auf einem System mit unterschiedlicher HAL, wenn Sie keine Neuinstallation ohne Backup wünschen.
- ▶ Überprüfen Sie auch die Datei *Boot.ini*. In ihr müssen die Starteinträge für das neue System angepasst werden.
- ▶ Verfügt das neue System über eine andere Grafikkarte oder Netzwerkkarte, so deinstallieren Sie diese Geräte über den Gerätemanager, bevor Sie die Wiederherstellung starten. Beim Neustart des Domänencontrollers werden die geänderten Geräte über Plug&Play erkannt, oder aber – sofern diese nicht Plug&Play-fähig sind – Sie können nun die neuen Treiber installieren.

21.8 Defragmentieren der Active Directory-Datenbank

Dieses Kapitel beschäftigt sich mit der Defragmentierung der Active Directory-Datenbank. Diese wird wie beim Defragmentieren herkömmlicher Datenträger zur Verbesserung der Performance durchgeführt. Dabei wird zwischen zwei verschiedenen Varianten unterschieden: der Online- und der Offline-Defragmentierung.

21.8.1 Die Online-Defragmentierung

Die Online-Defragmentierung wird vom Betriebssystem automatisch alle zwölf Stunden durchgeführt. Dabei bleibt der Domänencontroller online. Dieser Prozess gehört zur Windows-internen so genannten Garbage Collection. Dabei werden zunächst alle Objekte gelöscht, die zu diesem Zeitpunkt ein Tombstoning-Flag besitzen, das sie als älter als 60 Tage (Standard) kennzeichnet. Danach werden alle nicht mehr benötigten Logdateien entfernt. Zum Schluss findet die eigentliche Defragmentierung statt. Der so gewonnene Platz steht für neue Objekte zur Verfügung. Die Größe der Datenbankdatei *NTDS.DIT* wird beim Löschen der Objekte jedoch nicht reduziert. Es findet nur eine Optimierung für die Speicherung neuer Daten statt.

Das standardmäßige Intervall der Online-Defragmentierung von zwölf Stunden können Sie auch ändern. Öffnen Sie dazu beispielsweise mit *ADSIEDIT* das Objekt *garbageCollPeriod*. Dieses Objekt finden Sie unter *CN=DIRECTORY SERVICE,CN=WINDOWS NT,CN=SERVICES,CN=CONFIGURATION,DC=(DOMÄNENNAME),DC=(TLD)*.

21.8.2 Die Offline-Defragmentierung

Bei der Offline-Defragmentierung wird die Datenbankdatei *NTDS.DIT* neu geschrieben. Je nach Defragmentierungsgrad kann die neue *NTDS.DIT* dabei kleiner werden als die ursprüngliche Datei. Um diesen komplexeren Vorgang durchzuführen, muss der Domänencontroller offline genommen werden. Um die Offline-Defragmentierung durchzuführen, müssen Sie folgende Schritte ausführen:

1. Erstellen Sie zunächst mit dem Windows-Sicherungs-Assistenten ein Backup des Active Directory. Dieser Schritt ist zwar optional, sollte aber durchgeführt werden. Wählen Sie dazu die Option, den Systemstatus zu sichern.
2. Führen Sie auf dem Domänencontroller einen Neustart durch. Wählen Sie dabei die erweiterte Startoption VERZEICHNISDIENST WIEDERHERSTELLEN aus und melden sich mit dem Passwort des Administrators zur Systemherstellung an.
3. Starten Sie an der Eingabeaufforderung *NTDSUTIL*. Geben Sie dann `files` ein und danach `info` . Sie erhalten nun die aktuellen Angaben zur Größe und zum Pfad der Datenbank und deren Protokolldateien. Notieren Sie sich den Pfad zur Datenbank.
4. Legen Sie nun einen neuen Ordner an, in dem die komprimierte Datenbank gespeichert werden kann. Geben Sie dann `compact to <Laufwerk>:\<Verzeichnis>` zu dem eben erstellten Verzeichnis ein.
5. Dadurch wird eine neue Datenbankdatei *NTDS.DIT* in dem gewählten Ordner erstellt. Ist der Vorgang beendet, beenden Sie *NTDSUTIL* mit `quit` .
6. Kopieren Sie nun die neu erstellte *NTDS.DIT* über die alte Datenbankdatei, deren Pfad Sie sich vorhin notiert haben.
7. Danach wird der Domänencontroller neu gestartet.

Der Domänencontroller besitzt nun eine defragmentierte und wahrscheinlich auch in der Größe reduzierte neue Datenbankdatei. An dieser neuen Datenbankdatei wird wie oben beschrieben ab jetzt die Online-Defragmentierung alle zwölf Stunden durchgeführt. Die Online-Defragmentierung wird bis zur Durchführung einer erneuten Offline-Defragmentierung angewendet.

Die Offline-Defragmentierung muss für jeden Domänencontroller separat durchgeführt werden. Bei der Replikation spielt es keine Rolle, ob eine Datenbank offline defragmentiert wurde oder nicht. Die physischen Änderungen an der Datenbank durch die Defragmentierung werden auch nicht über die Replikation weitergegeben. Da die Domänencontroller immer in einer festen Reihenfolge die Änderungen der Objekte replizieren, verfügen sie auch fast immer über den gleichen Grad der Defragmentierung. Also sollten Sie zu einem bestimmten Zeitpunkt sämtliche Domänencontroller nach und nach der Offline-Defragmentierung unterziehen.

21.8.3 Die Größe der Datenbankdatei NTDS.DIT

Normalerweise würde man annehmen, dass die Datenbankdatei *NTDS.DIT* auf allen Domänencontrollern die gleiche Größe besitzt. Dies ist in der Realität jedoch oft nicht der Fall. Zum einen hängt die Größe vom Zustand der Fragmentierung ab. Wurde die Daten-

bank längere Zeit keiner Offline-Defragmentierung unterzogen, so nimmt die Größe zu. Bei der Online-Defragmentierung wird die Größe nicht reduziert.

Weiterhin wird vom NTFS-Dateisystem immer nur die Größe der Datei angezeigt, die sie zu dem Zeitpunkt hatte, als sie das erste Mal geöffnet wurde. Wurden zwischenzeitlich neue Objekte ins Active Directory aufgenommen, so wird die dadurch entstandene Größenänderung erst angezeigt, wenn der Domänencontroller neu gestartet wurde.

Gerade in Gesamtstrukturen mit zahlreichen Domänen sind die Datenbankdateien auf den Domänencontrollern, die gleichzeitig auch als globaler Katalog dienen, unter Umständen wesentlich größer als die der herkömmlichen Domänencontroller, da sie Informationen zu allen Objekten der vollständigen Gesamtstruktur speichern.

21.9 Active Directory-Kontingente unter Windows Server 2003

Active Directory-Kontingente sind ein neues Feature des Windows Server 2003. Wie bei NTFS-Datenträgerkontingenten wird auch bei dem Active Directory-Kontingent pro Benutzer eine Grenze festgelegt, wie viele Objekte er in einer Domäne erstellen darf, die damit in seinen Besitz übergehen. Standardmäßig kann jeder Benutzer in einer Domäne zehn Computerkonten anlegen, auch wenn er nicht über die Berechtigung „Computer erstellen“ verfügt. Dies gilt für Domänen unter Windows 2000 sowie 2003.

Dieser Wert wird im Attribut *ms-DS-MachineAccountQuota* des Domänennamensraums festgelegt. Dieses Attribut können Sie über das Support-Tool *ADSIEDIT* (siehe Kapitel 23.1.2) bearbeiten. Somit ist es auch möglich, Benutzern generell das Erstellen von Computerkonten in der Domäne zu untersagen.

Die neue Kontingentgrenze kann sowohl für einzelne Benutzer als auch für Gruppen und Computer festgelegt werden. Sofern Sie ein Kontingent für eine Gruppe einrichten, gilt dieses Kontingent für alle Mitglieder dieser Gruppe zusammen. Mit Hilfe dieses Kontingents kann beispielsweise erreicht werden, dass ein Unter-Administrator einer bestimmten OU maximal die vom Administrator vorgegebene Anzahl von Benutzer-Objekten erstellen kann. Der Domänencontroller unter Windows Server 2003 überwacht die Anzahl der erstellten Objekte. Deshalb kann auch kein Domänencontroller unter Windows Server 2000 verwendet werden. Es ist jedoch unerheblich, welche Domänenfunktions- und Gesamtstrukturfunktionsebene ausgeführt wird.

Um das Active Directory-Kontingent zu bearbeiten, verwenden Sie an der Kommandozeile die Befehle *DSADD Quota* und *DSMOD Quota*. Eine GUI-basierte Bearbeitung ist nicht möglich. Für diese beiden Befehle stehen die folgenden Parameter zur Verfügung (siehe Tabelle 21.4 und 21.5). Für die Einrichtung und Bearbeitung von Kontingentgrenzen müssen Sie über die Berechtigung eines Domänenadministrators verfügen.

Mit *DSADD QUOTA* können Sie ein Active Directory-Kontingent auf einer Verzeichnispartition anlegen.

Befehle für DSADD QUOTA	Beschreibung
-part <DN der Partition>	Gibt den Namen der Verzeichnispartment an, für die ein Kontingent erstellt werden soll. Dieser Parameter muss gesetzt werden.
-rdn <RDN>	Gibt den relativen definierten Namen des Datenträgerkontingents an. Wird der Parameter nicht gesetzt, wird automatisch der Name <Domäne>_<Konto> verwendet. Der Name für Domäne und Konto ergeben sich aus den unter -acct angegebenen Werten.
-acct Benutzername	Dieser erforderliche Parameter gibt das Sicherheitsprincipal (Benutzer, Computer, Gruppe) an, für die das Kontingent erstellt wird. Der Name kann als definierter Name oder in der Form Domäne\Benutzername angegeben werden.
-qlimit <Wert>	Dieser Wert gibt an, wie viele Objekte dem Benutzer in der angegebenen Partition maximal gehören dürfen. Wird der Wert -1 angegeben, ist das Kontingent unbegrenzt.
-desc <Beschreibung>	Dieser Parameter gibt eine Beschreibung für das zu erstellende Kontingent an.
-s <Server> -d <Domäne>	Wird hier ein Wert für einen Server oder eine Domäne angegeben, so wird eine Verbindung mit der angegebenen Domäne hergestellt und nicht mit der aktuellen Domäne, in der sich der Computer befindet.
-u <Benutzername>	Hier können Sie einen anderen Benutzernamen angeben als den aktuellen Anmeldennamen. Der Name kann im Format Benutzername, Domäne\Benutzername oder Benutzername@domäne angegeben werden.
-p <Kennwort>	Geben Sie hier das zum unter -u angegebenen Konto gehörige Kennwort an. Bei der Verwendung von * werden Sie zur Eingabe des Passworts aufgefordert.
-q	Dieser Parameter schaltet den silent-Modus ein. Es wird nur die Standardausgabe angezeigt.
-uc -uco -uci	Diese drei Parameter sind optional. Mit -uc wird die Ein- und Ausgabe im Unicode-Format angezeigt, mit -uco die Ausgabe und mit -uci die Eingabe.
/?	Dieser Parameter zeigt die Programm-Hilfe an.

Tabelle 21.4: Die Parameter für den Befehl DSADD QUOTA

Mit `DSMOD QUOTA` können Sie Attribute an bereits erstellten Active Directory-Kontingenten bearbeiten.

Befehle für <code>DSMOD QUOTA</code>	Beschreibung
<definierter Name des Datenträgerkontingents>	Hiermit geben Sie den definierten Namen des Kontingents an, über das Sie Informationen beziehen möchten. Dieser Parameter muss gesetzt sein.
-qlimit <Wert>	Dieser Wert gibt an, wie viele Objekte dem Benutzer in der angegebenen Partition maximal gehören dürfen. Wird der Wert -1 angegeben, ist das Kontingent unbegrenzt.
-desc <Beschreibung>	Dieser Parameter gibt eine Beschreibung für das zu erstellende Kontingent an.
-s <Server> -d <Domäne>	Wird hier ein Wert für einen Server oder eine Domäne angegeben, so wird eine Verbindung mit der angegebenen Domäne hergestellt und nicht mit der aktuellen Domäne, in der sich der Computer befindet.
-u <Benutzername>	Hier können Sie einen anderen Benutzernamen angeben als den aktuellen Anmeldenamen. Der Name kann im Format <code>Benutzername, Domäne\Benutzername</code> oder <code>Benutzername@domäne</code> angegeben werden.
-p <Kennwort>	Geben Sie hier das zum unter -u angegebenen Konto gehörige Kennwort an. Bei der Verwendung von * werden Sie zur Eingabe des Passworts aufgefordert.
-c	Ist dieser Parameter gesetzt, wird der Befehl auch fortgesetzt, wenn ein Fehler aufgetreten ist. Es wird nur eine Fehlermeldung ausgegeben. Es erfolgt jedoch kein Abbruch.
-q	Dieser Parameter schaltet den silent-Modus ein. Es wird nur die Standardausgabe angezeigt.
-uc -uco -uci	Diese drei Parameter sind optional. Mit -uc wird die Ein- und Ausgabe im Unicode-Format angezeigt, mit -uco die Ausgabe und mit -uci die Eingabe.

Tabelle 21.5: Die Parameter für den Befehl `DSMOD QUOTA`

Beispiele

Soll einem Benutzer mit dem Benutzernamen `pmustermann` aus der Domäne `firma.de` die Berechtigung zugewiesen werden, maximal 100 Objekte erstellen zu dürfen, so verwenden Sie den Befehl

```
DSADD QUOTA -PART DC=firma,DC=de -ACCT FIRMA\pmustermann -qlimit 100 
```

Das Limit ist nicht unbedingt dann erreicht, wenn ein Benutzer, der 100 Objekte in seinem Besitz haben darf, Objekt Nr. 101 erstellt. Da auch sämtliche bereits gelöschten Objekte, deren Tombstone-Intervall (siehe Kapitel 21.4) noch nicht abgelaufen ist, zu der Anzahl der aktuellen Objekte addiert werden, kann die Kontingentgrenze auch schon früher erreicht sein. Es ist jedoch möglich, dieses Verhalten so zu ändern, dass wirklich nur die aktuellen, nicht jedoch die gelöschten Objekte unter diese Kontingentgrenze fallen. Hierzu verwenden Sie den Befehl

```
DSMOD PARTITION _QTMBSNWT Prozentangabe [↵].
```

Die Prozentangabe definiert, zu welchem Prozentanteil ein gelöschttes Objekt zum aktuellen Besitzanteil gerechnet wird. Legen Sie den Wert auf 33% fest, wird ein gelöschttes Objekt nur zu einem Drittel berechnet. Ist für einen Benutzer eine Kontingentgrenze von 100 Objekten festgelegt, so kann er entweder 100 aktuelle Objekte besitzen oder bis zu 300 gelöschte Objekte – was sicherlich in der Realität nicht vorkommen wird – oder eine Kombination aus beiden Werten, z.B. 80 aktuelle Objekte sowie 60 gelöschte Objekte. Standardmäßig liegt der Wert für die Prozentangabe bei 100%, sodass aktuelle und gelöschte Objekte zu gleichen Anteilen zusammengerechnet werden.

Nachdem Sie dieses Kontingent erstellt haben, befindet sich im Container NTDS Quotas ein neues Objekt. In unserem Beispiel trägt es den Namen FIRMA_pmustermann. Um dieses Objekt betrachten zu können, müssen Sie in der mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER im Menü ANSICHT die Option ERWEITERTE FUNKTIONEN wählen. Trägt ein Active Directory-Kontingent den Wert „-1“, so ist keine Kontingentgrenze festgelegt.

Um nähere Informationen über das Active Directory-Kontingent zu erhalten, benutzen Sie an der Kommandozeile den Befehl DSGET QUOTA. Wollen Sie Informationen über das Quotas-Objekt FIRMA_pmustermann erhalten, so verwenden Sie folgenden Befehl:

```
DSGET QUOTA „CN=FIRMA_pmustermann, CN=NTDS Quotas, DC=firma, DC=de“ -ACCT -QLIMIT [↵]
```

Wollen Sie ermitteln, welcher Benutzer der Domäne *firma.de* die meisten Objekte besitzt, benutzen Sie den Befehl:

```
DSGET PARTITION DC=firma, DC=de -TOPOBJOWNER 0 [↵]
```

21.10 Regelmäßige administrative Aufgaben

Dieses Kapitel gibt Ihnen Empfehlungen, welche administrativen Aufgaben in welchem Intervall durchgeführt werden sollten. Dabei wird unterschieden in die Kategorien täglich, wöchentlich, monatlich sowie bei Bedarf. Die empfohlenen Werte können dabei abhängig von der Größe des Active Directory, der Anzahl der Benutzer, Standorte usw. abweichen, sollten aber nicht in größeren als den angegebenen Intervallen ausgeführt werden.

21.10.1 Tägliche Aufgaben

Zu den täglichen Aufgaben eines Administrators zählen die folgenden Arbeiten:

- ▶ Verfügbarkeitsprüfung sämtlicher Domänencontroller.
- ▶ Überprüfen jedes Domänencontrollers auf Fehler und Warnungen im Ereignisprotokoll und möglichst zeitnahe Lösung dieser. Dabei sind zunächst Fehler, dann Warnungen zu analysieren.
- ▶ Überprüfen, ob Probleme mit der Zeitsynchronisierung zwischen den Domänencontrollern vorliegen und die Clients über korrekte Zeiteinstellungen verfügen. Das Kerberos-Authentifizierungsprotokoll erfordert, dass die Zeiteinstellungen zwischen den Domänencontrollern und Clients, die diese Authentifizierungsmethode verwenden, synchronisiert sind.
- ▶ Prüfen Sie, ob die folgenden Dienste Fehlermeldungen ausgeben: Net Logon, FRS, W32Time, KDC und ISMSERV (Intersite Messaging Service). Active Directory beruht auf diesen Diensten, die auf jedem Domänencontroller ausgeführt werden müssen.
- ▶ Gibt es Fehlermeldungen bezüglich SYSVOL? Ist der SYSVOL-Ordner freigegeben? Sofern SYSVOL nicht freigegeben ist, können keine Gruppenrichtlinien angewendet werden.
- ▶ Prüfen Sie die DNS-Einträge des Domänencontrollers. Ist ein Domänencontroller nicht korrekt im DNS eingetragen, kann dieser keine LDAP- oder sonstigen Dienst Anfragen korrekt beantworten.
- ▶ Gibt es Standorte, an denen momentan kein globaler Katalogserver verfügbar ist?

21.10.2 Wöchentliche Aufgaben

Mindestens einmal pro Woche sollten die folgenden Aufgaben durchgeführt werden:

- ▶ Suchen Sie im Ereignisprotokoll nach allen Einträgen, die auf Probleme mit der Zeitsynchronisierung und der Authentifizierung hindeuten. Ansonsten kommt es zu Problemen bei der Kerberos-Authentifizierung.
- ▶ Deuten Fehlermeldungen auf abgelaufene Kennwörter hin? Diese Kennwörter müssen zurückgesetzt werden, damit sich Computer und Benutzer wieder an der Domäne authentifizieren können.
- ▶ Überprüfen Sie sämtliche Vertrauensstellungen. Sind die vorhandenen Vertrauensstellungen noch notwendig? Sind die Kennwörter für die Vertrauensstellungen zwischen Domänen oder Gesamtstrukturen noch gültig?
- ▶ Prüfen Sie die Aufzeichnungen der Überwachungsrichtlinie (siehe Kapitel 22.1).
- ▶ Führen Sie eine Sicherheitsanalyse durch (siehe Kapitel 22.6).

21.10.3 Monatliche Aufgaben

Diese Aufgaben sollten mindestens einmal pro Monat durchgeführt werden. Je nach Größe des Unternehmens kann das Intervall aber auch minimiert werden.

- ▶ Überprüfen Sie auf sämtlichen Domänencontrollern den verfügbaren Speicherplatz. Die Partitionen, auf denen sich die Active Directory-Datenbank sowie die Logdateien befinden, müssen immer über ausreichend freie Festplattenkapazität verfügen.

- ▶ Überprüfen Sie, ob auf allen Domänencontrollern dasselbe Servicepack und dieselben Hotfixes installiert sind. Verschiedene Versionen des Betriebssystems können zu unvorhersehbaren Problemen führen.
- ▶ Überprüfen Sie die globalen Katalogserver jedes Standorts.
- ▶ Führen Sie mindestens alle 30 Tage ein Backup des Active Directory durch, sodass Sie für ein Tombstoning-Intervall von 60 Tagen über mindestens zwei Backups verfügen.
- ▶ Betrachten Sie alle relevanten Logdateien und Protokolle. Sind darin stets wiederkehrende Einträge, die auf Probleme schließen lassen? Müssen für bestimmte Punkte Loglevel heraufgesetzt oder können Loglevel herabgesetzt werden?
- ▶ Sofern Sie MOM (Microsoft Operations Manager) einsetzen, überprüfen Sie die Health Monitoring Reports. Darunter sind alle auf die Performance bezogenen Reports zusammengefasst. Hieraus können Sie ableiten, ob sich an einigen Stellen Kapazitätsengpässe ergeben, die zu beheben sind.

21.10.4 Aufgaben bei Bedarf

Für die folgenden Aufgaben kann kein fester Zeitrahmen vorgegeben werden. Sie werden immer dann durchgeführt, wenn die Situation es erfordert, im Regelfall also, wenn ein Problem aufgetreten ist oder eine Erweiterung bzw. Umstrukturierung des Active Directory ansteht.

- ▶ Vorbereiten und Durchführen der Active Directory-Installation. Kontrolle der Installation und Integration der neu installierten Komponenten.
- ▶ Wiederherstellen eines Domänencontrollers durch Neuinstallation und evtl. Backup.
- ▶ Durchführen nicht autorisierender Wiederherstellungen.
- ▶ Durchführen autorisierender Wiederherstellungen für das gesamte Active Directory oder Teile davon.
- ▶ Hinzufügen oder Entfernen globaler Katalogserver zur Gesamtstruktur.
- ▶ Fehlerhafte Domänencontroller außer Betrieb nehmen.
- ▶ Fehlerhafte Betriebsmaster außer Betrieb nehmen.
- ▶ Übernehmen von Betriebsmasterrollen.
- ▶ Zuweisen von Betriebsmasterrollen.
- ▶ Einrichten von Standby-Betriebsmastern.
- ▶ Verschieben des SYSVOL-Ordners via Assistent oder manuell. Update des SYSVOL-Pfades sowie Wiederherstellen von SYSVOL.
- ▶ Neuen Speicherort für den Ordner Staging Area festlegen.
- ▶ Zugewiesenen Speicherplatz für Staging Area ändern.
- ▶ Hinzufügen und Konfigurieren neuer Standorte, Festlegen des Subnetzes für einen Standort. Hinzufügen von Domänencontrollern zum neuen Standort.
- ▶ Löschen von Standorten.
- ▶ Einrichten und Entfernen von externen Vertrauensstellungen.
- ▶ Festlegen einer externen Zeitquelle für die Gesamtstruktur. Konfiguration der Clients zum Benutzen einer bestimmten Zeitquelle.
- ▶ Umbenennen von Domänen und Domänencontrollern.

21.11 Das Umbenennen von Domänen

Eine häufig gestellte Frage lautet, ob es möglich ist, bereits bestehende Domänen umzubenennen. Auf diese Frage kann keine generelle Antwort gegeben werden. Im Einzelfall ist zu prüfen, welche Domänensituation vorliegt, d.h., wird die Domäne im einheitlichen oder gemischten Modus betrieben, oder verwenden Sie eine reine Windows 2003-Domänenlandschaft.

21.11.1 Umbenennen einer Windows 2003-Domäne

Benutzen Sie eine reine 2003-Domäne, so können Sie mithilfe des Tools *RENDOM* (siehe Kapitel 23.2.1) Domänen umbenennen sowie auch die Struktur der Domänen bearbeiten. So können Sie z.B. eine Subdomäne zu einer Domäne zweiter Ordnung heraufstufen, indem Sie ihren Namen ändern und ihr damit gleichzeitig die neue Position innerhalb der Hierarchie mitteilen. Hierbei bestehen jedoch folgende Einschränkungen:

- ▶ Sie können nicht ändern, welche Domäne die Root-Domäne einer Gesamtstruktur ist. Es ist lediglich möglich, den DNS- und / oder NetBIOS-Namen dieser Domäne zu ändern.
- ▶ Innerhalb eines Umbenennungsvorganges können Sie einer Domäne nicht denselben Namen geben wie einer Domäne, deren Name innerhalb desselben Arbeitsschrittes umbenannt wurde. Sie müssen also *RENDOM* zweimal ausführen, um einer Domäne den alten Namen einer umbenannten Domäne zu geben.
- ▶ Sie können zu einer Gesamtstruktur keine zusätzlichen Domänen hinzufügen bzw. aus dieser entfernen. Die Anzahl der Domänen muss vor und nach dem Umbenennen bzw. Umstrukturieren gleich sein.

21.11.2 Umbenennen einer Windows 2000-Domäne im einheitlichen Modus

Wird eine Domäne unter Windows 2000 im einheitlichen Modus ausgeführt, so besteht keine Möglichkeit, die Domäne umzubenennen. Der DNS- und NetBIOS-Name der Domäne kann nicht geändert werden. Sie können lediglich eine neue Domäne erstellen und in diese mithilfe des Support-Tools *MOVETREE* (siehe Kapitel 23.1.15) die vorhandenen Objekte verschieben. Die Domäne selbst kann nicht verschoben werden.

Auch für das Umstrukturieren der Domänenlandschaft müssen Sie einige Umwege gehen. Wollen Sie eine bestehende Domäne in zwei Domänen unterteilen, so müssen Sie eine neue Domäne erstellen und die gewünschten Objekte in diese via *MOVETREE* verschieben. Sollen beide neuen Domänen einen neuen Namen und eine neue Position erhalten, so müssen Sie beide Domänen neu erstellen und dann die Objekte verschieben. Wollen Sie hingegen zwei Domänen zu einer zusammenlegen, so müssen Sie zunächst sämtliche Objekte einer Domäne in die andere verschieben. Danach können Sie sämtliche Domänencontroller der nicht mehr benötigten Domäne herabstufen und damit die Domäne löschen.

21.11.3 Umbenennen einer Windows 2000-Domäne im gemischten Modus

Wird die 2000-Domäne noch im gemischten Modus betrieben, so können Sie die Domäne umbenennen, indem Sie den Umweg über einen zusätzlichen Windows NT-BDC gehen. Dabei wird ein NT-BDC auf einen Windows 2000-Domänencontroller aktualisiert, der bei der Installation des Active Directory den neuen DNS-Namen der Domäne erhält. Der NetBIOS-Name wird dabei nicht geändert. Alle bestehenden Windows 2000-Domänencontroller müssen zuvor zu Mitgliedsservern herabgestuft und später als zusätzliche Domänencontroller zur umbenannten Domäne hinzugefügt werden. Je nach Anzahl der Domänen und Domänencontroller sowie deren Verbindung untereinander kann dieser Prozess jedoch sehr langwierig werden, aber er stellt die einzige Möglichkeit dar, eine Windows 2000-Domäne umzubenennen.

Sofern sich unter der umzubenennenden Domäne untergeordnete Domänen befinden, so müssen Sie diese alle zuerst auf die Windows NT-Ebene bringen. Nachdem dann die übergeordnete Domäne umbenannt ist, erhalten die Domänencontroller beim Update den neuen Namen der untergeordneten Domäne.

Im Folgenden werden die Schritte aufgezeigt, die Sie zum Umbenennen einer Domäne durchführen müssen, die über keine untergeordneten Domänen verfügt. Verfügt die Domäne über untergeordnete Domänen, so muss zunächst in jeder dieser Domänen Schritt 1 bis 6 ausgeführt werden. Danach führen Sie in der übergeordneten Domäne alle acht Schritte aus sowie anschließend die Schritte 7 und 8 in der untergeordneten Domäne.

1. Erstellen Sie von sämtlichen Domänencontrollern ein Backup.
2. Installieren Sie entweder auf einem vorhandenen NT-BDC Servicepack 6a oder fügen einen neuen NT-BDC mit SP 6a zur Domäne hinzu. Optional können Sie einen zweiten BDC einrichten, der als Backup der aktuellen Domänendaten während der Umbenennung vom Netzwerk getrennt sein muss.
3. Um sicherzustellen, dass sich auf dem NT-BDC (und auch dem optionalen zweiten BDC) alle aktuellen Domänensicherheits- sowie SAM-Informationen befinden, warten Sie die Replikation ab oder führen auf dem NT-BDC den Befehl `net accounts /sync`  aus. Sehen Sie danach im Ereignisprotokoll des Systems nach, ob die vollständige Replikation erfolgreich durchgeführt wurde.
4. Befindet sich nur ein einziger Windows 2000-Domänencontroller in der Domäne, so trennen Sie diesen vom ursprünglichen Netzwerk. Der NT-BDC muss selbstverständlich mit dem Netzwerk verbunden bleiben.
5. Führen Sie nun auf sämtlichen Domänencontrollern den Befehl `DCPROMO` aus, um diese zu Mitgliedsservern herabzustufen. Ist nur noch ein Windows 2000-Domänencontroller übrig, so entfernen Sie diesen aus dem ursprünglichen Netzwerk. Auf diesem letzten Domänencontroller bzw. dem einzigem Domänencontroller, den Sie im letzten Schritt vom Netzwerk getrennt haben, führen Sie auch `DCPROMO` zum Herabstufen aus. Achten Sie darauf, dass die Option **DIESES IST DER LETZTE DOMÄNEN-CONTROLLER DER DOMÄNE** aktiviert ist. Zum Herabstufen muss jedoch eine aktive Netzwerkverbindung bestehen. Verbinden Sie den letzten Domänencontroller mit einem Switch oder Hub, an den keine weiteren Computer angeschlossen sind.

6. Der NT-BDC wird nun zum NT-PDC heraufgestuft. Diese Aufgabe wird über den Server-Manager ausgeführt. Während des Heraufstufens erhalten Sie möglicherweise die Fehlermeldung, dass keine Verbindung zum PDC hergestellt werden kann. Ignorieren Sie diese Meldung und fahren fort. Starten Sie den Server neu und prüfen, ob er im Server-Manager nun als PDC angezeigt wird.
7. Aktualisieren Sie den NT-PDC nun auf Windows 2000. Bei der Installation des Active Directory geben Sie den neuen DNS-Namen der Domäne an.
8. Als Letztes müssen Sie auf allen ehemaligen Domänencontrollern, die zu Mitglieds-
servern herabgestuft worden sind, das Active Directory neu installieren. Fügen Sie diese der umbenannten Domäne als zusätzliche Domänencontroller hinzu.

22 Überwachung und Sicherheit

Dieses Kapitel befasst sich mit der Überwachung und Sicherheit unter Windows 2000 und 2003 Server sowie speziellen Einstellungen dazu für das Active Directory. Zunächst lernen Sie die Überwachungsrichtlinien von GPOs sowie deren Konfiguration auf Domänencontrollern und Clients kennen. Ein weiterer Bestandteil der Überwachung ist die Zugriffsüberwachung auf Active Directory-Objekte, Drucker sowie Dateien und Ordner. Der zweite Teil des Kapitels widmet sich der Sicherheit. Es werden alle Richtlinien aufgezeigt, die zur Konfiguration der Sicherheit vorhanden sind. Weiterhin werden auch die Sicherheitsvorlagen vorgestellt. Sie bieten bereits vorkonfigurierte Richtlinien auf verschiedenen Sicherheitsleveln. Neben der Konfiguration wird auch die Analyse der Sicherheit besprochen. Als ein spezielles Beispiel werden zum Schluss die verschiedenen Optionen der Kerberos-Richtlinie und deren Auswirkungen bei Änderungen vorgeführt. Ferner wird auch die Leistungsüberwachung des Active Directory vorgestellt. Die zentralen Werkzeuge dazu sind der Systemmonitor, die Leistungsdatenprotokolle und die Ereignisanzeige, deren Protokolle mithilfe von Support-Tools z.B. an eine Tabellenkalkulation weitergeleitet werden können. Zusätzlich erfahren Sie, wie Sie weitere Logs aufzeichnen können, indem Sie das Diagnostic-Logging aktivieren.

22.1 Überwachungsrichtlinien

Mit Hilfe der Überwachung können Vorgänge verfolgt werden, die von einem Benutzer oder einem Computer am Betriebssystem oder einem Objekt durchgeführt werden. So können Sie beispielsweise überwachen, ob sich ein Benutzer erfolgreich an der Domäne authentifiziert hat oder nicht. Die zu überwachenden Ereignisse werden in der Überwachungsrichtlinie definiert und dann in der Ereignisanzeige in den Bereich Sicherheit geschrieben. Ereignisse, wie z.B. das erfolgreiche oder fehlgeschlagene Anmelden eines Benutzers an der Domäne, werden dabei nicht auf seinem lokalen Client-Computer, sondern im Ereignisprotokoll des Domänencontrollers aufgezeichnet.

22.1.1 Einrichten von Überwachungsrichtlinien

Die Überwachungsrichtlinien sind standardmäßig deaktiviert. Darin können die Kategorien festgelegt werden, die im Sicherheitsprotokoll angezeigt werden sollen.

Nach dem Wählen der zu überwachenden Computer und Kategorien müssen Sie entscheiden, ob Sie erfolgreiche und/oder fehlgeschlagene Ereignisse protokollieren möchten. Fehlgeschlagene Ereignisse, die sich in bestimmten Bereichen häufen, können auf unautorisierte Zugriffe und somit auf Sicherheitslücken schließen lassen. Aber auch aus erfolgreichen Zugriffen, z.B. auf bestimmte Drucker, können Sie Werte ermitteln, die Ihnen für eine künftige Planung von Ressourcen und Expansion wichtig sind. Hierbei ist auch die Auswertung von Ergebnissen über einen längeren Zeitraum wichtig.

Bei der Einrichtung der Überwachungsrichtlinie müssen Sie den Typ des zu überwachenden Computers unterscheiden. Handelt es sich um einen Domänencontroller, wird eine Richtlinie für alle DCs in der Domäne konfiguriert. Verwenden Sie zu diesem Zweck ein domänenweites GPO. Ist der zu überwachende Computer ein Mitgliedsserver, Standalone-Server oder Client-Computer, so sollten für diesen lokale Überwachungsrichtlinien eingerichtet werden.

Bevor Sie mit der Implementierung der Richtlinien beginnen, müssen Sie sicherstellen, dass sich die zu überwachenden Ressourcen auf NTFS-Laufwerken befinden. Außerdem müssen Sie über die Berechtigung Verwalten von Überwachungs- und Sicherheitsprotokollen für den zu überwachenden Computer verfügen. Standardmäßig besitzt nur ein Administrator diese Berechtigung.

Das Konfigurieren der Überwachung lässt sich in zwei Schritte unterteilen. Zunächst müssen Sie für die Überwachungsrichtlinie die Kategorien und die Ereignisse auswählen. Danach müssen Sie die Überwachung für spezielle Active Directory-Objekte wie Drucker, Freigaben usw. einrichten.

22.1.2 Überwachungsrichtlinien für Domänencontroller

Um eine Überwachungsrichtlinie für Domänencontroller einzurichten, führen Sie die folgenden Schritte aus:

1. Wählen Sie das gewünschte GPO aus, und öffnen Sie den Knoten COMPUTERKONFIGURATION / WINDOWS-EINSTELLUNGEN / SICHERHEITSEINSTELLUNGEN / LOKALE RICHTLINIE / ÜBERWACHUNGSRICHTLINIEN.



Abbildung 22.1: Die Kategorien der Überwachungsrichtlinie

2. Insgesamt stehen Ihnen neun verschiedene Kategorien zur Verfügung, die überwacht werden können. Damit die Richtlinie ACTIVE DIRECTORY-ZUGRIFF ÜBERWACHEN wirksam wird, müssen Sie die zu überwachenden Active Directory-Objekte konfigurieren. Dies wird in Kapitel 22.2.1 beschrieben.
3. Wählen Sie die gewünschte Richtlinienkategorie und wählen aus deren Kontextmenü SICHERHEITSEINSTELLUNGEN. In der Dialogbox VORLAGE FÜR SICHERHEITSRICHTLINIE markieren Sie die Checkbox ERFOLG oder FEHLGESCHLAGEN. Sie können auch beide Ereignistypen überwachen.
4. Fahren Sie fort, bis Sie alle Kategorien ausgewählt haben. Bedenken Sie aber auch, dass umfangreiche Protokollierungen auch Speicherplatz und Performance beanspruchen.
5. Damit die gewählten Richtlinien wirksam werden, starten Sie entweder den Rechner neu oder warten fünf Minuten ab. Diesen Zeitraum benötigt der Domänencontroller, damit er seine Gruppenrichtlinieneinstellungen aktualisieren kann. Sollen die Einstellungen sofort ohne Neustart wirksam werden, geben Sie an der Eingabeaufforderung folgenden Befehl ein:

```
secedit /refreshpolicy machine_policy 
```

Die Ergebnisse aller überwachten Richtlinien können Sie im Ereignisprotokoll unter Directory Service betrachten. Suchen Sie nur nach bestimmten Ereignissen, z.B. einer bestimmten Ereignisquelle oder einem bestimmten Benutzer, so sollten Sie einen entsprechenden Filter auf das Protokoll anwenden. Sie finden den Filter in den Eigenschaften des Protokolls DIRECTORY SERVICE auf der Registerkarte FILTER.

22.1.3 Überwachungsrichtlinien für Mitgliedsserver und Clients

Um Überwachungsrichtlinien für die Mitgliedsserver und Clients einer Domäne einzurichten, erstellen Sie zunächst eine Organisationseinheit, der Sie die Computerkonten für die zu überwachenden Computer hinzufügen.

Danach wählen Sie das GPO aus, das Sie auf diese Organisationseinheit anwenden möchten, und konfigurieren dieses, wie im letzten Kapitel beschrieben.

22.2 Zugriffsüberwachung auf Active Directory-Ressourcen

In diesem Kapitel wird beschrieben, wie Sie die Zugriffsüberwachung für Active Directory-Objekte, z.B. Drucker, oder aber auch für bestimmte unternehmenswichtige Dateien und Ordner konfigurieren.

22.2.1 Zugriffsüberwachung für Active Directory-Objekte

Sie können den Zugriff für beliebige Active Directory-Objekte wie Computer, Benutzer oder Organisationseinheiten konfigurieren. Voraussetzung für die Überwachung ist, dass Sie die Überwachungsrichtlinie ACTIVE DIRECTORY-ZUGRIFF ÜBERWACHEN (siehe Abbildung 22.1) aktiviert haben.

Um die Überwachung für ein bestimmtes Active Directory-Objekt zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Öffnen Sie die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER. Wählen Sie aus dem Menü ANSICHT die erweiterten Funktionen.
2. Markieren Sie das zu überwachende Objekt und wählen aus dem Kontextmenü EIGENSCHAFTEN die Registerkarte SICHERHEIT. Wählen Sie ERWEITERT.
3. Sie erhalten das Fenster ERWEITERTE SICHERHEITSEINSTELLUNGEN. Wählen Sie dort die Registerkarte ÜBERWACHUNG. Über HINZUFÜGEN werden die Benutzer und Gruppen ausgewählt, deren Zugriff auf das Objekt überwacht werden soll.
4. Wählen Sie dann die zu überwachenden Ereignisse aus. Sie können für jede Aktion ERFOLGREICH und / oder FEHLGESCHLAGEN auswählen.

Zugriffsüberwachung für Drucker

Im Active Directory veröffentlichte Objekte können auch Drucker sein. Für diese wird die Zugriffsüberwachung ähnlich konfiguriert wie eben beschrieben.

1. Öffnen Sie STARTMENÜ / EINSTELLUNGEN / DRUCKER und wählen die Eigenschaften des gewünschten Druckers.
2. Wählen Sie die Registerkarte SICHERHEITSEINSTELLUNGEN und dort die Schaltfläche ERWEITERT. Aktivieren Sie dann die Registerkarte ÜBERWACHEN und fügen die Benutzer und Gruppen hinzu, deren Zugriff auf den Drucker überwacht werden soll.
3. Sie können dann für die druckerspezifischen Zugriffe wie Drucken oder Drucker verwalten den erfolgreichen und / oder fehlgeschlagenen Zugriff überwachen.

22.2.2 Zugriffsüberwachung für Dateien und Ordner

Für spezielle unternehmenswichtige Dateien und Ordner sollte die Überwachung konfiguriert werden, damit rasch erkannt werden kann, wenn unbefugte Personen versuchen, auf bestimmte Dateien zuzugreifen. Damit diese Zugriffsüberwachung eingerichtet werden kann, müssen Sie aus den neun Kategorien der Überwachungsrichtlinie (siehe Abbildung 22.1) die Richtlinie OBJEKTZUGRIFFSVERSUCHE ÜBERWACHEN aktiviert haben.

Um die Überwachung für eine bestimmte Datei oder einen Ordner zu starten, führen Sie die folgenden Schritte aus:

1. Wählen Sie das gewünschte Objekt und öffnen die erweiterten Sicherheitseinstellungen. Wählen Sie dort die Registerkarte ÜBERWACHEN.
2. Klicken Sie auf HINZUFÜGEN, um die Benutzer, Gruppen oder Computer auszusuchen, deren Zugriffsversuche auf das Objekt protokolliert werden sollen.
3. Wählen Sie dann die Ereignisse aus, die aufgezeichnet werden sollen. Für jedes Ereignis können Sie ERFOLGREICH und / oder FEHLGESCHLAGEN wählen. Bestätigen Sie dann mit OK.
4. Bestimmen Sie dann – sofern es sich um einen Ordner handelt –, für welchen Bereich die Überwachung gelten soll (Ordner, Unterordner, Dateien).



Bei allen Arten der Überwachung sollten Sie bei der Auswahl der zu überwachenden Benutzer im Zweifelsfall die Gruppe „Jeder“ auswählen. Damit stellen Sie sicher, dass Sie jeden Benutzerzugriff protokollieren und nicht nur die Zugriffe der Benutzer, für die ein Benutzerkonto innerhalb der Domäne existiert.

22.3 Die Sicherheitsrichtlinien

Die Sicherheitsrichtlinien bestehen aus der Konfiguration, die Sie über GRUPPENRICHTLINIE / COMPUTER- / BENUTZERKONFIGURATION / WINDOWS-EINSTELLUNGEN / SICHERHEITSEINSTELLUNGEN für die Computer und Benutzer festlegen können. Als einen Teil davon haben Sie in Kapitel 22.2 bereits die Überwachungsrichtlinien der lokalen Richtlinien kennen gelernt. Sie öffnen die Sicherheitsrichtlinien über STARTMENÜ / VERWALTUNG / SICHERHEITSRICHTLINIE FÜR DOMÄNEN bzw. SICHERHEITSRICHTLINIE FÜR DOMÄNENCONTROLLER.

Für die Computerkonfiguration können Sie unter Windows 2000 neun, unter Windows Server 2003 sogar elf verschiedene Bereiche konfigurieren, für die Benutzerkonfiguration lediglich den Bereich RICHTLINIEN ÖFFENTLICHER SCHLÜSSEL.



Abbildung 22.2: Die Sicherheitseinstellungen eines GPO

Tabelle 22.1 gibt Ihnen einen Überblick über die Konfigurationsmöglichkeiten der einzelnen Bereiche:

Sicherheitsbereich	Beschreibung
Kontorichtlinien	Hier werden die Richtlinien für die Benutzerkonten festgelegt. Es handelt sich um die Bereiche Kennwörter, Kontosperrung und Kerberos. Es werden in einer Domäne die Einstellungen der Stammdomäne benutzt, es sei denn, auf OU-Ebene sind andere Kontorichtlinien definiert.
Lokale Richtlinien	Hier werden Einstellmöglichkeiten für Überwachungsrichtlinien, Zuweisung von Benutzerrechten und Sicherheitsoptionen geboten.
Ereignisprotokoll	Hier werden Einstellungen wie Aufbewahrungsdauer und maximale Größe des Anwendungs-, Sicherheits- und Systemprotokolls vorgenommen.
Eingeschränkte Gruppen	Über die eingeschränkten Gruppen wird die Mitgliedschaft der Standardgruppen überprüft. Angenommen, es werden temporär Benutzer über die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER zur Gruppe der Hauptbenutzer hinzugefügt, aber nicht wieder gelöscht, sobald sie die Berechtigungen nicht mehr benötigen. Hier können Sie die dauerhaften Mitglieder der Gruppen konfigurieren. Personen, die hier nicht aufgelistet sind, werden aus der Gruppe entfernt, sobald das GPO angewendet wird.
Systemdienste	Für jeden Dienst können Sie Startoptionen sowie die Zugriffsrechte für die Benutzer konfigurieren.
Registrierung	Hier können die Sicherheitseinstellungen für Benutzer und Gruppen an bestimmten Registry-Schlüsseln konfiguriert werden.
Dateisystem	Hier können die Sicherheitseinstellungen für Benutzer und Gruppen an Dateien und Ordnern konfiguriert werden.
Drahtlosnetzwerkrichtlinien (nur Windows Server 2003)	Hier können Richtlinien für drahtlose Netzwerke nach dem IEEE 802.11-Standard eingerichtet werden.
Richtlinien öffentlicher Schlüssel	Hier werden die Wiederherstellungsagenten für EFS, Zertifizierungsstellen und Zertifikatsvertrauenslisten eingerichtet.
Richtlinien für Softwareeinschränkung (nur Windows Server 2003/XP)	Hier können Zugriffsrechte für Software definiert werden. Es ist möglich, die bestehenden Berechtigungen außer Kraft zu setzen, diese Durchsetzung für alle Softwaredateien durchzusetzen oder die Dateitypen dafür zu bestimmen. Eine detaillierte Beschreibung dieser Richtlinien finden Sie in Kapitel 22.4.
IP-Sicherheitsrichtlinien	Hier wird die IP-Sicherheit im Netzwerk für Clients, Server und Secure Server konfiguriert.

Tabelle 22.1: Die Sicherheitsbereiche der Gruppenrichtlinien

22.4 Richtlinien zur Softwareeinschränkung unter Windows Server 2003

Der Windows Server 2003 sowie Windows XP bringen zwei neue Sicherheitsrichtlinien mit. Eine davon ist die Richtlinie für Softwareeinschränkung. Diese Richtlinie erleichtert Administratoren die Standardisierung verwendeter Software, indem das Benutzen und Ausführen zusätzlicher Applikationen, die nicht dem Unternehmensstandard entsprechen, dem Benutzer verweigert werden kann. Es sind in diesem Fall nicht nur Moorhühner und andere Spiele, die auf diese Weise gesichtet werden, sondern auch kleine Programme und Tools, die der Anwender zwar im guten Glauben installiert hat, damit seine Arbeit zu erleichtern, die aber möglicherweise im Zusammenspiel mit den Applikationen des Unternehmens in Konflikt treten können oder sogar möglicherweise Viren oder Trojanische Pferde enthalten. Durch diese zu lösenden Konflikte werden Helpdesk und Administratoren unnötig belastet. Unter Windows 9x kann der Benutzer quasi installieren, was er möchte. Aber auch die Betriebssysteme Windows NT/2000/XP minimieren bei einem gewöhnlichen Benutzer lediglich die Installationsmöglichkeiten, schließen sie aber keinesfalls vollständig aus.

Die Richtlinien für Softwarebeschränkung basieren auf Regeln, die die Benutzung von Software reglementieren. Dabei wird zunächst jede Applikation identifiziert und in einem zweiten Schritt geprüft, ob diese Software auf dem Computer des Benutzers autorisiert ist. Je nachdem, welche Sicherheitsebene angewendet wird, kann einer Applikation die Funktion untersagt oder gestattet werden.

Über insgesamt vier Regeln können Sie das Ausführen oder Verweigern einer Applikation steuern. Dabei handelt es sich um die Hashregeln, Internetzonenregeln, Pfadregeln sowie Zertifikatsregeln. Bei jeder dieser vier Regeln müssen Sie sich für eine der beiden möglichen Sicherheitsstufen entscheiden. Diese beiden Einstellungen finden Sie unter RICHTLINIEN FÜR SOFTWAREEINSCHRÄNKUNG/SICHERHEITSEBENEN. Die Option NICHT ERLAUBT verweigert das Ausführen einer Applikation auch in dem Fall, wenn der Benutzer über ausreichende Berechtigungen verfügt. Mit der Option NICHT EINGESCHRÄNKT ist dem Benutzer der Zugriff auf die Applikation gestattet. Die Ausführung wird in diesem Fall lediglich dann verweigert, wenn dem Benutzer nicht ausreichende Zugriffsberechtigungen für die Applikation zur Verfügung stehen.

22.4.1 Die Hashregeln

Jede Datei wird eindeutig über ihren Hash identifiziert. Ein Hash ist eine Zahl, die auf einem bestimmten mathematischen Algorithmus basiert und für jede Datei einmalig ist. Häufig verwendete Algorithmen sind der MD5-Algorithmus sowie der Secure Hash Algorithm (SHA-1). Die Hashregeln erkennen erlaubte und unerlaubte Dateien anhand dieser Hash-Information. Da Dateien ihren Hash unabhängig von ihrem Installationspfad beibehalten, können diese Dateien auch gefunden werden, wenn Sie sich in keinem standardisierten Pfad wie dem Ordner Programme befinden. Dies gilt auch, wenn der Benutzer die Datei umbenennt oder verschiebt. Allerdings ändert sich der Hash einer Datei, wenn die komplette Applikation modifiziert wird. Dies ist bei der Installation eines Servicepacks der Fall. Die angewendete Hashregel für diese Applikation ist dann nicht länger gültig.

Beim Definieren einer Hashregel müssen Sie den originalen Hash der Software benutzen. Sie können keinen neuen Hash importieren, der von einer anderen Softwarekomponente als der Software der Richtlinienbeschränkung errechnet wurde, auch nicht, wenn Sie denselben Hash-Algorithmus und Namen verwenden.

1. Um eine neue Hashregel zu erstellen, wählen Sie aus dem Kontextmenü von RICHTLINIEN FÜR SOFTWAREBESCHRÄNKUNG / ZUSÄTZLICHE REGELN den Eintrag NEUE HASH-REGEL. Sie erhalten das Fenster Neue Hashregel (siehe Abbildung 22.3).



Abbildung 22.3: Erstellen einer neuen Hashregel

2. Sie müssen nun über DURCHSUCHEN die Datei auswählen, für die eine Hashregel definiert werden soll. Sobald Sie die Datei ausgewählt haben, werden automatisch die Felder DATEIHASH sowie DATEIINFORMATIONEN ausgefüllt. Optional können Sie eine Beschreibung für die neue Regel festlegen.
3. Abschließend legen Sie die Sicherheitsstufe fest. Hier haben Sie die Wahlmöglichkeiten NICHT ERLAUBT und NICHT EINGESCHRÄNKT. Im ersten Fall darf die Applikation nicht benutzt werden, im zweiten Fall ist das Ausführen gestattet, sofern keine Zugriffsrechte des Benutzers dagegen sprechen.

22.4.2 Die Internetzonenregeln

Die Internetzonenregeln basieren auf dem Konzept der Sicherheitseinstellungen an den Internet Explorer Zonen. Ob das Ausführen einer Applikation gestattet ist oder nicht, basiert bei Anwendung dieser Regel darauf, aus welcher Internetzone die Software stammt. Die größte Einschränkung dieser Regel besteht darin, dass sie nur für Applikationen angewendet werden kann, die die Windows Installer-Technologie verwenden. Selbstverständlich müssen Sie vor dem Einsatz dieser Regel die Internetzonen entsprechend Ihren Anforderungen eingerichtet haben.

1. Um eine neue Internetzonenregel zu erstellen, wählen Sie aus dem Kontextmenü von RICHTLINIEN FÜR SOFTWAREBESCHRÄNKUNG / ZUSÄTZLICHE REGELN den Eintrag NEUE INTERNETZONENREGEL.
2. Wählen Sie nun aus der Listbox INTERNETZONE eine der vorhandenen Internetzonen aus (siehe Abbildung 22.4). Sämtliche Windows Installer-Dateien, die aus der angegebenen Zone stammen, dürfen nun je nach der gewählten Sicherheitsstufe ausgeführt werden oder nicht. Auch hier haben Sie die Wahlmöglichkeiten NICHT ERLAUBT und NICHT EINGESCHRÄNKT. Das Ausführen sollten Sie nur für Dateien gestatten, die von vertrauenswürdigen Internetseiten stammen.



Abbildung 22.4: Erstellen einer Internetzonenregel

22.4.3 Die Pfadregeln

Bei Verwendung der Pfadregeln ist der Pfad der Applikation entscheidend dafür, ob das Programm ausgeführt werden darf oder nicht. Sie können z.B. eine Regel definieren, die lediglich das Ausführen von Programmen erlaubt, die sich in C:\Programme\ befinden. Diese Regeln greifen jedoch nur, wenn der Benutzer die vom Unternehmen vorgegebenen Applikationen nicht in beliebigen Verzeichnissen installieren kann. Ansonsten wäre der Zugriff auf diese nicht mehr möglich. Die Pfadregeln unterstützen den Gebrauch von Variablen wie %Systemroot%, %Windir% oder %Temp%.

1. Um eine neue Pfadregel zu erstellen, wählen Sie aus dem Kontextmenü von RICHTLINIEN FÜR SOFTWAREBESCHRÄNKUNG / ZUSÄTZLICHE REGELN den Eintrag NEUE PFADREGEL. Sie erhalten das Fenster NEUE PFADREGEL (siehe Abbildung 22.5).
2. Geben Sie hier lediglich den gewünschten Pfad ein bzw. wählen diesen über DURCHSUCHEN aus. Danach entscheiden Sie sich für die gewünschte Sicherheitsstufe und geben eine optionale Beschreibung für diese Regel an.



Abbildung 22.5: Erstellen einer Pfadregel



Wenn Sie erreichen möchten, dass möglichst wenige Applikationen ausgeführt werden können, sollten Sie eine Pfadregel definieren, die es Programmen untersagt, in dem Pfad %WINDIR%\SYSTEM32\DLLCACHE ausgeführt zu werden. Dies ist der Pfad zu einem Cache-Ordner, der oftmals die Kopien von Applikationen enthält. Die Applikation kann von diesem Cache-Ordner aus auch dann starten, wenn für das eigentliche Installationsverzeichnis eine Pfadregel definiert ist, die das Ausführen untersagt.

22.4.4 Die Zertifikatsregeln

Die vierte Möglichkeit stellen die Zertifikatsregeln dar. Zertifikatsregeln können lediglich auf Windows Installer-Pakete sowie -Skripte angewendet werden. Sie funktionieren jedoch nicht bei .exe- oder .dll-Dateien. Die Anwendung dieser Regel bietet sich für Applikationen an, deren Installationsquelle sich innerhalb der gesicherten Domäne befindet. In diesem Fall müssen die Benutzer bei der Installation nicht mehr entscheiden, ob sie bestimmte Signaturen akzeptieren. Ihnen wird auch nicht mehr angezeigt, von welcher Instanz der Programmcode signiert wurde. Selbstverständlich können über die Zertifikatsregeln auch bestimmte Zertifikate verweigert werden. Leider gibt es nicht die Möglichkeit, unsignierten Code zu verweigern.

1. Um eine neue Zertifikatsregel zu erstellen, wählen Sie aus dem Kontextmenü von RICHTLINIEN FÜR SOFTWAREBESCHRÄNKUNG / ZUSÄTZLICHE REGELN den Eintrag NEUE ZERTIFIKATSREGEL. Sie erhalten das Fenster NEUE ZERTIFIKATSREGEL (siehe Abbildung 22.6).



Abbildung 22.6: Erstellen einer Zertifikatsregel



Beim Erstellen einer neuen Zertifikatsregel wird die bisherige Standard-Sicherheitsstufe überschrieben, die mit einem signierten Skript oder einem Windows Installer-Paket verbunden ist.

2. Wählen Sie über DURCHSUCHEN das neue Zertifikat aus, das Sie für die Regel verwenden möchten. Setzen Sie dann die gewünschte Sicherheitsstufe und geben eine Beschreibung an. Die Beschreibung sollte bei den Zertifikatsregeln obligatorisch sein, da die Zertifikate alle sehr ähnlich aussehen und erst durch einen entsprechenden Zusatz besser identifiziert werden können.

22.4.5 Die Priorität der Regeln

Nachdem Sie nun die verschiedenen Regeln kennen gelernt haben, wird nun die Priorität beschrieben, nach der die einzelnen Regeln abgearbeitet und angewendet werden. Diese Reihenfolge ist wichtig, da sich die Einstellungen der verschiedenen Regeln untereinander widersprechen können. Oberste Priorität besitzen die Hashregeln. Danach folgen die Zertifikatsregeln, Pfadregeln und mit niedrigster Priorität die Internetzonenregeln. Gestattet also eine Hashregel das Ausführen einer Applikation, während die Zertifikatsregel das Ausführen verbietet, so gilt die Einstellung der übergeordneten Hashregel.

Diese Regeln können sowohl für sämtliche Computer im Netzwerk als auch nur für einen bestimmten lokalen Computer angewendet werden. Im ersten Fall benutzen Sie die Gruppenrichtlinie, im zweiten Fall die lokale Sicherheitsrichtlinie eines Computers.

Bevor Sie neue Richtlinien zur Softwarebeschränkung produktiv einsetzen, sollten Sie diese ein bis zwei Wochen lang testen. In dieser Zeit können Sie unerwünschte Nebeneffekte feststellen und beseitigen. Je restriktiver Sie diese Richtlinien einsetzen, desto höher wird auch die Wahrscheinlichkeit, dass Applikationen nicht mehr einwandfrei funktionieren, die nicht von den Richtlinien betroffen sein sollten. Komplexe Applikationen wie etwa das Microsoft Office-Paket rufen ihrerseits weitere Applikationen oder Skripte für bestimmte Funktionen auf.

Ferner sollten Sie nachsehen, welche Programme beim Start automatisch ausgeführt werden sollen. Zu restriktiv gesetzte Richtlinien können etwa Startskripte in ihrer Funktion behindern. Überprüfen Sie, welche Programme sich im Autostartordner befinden und welche Einträge zusätzlich im Registry-Schlüssel `HKEY_Current_User\Software\Microsoft\Windows\CurrentVersion\Run` eingetragen sind.

22.5 Die Sicherheitsvorlagen

Eine Sicherheitsvorlage ist eine einzelne Datei, in der eine Reihe von vorkonfigurierten Einstellungen der Sicherheitsrichtlinie gespeichert ist. Die Vorlagen werden alle als .inf-Datei gespeichert. Es gibt eine Reihe von Vorlagen, die Sicherheitseinstellungen für verschiedene Sicherheitslevel umfassen. Die Sicherheitsvorlagen können auf Benutzer und Computer in lokalen und domänenweiten GPOs angewendet werden.

Insgesamt stellt Windows 13 verschiedene Sicherheitsvorlagen bereit. Selbstverständlich können alle diese Vorlagen nach dem Import in ein GPO noch weiter angepasst werden. Sämtliche Vorlagen befinden sich im Verzeichnis `%SYSTEMROOT%\SECURITY\TEMPLATES`. Tabelle 22.2 gibt Ihnen eine Übersicht über die Sicherheitsvorlagen und deren Einsatzgebiet.

Sicherheitsvorlage	Beschreibung
Basicdc.inf	Basis-Sicherheitseinstellungen für Domänencontroller
Basicsv.inf	Basis-Sicherheitseinstellungen für Server
Basicwk.inf	Basis-Sicherheitseinstellungen für Client-Computer
Compatws.inf	Kompatible Sicherheitseinstellungen für Server und Client-Computer
DC security.inf	Aktualisierte Basis-Sicherheitseinstellungen für Domänencontroller
Hisecdc.inf	Hochsicherheitseinstellungen für Domänencontroller
Hisecws.inf	Hochsicherheitseinstellungen für Server und Client-Computer
Notssid.inf	Die Benutzer-SID des Terminalservers wird vom Windows 2000 Server entfernt.
Ocfiless.inf	Optionale Komponentendateisicherheit für Server
Ocfilesw.inf	Optionale Komponentendateisicherheit für Client-Computer
Securedc.inf	Sichere Sicherheitseinstellungen für Domänencontroller
Securews.inf	Sichere Sicherheitseinstellungen für Server und Client-Computer
Setup security.inf	Vordefinierte standardmäßige Sicherheitseinstellungen

Tabelle 22.2: Die Sicherheitsvorlagen und ihre Bedeutungen

Mit den Basis-Sicherheitseinstellungen (basic*.inf) werden alle Sicherheitsbereiche abgedeckt bis auf die Bereiche, die mit speziellen Benutzerrechten verknüpft sind. Diese Bereiche können beispielsweise durch die Installation einer Applikation mit den entsprechenden Benutzerrechten angepasst werden.

Die kompatible Sicherheitseinstellung (compat*.inf) schränkt die Berechtigungen der Gruppe „Hauptbenutzer“ ein. Dieser Gruppe gehören unter Windows standardmäßig alle authentifizierten Benutzer an. Allerdings kann diese Gruppenzugehörigkeit ein zu hohes Risiko bedeuten, sodass die Benutzer lieber nur mit den Berechtigungen der Gruppe „Benutzer“ ausgestattet werden sollten. Die Berechtigungen werden für Dateien, Ordner oder auch Registry-Schlüssel so eingestellt, dass die Benutzer zwar noch ihre Applikationen ausführen können, aber keine darüber hinausgehenden Rechte besitzen.

Die Hochsicherheitseinstellungen (hise*.inf) sorgen für hohe Sicherheit im Netzwerkverkehr. Deshalb können die Windows 2000/XP-Computer, die eine Hochsicherheitsvorlage benutzen, nur mit anderen Windows 2000/XP-Computern kommunizieren. Ein Austausch mit Computern, die das Betriebssystem Windows 9x oder NT ausführen, ist nicht möglich.

Über die sicheren Sicherheitsvorlagen (secure*.inf) werden sichere, empfohlene Einstellungen an allen Bereichen außer Dateien, Ordnern und Registry-Schlüsseln durchgesetzt. Die Bereiche der Registry und des Dateisystems sind bereits standardmäßig sicher konfiguriert.

22.5.1 Arbeiten mit einer Sicherheitsvorlage

Um mit den Sicherheitsvorlagen arbeiten zu können, sollten Sie zunächst eine eigene mmc einrichten. Fügen Sie dazu das Snap-In SICHERHEITSVORLAGEN zu einer leeren mmc hinzu. In dieser mmc können Sie nun darangehen, die eben beschriebenen Vorlagen zu bearbeiten.

Wenn Sie eine Vorlage öffnen, befinden sich darin die Knoten, die auch in der Sicherheitsrichtlinie enthalten sind (siehe Abbildung 22.7). Sie können hier nun beliebige Änderungen und Anpassungen durchführen.

Nach Abschluss der Änderungen sollten Sie die neue Vorlage unter einem anderen Namen speichern. Diese neue Vorlage erscheint dann ebenfalls in der mmc. Wählen Sie aus dem Kontextmenü der neuen Vorlage BESCHREIBUNG FESTLEGEN und geben dann eine Beschreibung für die neue Vorlage an. So werden Sie immer schnell den Überblick über die Inhalte der selbst definierten Vorlagen behalten.

Um eine neue Sicherheitsvorlage zu erzeugen, wählen Sie aus dem Kontextmenü des Pfades NEUE VORLAGE. Geben Sie der neuen Vorlage einen Namen und eine Beschreibung. Die neue Vorlage enthält alle Knoten, die auch die übrigen Sicherheitsvorlagen enthalten. Sie können hier nun die gewünschten Richtlinien einrichten.



Abbildung 22.7: Die mmc Sicherheitsvorlagen

Sämtliche Vorlagen können auch importiert bzw. Einstellungen daraus exportiert werden.

1. Um eine Sicherheitsvorlage in ein GPO zu importieren, wählen Sie in der mmc des GPO den Knoten COMPUTERKONFIGURATION / WINDOWS-EINSTELLUNGEN / SICHERHEITSEINSTELLUNGEN und aus dessen Kontextmenü den Eintrag RICHTLINIE IMPORTIEREN.
2. Im folgenden Fenster sehen Sie dann alle Vorlagen, die im Pfad %SYSTEMROOT%\SECURITY\TEMPLATES abgelegt sind. Wählen Sie dort die gewünschte Vorlage aus.

Die neue Sicherheitsvorlage wird erst ab dem Moment gültig, in dem das GPO auf den Computer angewendet wird. Die Richtlinienübertragung findet standardmäßig alle acht Stunden statt. Wollen Sie nicht so lange warten, starten Sie entweder den Computer neu oder geben an der Eingabeaufforderung folgenden Befehl ein: `secedit /refreshpolicy machine_policy` .

Weiterhin besteht auch die Möglichkeit, Einstellungen an den Sicherheitsrichtlinien zu exportieren. Wählen Sie dazu STARTMENÜ / PROGRAMME / VERWALTUNG / LOKALE SICHERHEITSRICHTLINIE. Aus dem Kontextmenü des Knotens SICHERHEITSEINSTELLUNGEN wählen Sie RICHTLINIE EXPORTIEREN. Sie können dann entscheiden, ob Sie die lokale oder effektive Richtlinie exportieren möchten. Als Zielverzeichnis zum Speichern wird Ihnen der Ordner %SYSTEMROOT%\SECURITY\TEMPLATES angegeben. Das Exportieren der lokalen Richtlinie kann sinnvoll sein, um diese Einstellungen zu einem späteren Zeitpunkt wieder zurückzuspielen, da das lokale GPO von domänenbasierten GPOs außer Kraft gesetzt wird.

22.6 Die Sicherheitskonfiguration und -analyse

Die Sicherheitskonfiguration und -analyse wird zum Überprüfen und Einstellen der Sicherheit verwendet. Hierzu wird eine eigene Sicherheitsdatenbank benutzt. Zur Einrichtung und Steuerung kann die mmc SICHERHEITSKONFIGURATION UND -ANALYSE eingerichtet werden. Fügen Sie dazu einer leeren Konsole das gleichnamige Snap-In hinzu.

Sobald Sie die neue mmc erstellt haben, befinden sich noch keine untergeordneten Knoten darin. Als Erstes müssen Sie eine Sicherheitsdatenbank anlegen. Diese Datenbank ist das Arbeitsverzeichnis für sämtliche Konfigurations- und Analysevorgänge. Wählen Sie aus dem Kontextmenü DATENBANK ÖFFNEN. Sie können nun entweder eine neue Sicherheitsdatenbank (.sdb-Datei) anlegen oder eine bereits bestehende öffnen. Wenn Sie eine neue Datenbank angelegt haben, müssen Sie im Fenster VORLAGE IMPORTIEREN eine Sicherheitsvorlage auswählen, die in die Datenbank geladen werden soll. Sie haben alle Vorlagen des Verzeichnisses %SYSTEMROOT%\SECURITY\TEMPLATES zur Auswahl. Sobald die Datenbank angelegt ist, erscheinen die Knoten mit ihren Einstellungen in der mmc.

Sie haben auch die Möglichkeit, mehrere Datenbanken anzulegen und in jede Datenbank eine Vorlage zu importieren. Die Inhalte der verschiedenen Arbeitsdatenbanken werden automatisch zu einer Verbundvorlage zusammengefasst. Wollen Sie hingegen in eine bestehende Datenbank eine neue Vorlage importieren, die die bereits geladene Vorlage überschreiben soll, so wählen Sie aus dem Kontextmenü **VORLAGE IMPORTIEREN**, und aktivieren Sie die Checkbox **DATENBANK VOR DEM IMPORTIEREN AUFRÄUMEN** bei der Auswahl der Vorlage (siehe Abbildung 22.8).



Abbildung 22.8: Importieren von Vorlagen in die Sicherheitsdatenbank

Wird die Checkbox nicht aktiviert, so gelten bei Unterschieden zwischen den Vorlagen die Einstellungen der zuletzt importierten Sicherheitsvorlage. Außerdem wird keine Verbundvorlage angelegt, wenn das Überschreiben aktiviert ist.

22.6.1 Die Sicherheitsanalyse

Anhand der in die Arbeitsdatenbank importierten Sicherheitsvorlagen können Sie die Sicherheit des Systems analysieren. Dabei wird der aktuelle Sicherheitsstand des Computers mit der importierten Sicherheitsvorlage verglichen. Bei der Wahl der geladenen Vorlagen sollten Sie immer darauf achten, dass diese zum Typ des zu prüfenden Rechners passen. Es macht wenig Sinn, Vorlagen für Domänencontroller auf einem Client-Computer zu testen oder umgekehrt. Um die Analyse zu starten, wählen Sie aus dem Kontextmenü **COMPUTER JETZT ANALYSIEREN**. Geben Sie dann den Pfad an, in dem das Protokoll der Analyse gespeichert werden soll. Während der Durchführung der Analyse erhalten Sie Statusinformationen über den gerade analysierten Bereich (siehe Abbildung 22.9).



Abbildung 22.9: Statusanzeige der Sicherheitsanalyse

Um die Ergebnisse zu betrachten, wählen Sie aus dem Kontextmenü **PROTOKOLLDATEN ANSEHEN**. Im Detailbereich der mmc sehen Sie alle getesteten Bereiche. Wollen Sie für spezielle Richtlinien die Ergebnisse sehen, so markieren Sie diese Richtlinie. Sie finden eine Gegenüberstellung der Datenbankeinstellung und der aktuellen Computereinstellung. Dabei werden übereinstimmende Werte mit einem grünen Häkchen gekennzeichnet, während Fehler ein rotes Kreuz aufweisen. Sind an einigen Richtlinienereinstellungen keine Symbole vorhanden, befand sich diese Richtlinie nicht in der importierten Vorlage und konnte deshalb nicht analysiert werden.

Die in die Arbeitsdatenbank importierten Vorlagen können nach der Analyse auf den Computer angewendet werden. Wählen Sie dazu aus dem Kontextmenü **SYSTEM JETZT KONFIGURIEREN**. Geben Sie einen Pfad für die Protokolldatei an. Während der Konfiguration sehen Sie wie bei der Analyse einen Statusbalken mit dem aktuellen Fortschritt. Die bei der Konfiguration vorgenommenen Änderungen werden jedoch nicht in der Sicherheitsvorlage, sondern in der Verbundvorlage in der Arbeitsdatenbank gespeichert. Um die Sicherheitsvorlage endgültig zu überschreiben, müssen Sie die Konfiguration unter demselben Namen wie dem der ursprünglichen Sicherheitsvorlage abspeichern.

Alternativ können Sie die Verbundvorlage der Arbeitsdatenbank auch als neue Sicherheitsvorlage exportieren. Wählen Sie dazu aus dem Kontextmenü **VORLAGE EXPORTIEREN** und geben einen Namen und Pfad für die Datei an.

22.7 Die Konfiguration des Kerberos-Protokolls

Unter den eben vorgestellten Sicherheitsrichtlinien befindet sich auch die Kerberos-Richtlinie. Über diese werden die zentralen Einstellungen des Kerberos-Protokolls konfiguriert. Bereits in Kapitel 2.2.3 haben Sie die Funktionsweise des Kerberos-Authentifizierungsprotokolls kennen gelernt. In den meisten Fällen wird dieses Protokoll vom Administrator nicht speziell angepasst, sondern so verwendet, wie es standardmäßig eingestellt ist. Sie können diese Einstellungen jedoch alle anpassen und ändern. Sie finden die Einstellungen des Kerberos-Protokolls in der Gruppenrichtlinie unter **COMPUTERKONFIGURATION / SICHERHEITSEINSTELLUNGEN / KONTORICHTLINIEN / KERBEROS-RICHTLINIEN**. Das Kerberos-Protokoll arbeitet mit den Standardeinstellungen der folgenden fünf Bereiche (siehe Tabelle 22.3):

Kerberos-Bereich und Beschreibung	Standardeinstellung
BENUTZERANMELDEEINSCHRÄNKUNGEN ERZWINGEN: Hiermit werden Anmeldebeschränkungen, wie z.B. begrenzte Anmeldezeiträume, durchgesetzt. Trifft eine Einschränkung zu, wird kein Ticket ausgestellt.	aktiviert
MAX. GÜLTIGKEITSDAUER DES BENUTZERTICKETS: Bestimmt, wie lange der Benutzer das Ticket benutzen darf. Nach Ablauf der Frist muss er es erneuern (sofern dieses gestattet ist) oder ein neues Benutzerticket anfordern.	10 Stunden
MAX. GÜLTIGKEITSDAUER DES DIENSTTICKETS: Gibt an, wie lange ein Dienst das Ticket benutzen darf. Ist der Zeitraum abgelaufen, muss der Dienst ein neues Ticket anfordern.	600 Minuten
MAX. TOLERANZ FÜR DIE SYNCHRONISATION DES COMPUTERTAKTS: Gibt den Toleranzbereich für die Kerberos-Benutzer an, innerhalb dessen sich nicht synchrone Computeruhren befinden müssen.	5 Minuten
MAX. ZEITRAUM, IN DEM EIN BENUTZERTICKET ERNEUERT WERDEN KANN: Innerhalb dieses Zeitraums kann der Benutzer sein Ticket erneuern, bevor das KDC ein neues ausstellen muss.	7 Tage

Tabelle 22.3: Die Standardeinstellungen des Kerberos-Protokolls

Wenn Sie die Einstellungen des Kerberos-Protokolls ändern möchten, sollten Sie dies nur tun, wenn spezielle Gründe dafür sprechen. Ansonsten sollten Sie die Standardwerte gelten lassen. Bei Änderungen sollten Sie die folgenden Aspekte in Ihre Überlegungen einbeziehen:

- Sämtliche dieser Einstellungen beeinflussen die Leistung des Netzwerks. Wenn Sie die Gültigkeitsdauer der Benutzertickets herabsetzen, werden die Clients wesentlich häufiger Anfragen senden, um ihr Ticket zu erneuern. Haben Sie dabei zusätzlich den Wert für den Erneuerungszeitraum auf 0 gesetzt, so kann das Ticket nicht erneuert werden, sondern muss bei jeder Erneuerungsanfrage neu erstellt werden. Der Gültigkeitswert für ein Benutzerticket sollte ungefähr der Stundenanzahl eines Arbeitstages entsprechen. Damit benötigt der Benutzer nur ein einziges Kerberos-Ticket pro Tag. Haben Sie das Gültigkeitsintervall auf die Länge eines Arbeitstages oder etwas höher angesetzt, so können Sie in diesem Fall auch den Zeitraum für die Erneuerung auf 0

setzen. Da sich der Benutzer am nächsten Arbeitstag ohnehin neu anmelden wird, muss er ein neues Ticket anfordern. Bestehende Tickets werden gelöscht, sobald sich ein Benutzer abmeldet oder seinen Computer ausschaltet.

- Bei der Erneuerung des Tickets muss sich der Benutzer nicht neu anmelden. Es werden dieselben Benutzerdaten benutzt wie beim erstmaligen Ausstellen des Tickets. Deshalb bedeutet das Einstellen einer nur kurzen Lebensdauer für Tickets keine Erhöhung der Netzwerksicherheit, sondern lediglich eine Erhöhung des Netzwerkverkehrs.

Dieses Kapitel beschäftigt sich mit der Leistungsüberwachung des Active Directory. Die zentralen Werkzeuge dazu sind der Systemmonitor, die Leistungsdatenprotokolle und die Ereignisanzeige, deren Protokolle mithilfe von Support-Tools z.B. an eine Tabellenkalkulation weitergeleitet werden können. Zusätzlich erfahren Sie, wie Sie weitere Logs aufzeichnen können, indem Sie das Diagnostic-Logging aktivieren.

22.8 Der Systemmonitor und die Leistungsprotokolle

Das zentrale Werkzeug zur Leistungsüberwachung ist der Systemmonitor. Sie finden diesen in der vorkonfigurierten mmc SYSTEMMONITOR unter Windows 2000 bzw. LEISTUNG unter Windows XP/Windows Server 2003. Mithilfe des Systemmonitors können Sie wichtige Informationen über die Performance und Auslastung des Systems sammeln. Es können Echtzeitdaten an lokalen und Remote-Systemen aufgezeichnet und grafisch aufbereitet dargestellt werden. Der Systemmonitor bietet eine Reihe Kategorien, die beobachtet werden können. Diese Kategorien werden Datenobjekte genannt.

Im Zusammenhang mit Active Directory ist hier das Datenobjekt NTDS (NT Directory Service) wichtig. Für jedes der Datenobjekte können spezielle Leistungsindikatoren hinzugefügt werden. Für das Objekt NTDS können weit über 30 Indikatoren festgelegt werden, beispielsweise komprimierte und unkomprimierte Größen der Replikationsdaten, Kerberos-Authentifizierungen, Anzahl von LDAP-Clientsitzungen oder LDAP-Bindungsdauer, die Anzahl von Schreib- und Lesezugriffen auf das Verzeichnis usw. Eine Beschreibung der einzelnen Leistungsindikatoren finden Sie, wenn Sie den entsprechenden Indikator markieren und auf ERKLÄRUNG klicken. Um die gewählten Indikatoren grafisch anzuzeigen, klicken Sie auf HINZUFÜGEN. Um einen neuen Satz von Leistungsindikatoren hinzuzufügen, klicken Sie auf die Schaltfläche NEUER LEISTUNGSINDIKATORENSATZ und wählen dann aus dem Kontextmenü des Detailbereichs LEISTUNGSINDIKATOREN HINZUFÜGEN. Damit erhalten Sie das gleichnamige Fenster (siehe Abbildung 22.10).



Abbildung 22.10: Hinzufügen von Leistungsindikatoren für den Systemmonitor

So können Sie beispielsweise ermitteln, ob die vorhandenen Domänencontroller überlastet sind und deshalb neue Server hinzugefügt werden müssen. Allerdings müssen in diesem Fall die Domänencontroller auch nur als solche betrieben werden. Agieren diese zusätzlich als DHCP-, DNS-, Exchange- oder Webserver oder dienen als Applikationsserver – was auch von Microsoft nicht empfohlen wird –, so ist es wesentlich schwieriger zu bestimmen, ob der Domänencontroller mit den Active Directory-Aufgaben überlastet ist.

Die Werte für die folgenden Leistungsindikatoren sollten Sie auf jeden Fall beobachten. Dabei sollten die angegebenen Schwellenwerte nicht zu weit überschritten werden. Werden die Werte regelmäßig überschritten, könnte die Installation eines neuen zusätzlichen Domänencontrollers erforderlich werden.

- ▶ Zunächst sollte die Prozessorzeit bewertet werden. Dieser Leistungsindikator des Datenobjekts Prozessor wird bereits standardmäßig vom Systemmonitor überwacht. Die durchschnittliche Prozessorzeit auf einem Domänencontroller sollte 80% nicht überschreiten, wobei durchaus einige Spitzenbelastungen von 100% Auslastung auftreten können.
- ▶ Die NTLM-Authentifizierungen pro Sekunde geben an, wie viele Windows 9x- und NT-Client-Logins der Domänencontroller verarbeiten muss. Zusätzlich sollte auch der Indikator für Kerberos-Authentifizierungen ausgewählt werden. Wenn diese beiden Zähler zusammen mit der Prozessorauslastung einen hohen Wert ergeben, so ist der vorhandene Domänencontroller mit den Logging-Aktivitäten stark belastet. In diesem Fall sollte über einen alternativen Domänencontroller nachgedacht werden.
- ▶ Auch der Indikator für die LDAP-Bindungsdauer ist wichtig. Dieser Indikator gibt an, wie lange der Domänencontroller für die Bindung der letzten LDAP-Anfrage benötigt hat. Ist dieser Wert nicht auf einem sehr niedrigen Level, sondern zeigt stattdessen rege Aktivität, so ist die Hardware des Domänencontrollers mit den Zugriffen überfordert.

Die Leistungsprotokolle

Die Leistungsindikatoren können nicht nur in Echtzeit im Systemmonitor angezeigt werden, sondern auch als Protokoll aufgezeichnet werden. Dies geschieht über den Knoten Leistungsdatenprotokolle und Warnungen, der sich wie der Systemmonitor in der mmc Systemmonitor bzw. Leistung befindet. Diese Protokolle und Warnungen können ebenfalls für den lokalen oder für Remote-Computer erstellt werden. Es können Leistungsindikator- und Ablaufverfolgungsprotokolle sowie Warnungen erstellt werden.

1. Sie erstellen ein neues Leistungsindikatorenprotokoll, indem Sie den Knoten LEISTUNGSINDIKATORENPROTOKOLL doppelklicken und aus dem Kontextmenü eines freien Bereichs im Detailbereich den Eintrag NEUE PROTOKOLLEINSTELLUNGEN wählen. Legen Sie einen Namen und Pfad für das Protokoll fest. Wählen Sie wie für den Systemmonitor die zu überwachenden Datenobjekte und ihre Leistungsindikatoren sowie den zu überwachenden Computer aus.
2. Auf der Registerkarte ALLGEMEIN können Sie zusätzlich das Intervall der Erfassung einstellen.
3. Wechseln Sie dann auf die Registerkarte PROTOKOLLDATEN. Hier können Sie die Dateierweiterung des Protokolls (z.B. numerisch oder mit einer Datumsangabe in beliebigen Formaten) auswählen. Auch das Format der Datei kann bestimmt werden. Das Protokoll kann als kommaseparierte oder tabulatorseparierte Textdatei sowie als Binär- oder zirkuläre Binärdatei gespeichert werden. Die Protokolldatei kann als Textdatei in einer Tabellen- oder Datenbankanwendung weiterverarbeitet werden.
4. Auf der Registerkarte ZEITPLAN können Sie bestimmen, wann die Protokollierung beginnen und enden soll.

Das Erstellen eines Ablaufverfolgungsprotokolls geschieht auf ähnliche Art und Weise.

1. Doppelklicken Sie hier den Knoten PROTOKOLLE DER ABLAUFVERFOLGUNG und wählen aus dem Kontextmenü des Detailbereichs den Eintrag NEUE PROTOKOLLEINSTELLUNGEN. Sie haben die Möglichkeit, vom Systemanbieter und vom Nicht-Systemanbieter protokollierte Ereignisse auszuwählen. Zur ersten Kategorie zählen Ereignisse des Windows-Anbieters wie Prozesse und Threads erstellen/löschen, Datenträger-E/A, Netzwerk-TCP/IP, Seitenfehler und Dateidetails. Sie können auch Nicht-Systemanbieter auswählen, z.B. LSA (Local Security Authority). Es können zwar für ein Protokoll mehrere Nicht-Systemanbieter ausgewählt werden, jedoch nicht ein System- und Nicht-Systemanbieter.
2. Auf den Registerkarten PROTOKOLLDATEN und ZEITPLAN nehmen Sie dieselben Einstellungen wie für die Leistungsindikatorprotokolle vor.

Die Warnungen werden quasi analog zu den Leistungsindikatorprotokollen erstellt. Auch hier müssen die Indikatoren der gewünschten Datenobjekte gewählt werden. Für jeden Indikator müssen Sie hier zusätzlich ein Limit angeben, bei dessen Überschreitung eine Warnung ausgegeben werden soll.

1. Wählen Sie dazu auf der Registerkarte ALLGEMEIN aus der Listbox GRÖßER ALS oder KLEINER ALS und geben manuell den Schwellenwert ein.
2. Auf der Registerkarte VORGANG wird festgelegt, welche Aktion beim Eintreten einer Warnung durchgeführt werden soll. So kann z.B. über den Nachrichtendienst eine Meldung an einen bestimmten Computer gesendet, ein bestimmtes Programm ausgeführt oder ein Eintrag in das Ereignisprotokoll geschrieben werden.

22.8.1 Die Ereignisanzeige

In der Ereignisanzeige werden Protokolle verschiedener Kategorien angezeigt. Standardmäßig sind auf jedem Windows 2000/2003/XP-Computer die Ereignisprotokolle Anwendung, Sicherheit und System vorhanden. Handelt es sich um einen Domänencontroller, sind zusätzlich die Protokolle Directory Service und Dateireplikationsdienst vorhanden. Auf einem DNS-Server findet sich auch noch das Protokoll DNS-Server.

Im Zusammenhang mit dem Ereignisprotokoll sind zwei Support-Tools von Bedeutung, mit deren Hilfe Sie die Inhalte der Protokolle in spaltenseparierte Textdateien konvertieren und zur Auswertung in eine Tabellenkalkulation oder Datenbankanwendung exportieren können. Dabei handelt es sich um die Programme *elogdmp.exe* sowie *dumpel.exe*. *Elogdmp.exe* ist Bestandteil des Windows 2000 Resource Kit, *dumpel.exe* steht zum freien Download bereit. Standardmäßig werden beide Programme auf der Systempartition in das Verzeichnis \PROGRAMME\RESOURCE KIT installiert.

Elogdmp.exe ist ein Kommandozeilenprogramm. Sie können sich damit die Inhalte einzelner Ereignisprotokolle ausgeben lassen. Verwenden Sie dazu die folgende Syntax: `elogdmp \\<Computernamen> <Name des Ereignisprotokolls> >Name der Ausgabedatei [↵]`.

Um das Ereignisprotokoll des lokalen Rechners auszugeben, geben Sie `\\.` an. Gültige Werte für die Variable Name des Ereignisprotokolls sind: Anwendung, Sicherheit, System, Directory Service, Dateireplikationsdienst und DNS-Server. Die Ausgabedatei wird im Installationsverzeichnis von *elogdmp* erstellt. Die Ausgabedatei ist eine kommaseparierte Textdatei, die z.B. in Microsoft Excel weiterverarbeitet werden kann. Unter Windows XP kann das mitgelieferte Skript *eventquery.vbs* verwendet werden, um sich bestimmte Ereignisprotokolle ausgeben zu lassen.

Auch bei *dumpel.exe* handelt es sich um ein Kommandozeilenprogramm. *Dumpel* steht für *dump event log*. Sie können damit Ereignisprotokolle des lokalen oder von Remote-Rechnern als tabulatorseparierte Textdateien ausgeben lassen. Zusätzlich können die Ereignisprotokolle nach bestimmten Ereignistypen gefiltert werden. Es stehen folgende Parameter zur Verfügung:

`Dumpel -f [-s] [-l] [-m] [-e] [-r] [-t] [-d]`

Die Parameter für *dumpel.exe* sind in Tabelle 22.4 beschrieben.

Parameter	Beschreibung
-f	Name der Ausgabedatei. Diese wird im Installationsverzeichnis von <i>dumpel.exe</i> angelegt.
-s	Gibt den Namen des Servers an, dessen Ereignisprotokoll ausgegeben werden soll. Vor den Servernamen können Sie <code>\\</code> setzen.
-l	Gibt den Namen des auszugebenden Ereignisprotokolls an, z.B. System, Anwendung usw.
-m	Gibt die Quelle im Ereignisprotokoll an, z.B. Print, Netlogon usw. Es kann nur immer eine Quelle ausgewählt werden. Ist dieser Parameter nicht gesetzt, werden alle Quellen durchsucht.

Parameter	Beschreibung
-e	Setzt einen Filter für die Ereignis-ID. Sie können bis zu zehn IDs hintereinander durch Leerzeichen getrennt angeben. Dazu muss die Option -m gesetzt sein. Ist zusätzlich die Option -r gesetzt, werden alle Aufzeichnungen exklusive der gewählten Ereignis-IDs ausgegeben. Ist -r nicht gesetzt, werden nur die gewählten Ereignis-IDs durchsucht.
-r	Gibt an, ob nach bestimmten Quellen oder Aufzeichnungen gesucht oder ob diese herausgefiltert werden sollen.
-t	Ist -t gesetzt, werden die Spalten durch Tabulatoren getrennt. Andernfalls werden Leerzeichen als Trennzeichen benutzt.
-d	Durchsucht nur Ereignisse, die nicht älter als die hinter -d angegebene Tagesanzahl sind.

Tabelle 22.4: Die Parameter von *dumpe.exe*

22.8.2 Aktivieren des Diagnostic-Event-Logging

Wenn im Zusammenhang mit Active Directory Probleme oder Fehler auftreten, sollten Sie immer möglichst viele Ereignisse protokollieren. Hierzu aktivieren Sie am besten das Diagnostic-Event-Logging, das standardmäßig deaktiviert ist, da zu viele Ereignisse das Ereignisprotokoll füllen würden. Um das Logging zu aktivieren, müssen Sie über *regedt32* die Registry modifizieren. Öffnen Sie den Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics`. Dort geben Sie für jedes gewünschte Log einen der folgenden Werte an:

0 = Kein Logging (Standard)

1 = Minimum

3 = Mittlere Einstellung

5 = Maximum

Beim Diagnostic-Logging können für die folgenden Bereiche Einstellungen über die jeweiligen Schlüssel getroffen werden:

Backup, Directory Access, ExDS Interface Events, Field Engineering, Garbage Collection, Global Catalog, Initialization/Termination, Internal Configuration, Internal Processing, Intersite Messaging, Knowledge Consistency Checker, LDAP Interface Events, MAPI Interface Events, Name Resolution, Performance Counters, Replication Events, Security Events, Service Control und Setup.



Um den Domänencontroller nicht unnötig zu belasten, sollten Sie nach der Fehlerbehebung die Logging-Einstellungen wieder auf die Standardwerte zurücksetzen.

23 Die Windows-eigenen Active Directory-Support-Tools

Windows Server 2000 und 2003 stellen Ihnen eine Reihe von Programmen zur Verfügung, die der Konfiguration, Verwaltung, Überwachung und Fehlersuche am Active Directory dienen. Diese Programme gehören zu den Windows 2000-Support-Tools. Sie sind zum Teil im Lieferumfang von Windows 2000 Server enthalten und befinden sich auf der CD im Verzeichnis \SUPPORT\TOOLS. Die Installation erfolgt über die Datei 2000rkst.msi. Auch unter Windows Server 2003 befinden sich die Support-Tools auf der Installations-CD im Verzeichnis \SUPPORT\TOOLS. Diese Tools können Sie auch in der jeweils aktuellen Version von der Microsoft-Webseite

<http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp>

kostenlos downloaden. Weitere über 300 Support-Tools stehen Ihnen auf der Windows 2000 Server Resource Kit-CD zur Verfügung. Diese kann direkt bei Microsoft erworben werden. Eine Übersicht über alle auf dieser CD enthaltenen Programme finden Sie unter

http://www.microsoft.com/windows2000/techinfo/reskit/rktour/server/S_tools.asp

23.1 Support-Tools für das Windows 2000 und Windows 2003 Active Directory

In diesem Kapitel werden Ihnen aus der Vielzahl der verfügbaren Support-Tools jedoch nur diejenigen vorgestellt, die im Zusammenhang mit Active Directory wichtig sind. Alle Programme der Resource Kit-CD werden standardmäßig auf der Systempartition in das Verzeichnis \PROGRAMME\RESOURCE KIT, die übrigen in das Verzeichnis \PROGRAMME\SUPPORT TOOLS installiert. Die in diesem Kapitel beschriebenen Programme können Sie sowohl in einem Windows 2000, als auch in einem Windows 2003 Active Directory verwenden.

Tabelle 23.1 gibt eine Übersicht über die Programme, die im Zusammenhang mit Active Directory eine wichtige Rolle spielen. Sie finden hier zunächst als Überblick eine kurze Beschreibung der jeweiligen Funktion, während die folgenden Kapitel spezielle Optionen der Programme erläutern.

Support-Tool	Beschreibung
<i>ACLDIAG</i>	Kommandozeilenprogramm, mit dem die Zugriffsberechtigungen für bestimmte Objekte geprüft und mit denen des Standardschemas verglichen werden können.
<i>ADSIEDIT</i>	Über diese mmc können Sie alle Active Directory-Objekte sowie auch die Schemainformationen auf Attributebene bearbeiten. Auch die Sicherheitseinstellungen für die Objekte können bearbeitet werden.
<i>ADSIZER</i>	Ermöglicht über einen Wizard das Berechnen des Hardwarebedarfs an Servern, bevor mit der Implementierung von Active Directory begonnen wird.
<i>DCDIAG</i>	Universalprogramm zur Diagnose zahlreicher Active Directory-Probleme, besonders der Domänencontroller und Replikation.
<i>DNSCMD</i>	Kommandozeilentool zur Konfiguration und Überprüfung aller DNS-bezogenen Aufgaben.
<i>DOMMON</i>	Grafisches Tool zum Überprüfen des Status der Domänencontroller in einer Domäne, zum Replikationsstatus und Status der vertrauenden Domänen.
<i>DSACLS</i>	Kommandozeilenprogramm zur Verwaltung von Sicherheitseinstellungen für Active Directory-Objekte.
<i>DSASTAT</i>	Kommandozeilenprogramm zum Ermitteln und Vergleichen von Verzeichnisinformationen auf Domänencontrollern.
<i>DUMPFSMOS</i>	Kommandozeilenprogramm, mit dem die aktuellen Betriebsmasterrollen eines Domänencontrollers ausgegeben werden können.
<i>FAZAM2000</i>	Eigene mmc zum erweiterten Bearbeiten von GPOs wie z.B. Sichern, Wiederherstellen oder Diagnosefunktion.
<i>GPOTOOL</i>	Kommandozeilenprogramm zur Konsistenzprüfung von GPOs.
<i>GPRESULT</i>	Kommandozeilenprogramm zum Anzeigen von Details der aktuell verwendeten GPOs.
<i>GUID2OBJ</i>	Kommandozeilenprogramm, das GUIDs in definierte Namen der Objekte übersetzt.
<i>LDP</i>	Über eine GUI können die Active Directory-Objekte auf LDAP-Ebene angezeigt (z.B. ACE oder Replikationsdaten) und bearbeitet werden.
<i>MOVETREE</i>	Kommandozeilenprogramm zum Verschieben von OUs, Benutzern und Gruppen zwischen Domänen.
<i>NETDIAG</i>	Kommandozeilenprogramm, das umfangreiche Tests zur Netzwerkdiagnose durchführt.
<i>NETDOM</i>	Kommandozeilenprogramm zum Verschieben von Computern und Mitgliedsservern zwischen Domänen, Überprüfen und Herstellen von Vertrauensstellungen und sicheren Client-Server-Verbindungen.
<i>NTDSUTIL</i>	Kommandozeilenprogramm mit umfangreichen Funktionen zur autorisierenden Wiederherstellung, Domänenmanagement, Löschen von ungültigen Objekten, Übertragung der Betriebsmasterrollen oder SID-Management.
<i>PERMS</i>	Kommandozeilenprogramm, das die Berechtigungen eines Benutzers für eine Datei oder einen Ordner anzeigt.

Support-Tool	Beschreibung
<i>REPADMIN</i>	Kommandozeilenprogramm zum Prüfen von Replikationsmetadaten, Anzeigen des Replikationsstatus, Erzwingen der Replikation sowie Neuberechnen der Konsistenzprüfung.
<i>REPLMON</i>	Erfüllt dieselben Aufgaben wie REPADMIN, allerdings via GUI. Replikationstopologien können grafisch angezeigt werden.
<i>SDCHECK</i>	Kommandozeilenprogramm zum Betrachten der ACLs von Objekten.
<i>User State Migration Tool</i>	Kommandozeilenprogramm, zum Sichern und Wiederherstellen der Benutzerkonfiguration bei einer Migration auf Windows 2000/XP.

Tabelle 23.1: Übersicht über die Windows-Support-Tools für das Active Directory

23.1.1 ACLDIAG

ACLDIAG wird auch als ACL Diagnostics bezeichnet. Es handelt sich um ein Kommandozeilenprogramm, das für Diagnosezwecke bei Problemen mit Berechtigungen an Active Directory-Objekten benutzt wird. Dabei werden die ACLs ausgelesen und als Textdatei oder tabulatorgetrennte Datei ausgegeben. Es werden jedoch nur Berechtigungen für die Active Directory-Objekte angezeigt, für die der Benutzer selbst über die Anzeigeberechtigung verfügt. Die Syntax für *ACLDIAG* sieht folgendermaßen aus:

```
Acldiag <DN des Objekts> [/schema] [/chkdeleg] [/geteffective:<Benutzer/Gruppe>] [/cdo] [/skip] >Ausgabedatei
```

Die Parameter für *ACLDIAG* zeigt Tabelle 23.2.

Parameter	Beschreibung
DN des Objekts	Hier ist der definierte Name des zu analysierenden Objekts in der Form CN=,CN=,DC=,DC= anzugeben. Befinden sich Leerzeichen in einem Namensteil, so ist dieser in Anführungszeichen zu setzen.
/schema	Vergleicht, ob die Berechtigungen im ACL des Objekts mit den im Schema standardmäßig definierten übereinstimmen.
/chkdeleg	Überprüft, ob die auf das Objekt angewendete Sicherheit mit einer Vorlage des Assistenten zur Verwaltungsdelegierung (siehe Kapitel 8.5.1) erstellt wurde.
/geteffective:	Geben Sie hinter diesem Parameter den Namen eines Benutzers oder einer Gruppe an, deren spezielle Berechtigungen für das Objekt ausgegeben werden sollen. Geben Sie stattdessen * an, so werden die effektiven Berechtigungen aller Benutzer angezeigt.
/cdo	Geben Sie stattdessen /tdo an, so erhalten Sie eine tabulator-separierte Datei anstelle einer reinen Textdatei, die in einer anderen Applikation weiterverarbeitet werden kann.
/skip	Über diesen Parameter wird die Anzeige der Sicherheitsbeschreibungen ausgeschaltet.

Tabelle 23.2: Die Parameter für *ACLDIAG*

Beispielsweise erzeugt der Befehl

```
acldiag cn="mac user",cn=users,dc=firma,dc=de /schema /chkdeleg /tdo
```

folgende Ausgabe (siehe Abbildung 23.1). Fügen Sie an den Befehl als Ausgabedatei >macuser.txt an, so erfolgt die Ausgabe nicht auf dem Monitor, sondern in einer tabularseparierten Textdatei.

```

C:\Programme\Support Tools>acldiag cn="mac user",cn=users,dc=firma,dc=de /schema
/chkdeleg /tdo

cn="mac user",cn=users,dc=firma,dc=de
Owner: FIRMA\Domain-Admins
Permissions Not Protected. Auditing Not Protected

This object allow FIRMA\Domain-Admins Create all subobjects
This object allow FIRMA\Domain-Admins Delete all subobjects
This object allow FIRMA\Domain-Admins Read all properties
This object allow FIRMA\Domain-Admins Write all properties
This object allow FIRMA\Domain-Admins List contents
This object allow FIRMA\Domain-Admins List object
This object allow FIRMA\Domain-Admins All control accesses
This object allow FIRMA\Domain-Admins Modify Membership
This object allow NT-AUTORITÄT\SYSTEM Create all subobjects
This object allow NT-AUTORITÄT\SYSTEM Delete all subobjects
This object allow NT-AUTORITÄT\SYSTEM Read all properties
This object allow NT-AUTORITÄT\SYSTEM Write all properties
This object allow NT-AUTORITÄT\SYSTEM List contents
This object allow NT-AUTORITÄT\SYSTEM List object
This object allow NT-AUTORITÄT\SYSTEM All control accesses
This object allow NT-AUTORITÄT\SYSTEM Modify Membership
This object allow WOEDEFINIERT\Konten-Operatoren Create all subobjects
This object allow WOEDEFINIERT\Konten-Operatoren Delete all subobjects
This object allow WOEDEFINIERT\Konten-Operatoren Read all properties
This object allow WOEDEFINIERT\Konten-Operatoren Write all properties
This object allow WOEDEFINIERT\Konten-Operatoren List contents
This object allow WOEDEFINIERT\Konten-Operatoren List object
This object allow WOEDEFINIERT\Konten-Operatoren All control accesses
This object allow WOEDEFINIERT\Konten-Operatoren Modify Membership
This object allow NT-AUTORITÄT\SELBST Read all properties
This object allow NT-AUTORITÄT\SELBST List contents
This object allow NT-AUTORITÄT\SELBST List object
This object allow NT-AUTORITÄT\SELBST Change Password
This object allow NT-AUTORITÄT\SELBST Send As
This object allow NT-AUTORITÄT\SELBST Receive As

```

Abbildung 23.1: Die Ausgabe eines ACLDIAG-Aufrufs

23.1.2 ADSIEDIT

Bei *ADSIEDIT* handelt es sich um einen Active Directory-Editor in Form einer mmc. In dieser mmc können Sie manuell die Einstellungen vornehmen, die automatisch beispielsweise über die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER, ACTIVE DIRECTORY-STANDORTE UND -DIENSTE und ACTIVE DIRECTORY-SCHEMA eingetragen werden. *ADSIEDIT* ist ein Low-Level-Editor für das gesamte Active Directory und vergleichbar mit *regedit* oder *regedt32* für die Systemregistrierung. Allerdings birgt dieses Tool auch eine große Gefahr: In den übrigen mmcs erhalten Sie zusätzliche Sicherheitsabfragen, bevor ein Objekt verschoben oder sogar gelöscht werden soll. Dies ist bei *ADSIEDIT* nicht der Fall. Es steht auch keine Undo-Funktion zur Verfügung. Bevor Sie also daran gehen, möglicherweise Ihre Domäne zu zerstören, sollten Sie ein Backup anlegen.

Sobald Sie das Tool über STARTMENÜ / PROGRAMME / WINDOWS 2000 SUPPORT TOOLS / TOOLS / ADSIEDIT gestartet haben, versucht es sich mit der Domäne zu verbinden, an der Sie aktuell angemeldet sind (siehe Abbildung 23.2). Sind Sie an keiner Domäne angemeldet, erhalten Sie Fehlermeldungen. Sie sollten in diesem Fall eine neue mmc erstellen und dieser das Snap-In ADSIEDIT hinzufügen.

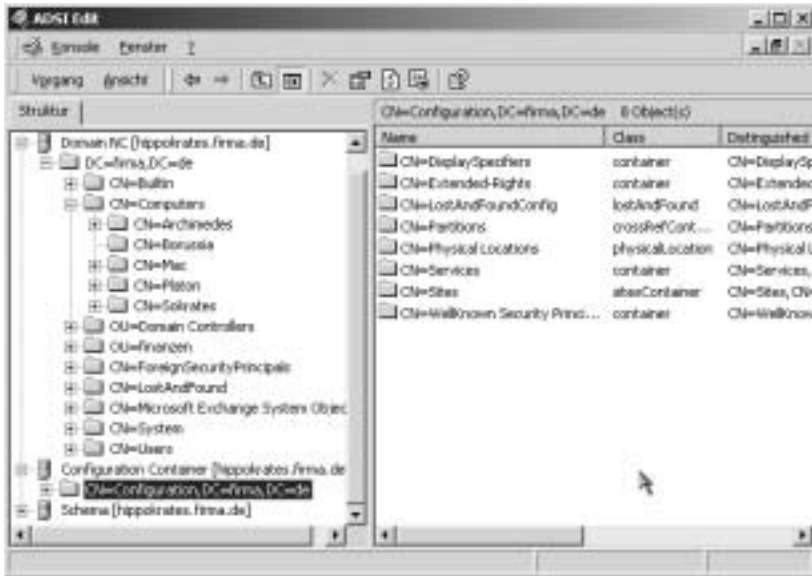


Abbildung 23.2: Die mmc ADSIEDIT

ADSIEDIT bietet Ihnen im Knoten DOMAIN NC eine hierarchische Ansicht des Namenskontextes der Domäne. Diese enthält alle Objekte der mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER. Der Knoten CONFIGURATION CONTAINER enthält Angaben über z.B. die Standorte, erweiterte Berechtigungen, die Konfiguration von LostAndFound, Partitionen oder Services. Der Knoten SCHEMA enthält alle Informationen des Active Directory-Schemas. Unter jedem Knoten befinden sich die zugehörigen Untercontainer und Objekte. Sämtliche Bearbeitungsoptionen der Objekte finden Sie im Kontextmenü. Sie können bestehende Objekte umbenennen, verschieben und löschen sowie neue Objekte erstellen. Über die Eigenschaften erhalten Sie ein neues Fenster mit den Registerkarten ATTRIBUTES und SICHERHEITSEINSTELLUNGEN. Über ATTRIBUTES können Sie sämtliche Attribute eines Objekts editieren (siehe Abbildung 23.3).

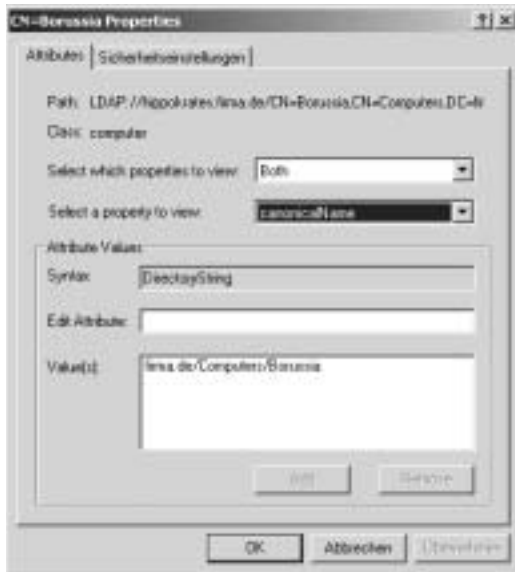


Abbildung 23.3: Editieren von Attributen mit ADSIEDIT

Zuerst müssen Sie entscheiden, ob Sie nur die Eigenschaften, die bei einem Objekt angegeben sein müssen, oder nur die optionalen oder beide anzeigen möchten. Wählen Sie dazu aus der Listbox SELECT WHICH PROPERTIES TO VIEW entweder MANDATORY, OPTIONAL oder BOTH. Dementsprechend erhalten Sie eine Liste der Eigenschaften unter SELECT A PROPERTY TO VIEW. Markieren Sie das Attribut, und Sie sehen unten im Feld VALUE(S) den aktuellen Wert. Sie können einen neuen Wert im Feld EDIT ATTRIBUTE eingeben und über ADD hinzufügen. Bestehende Werte können mit REMOVE gelöscht werden. Beachten Sie jedoch, dass Sie die im Feld SYNTAX vorgegebene Schreibweise einhalten. Ansonsten kann das Attribut nicht korrekt verarbeitet werden.

Auf der Registerkarte SICHERHEITSEINSTELLUNGEN können Sie die standardmäßigen und erweiterten Sicherheitseinstellungen für jedes Objekt konfigurieren.

ADSIEDIT ist aufgrund seiner Komplexität und auch der Gefahren, die das Programm birgt, nicht zum standardmäßigen Editieren oder Erstellen von Objekten geeignet. Verwenden Sie hierzu lieber ADSI-Skripte (siehe Kapitel 32). ADSIEDIT dient eher Zwecken des Troubleshooting. Hier können manuell Einträge entfernt werden, die das Active Directory an ordnungsgemäßer Funktion hindern. Dies kann z.B. der Fall sein, wenn sich ein Domänencontroller über DCPROMO nicht mehr herabstufen lässt. Wird DCPROMO nicht ordnungsgemäß abgeschlossen, werden im Active Directory möglicherweise nicht mehr aktuelle Informationen über den alten Domänencontroller beibehalten, was zu Problemen führen kann. Dies kann auch dazu führen, dass sich ein Domänencontroller nicht mehr aus dem Active Directory löschen lässt und Sie stattdessen die Fehlermeldung: FEHLER 2094. DAS DSA-OBJEKT KANN NICHT GELÖSCHT WERDEN 0x2094 erhalten. Über ADSIEDIT haben Sie die Möglichkeit, das Domänencontroller-Objekt aus dem Domain NC zu entfernen. Weitere Hinweise zum Entfernen eines Domänencontrollers finden Sie unter dem Link <http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q216498>

23.1.3 ADSIZER

Mit dem Active Directory Sizer (*ADSIZER*) können Sie bereits vor der Implementierung von Active Directory den dafür erforderlichen Hardwarebedarf bestimmen. Basierend auf Ihren Angaben zur Anzahl der Benutzer, Anzahl der Objekte oder auch der DHCP-Leasedauer von IP-Adressen usw. errechnet Ihnen dieses Programm die Anzahl der benötigten Domänencontroller, Bridgehead-Server und globalen Katalogserver, die Größe der Active Directory-Datenbank sowie die Auslastung der Netzwerkbandbreite.

Der ADSIZER arbeitet in Form eines Wizards, in dem Sie nacheinander Ihre Angaben machen können. Für jede Angabe finden Sie einen Link, der Ihnen kurz erklärt, was mit dem jeweiligen Wert gemeint ist. Sie haben die Möglichkeit, die folgenden Daten anzugeben:

1. Name der Domäne
2. Anzahl der Benutzer der Domäne, Prozentsatz der Benutzer, die zu Spitzenzeiten gleichzeitig eingeloggt sind, Anzahl der zusätzlichen selbst definierten Attribute pro Benutzer.
3. Anzahl der Gruppen, zu denen jeder Benutzer gehört, Ablaufdatum des Passworts, Durchschnittliche Login-Rate pro Sekunde zu Spitzenzeiten getrennt nach Netzwerk-, interaktiven (z.B. Terminalserver) und Batch-Anmeldungen. Dieser Wert kann auch basierend auf Ihren Angaben zu Benutzeranzahl und Anzahl der gleichzeitig eingeloggten Benutzer automatisch für interaktive und Netzwerkanmeldungen errechnet werden.
4. Anzahl der Windows 2000- und Windows 9x/NT-Rechner, Anzahl der übrigen Objekte wie Drucker, Benutzergruppen, Kontakte, Freigaben usw.
5. Das Limit der CPU-Auslastung pro Domänencontroller, der gewünschte Prozessortyp und Anzahl der Prozessoren pro Domänencontroller.
6. Anzahl der Objekte, die täglich, wöchentlich oder jährlich von den Administratoren hinzugefügt, gelöscht und bearbeitet werden.
7. Weitere Bestandsaufnahmen, wenn der Einsatz von Exchange 2000 geplant ist, z.B. Anzahl der täglichen Mails, Anzahl der Empfänger pro Mail, Anzahl der Exchange Server- und Exchange Routing-Gruppen.
8. Optionale Angaben für weitere Dienste, z.B. Anzahl der Wählverbindungen von Domänencomputern aus, DHCP-Leasedauer, Verwendung von Active Directory-integrierten DNS-Zonen und NoRefreshInterval des DNS-Servers.
9. Änderungen, Modifizierungen und Suchaufträge, die von Programmen zur Zeichnisynchronisierung oder dem Active Directory Connector (ADC) vorgenommen werden

Sie erhalten dann eine Zusammenfassung über die benötigte Anzahl der Domänencontroller, globalen Katalogserver und Bridgehead-Server, der Anzahl der Active Directory-Objekte, der Datenbankgröße auf dem Domänencontroller und globalen Katalogserver sowie der Anzahl der Benutzer.

Doch mit der Berechnung dieser Daten sind die Fähigkeiten des ADSIZER bei weitem noch nicht ausgeschöpft. Abbildung 23.4 zeigt die mmc des ADSIZER, mit dem die fiktive Domäne weiter konfiguriert wurde.

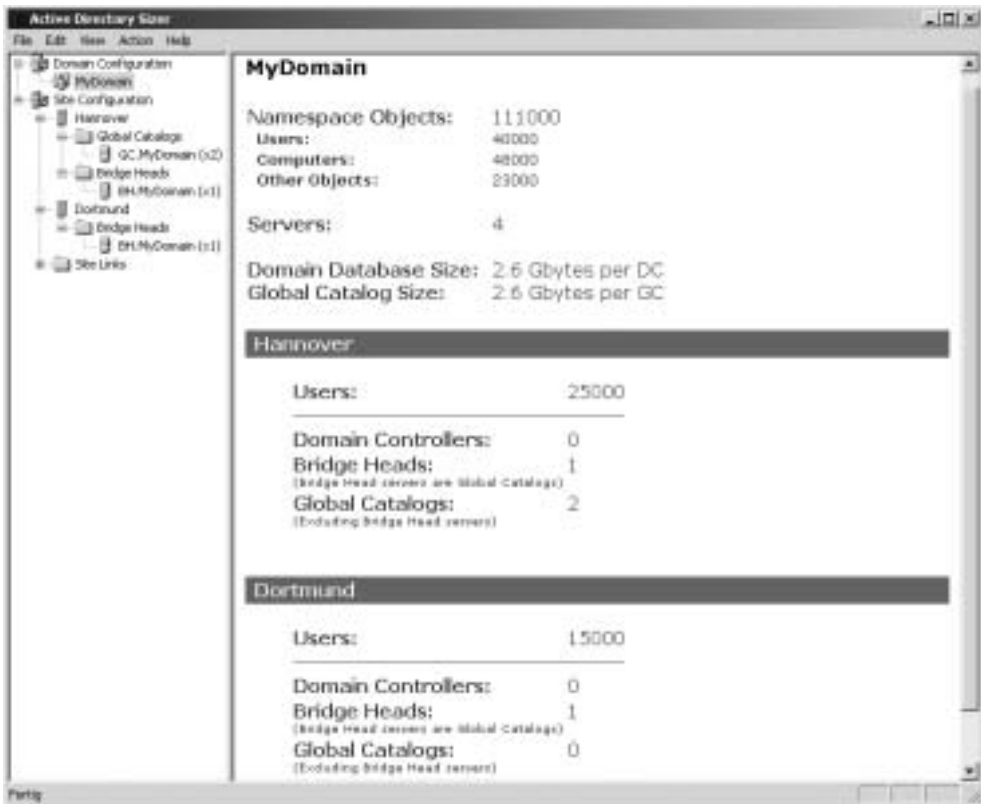


Abbildung 23.4: Die Konfiguration einer Domäne mit ADSIZER

Sie haben nach Errechnung der Basisdaten die Möglichkeit, für die Domäne verschiedene Standorte und Standortverknüpfungen anzulegen sowie weitere Domänen hinzuzufügen. Für jeden Standort können Sie in dessen Eigenschaften den Namen und sein Subnetz angeben. Jede Standortverknüpfung können Sie mit einem Faktor für die Kosten sowie der Netzwerkbandbreite versehen. Weiterhin können Sie die Topologie der Standorte verändern, indem Sie die Standorte zu verschiedenen Standortverknüpfungen hinzufügen oder aus diesen wieder entfernen. Zwischen mehreren Standorten können Sie auch die Gesamtanzahl der Benutzer verteilen. Außerdem können Sie auch jederzeit die Stammdaten der Domäne überarbeiten, ohne diese komplett neu angeben zu müssen. Sämtliche der eben genannten Einstellungen können Sie ändern, indem Sie in der mmc den jeweiligen Knoten markieren und aus dessen Kontextmenü den Eintrag **PROPERTIES** wählen.

Sie haben also mithilfe dieses Tools bereits vor der Implementierung die Möglichkeit zu bestimmen, welche und wie viel Hardware serverseitig benötigt wird. Diese Hardware müssen Sie nur noch an den entsprechenden Standorten aufstellen. Auch wenn Ihr Unternehmen zu einem späteren Zeitpunkt weiter expandiert, können Sie mit diesem Programm berechnen, ob die Server-Hardware noch ausreichend ist oder an welchen Standorten nachgebessert werden muss.

23.1.4 DCDIAG

Bei *DCDIAG* handelt es sich um ein Kommandozeilenprogramm, das für etliche Diagnosen und Tests im Zusammenhang mit Active Directory-Problemen benutzt werden kann. *DCDIAG* für Windows 2000 Server unterstützt insgesamt 17 verschiedene Tests. *DCDIAG* kann mit den folgenden Parametern ausgeführt werden (siehe Tabelle 23.3):

Parameter	Beschreibung
/s:	Gibt den Namen des zu überprüfenden Domänencontrollers an.
/u:	Gibt das Benutzerkonto in der Form Domäne\Benutzer an. Ist kein Parameter /u: angegeben, wird das aktuelle Konto benutzt. /p: muss auch angegeben werden.
/p:	Das Passwort des unter /u: angegebenen Kontos
/a:	Testet alle Server des Standorts
/e:	Testet alle Server im gesamten Unternehmen. Dieser Parameter überschreibt /a:.
/q:	In diesem Modus werden nur die Fehlermeldungen ausgegeben.
/v:	In diesem Modus erfolgen erweiterte Ausgaben.
/i:	Es werden nur die nötigsten Fehlermeldungen ausgegeben.
/fix:	Führt Reparaturen durch, die als sicher gelten.
/f:	Leitet die Ausgaben an die angegebene Datei weiter.
/ferr:	Die Ausgaben schwerwiegender Fehler werden an die angegebene Datei weitergeleitet.
/c:	Es werden alle verfügbaren Tests durchgeführt. Kann zusammen mit /skip verwendet werden.
/test:	Es wird nur der angegebene Test ausgeführt. Auch die Ausführung mehrerer Tests ist möglich. Darf nicht zusammen mit /skip verwendet werden.
/skip:	Der angegebene Test wird übersprungen. Darf nicht zusammen mit /test: verwendet werden.

Tabelle 23.3: Die Parameter für das Programm *DCDIAG*

Tabelle 23.4 gibt eine Übersicht über die verfügbaren Tests und ihre durchgeführten Prüfungen.

Testname	Beschreibung
Connectivity	Dieser Test wird bei jedem Ausführen von DCDIAG durchgeführt. Hiermit wird überprüft, ob die Domänencontroller erreichbar sind (Ping), im DNS registriert sind und über eine LDAP/RPC-Verbindung verfügen. In vielen Fällen ist ein simpler Neustart ausreichend, um die Verbindungsprobleme zu beheben.
Replications	Überprüft, ob die Replikation zwischen den Domänencontrollern rechtzeitig stattfindet. Es werden die Domänencontroller angegeben, bei denen dies nicht der Fall ist. Prüfen Sie die Ereignisprotokolle der aufgelisteten DCs, um die Ursache bestimmen zu können.
Topology	Überprüft, ob innerhalb der Replikationstopologie alle Domänencontroller enthalten und verbunden sind.
CutoffServers	Sucht nach Servern, die keine Replikationsdaten erhalten, da ihre Replikationspartner nicht verfügbar sind. Diese DCs können Probleme bereiten, da sie aufgrund fehlender Replikation veraltete Daten der Active Directory-Datenbank bereitstellen.
NCSecDesc	Überprüft die Sicherheitsbeschreiber des Namenskontextes daraufhin, ob für die Replikation ausreichende Berechtigungen bestehen.
NetLogons	Überprüft die Logon-Berechtigungen daraufhin, ob die Replikation erfolgreich durchgeführt werden kann. Schlägt der Test fehl, werden die AD-Objekte angegeben, deren Berechtigungen geändert werden müssen.
Advertising	Prüft, ob sich der Domänencontroller korrekt in seiner Rolle ausgibt.
KnowsOfRoleHolders	Überprüft, ob der Domänencontroller die Inhaber der Betriebsmasterrollen erkennt, und gibt die identifizierten Rolleninhaber aus.
Intersite	Sucht nach Fehlern, die für eine temporäre oder dauerhafte Störung oder Verzögerung der standortübergreifenden Replikation verantwortlich sind. Möglicherweise ist ein Bridgehead-Server nicht verfügbar.
FsmoCheck	Prüft, ob die globalen Betriebsmaster bekannt und erreichbar sind.
RidManager	Prüft, ob der RIDMaster erreichbar ist und die korrekten Informationen liefert. Möglicherweise bietet der RIDMaster nicht genügend Performance zur Durchführung seiner Aufgaben. Ein leistungsstärkerer Server könnte die Lösung sein.
MachineAccount	Überprüft, ob der Maschinen-Account über korrekte Informationen verfügt.
Services	Prüft, ob alle erforderlichen Domänencontroller-Dienste laufen. Ist dies nicht der Fall, prüfen Sie das Ereignisprotokoll des betroffenen DCs.
OutboundSecure-Channels	Überprüft die Sicherheits-Channel von allen Domänencontrollern der in unter /Domänenname angegebenen Domäne. Mit dem zusätzlichen Parameter /nositerestriction werden nicht nur die Domänencontroller innerhalb des Standortes überprüft, sondern alle.

Testname	Beschreibung
ObjectsReplicated	Überprüft die replizierten Objekte. Für zusätzliche Objekte geben Sie /objectdn:<DN des Objekts> mit /n:<Namenskontext> an.
Frssysvol	Überprüft, ob FRS (File Replication Service) SYSVOL bereit ist.
Systemlog	Überprüft, welche im System-Ereignisprotokoll aufgezeichneten Fehler auf dem Computer vorhanden sind.
Kccevent	Überprüft, ob der Knowledge Consistency Checker fehlerfrei durchläuft.

Tabelle 23.4: Die verfügbaren Tests unter DCDIAG für Windows Server 2000

Unter Windows Server 2003 gibt es neben den eben genannten Tests noch eine Reihe weiterer Tests. Diese führt Tabelle 23.5 auf.

Testname	Beschreibung
DcPromo	Überprüft die DNS-Infrastruktur, bevor ein Server zum Domänencontroller heraufgestuft wird.
RegisterInDNS	Überprüft, ob der Domänencontroller die DNS-Ressourceneinträge (die Domain Controller Locator-Einträge) registrieren kann. Über den Parameter /DnsDomain: wird der DNS-Name der Active Directory-Domäne angegeben.
DeadCRTest	Überprüft, ob nach der fehlerhaften Erstellung einer Applikationspartition noch überflüssige Referenzen vorhanden sind.
CheckSDRefDom	Überprüft, ob für alle Applikationspartitionen die Sicherheitsbeschreiber der referenzierten Domänen korrekt sind.
VerifyReplicas	Überprüft, ob auf allen Servern die Applikationspartitionen vollständig instanziiert sind.
CrossRefValidation	Überprüft die Gültigkeit der kreuzweisen Beziehungen.
VerifyReferences	Überprüft die Systemreferenzen, die für die Replication und FRS (File Replication Service) benötigt werden.
VerifyEnterpriseReferences	Überprüft die Systemreferenzen, die für die Replication und FRS (File Replication Service) benötigt werden. Dieser Test erstreckt sich über alle Objekte auf jedem Domänencontroller des Unternehmens.

Tabelle 23.5: Die verfügbaren Tests unter DCDIAG für Windows Server 2003

23.1.5 DNSCMD

DNSCMD ist ein Kommandozeilenprogramm, mit dem Informationen über DNS-Server und deren Konfiguration angezeigt und Probleme behoben werden können. Die wichtigsten Befehle für *DNSCMD* wurden bereits in Kapitel 16.6.3 aufgeführt. Mit *DNSCMD* können Sie alle Aufgaben durchführen, die alternativ auch an der GUI der DNS-mmcc erledigt werden können.

Tabelle 23.6 gibt Ihnen einen Überblick über die wichtigsten Befehle. Alle weiteren Befehle finden Sie über den Aufruf `dnscmd -? [↵]`.

Befehl	Funktion
/Info	Zeigt die Informationen über den DNS-Server an.
/Config	Setzt die Informationen des DNS-Servers oder der Zone zurück. Sollten nach dem Befehl <code>dnscmd /Config ..AllZones /AllowUpdate 0x2</code> beim Start im Ereignisprotokoll des DNS-Servers Fehlermeldungen mit der ID 500 oder 501 auftreten, so müssen Sie unter Windows 2000 das Servicepack 3 installieren.
/EnumZones	Listet die eingerichteten DNS-Zonen auf.
/ClearCache	Löscht den DNS-Cache des Servers. Sofern nicht mindestens das Servicepack 2 unter Windows 2000 installiert ist, können Sie folgende Fehlermeldung erhalten: <code>failed: status = 9718 (0x000025f6)</code>
/ResetListenAddresses	Hinzufügen von IP-Adressen von weiteren DNS-Servern für Abfragen.
/ResetForwarders	Hinzufügen von DNS-Servern, an die rekursive Abfragen gesendet werden können.
/ZoneInfo	Zeigt die Informationen der Zone an.
/ZoneAdd	Erstellt eine neue DNS-Zone. Bei Active Directory-integrierten Zonen müssen Sie darauf achten, dass die Zonennamen keine von Windows reservierten Wörter enthalten. Reservierte Wörter sind: CON, AUX, COM1, COM2, COM3, COM4, LPT1, LPT2, LPT3, PRN und NUL. Eine Zone darf also z.B. nicht <code>nul.ktc.de</code> heißen.
/ZoneDelete	Löscht eine DNS-Zone.
/ZonePause	Hält eine DNS-Zone vorübergehend an.
/ZoneResume	Startet eine DNS-Zone neu.
/ZoneReload	Lädt eine Zone neu aus der Datenbank (dem Active Directory oder der Textdatei).
/ZoneRefresh	Erzwingt die Aktualisierung einer sekundären Zone vom Master.
/ZoneUpdateFromDs	Aktualisiert die Daten einer Active Directory-integrierten Zone mit den Daten aus dem Active Directory.
/ZoneResetType	Ändert den Zonentyp Active Directory-integriert, Standard primär und sekundär.
/ZoneResetMasters	Erstellt die Master-Server für eine sekundäre Zone neu.

Tabelle 23.6: Die Befehle für DNSCMD

Um die Parameter der jeweiligen Befehle zu erhalten, rufen Sie `dnscmd` gefolgt von dem jeweiligen Befehl auf, also z.B. `dnscmd /ZoneInfo` .

Alle Befehle werden nach dem folgenden Schema ausgeführt:

`Dnscmd <Server> <Befehl> [optionale Parameter]`

Unter `<Server>` können Sie einen Punkt (.) für den lokalen Server setzen oder Remote Procedure Calls (RPCs) auf andere DNS-Server über die IP-Adresse oder den DNS-Namen durchführen.

23.1.6 DOMMON

DOMMON ist ein grafisches Programm, mit dem Sie den Status der Domänencontroller und Server innerhalb seiner Domäne sowie auch der Domänencontroller der vertrauten Domänen überwachen können (siehe Abbildung 23.5).

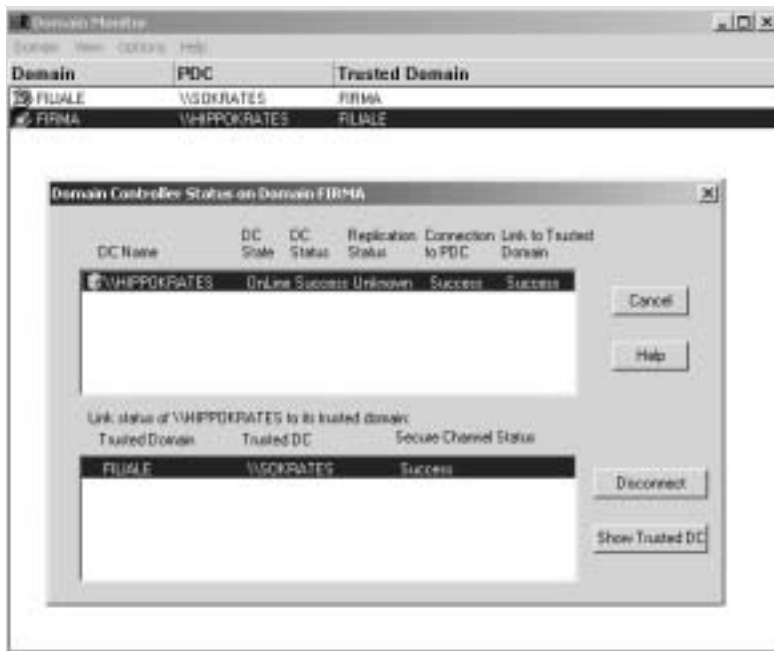


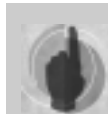
Abbildung 23.5: Das Domänenüberwachungsprogramm DOMMON

Über das Menü DOMAIN/PROPERTIES werden die spezifischen Daten der Domänencontroller angezeigt. Die einzelnen Spalten haben folgende Bedeutungen (siehe Tabelle 23.7):

Status	Bedeutung und Werte
DC Names	Gibt den Namen des Domänencontrollers an. Verwenden Sie in einer gemischten Umgebung auch Windows NT-Domänen, so haben die Domänencontroller und BDCs verschiedene Symbole.
DC State	Online gibt an, dass der Server läuft. Findet sich hier der Wert Offline, so ist der DC entweder ausgeschaltet, oder einer der Dienste Server, Workstation oder Netlogon arbeitet nicht korrekt.
Replication Status	Gibt den Status der Replikation an. Mögliche Werte sind: InSync: Die Daten auf dem Server sind identisch mit denen des Domänencontrollers. InProgress: Die Replikation wird gerade durchgeführt. ReplRequired: Die Daten des Servers sind älter als die des Domänencontrollers. Unknown: Der Domänencontroller kann nicht mit dem eigenen Status verglichen werden.
Connection to PDC	Gibt den Status (Success oder Fehlercode) zu den Domänencontrollern der gewählten Domäne an.
Link to Trusted Domain	Gibt an, ob eine Verbindung zur vertrauenden Domäne hergestellt werden kann.

Tabelle 23.7: Die Statusbeschreibungen eines Domänencontrollers im Programm DOMMON

Über die Schaltfläche SHOW TRUSTED DC können Sie die eben beschriebenen Daten auch für die Domänencontroller der vertrauenden Domänen abrufen. Zusätzlich kann unter OPTIONS/INTERVALS auch das Aktualisierungsintervall für die Statusanzeige eingestellt werden.



Das Programm *DOMMON* war bereits im Lieferumfang der Support-Tools für Windows NT enthalten. Deshalb finden sich hier auch noch die Begrifflichkeiten PDC und BDC.

23.1.7 DSACLS

DSACLS ist ein Kommandozeilenprogramm, mit dem die Zugriffssteuerungslisten (ACLs) für Active Directory-Objekte bearbeitet und angezeigt werden können. Das Programm bietet eine sehr umfangreiche Syntax.

Als Erstes wird nach der Eingabe von `dscls`  der Name des zu bearbeitenden Objekts aufgerufen. Dieser muss in der Form `CN=,CN=,DC=,DC=` angegeben werden. Um das Objekt auf einem speziellen Domänencontroller aufzurufen, setzen Sie vor den Objektpfad `\\[Name des Domänencontrollers]\CN=,....` Sind keine weiteren Optionen angegeben, werden Ihnen die aktuellen Sicherheitseinstellungen des Objekts angezeigt. Für alle weitergehenden Aufgaben stehen Ihnen zahlreiche Optionen zur Verfügung.

Option	Beschreibung
/I:TSP	Gibt die Flags für die Vererbung an. T: das aktuelle Objekt mit untergeordneten Objekten; S: nur die untergeordneten Objekte; P: vererbte Optionen werden nur eine Ebene weitergeleitet.
/N	Ersetzt die aktuellen Sicherheitseinstellungen, anstatt sie zu editieren.
/P:YN	Markiert das Objekt als geschützt (Y). Ist das Flag nicht gesetzt, wird das aktuelle Protection-Flag beibehalten.
/G:<Gruppe/Benutzer>: <Berechtigungen>	Erteilt dem Benutzer oder der Gruppe die Berechtigungen. Die Berechtigungen werden weiter unten erläutert. Der Benutzer oder die Gruppe ist im Format Domäne\Gruppe bzw. Benutzer oder Gruppe bzw. Benutzer@Domäne anzugeben.
/D:	Verweigert dem Benutzer oder der Gruppe die angegebenen Berechtigungen. Format siehe unter /G.
/R:	Entfernt alle Berechtigungen für den Benutzer oder die Gruppe.
/S	Stellt wieder die im Active Directory-Schema angegebenen Standardsicherheitseinstellungen für das Objekt her.
/T	Setzt die Sicherheit für den Objektbaum wieder auf die Einstellungen der Objektklasse zurück. Dazu muss /S gesetzt sein.
/A	Zeigt neben den Sicherheitseinstellungen auch die Auditing-Informationen sowie den Besitzer des Objekts an.
<Berechtigungen>	Berechtigungen werden im folgenden Format angegeben: [Rechte];[Objekt/Eigenschaft];[vererbter Objekttyp]. Siehe dazu die jeweiligen Einträge in der Zeilen Rechte und Objekt/Eigenschaft.
[Rechte]	Generelle Berechtigungen: GR=lesen, GE=ausführen, GW=schreiben, GA=Vollzugriff, Spezielle Berechtigungen: SD=löschen, DT=löschen eines Objekts mit untergeordneten Objekten, RC=lesen der Sicherheitsinformationen, WD=ändern der Sicherheitsinformationen, WO=ändern der Besitzerinformationen, LC=auflisten der untergeordneten Objekte des Objekts, CC=erstellen eines untergeordneten Objekts, DC=löschen eines untergeordneten Objekts, WS=schreiben ins selbe Objekt; WP=lesen der Eigenschaften, RP=schreiben von Eigenschaften, CA=Kontrolle der Zugriffsberechtigungen, LO=auflisten des Objektzugriffs. Weitere Hinweise finden Sie unter dsac ls /?.
[Objekt/Eigenschaft]	Hier muss der Anzeigename des Objekts oder der Eigenschaft angegeben werden, z.B. Benutzer für die Benutzerobjekte oder Telefonnummer für die Objekt-Eigenschaft Telefonnummer.
[vererbter Objekttyp]	Hier ist der Anzeigename des Objekts oder der Eigenschaft anzugeben, an das/die die Berechtigungen vererbt werden sollen. Hiermit werden die im Schema definierten Standardberechtigungen für ein Objekt überschrieben.

Tabelle 23.8: Die Optionen für das Programm DSACLS

23.1.8 DSASTAT

DSASTAT ist ein Kommandozeilenprogramm, mit dem Sie überprüfen können, ob die einzelnen Active Directory-Partitionen korrekt repliziert worden sind. Die Partitionen auf verschiedenen Domänencontrollern werden dabei miteinander verglichen. Es werden die Daten wie Megabyte pro Server, Objekte pro Server und Megabytes pro Objektklasse ausgelesen. Dann werden die Attribute der replizierten Objekte miteinander verglichen. Es können sowohl zwei Verzeichniszweige innerhalb derselben Domäne als auch zwischen verschiedenen Domänen durchsucht werden. Letzteres gilt, wenn die Einträge des globalen Katalogs verglichen werden sollen.

DSASTAT kann mit den folgenden Parametern gestartet werden (siehe Tabelle 23.9):

Parameter	Beschreibung
-s:	Name des/der Server, über die Informationen bezogen bzw. deren Datenbankinhalte miteinander verglichen werden sollen. Mehrere Namen werden mit ; voneinander getrennt.
-b:	Hier ist der definierte Name (DN) des zu durchsuchenden Basis-Objekts anzugeben, z.B. OU=Finanzen,DC=Firma,DC=de.
-output:	Gültige Werte für die Ausgabe sind file, screen und both. Ist kein Parameter gesetzt, wird both benutzt.
-loglevel:	Mögliche Werte für den Log-Level sind debug, trace und info. Debug gibt die meisten, info die wenigsten Informationen an. Ist kein Parameter gesetzt, wird info benutzt.
-scope:	Gibt den Bereich der Suche an. Mögliche Werte sind BASE, ONELEVEL und SUBTREE. Der Standardwert ist SUBTREE.
-filter:	Es können Filter für die Suche gesetzt werden. Der Standardfilter lautet (objectclass=*). Es können auch mehrere Filter miteinander verknüpft werden. Um z.B. nur die Benutzerobjekte, nicht aber die Computerobjekte in die Suche einzubeziehen, wird folgender Filter gesetzt: -filter:"(&(objectclass=user)(!objectclass=computer))" 
-gcattr:	Gibt die Attribute an, die beim Vergleich berücksichtigt werden sollen. Sind keine speziellen Attribute angegeben, werden alle durchsucht.
-sort:	Die möglichen Werte sind true und false für eine sortierte Reihenfolge. Der Standardwert ist false.
-t:	Gibt an, ob der komplette Inhalt verglichen werden soll (false) oder nur ein statistischer Wert (true).
-p:	Gibt die Anzahl der Einträge auf einer Seite an. Der Standardwert liegt bei 64.
-u: -d: -pwd:	-u: gibt den Benutzernamen, -d: die Domäne und -pwd: ein gültiges Passwort für ein Benutzerkonto an, unter dem DSASTAT ausgeführt werden soll.

Tabelle 23.9: Die Parameter für das Programm DSASTAT

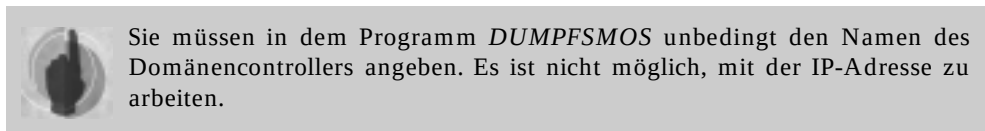
23.1.9 DUMPFMOS

Mit dem Kommandozeilenprogramm *DUMPFMOS* können Sie die Betriebsmasterrollen (Flexible Single Master Operation/FSMO, siehe Kapitel 11) ermitteln. Sie erhalten alle Rollen des angegebenen Servers, und zwar sowohl die domänenweiten Betriebsmasterrollen (PDC-Emulator, RID-Master und Infrastrukturmaster) als auch die Betriebsmasterrollen der Gesamtstruktur (Schemamaster und Domännennamen-Master).

Um die Rollen für einen bestimmten Domänencontroller zu sehen, geben Sie folgenden Befehl ein:

Dumpfsmos <Name des Domänencontrollers> 

Sie erhalten damit die Informationen, wie in Abbildung 23.6 dargestellt.



```

D:\Programme\Resource Kit>dumpfsmos hippokrates
Der Befehl "hippokrates" ist entweder falsch geschrieben oder
kannote nicht gefunden werden.
ntdsutil: rules
fsmo maintenance: Connections
server connections: Connect to server hippokrates
Bindung mit "hippokrates" ...
Eine Verbindung mit "hippokrates" wurde unter Verwendung der Benutzerinformation
en des lokal angemeldeten Benutzers wurde hergestellt.
server connections: Quit
fsmo maintenance: select Operation target
select operation target: List roles for connected server
Server "hippokrates" besitzt 5 Funktionen.
Schema - CN-MTBE Settings,CN-HIPPOKRATES,CN-Servers,CN-Barzingshausen,CN-Sites,CN-
Configuration,DC-firma,DC-de
Domäne - CN-MTBE Settings,CN-HIPPOKRATES,CN-Servers,CN-Barzingshausen,CN-Sites,CN-
Configuration,DC-firma,DC-de
PDC - CN-MTBE Settings,CN-HIPPOKRATES,CN-Servers,CN-Barzingshausen,CN-Sites,CN-Co
nfiguration,DC-firma,DC-de
RID - CN-MTBE Settings,CN-HIPPOKRATES,CN-Servers,CN-Barzingshausen,CN-Sites,CN-Co
nfiguration,DC-firma,DC-de
Infrastruktur - CN-MTBE Settings,CN-HIPPOKRATES,CN-Servers,CN-Barzingshausen,CN-S
ites,CN-Configuration,DC-firma,DC-de
select operation target: Quit
fsmo maintenance: Quit
ntdsutil: Quit
Die Verbindung mit "hippokrates" wird getrennt...

```

Abbildung 23.6: Die Ausgabewerte des Programms *DUMPFMOS*

23.1.10 FAZAM 2000

FAZAM 2000 erweitert die Funktionalitäten des Gruppenrichtlinien-Managements. Dazu bietet das Programm eine eigene mmc. Das Programm ist ein Bestandteil der frei downloadbaren Resource Kit-Tools. Sie erhalten das Programm zum Download unter der Adresse

<http://www.microsoft.com/windows2000/techno/reskit/tools/existing/fazam2000-o.asp>.



Allerdings ist das hier angebotene freie Tool im Funktionsumfang eingeschränkt. Eine Vollversion kann direkt bei FullArmor bezogen werden (<http://www.fullarmor.com>). Das Tool – auch die Vollversion – ist jedoch nur für Domänen geeignet, in denen maximal 500 Benutzer oder Computer vorhanden sind.

Als Weiterentwicklung des Programms *FAZAM 2000* ist unter Windows Server 2003 die Group Policy Management Console (GPMC, siehe Kapitel 20.3) zu sehen.

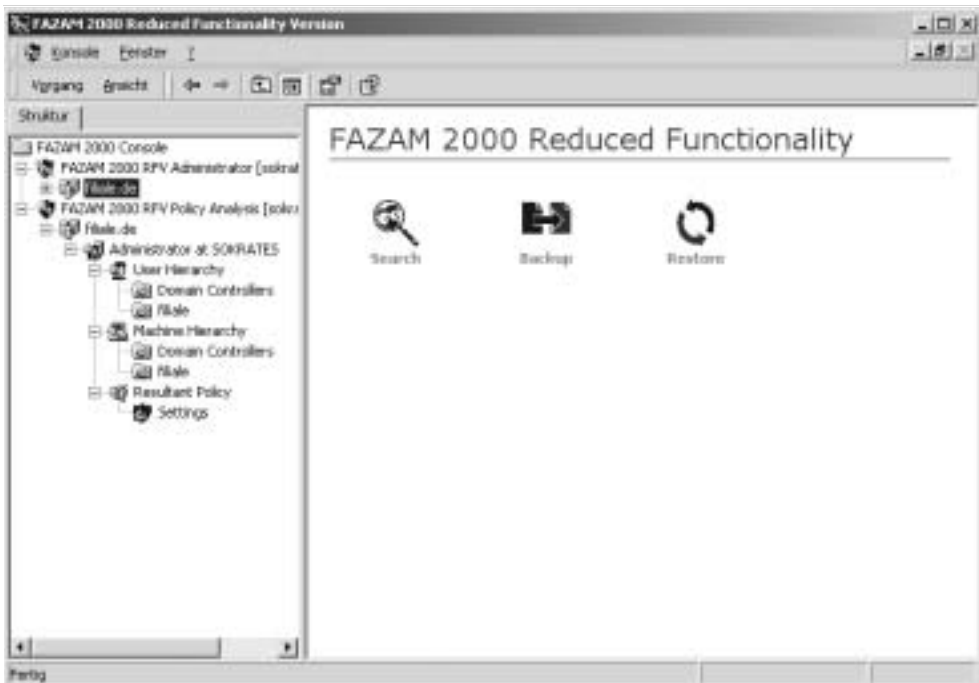


Abbildung 23.7: Die mmc des Programms *FAZAM 2000*

Die mmc ist in die Bereiche *FAZAM 2000 RFV ADMINISTRATOR* und *FAZAM 2000 RFV POLICY ANALYSIS* aufgeteilt (siehe Abbildung 23.7). Unter dem Knoten *ADMINISTRATOR* finden Sie eine Auflistung aller OUs der aktuellen Domäne sowie der GPOs, die den einzelnen OUs zugeordnet sind. Sie haben hier die Möglichkeit, über das Kontextmenü nach bestehenden GPOs zu suchen (*SEARCH GROUP POLICY*), GPOs den OUs zuzuordnen (*LINK GROUP POLICY*) oder neue GPOs zu erstellen (*NEW*). Die Suche kann über den Namen des GPOs oder dessen GUID erfolgen. Ferner haben Sie die Möglichkeit, über die Eigenschaften der Domäne die Abarbeitungsreihenfolge der vorhandenen GPOs zu ändern. Über das Kontextmenü der einzelnen OUs können dieselben Einstellungen auch OU-bezogen vorgenommen werden. Sie können auch gezielt die einzelnen GPOs bearbeiten. Es können GPOs importiert und damit bestehende GPOs überschrieben werden, durch Kopieren können GPOs zu anderen hinzugefügt werden und diese ergänzen, und

selbstverständlich können GPOs auch gelöscht werden. Über die Settings der einzelnen GPOs können Sie die Inhalte der einzelnen Objekte auflisten und den Report drucken, als HTML-Datei ausgeben oder nach MS Access exportieren.

Weiterhin besteht die Möglichkeit, ein Backup der GPOs durchzuführen. Dabei können Sie wählen, ob das komplette GPO oder nur die Einstellungen, die Verknüpfungen bzw. die Sicherheitseinstellungen gesichert werden sollen. Bei der Wiederherstellung können Sie wählen, ob das GPO in der aktuellen Domäne oder in einer untergeordneten Domäne wieder eingespielt werden soll. Allerdings können beim Wiederherstellen in untergeordneten Domänen nur die Einstellungen, nicht aber die Verknüpfungen und Sicherheitseinstellungen zurückgespielt werden.

Über den Kontextmenüeintrag FILTERS/ ADJUST FILTERS eines GPOs können Sie die Verwaltung dieses Objekts an andere Benutzer delegieren. Sobald Sie die Verwaltung delegiert haben, können Sie die Berechtigungen für diese Benutzer spezifizieren, indem Sie ihnen ADM-Files zuweisen. Die Datei *conf.adm* erteilt Zugriff auf die administrativen Vorlagen der Computer- und Benutzerkonfiguration, *inetres.adm* ermöglicht Einstellungen für den Bereich Internet Explorer und *system.adm* für alle übrigen Einstellungen.

Über den zweiten Knoten POLICY ANALYSIS können Sie eine Analyse der GPO-Konfiguration für einen bestimmten Benutzer auf einem Computer durchführen (PERFORM ANALYSIS im Kontextmenü der Domäne). Dabei werden alle GPOs angezeigt, die für einen Benutzer angewendet werden sollen. Sehr nützlich ist auch die Funktion, Resultate von Was-Wenn-Szenarien quasi vorherzusagen (WHAT-IF-ANALYSIS unter PERFORM ANALYSIS). Hierzu können Sie ein Benutzer- oder Computer-Objekt auswählen, an dem eine bestimmte Operation, z.B. das Verschieben in eine andere OU oder die Mitgliedschaft in einer anderen Gruppe, durchgeführt werden soll.

Im Diagnose-Modus können Sie für einen bestimmten Benutzer alle GPO-Einstellungen zeigen, die momentan auf ihn angewendet werden, also das effektive Ergebnis der GPOs. Über PERFORM ANALYSIS werden lediglich die GPO-Einstellungen vorhergesagt, die angewendet werden sollten. Um die Diagnose durchzuführen, starten Sie an der Kommandozeile das Programm *fadiag.exe*. Dieses befindet sich im Installationsverzeichnis von *FAZAM 2000*. Dabei müssen Sie den Namen für die zu erstellende Diagnosedatei (*.dgn) angeben. Der Aufruf kann folgendermaßen aussehen: `C:\Programme\Full Armor\Fazam 2000\fadiag.exe diagnose.dgn` 

Um die Diagnosedatei einzulesen, markieren Sie die aktuelle Domäne im Knoten POLICY ANALYSIS, klicken rechts auf DIAGNOSE und wählen die zu importierende Diagnosedatei. Es werden nun alle Einstellungen der GPOs angezeigt, die aktuell auf den Benutzer angewendet werden. Die eingeschränkte Version von *FAZAM 2000* ist allerdings sehr sparsam mit den angezeigten Informationen. Die Vollversion zeigt alle Einzelheiten an.

23.1.11 GPOTOOL

GPOTOOL ist ein Kommandozeilenprogramm, mit dem die Konsistenz der GPOs auf den Domänencontrollern getestet werden kann. Dieses Programm sollte verwendet werden, wenn Gruppenrichtlinien nicht mehr korrekt verarbeitet werden oder Probleme bei der Replikation auftreten. Tabelle 23.10 zeigt die möglichen Parameter für *GPOTOOL*.

Parameter	Beschreibung
/gpo:GPO[,GPO,GPO..]	In dieser Liste können bestimmte zu prüfende GPOs angegeben werden. Geben Sie entweder den friendly Name oder die GUID des GPOs an. Wird dieser Parameter nicht gesetzt, werden alle GPOs abgearbeitet.
/domain:Name	Hier können Sie den DNS-Namen einer Domäne angeben, in der die GPOs gesucht werden sollen. Ist dieser Parameter nicht gesetzt, wird die aktuelle Domäne benutzt.
/dc:DC[,DC,DC..]	In dieser Liste können Sie die bevorzugten Domänencontroller angeben. Werden keine DCs definiert, werden alle Domänencontroller der Domäne angezeigt.
/checkacl	Überprüft die ACL des SYSVOL-Verzeichnisses.
/verbose	Schaltet in den ausführlichen Anzeigemodus um. Sie erhalten zusätzliche Informationen zu den GPOs, z.B. Erstell- und Änderungsdatum.

Tabelle 23.10: Die Parameter für das Programm GPOTOOL

Bei der Konsistenzprüfung eines GPOs werden dessen folgende Daten ausgelesen und angezeigt: Friendly Name, GUID, Erstell- und Änderungsdatum sowie die Versionsnummer im Verzeichnisdienst und in SYSVOL. Der Ausgabewert für die Functionality-Version muss 2 lauten. Ansonsten sind Fehler in der Konsistenzprüfung aufgetreten. Im ausführlichen Modus werden bei Fehlern die Informationen über die korrupten GPOs ausgegeben.

Die Werte für die Functionality-Version oder Erweiterungs-GUIDs können nur über GPOTOOL eingesehen werden. Eine Überprüfung dieser Werte über das Gruppenrichtlinien-Snap-In ist nicht möglich, da dort diese Werte nicht angezeigt werden.

Wenn in der Domäne mehrere Domänencontroller vorhanden sind, so wird auch der Replikationsstatus des GPO auf sämtlichen Domänencontrollern verglichen. Auf jedem DC werden die Instanzen des GPO ausgelesen. Dabei wird ein vollständiger Vergleich des GPT durchgeführt sowie ein Vergleich einiger ausgewählter GPC-Eigenschaften.

23.1.12 GPRESULT

Mit dem Kommandozeilenprogramm *GPResult* haben Sie die Möglichkeit, die aktuell angewendeten GPO-Einstellungen für einen Computer und / oder angemeldeten Benutzer zu sehen. Das Programm *GPResult* können Sie unter folgender Adresse downloaden:

<http://www.microsoft.com/windows2000/techinfo/reskit/tools/default.asp>

Nach der Installation wechseln Sie an der Eingabeaufforderung in das Installationsverzeichnis des Programms und rufen die *GPResult.exe* auf. Für den Aufruf stehen vier verschiedene Parameter zur Verfügung (siehe Tabelle 23.11).

Parameter	Beschreibung
/v	Schaltet den ausführlichen Modus ein. Folgende Details werden angegeben: Liste der Sicherheitsprivilegien der Benutzer, GPO-Details (friendly Name, GUID, Version, Quelle) sowie die GPO-Bereiche administrative Vorlagen, Softwareeinstellungen, Ordnerumleitung, Sicherheitseinstellungen und Skripte.
/s	Es werden die Details wie mit /v angezeigt sowie zusätzlich: die beiden Versionsnummern des GPO (GPC und GPT), eine Liste der Programme, die unter SYSTEMSTEUERUNG/SOFTWARE/HINZUFÜGEN/ENTFERNEN vorhanden sind, und Binärwerte von Registry-Einstellungen (sofern vorhanden).
/c	Zeigt lediglich die Informationen der Computerkonfiguration an.
/u	Zeigt lediglich die Informationen der Benutzerkonfiguration an.

Tabelle 23.11: Die Parameter für das Programm GPRresult

Die angezeigten Informationen beziehen sich immer auf den Benutzer, der aktuell angemeldet ist, und den Computer, an dem der Benutzer angemeldet ist. Da die Menge der Daten sehr umfangreich werden kann (besonders bei Verwendung von /v), sollten Sie die Daten an eine Textdatei weiterleiten.

Zusätzlich zu den oben beschriebenen Informationen erhalten Sie auch weitere allgemeine Angaben zum Betriebssystem (Build Nummer, Servicepack, Typ), zum Benutzer (Benutzername und Ort im Active Directory, Domänenname und -typ, Name des Standorts, Mitgliedschaft in Sicherheitsgruppen und Berechtigungen) und zum Computer (Computernamen und Ort im Active Directory, Domänenname und -typ sowie Name des Standorts und Mitgliedschaften in Sicherheitsgruppen).

Zu jedem GPO gibt *GPRESULT* zusätzlich an, wann es das letzte Mal angewendet wurde und von welchem Domänencontroller aus dies geschah.

23.1.13 GUID2OBJ

Mit dem Kommandozeilenprogramm *GUID2OBJ* können Sie die kryptischen GUIDs in definierte Namen (DN) übersetzen. Im Active Directory besitzt jedes sicherheitsbezogene Objekt wie Benutzer, Computer oder Gruppen eine eindeutige SID in Form einer GUID. Das Programm kann mit den drei folgenden Parametern gestartet werden (siehe Tabelle 23.12):

Parameter	Beschreibung
{GUID}	Die GUID kann entweder in geschweifte Klammern gesetzt oder auch ohne Klammern angegeben werden.
/server:Servername	Sie können einen bestimmten Server für die Verbindung angeben. Ist der Parameter nicht gesetzt, wird eine Verbindung mit dem globalen Katalogserver hergestellt.
/site:Standortname	Die Verbindung wird zu einem Domänencontroller am definierten Standort hergestellt. Ist der Parameter nicht gesetzt, wird die Verbindung am aktuellen Standort hergestellt.

Tabelle 23.12: Die Parameter für das Programm GUID2OBJ

Ein Programmaufruf mit zugehörigem Ausgabewert kann folgendermaßen aussehen:

```
guid2objj {581c8d61-8958-4270-8876-8df300e58a0b} 
CN=Administrator,CN=Users,DC=Firma,DC=De
```

23.1.14 LDP

Das Programm *LDP* ermöglicht es, über eine grafische Oberfläche direkt auf die Informationen des LDAP-Protokolls zuzugreifen. Sie können hiermit die Metadaten betrachten. *LDP* ermöglicht den Zugriff auf jedes LDAP-fähige Verzeichnis, also nicht nur auf Active Directory. Nach dem Programmstart müssen Sie zunächst die Verbindung zu einem Verzeichnis herstellen. Wählen Sie hierzu aus dem Menü CONNECTION den Eintrag CONNECT. Geben Sie dort den Namen oder die IP-Adresse des Domänencontrollers an. Verwenden Sie nicht den standardmäßigen LDAP-Port 389, können Sie hier auch einen anderen angeben. Danach müssen Sie noch gültige Benutzerinformationen angeben. Wählen Sie hierzu aus dem Menü CONNECTION den Eintrag BIND. Dort geben Sie den Benutzernamen, Passwort und die Domäne an. Sie erhalten eine Bestätigung der erfolgreichen Authentifizierung.

```
>> Dn: CN=HIPPOKRATES,OU=Domain Controllers,DC=Firma,DC=de
  5) objectClass: top, person, organizationalPerson, user, computer;
  1) cn: HIPPOKRATES;
  1) distinguishedName: CN=HIPPOKRATES,OU=Domain Controllers,DC=Firma,DC=de;
  1) instanceType: 4;
  1) whenCreated: 01/12/2002 18:33:12 Westeuropäische Normalzeit Westeuropäische Sommerzeit;
  1) whenChanged: 11/11/2002 7:58:52 Westeuropäische Normalzeit Westeuropäische Sommerzeit;
  1) sNCreated: 1794;
  1) memberOf: CN=IAS- und IAS-Server,CN=Users,DC=Firma,DC=de;
  1) sNChanged: 6689;
  1) name: HIPPOKRATES;
  1) objectGUID: 231cccc5-45be-4374-a1bb-8d1e1c216514;
  1) userAccountControl: 532400;
  1) badPwdCount: 0;
  1) codePage: 0;
  1) countryCode: 0;
  1) badPasswordTime: 1267915946096000000;
  1) lastLogon: 0;
  1) lastLogon: 126815671011017168;
  1) localPolicyFlags: 0;
  1) pwdLastSet: 126791603612645040;
  1) primaryGroupID: 516;
  1) objectSid: S-15-57DAD0E1D-1E4640FD-323EB40E-3ED;
  1) accountExpires: 9223372036854775807;
  1) logonCount: 28;
  1) sAMAccountName: HIPPOKRATES;
  1) sAMAccountType: 895306369;
  1) operatingSystem: Windows .NET Server;
  1) operatingSystemVersion: 5.1 (2600);
  1) serverReferenceBL: CN=HIPPOKRATES,CN=Servers,CN=Barsinghausen,CN=Sites,CN=Configuration,DC=Firma,DC=de;
  1) dRSRefName: hippokrates.firma.de;
  1) dRSRefReference: CN=RID Set,CN=HIPPOKRATES,OU=Domain Controllers,DC=Firma,DC=de;
  1.7) servicePrincipalName: SMTPSVC/hippokrates.firma.de;
  NFr=0815426d-9445-11d2-a543-00c04fc20cd2/hippokrates.firma.de; exchangeAB/hippokrates.firma.de; exchangeAB/HIPPOKRATES;
  GC/hippokrates.firma.de/firma.de; HOST/hippokrates.firma.de/FIRMA; HOST/HIPPOKRATES; HOST/hippokrates.firma.de;
  HOST/hippokrates.firma.de/firma.de; E3514235-4B06-11D1-AB84-00C04FC20CD2/0815426d-9445-11d2-a543-00c04fc20cd2/hippokrates.firma.de;
  LDAP/0815426d-9445-11d2-a543-00c04fc20cd2/_msdos.firma.de; LDAP/hippokrates.firma.de/FIRMA; LDAP/HIPPOKRATES;
  LDAP/hippokrates.firma.de; LDAP/hippokrates.firma.de/firma.de; DNS/hippokrates.firma.de;
  1) objectCategory: CN=Computers,CN=Schema,CN=Configuration,DC=Firma,DC=de;
  1) isCriticalSystemObject: TRUE;
  1) isComputerReferenceBL: CN=HIPPOKRATES,CN=Domain System Volume (SYSVOL share),CN=File Replication
  Service,CN=System,DC=Firma,DC=de;
  1) msSFU30Gems: NIS Server;
```

Abbildung 23.8: Vom Programm *LDP* ermittelte LDAP-Informationen über ein Domänencontroller-Objekt

Als Nächstes können Sie festlegen, ob Sie den gesamten Verzeichnisbaum oder nur einen Teil daraus anzeigen möchten. Wählen Sie hierzu aus dem Menü VIEW den Eintrag TREE und geben im Feld BASEDN das Verzeichnisobjekt an, das als Root-Objekt in der Darstellung dienen soll. Um eine OU auszuwählen, geben Sie an OU=,DC=,DC=. Wählen Sie z.B. das Objekt des Domänencontrollers aus, erhalten Sie die folgenden ausführlichen Daten (Auszug, siehe Abbildung 23.8):

Darin enthalten sind Werte wie die GUID, SID, uSNCreated und uSNChanged, Informationen zum Betriebssystem, sAMAccountName usw.

Selbstverständlich können Sie mit *LDP* diese Informationen nicht nur betrachten, sondern diese auch bearbeiten. Sämtliche Bearbeitungsmöglichkeiten erreichen Sie über das Menü BROWSE. Dort können Sie neue Objekte hinzufügen sowie bestehende modifizieren, den RDN der Objekte ändern oder Objekte löschen. Zusätzlich können Objekte unter Zuhilfenahme von Filtern gesucht werden, Objekte miteinander verglichen werden, der Security Descriptor sowie die Metadaten der Replikation angezeigt werden. Abbildung 23.9 zeigt einen Auszug aus den Metadaten der Replikation.

ANID	Ver	Loc.USN	Originating DSA	Org.USN
0	1	1410	d862368b-199e-4a7b-b072-ef94957d1dde	1410
18:27.12				
20801	1	1410	d862368b-199e-4a7b-b072-ef94957d1dde	1410
18:27.12				
20802	1	1410	d862368b-199e-4a7b-b072-ef94957d1dde	1410
18:27.12				
20113	2	1729	d862368b-199e-4a7b-b072-ef94957d1dde	1729
18:27.30				
90801	1	1410	d862368b-199e-4a7b-b072-ef94957d1dde	1410
18:27.12				
9081a	2	1793	d862368b-199e-4a7b-b072-ef94957d1dde	1793
18:23.11				
90827	1	1729	d862368b-199e-4a7b-b072-ef94957d1dde	1729
18:27.30				
9083c	1	1729	d862368b-199e-4a7b-b072-ef94957d1dde	1729
18:27.30				
9083d	1	1729	d862368b-199e-4a7b-b072-ef94957d1dde	1729
18:27.30				
90849	1	1729	d862368b-199e-4a7b-b072-ef94957d1dde	1729
18:27.30				
9084a	1	1729	d862368b-199e-4a7b-b072-ef94957d1dde	1729
18:27.30				
9084c	1	1729	d862368b-199e-4a7b-b072-ef94957d1dde	1729
18:27.30				
9084f	1	1729	d862368b-199e-4a7b-b072-ef94957d1dde	1729
18:27.30				

Abbildung 23.9: Vom Programm LDP ermittelte Metadaten der Replikation

Für sämtliche Operationen müssen Sie immer unter BASEDN das Objekt in der Form CN=,CN=,DC=,DC= angeben. Sämtliche Ergebnisse sind über das Menü CONNECTION / PRINT ausdrückbar.

23.1.15 MOVETREE

Mit dem Kommandozeilenprogramm *MOVETREE* können Sie Objekte, z.B. OUs, Benutzer oder Gruppen, zwischen zwei Domänen in einer Gesamtstruktur verschieben. Unter Windows 2000 steht Ihnen dafür keine Möglichkeit zur Verfügung, dies per Drag&Drop zu erledigen. Wollen Sie hingegen Computer oder Mitgliedsserver verschieben, so benutzen Sie das Programm *NETDOM* (siehe Kapitel 23.1.17). Das Verschieben von Objekten innerhalb der Gesamtstruktur kann beispielsweise dann notwendig werden, wenn Sie eine bestehende Domäne in der Gesamtstruktur auflösen und die Objekte in andere Domänen verschieben möchten. *MOVETREE* bietet die folgenden Parameter (siehe Tabelle 23.13):

Parameter	Beschreibung
/start	Startet den Befehl. Standardmäßig wird vor dem eigentlichen Verschieben ein Test des Befehls durchgeführt. Wollen Sie diesen Test auslassen, starten Sie mit /startnocheck.
/check	Testet den MOVETREE-Befehl, ohne die Objekte wirklich zu verschieben.
/verbose	Schaltet in den ausführlicheren Anzeigemodus.
/s Quellserver	Gibt den vollqualifizierten DNS-Namen des Quellservers an.
/d Zielserver	Gibt den vollqualifizierten DNS-Namen des Zielserver an.
/sdn Name der Quelle	Gibt den definierten Namen (DN) des Objekts an, das von der Quelldomäne verschoben wird. Dabei kann es sich um einen Endknoten, einen Container oder eine Teilstruktur handeln.
/ddn Name des Ziels	Gibt den definierten Namen (DN) des Objekts an, das zur Zieldomäne verschoben wird. Dabei kann es sich um einen Endknoten, einen Container oder eine Teilstruktur handeln.
/u /p	Hier können Sie ein Benutzerkonto in der Form /u [Domäne\]Benutzer /p Kennwort angeben, unter dem der Befehl ausgeführt werden soll.
/continue	Fehlgeschlagene oder angehaltene Operationen werden fortgesetzt.

Tabelle 23.13: Die Parameter für das Programm MOVETREE

Zum besseren Verständnis nehmen wir folgendes Szenario an: Aus der Domäne *firma.de* mit dem Server Hippokrates soll die OU Verwaltung in die Domäne *filiale.de* mit dem Server Sokrates verschoben werden. Der neue Name der OU soll dort Administration lauten. Hierzu verwenden Sie den Befehl

```
movetree /start /s Hippokrates.firma.de /d Sokrates.filiale.de
/sdn OU=Verwaltung,DC=Firma,DC=De
/ddn OU=Administration,DC=Filiale,DC=De 
```

Nach jedem Ausführen von *MOVETREE* werden verschiedene Protokolldateien angelegt. Diese befinden sich im Installationsverzeichnis von *MOVETREE*. Im *MOVETREE.LOG* finden Sie sämtliche statistischen Protokolle der Operation, unter *MOVETREE.ERR* sind alle Fehler der Operation aufgelistet, und in *MOVETREE.CHK* werden potenzielle Fehler angezeigt, die im Testdurchlauf des *MOVETREE*-Befehls erkannt worden sind.



MOVETREE ist zwar in der Lage, Gruppenobjekte von einer Domäne in eine andere zu verschieben. Dies gilt jedoch nicht für globale Gruppen. In diesem Fall müssen die Benutzerobjekte mit **LDIFDE** exportiert und nach Änderung der definierten Namen in die neue Domäne importiert werden (siehe Kapitel 25.2.1).

Das Active Directory Migration Tool (ADMT, siehe Kapitel 27.5) ist zwar das eigentliche Programm, wenn es darum geht, Objekte beim Auflösen von Domänen in andere Domänen zu verschieben. ADMT hat aber seine Grenzen, da mit diesem Tool keine Gruppenrichtlinien-Verknüpfungen verschoben werden. Dies funktioniert nur mit **MOVETREE**. Allerdings bleibt beim Verschieben von Gruppenrichtlinien immer die Verknüpfung mit der OU erhalten. Diese Verknüpfungen verweisen jedoch immer noch auf die ursprüngliche Domäne. Es muss also die alte Domäne immer noch bestehen bleiben, damit den Benutzern die GPOs zugewiesen werden können, selbst wenn die alte Domäne über keinerlei Objekte mehr verfügt. Soll die alte Domäne endgültig gelöscht werden, müssen die Gruppenrichtlinien von Hand migriert oder neu erstellt werden.

23.1.16 NETDIAG

Mit dem Kommandozeilenprogramm **NETDIAG** können Sie 25 verschiedene netzwerk-spezifische Tests durchführen. Treten auf einem Client oder auch unter den Domänencontrollern Verbindungsprobleme auf, so sollten Sie immer erst dieses Programm anwenden. Dieses Programm ist sehr komfortabel zu bedienen, da es mit sehr wenigen Parametern auskommt. Folgende optionale Parameter stehen zur Verfügung (siehe Tabelle 23.14):

Parameter	Beschreibung
/test:Testname	Es können auch nur einzelne der gültigen Tests aufgerufen werden. Die Testnamen sind weiter unten aufgelistet.
/l	Die Ergebnisse werden ins NetDiag.log im Installationsverzeichnis geschrieben.
/q	Quiet-Modus, es werden nur die Fehler ausgegeben.
/v	Ausführlicherer Ausgabemodus.
/debug	Noch ausführlicherer Ausgabemodus als /v.
/fix	Berichtigt automatisch leichte Fehler, die durch NETDIAG aufgedeckt werden.
/d:Domänenname	Findet einen Domänencontroller in der angegebenen Domäne.
/DcAccountEnum	Zählt die Domänencontroller-Computerkonten auf.

Tabelle 23.14: Die Parameter für das Programm **NETDIAG**

Mit NETDIAG können die folgenden Tests ausgeführt werden:

1. Ndis – Abfrage der Netzwerkkarten
2. IpConfig – IP-Konfigurationstest
3. Member – Prüfung der Domänenmitgliedschaft
4. NetBTTransports – NetBT Transport-Test
5. Autonet – Autonet Adresstest
6. IpLoopBk – IP Loopback Ping-Test
7. DefGw – Prüfung des Standard-Gateway
8. NbtNm – NetBT-Namenstest
9. WINS – Test des WINS-Dienstes
10. Winsock – Test von Winsock
11. DNS – DNS-Test
12. Browser – Redir- und Browser-Test
13. DsGetDc – Suchen der Domänencontroller
14. DcList – Auflisten der Domänencontroller
15. Trust – Test der Vertrauensstellungen
16. Kerberos – Kerberos-Test
17. Ldap – LDAPTest
18. Route – Test der Routing-Tabelle
19. Netstat – Test der Netstat-Informationen
20. Bindings – Verbindungstest zwischen Netzwerkadapter und Kommunikationsprotokoll
21. WAN – WAN-Konfigurationstest
22. Modem – Modem-Diagnose
23. Netware – Test der Netware-Konfiguration
24. IPX – IPX-Test
25. IPSec – Test von IPSec

In der Logdatei sehen Sie, sofern nicht der Parameter `/q` gesetzt ist, zu jedem einzelnen Test ein ausführliches Ergebnis und zu einigen Fehlern auch Hinweise zur Lösung des Problems. Die Fehler werden dabei in verschiedene Schwierigkeitsgrade eingeteilt. Leichte Fehler können dabei möglicherweise mit der Option `/fix` behoben werden.

23.1.17 NETDOM

Das Kommandozeilenprogramm *NETDOM* erfüllt wie *MOVETREE* die Aufgabe, Objekte zwischen zwei Domänen zu verschieben. Allerdings wird *NETDOM* nur beim Verschieben von Computern und Mitgliedsservern benutzt. Sie können auch zusätzliche Rechner hinzufügen und entfernen, umbenennen, Passwörter zurücksetzen oder Vertrauensstellungen zwischen zwei Domänen herstellen. *NETDOM* verfügt dazu über die folgenden Untermenüs:

- ▶ NETDOM ADD: Fügt neue Computer und Mitgliedsserver ohne weitere Informationen der Domäne hinzu.
- ▶ NETDOM JOIN: Fügt dem Computer die Informationen hinzu, die er für die Authentifizierung an der Domäne benötigt.
- ▶ NETDOM MOVE: Verschiebt Computerkonten zwischen zwei Domänen.
- ▶ NETDOM QUERY: Fragt Informationen der Domäne ab (vorhandene DCs, OUs usw.).
- ▶ NETDOM REMOVE: Entfernt Computerkonten aus einer Domäne.
- ▶ NETDOM RENAME: Umbenennen von Computerkonten.
- ▶ NETDOM RESET: Führt einen Reset der sicheren Verbindung zwischen dem Domänencontroller und einer Workstation durch.
- ▶ NETDOM RESETPWD: Setzt das Passwort auf dem Computer zurück, auf dem das Programm lokal ausgeführt wird. Eine Remote-Funktion wird nicht angeboten.
- ▶ NETDOM TIME: Überprüft, ob die Zeit zwischen einem Domänencontroller und einer Workstation übereinstimmt, und modifiziert diese bei Bedarf.
- ▶ NETDOM TRUST: Stellt Vertrauensstellungen zwischen zwei Domänen her.
- ▶ NETDOM VERIFY: Überprüft die sichere Verbindung zwischen dem Domänencontroller und einer Workstation.

Eine ausführliche Beschreibung der jeweils gültigen Parameter erhalten Sie, indem Sie NETDOM HELP [Untermenü] aufrufen.

Tabelle 23.15 beschreibt die Parameter, die für den Befehl NETDOM MOVE benutzt werden. Diese gelten im Wesentlichen auch für die Befehle ADD, JOIN und REMOVE.

Parameter	Beschreibung
/D:Domäne	Gibt die Zieldomäne für das zu verschiebende Objekt an.
/OU:OU	Gibt die Ziel-OU an (Format: OU=,DC=,DC=). Wird dieser Parameter nicht gesetzt, werden die Computer im Standardcontainer COMPUTERS angelegt.
/Ud:Benutzer	Das Benutzerkonto für die unter /d angegebene Domäne im Format Domäne\Benutzer. Ist kein Konto angegeben, wird das aktuelle Konto benutzt.
/Pd:Passwort	Das Passwort für das Benutzerkonto unter /Ud. Geben Sie "*" an, werden Sie zur Eingabe des Passworts aufgefordert.
/Uo:Benutzer	Das Benutzerkonto, das für die Verbindung mit dem Objekt benutzt werden soll. Ist kein Konto angegeben, wird das aktuelle Konto benutzt.
/Po:Passwort	Das Passwort für das Benutzerkonto unter /Uo. Geben Sie "*" an, werden Sie zur Eingabe des Passworts aufgefordert.
/Reboot:Sekunden	Der zu verschiebende Computer wird heruntergefahren und nach der angegebenen Anzahl von Sekunden wieder neu gestartet.

Tabelle 23.15: Die Parameter für das Programm NETDOM

Wollen Sie also den Computer Archimedes in die OU-Verwaltung der Domäne *filiale.de* verschieben, so benutzen Sie den folgenden Befehl:

```
NETDOM MOVE /d:Filiale.de Archimedes  
/OU:OU=Verwaltung,DC=Filiale,DC=De  
/Ud:Administrator\Filiale /Pd:Kennwort 
```

Lassen Sie den Parameter /OU: weg, so wird der Rechner im Standardverzeichnis COMPUTERS angelegt. Mit dem Befehl NETDOM ADD und denselben Parametern wird das Computerkonto in der Domäne angelegt, mit NETDOM JOIN wird er der Domäne hinzugefügt, sodass eine Anmeldung von diesem Computer aus erfolgen kann.

Beim Verschieben von Computern sind allerdings einige Punkte zu bedenken, denn es können keine Computer in eine neue Domäne verschoben werden, die als Betriebssystem Windows NT 4.0 oder früher besitzen. Die eben beschriebenen Verfahren greifen nur für Windows 2000- und XP-Maschinen. Beim Verschieben wird das Computerkonto in der alten Domäne jedoch nicht gelöscht. Das Konto wird dort nur deaktiviert, sofern die Quelldomäne eine Windows 2000- oder 2003-Domäne ist.

Das Verschieben von Domänencontrollern ist nur zwischen verschiedenen Standorten innerhalb derselben Domäne möglich. Allerdings müssen Sie hierfür nicht *NETDOM* anwenden, sondern Sie verschieben die Domänencontroller über die mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE. Weitere Hinweise dazu finden Sie in Kapitel 14.1.4.

Wollen Sie einen Domänencontroller jedoch in eine andere Domäne verschieben, so erfordert dies eine gründliche Planung. Zuerst müssen Sie überprüfen, welche Rollen der Domänencontroller zusätzlich erfüllt. Agiert er als DNS- oder DHCP-Server, ist er als File- oder Print-Server konfiguriert? In diesem Fall müssen Sie ihm zuerst diese Aufgaben abnehmen und an andere Server übergeben. Erfüllt er schließlich nur noch die Rolle des Domänencontrollers, so können Sie ihn mit DCPROMO zum Mitgliedsserver herabstufen. Dieser Mitgliedsserver wird wie oben beschrieben über *NETDOM MOVE* in eine andere Domäne verschoben. Starten Sie dort wieder DCPROMO, um den Mitgliedsserver wieder zum Domänencontroller heraufzustufen. Bedenken Sie dabei, dass der Prozess des Herunter- und Heraufstufens unter Umständen längere Zeit in Anspruch nehmen kann. Dies hängt davon ab, wie viele Objekte sich im Active Directory befinden. Verlegen Sie diese Prozesse deshalb idealerweise auf die Nachtstunden oder ein Wochenende.

In Kapitel 23.2.1, Schritt 8, erfahren Sie, wie unter Windows Server 2003 Domänencontroller über *NETDOM* umbenannt werden können.

23.1.18 NTDSUTIL

NTDSUTIL ist ein Kommandozeilenprogramm zur Pflege und Fehlersuche im Active Directory. Das Programm befindet sich in %SYSTEMROOT%\SYSTEM32. Es besitzt eine sehr große Anzahl an Befehlen. *NTDSUTIL* verfügt über elf verschiedene Menüs mit jeweils speziellen Unterbefehlen. Diese können Sie beim Start mit dem Parameter *help* oder ? aufrufen.

Menü	Funktion
Authoritative restore	Befehle zur autorisierenden Wiederherstellung der Active Directory-Datenbank.
Domain management	Bietet eine Anzahl von domänenbezogenen Befehlen, z.B. das Erstellen neuer Domänen.
Files	Managt die Dateien der Active Directory-Datenbank.
IP deny list	Konfigurieren einer Liste von IP-Adressen, von denen der Domänencontroller LDAP-Informationen zu empfangen akzeptiert.
LDAP policies	Managen der LDAP-Berechtigungen im Active Directory.
Metadata cleanup	Durchführen von Lösch- und Aufräumprozessen im Active Directory, z.B. bereinigen von ungültigen Servern.
Popups	Automatisierung von <i>NTDSUTIL</i> . <i>POPUPS ON/OFF</i> wird (de)aktiviert. Weitere Hinweise dazu siehe Abschnitt Automatisierung.
Roles	Managen der Betriebsmaster (FSMO) in der Domäne.
Security Account Management	Hier sind die Tools für das SID-Management zu erreichen.
Semantic Database Analysis	Besitzt verschiedene Optionen zur Datenbankanalyse
Set DSRM Password	Setzt das Administrator-Passwort für die Verzeichnisdienst-Wiederherstellung zurück. Diese Option ist lediglich unter Windows Server 2003 verfügbar.

Tabelle 23.16: Die Menüs des Programms *NTDSUTIL*

Jedes dieser Menüs kann mit `quit` beendet werden. *NTDSUTIL* kann unabhängig davon ausgeführt werden, ob der Domänencontroller online oder offline geschaltet ist. Am häufigsten werden die Befehle der Menüs Roles, Metadata cleanup, IP deny list, Files und Authoritative restore benutzt.

Roles

Über dieses Menü können Sie die Rollen der Betriebsmaster (FSMO) bearbeiten.

- ▶ `Abandon all roles` zwingt den Domänencontroller, mit dem Sie verbunden sind, alle Betriebsmasterrollen aufzugeben, die er innehat. Stellen Sie jedoch sicher, dass ein anderer Domänencontroller diese Rolle übernehmen kann.
- ▶ `Seize` zwingt den Domänencontroller, eine neue Betriebsmasterrolle zu übernehmen. Die neue der fünf Rollen ist hinter `seize` anzugeben. Der Domänencontroller, der bisher diese Rolle innehatte, wird über den Wechsel nicht informiert.
- ▶ `Transfer`: Auch hierbei übernimmt der Domänencontroller eine neue anzugebende Betriebsmasterrolle. Allerdings wird der Domänencontroller, der bisher die Rolle innehatte, über den Wechsel informiert.

Metadata cleanup

Mit diesem Menü können nicht mehr benötigte Informationen aus dem Active Directory entfernt werden.

- ▶ **Remove selected domain** entfernt die Domäne, die gerade im Menü **Select Operation Target** gewählt ist. Siehe dazu den Abschnitt „Weitere Befehle“ weiter unten. Gehen Sie mit diesem Befehl vorsichtig um. Verwenden Sie ihn, um verwaiste Domänen zu entfernen, deren letzter Domänencontroller nicht korrekt entfernt werden konnte.
- ▶ **Remove selected server** entfernt einen Server, der im Menü **Select Operation Target** gewählt ist. Es ist sinnvoll, hierüber Server zu entfernen, die nicht wieder in Betrieb genommen werden sollen.

IP deny list

Über IP deny list wird verhindert, dass LDAP-Informationen von den in der Liste angegebenen IP-Adressen empfangen werden. Es kann somit speziellen Servern verboten werden, die Active Directory-Informationen abzufragen oder zu verändern.

- ▶ **Add IP-Adresse Subnetz** fügt einen Satz von IP-Adressen zur Liste hinzu.
- ▶ **Add IP-Adresse NODE** fügt eine einzelne bestimmte Adresse hinzu.
- ▶ **Show** zeigt die Liste der bisherigen Einträge.
- ▶ **Commit** speichert die aktualisierte Liste im Active Directory.
- ▶ **Test IP-Adresse** überprüft basierend auf den Einträgen der Deny-Liste, ob sich die angegebene Adresse verbinden darf oder nicht.

Files

Über dieses Menü können Sie direkt mit den Dateien der Datenbank arbeiten. Wichtig sind die folgenden Befehle:

- ▶ **Integrity** unterzieht die Dateien einem grundsätzlichen Integritäts-Check. Wurden dabei interne Fehler in den Dateien festgestellt, werden entsprechende Meldungen ausgegeben.
- ▶ **Repair** führt Reparaturen an den Datenbankdateien aus. Dabei werden jedoch nur interne Fehler korrigiert.
- ▶ **Compact to Pfad** packt die Dateien in den angegebenen Pfad komprimiert zusammen. Es handelt sich um den in Kapitel 21.8.2 beschriebenen Vorgang der Offline-Defragmentierung. Die komprimierten Dateien müssen manuell über die ursprünglichen Datenbankdateien kopiert werden, um diese zu ersetzen.
- ▶ **Move DB to Pfad** verschiebt die komplette Datenbank in den angegebenen Pfad. Dies kann sinnvoll sein, wenn Sie dem Domänencontroller eine größere Festplatte eingebaut haben, auf der auch die Datenbank liegen soll.
- ▶ **Move Logs to Pfad** verschiebt die Active Directory-Logdateien in den angegebenen Pfad. Wenn die Datenbank und die Logdateien auf zwei physikalisch unterschiedlichen Laufwerken abgelegt sind, verbessert dieses die Performance deutlich.

Authoritative restore

Diesen Befehl haben Sie bereits im Zusammenhang mit der autorisierenden Wiederherstellung der Active Directory-Datenbank in Kapitel 21.7.2 Kennen gelernt. Diese Wiederherstellung kann nur durchgeführt werden, wenn der Domänencontroller offline geschaltet ist. Es wird zwischen den Befehlen **restore databases** und **restore subtree**

Namenskontext unterschieden. Beim ersten Befehl wird der gesamte Inhalt der Datenbank als autorisierend gekennzeichnet. Beim zweiten Befehl wird nur der unter Namenskontext angegebene Zweig auf den anderen Domänencontrollern überschrieben. Das Format dieses Befehls lautet:

```
restore subtree OU=Finanzen,DC=Firma,DC=de ↵
```

Alle anderen Bereiche der Datenbank werden von den übrigen Domänencontrollern auf diesem überschrieben.

Automatisierung

Die umfangreiche Befehlssammlung von *NTDSUTIL* kann auch automatisiert werden. Bei zahlreichen Befehlen werden Sie aufgefordert, Ihre Eingabe zu bestätigen. Diese Sicherheitsabfragen sind zwar nützlich, um möglicherweise irreparablen Fehlern vorzubeugen. Sie sind aber eher hinderlich, wenn Sie *NTDSUTIL* interaktiv, beispielsweise über eine Batchdatei, ausführen möchten. Um die Sicherheitsabfragen zu umgehen, arbeiten Sie mit dem Befehl `popups`. Mit `popups off` deaktivieren Sie die Sicherheitsabfragen, mit `popups on` werden sie wieder aktiviert. Sie können nun eine Reihe von Befehlen nacheinander abarbeiten, indem Sie Folgendes eingeben: `NTDSUTIL popups off <Befehle> quit`.

Weitere Befehle

Die Menüs Domain Management, IP Deny List, LDAP Policies, Metadata Cleanup sowie Roles besitzen ein Untermenü *Connections*. Die Untermenüs können aufgerufen werden, indem Sie das Menü mit dem Parameter `help` oder `?` eingeben. Jedes *Connections*-Untermenü unterstützt die folgenden Befehle (siehe Tabelle 23.17):

Befehl	Beschreibung
<code>Clear creds</code>	Löscht alle bestehenden Verbindungen und das unter <code>set creds</code> angegebene Konto
<code>Connect to domain</code>	Geben Sie den DNS-Namen der Domäne an. Es wird eine Verbindung zu einem Domänencontroller dieser Domäne aufgebaut.
<code>Connect to server</code>	Geben Sie den Namen oder die IP-Adresse an, um sich mit einem speziellen Server zu verbinden.
<code>Help</code>	Gibt genauso wie <code>?</code> die Hilfeinformationen an.
<code>Info</code>	Gibt den Verbindungsstatus von <i>NTDSUTIL</i> zu anderen Servern an sowie das Konto, unter dem die Befehle ausgeführt werden.
<code>Quit</code>	Beendet das aktuelle Menü und kehrt zum übergeordneten zurück.
<code>Set creds x y z</code>	Geben Sie hier anstelle der Variablen den Namen der Domäne, des Benutzers und des Kennworts an, um sich unter diesem Konto <i>NTDSUTIL</i> anzumelden. Ansonsten wird das Konto benutzt, unter dem Sie gerade angemeldet sind.

Tabelle 23.17: Die Befehle für das *NTDSUTIL*-Untermenü *Connections*

Die Menüs Domain Management, Metadata Cleanup sowie Roles bieten zusätzlich das Untermenü *SELECT OPERATIONS TARGET*. In diesem Menü werden über die *Select*-Befehle

wie `select domain` oder `select server` die Ziele gewählt, an denen eine bestimmte Operation durchgeführt werden soll. Zuvor ist der entsprechende `List`-Befehl durchzuführen, um die zur Verfügung stehenden Domänen oder Server aufzulisten, die mit `select` als Ziel gewählt werden können. Beispielsweise gibt der Befehl `list servers in site`  eine Liste aller Server des Standorts aus. Wollen Sie den Server als Ziel auswählen, der an zweiter Stelle der Liste steht, so geben Sie zur Auswahl den Befehl `select server 2`  an.

23.1.19 PERMS

PERMS ist ein Kommandozeilenprogramm, mit dem Sie die Berechtigungen eines Benutzers für eine Datei oder ein Verzeichnis anzeigen können. Dabei wird der ACE der Datei oder des Ordners abgefragt. Um **PERMS** korrekt ausführen zu können, müssen Sie über Administratorrechte für den Computer verfügen, auf dem das Benutzerkonto definiert ist und über die Berechtigung zum Backup von Dateien und Ordnern für den Computer, auf dem sich die Datei befindet. Ansonsten erhalten Sie die Fehlermeldung Zugriff verweigert. **PERMS** verwendet die folgenden Parameter (siehe Tabelle 23.18):

Parameter	Beschreibung
[Domäne\Computer\ Benutzer	Name des Benutzers, dessen Berechtigungen angezeigt werden sollen.
Pfad	Pfad zur Datei oder zum Ordner. Dabei sind Wildcards (*) und (?) gestattet.
/i	Nimmt eine interaktive Anmeldung des Benutzers am Computer mit der gewünschten Datei an. Dabei wird der Benutzer als zur Gruppe Interaktiv gehörig gekennzeichnet.
/s	Überprüft auch die Berechtigungen in den Unterverzeichnissen.

Tabelle 23.18: Die Parameter für das Programm **PERMS**

Als Ausgabe erhalten Sie die folgenden Abkürzungen, die für diese Berechtigungen stehen:

R = Lesen

W = Schreiben

X = Ausführen

D = Löschen

P = Ändern von Berechtigungen

O = Übernahme des Besitzes

A = Vollzugriff

- = Kein Zugriff

* = Der Benutzer ist Eigentümer der Datei oder des Ordners.

= Die Gruppe, in der der Benutzer Mitglied ist, ist Eigentümer der Datei oder des Ordners.

? = Die Berechtigungen können nicht bestimmt werden.

23.1.20 REPADMIN

REPADMIN ist ein Kommandozeilenprogramm, das Sie zur Analyse und Behebung von Replikationsproblemen einsetzen können. So kann beispielsweise der Replikationsstatus eines Domänencontrollers überprüft werden. Weiterhin kann die Replikation zwischen zwei Replikationspartnern erzwungen werden. Ferner können die Metadaten der Replikation sowie der Up-to-Dateness-Vektor (siehe Kapitel 17.1.1) angezeigt werden. Auch für ein einzelnes Objekt kann ermittelt werden, ob dieses auf dem aktuellen Stand ist. In den folgenden Abschnitten werden die wichtigsten Funktionen von *REPADMIN* je anhand eines Beispiels vorgestellt.

Erzwingen der Replikation

Um die Replikation eines Domänencontrollers mit einem bestimmten Replikationspartner zu erzwingen, verwenden Sie folgenden Befehl: `repadmin /sync <NC> <Servername> <ObjektGUID>` . Unter NC geben Sie den Namensraum und den Namen des Servers an. Die Objekt-GUID ist die GUID des gewünschten Replikationspartners, z.B.: `repadmin /sync dc=firma,dc=de Hippokrates a36b7d84-65cc-367e-a7b4-210b33c7bac5` 

Die GUID der Replikationspartner lässt sich über `repadmin /showreps`  anzeigen.

Wollen Sie die Replikation mit allen Partnern erzwingen, so verwenden Sie den Befehl `repadmin /syncall <Servername> <NC>` , wobei der Namensraum in Anführungszeichen gesetzt werden muss, also z.B.:

`repadmin /syncall Hippokrates "dc=firma,dc=de"` 

Überprüfen der Replikation

Zum Überprüfen der Replikation gehören Angaben über die Replikationspartner sowie den Zeitpunkt der letzten Replikation. Über `repadmin /showreps`  werden die Replikationspartner, deren GUID sowie der Zeitpunkt der letzten Replikation ausgegeben. Bei der Replikation wird zusätzlich angegeben, ob diese erfolgreich durchgeführt werden konnte oder nicht.

Anzeige der Replikationsmetadaten

Mit *REPADMIN* können Sie die Metadaten der Replikation für jedes Objekt anzeigen. Dabei ist der komplette Namensraum (in Anführungszeichen gesetzt) sowie der Server anzugeben, von dem die Informationen bezogen werden sollen. Der Befehl `repadmin /showmeta "cn=administrator,cn=users,dc=filiale,dc=de"`  liefert für jedes Attribut des Objekts die folgenden Informationen: Die locating USN, den originating DSA, die originating USN, den Zeitstempel sowie die Version. Die Ausgabe sollte an eine Datei umgeleitet werden, da ansonsten ein Teil der Informationen abgeschnitten wird (siehe Abbildung 23.10).

23.1.21 REPLMON

REPLMON erfüllt wie *REPADMIN* den Zweck, die Replikation zu überwachen und Probleme zu beheben. Allerdings bietet *REPLMON* hierzu eine grafische Oberfläche. Der Schwerpunkt für die Darstellung der Replikation liegt bei *REPLMON* mehr bei den Standorten als bei den Domänen. Insgesamt gesehen können Sie mit *REPLMON* dieselben Aufgaben durchführen wie mit *REPADMIN*, nur eben über eine GUI anstatt über die Kommandozeile. Hier bleibt es dem Geschmack des Administrators überlassen, für welches Tool er sich entscheidet.

Beim Start von *REPLMON* erhalten Sie eine leere mmc. Sie müssen zunächst die zu überwachenden Server auswählen. Wählen Sie dazu aus dem Kontextmenü von MONITORED SERVERS den Eintrag ADD MONITORED SERVER. Ein Assistent ist Ihnen bei der Serverwahl behilflich. Sie erhalten danach folgendes Fenster (siehe Abbildung 23.11):



Abbildung 23.11: Die mmc des Programms *REPLMON*

Über das Kontextmenü des Servereintrags können Sie sämtliche serverbezogenen Aufgaben durchführen, z.B.:

- ▶ Überprüfen der Replikationstopologie
- ▶ Synchronisation jeder Verzeichnispartition mit allen anderen Servern
- ▶ Anzeige der Domänencontroller, der globalen Katalogserver und Bridgehead-Server, der Replikationstopologie, der Vertrauensstellungen sowie der Metadaten der Objekte.

Für jede der Verzeichnispartitionen können Sie einzeln eine Synchronisation mit den übrigen Servern durchführen. Sie können auch die Änderungsbenachrichtigungen an die Replikationspartner für jede Verzeichnispartition aufrufen. Diese beiden Vorgänge werden über das Kontextmenü der gewünschten Partition aufgerufen.

Eine sehr nützliche Funktion besteht darin, sich die Replikationstopologie grafisch aufbereitet anzeigen zu lassen. Wählen Sie hierzu aus dem Kontextmenü des Servers den Eintrag **SHOW REPLICATION TOPOLOGY**. Wählen Sie dort aus dem Menü **VIEW** den Eintrag **CONNECTION OBJECT ONLY**. Über die Eigenschaften des dargestellten Serverobjekts können Sie die Replikationstopologie des Standorts (**SHOW INTRA-SITE CONNECTIONS**) oder die Verknüpfungen zwischen den Standorten (**SHOW INTER-SITE CONNECTIONS**) anzeigen.

23.1.22 SDCHECK

SDCHECK (Security Descriptor Check) ist ein Kommandozeilenprogramm, mit dem die Sicherheitsbeschreiber auf LDAP-Ebene für ein Objekt angezeigt werden können. In einem Sicherheitsbeschreiber sind für jedes Objekt die Sicherheitsinformationen enthalten. Dazu zählen die SIDs, die DACLs und SACLs (siehe Kapitel 19.1) sowie eine Reihe von sicherheitsrelevanten Flags für das Objekt. Für **SDCHECK** wird die folgende Syntax benutzt: **SDCHECK** Servername Objektname [Parameter]. Dabei stehen folgende Parameter bereit (siehe Tabelle 23.19):

Parameter	Beschreibung
-dumpSD	Zeigt den Inhalt aller ACEs des ersten Sicherheitsbeschreibers an.
-dumpAll	Zeigt den Inhalt aller ACEs aller Sicherheitsbeschreiber an.
-debug	Zeigt eine ausführlichere Ausgabe an.
-domain:Domänenname -user:Benutzername -pwd:Passwort	Diese Parameter werden benutzt, um sich unter einem anderen Benutzerkontext anzumelden.

Tabelle 23.19: Die Parameter für das Programm **SDCHECK**

Für jedes Objekt werden sämtliche ACEs (Access Control Entries, siehe Kapitel 19.1) aufgelistet. Für jeden ACE erhalten Sie tiefgehende Informationen auf LDAP-Ebene wie Größe, Typ, gesetzte Flags, ACE-Mask sowie die zugehörige SID und Besitzer des Objekts. Dieses Programm wird Ihnen sehr nützlich sein, wenn Sie mit dem Aufbau von ACEs vertraut geworden sind. Der Aufbau von ACEs wird ausführlich im Zusammenhang mit ADSI-Skripten in Kapitel 32.3.1 vorgestellt.

Der Befehl `sdcheck sokrates.filiale.de cn=administrator,cn=Users,dc=filiale,dc=de /dumpSD`  bringt folgendes Ergebnis (siehe Abbildung 23.12):

```

sdccheck.exe - Editor
Date: 09/02/2002 11:05:52
Format: ?

*** warning: No values returned for dScorePropagationData on CN=Administrator,CN=Users,DC=Filiale,DC=de
*** warning: No values returned for dScorePropagationData on CN=Users,DC=Filiale,DC=de
*** warning: No values returned for dScorePropagationData on DC=Filiale,DC=de

object: CN=Administrator,CN=Users,DC=Filiale,DC=de
Classes: top person organizationalPerson user
SD: 632 bytes
Metadata: 09/02/2002 11:05:52 @ sokrates.filiale.de ver: 2

object: CN=Users,DC=Filiale,DC=de
Classes: top container
SD: 792 bytes
Metadata: 09/02/2002 10:43:24 @ sokrates.filiale.de ver: 1

object: DC=Filiale,DC=de
Classes: top domain domainNS
SD: 932 bytes
Metadata: 09/02/2002 10:43:36 @ sokrates.filiale.de ver: 2

Checking ACL inheritance ...
Parent: 2 - DC=Filiale,DC=de
Child: 1 - CN=Users,DC=Filiale,DC=de

Checking ACL inheritance ...
Parent: 1 - CN=Users,DC=Filiale,DC=de
Child: 0 - CN=Administrator,CN=Users,DC=Filiale,DC=de

SD for CN=Administrator,CN=Users,DC=Filiale,DC=de
SD Revision: 1
SD Control: 0x9C14
SE_DACL_PRESENT
SE_SACL_PRESENT
SE_DACL_AUTO_INHERITED
SE_SACL_AUTO_INHERITED
SE_DACL_PROTECTED
SE_SELF_RELATIVE
Owner: FILIALE\domänen-admins S-1-5-21-1229272821-813497703-1060284298-532
Group: FILIALE\domänen-admins S-1-5-21-1229272821-813497703-1060284298-532
DACL:
Revision: 4
Size: 528 bytes
# Aces: 32
Ace[0]:
Ace Type: 0x0 - ACCESS_ALLOWED_ACE_TYPE
Ace Size: 20 bytes
Ace Flags: 0x0
Ace Mask: 0x00020094
READ_CONTROL
ACTRL_DS_LIST
ACTRL_DS_READ_PROP
ACTRL_DS_LIST_OBJECT
Ace Sids: NT-AUTORITÄT\authentifizierte Benutzer S-1-5-21
Ace[1]:
Ace Type: 0x0 - ACCESS_ALLOWED_ACE_TYPE

```

Abbildung 23.12: Die Ausgabedatei des Programms SDCHECK

23.1.23 User State Migration Tool

Mit diesem Kommandozeilenprogramm können Sie für Benutzer den Status persönlicher Einstellungen sichern und diese Sicherung nach der Migration auf Windows 2000 wieder einstellen. Sie benötigen dieses Programm lediglich bei einer Migration von Windows 9x/NT auf Windows 2000/XP, nicht jedoch bei einem Update. User State Migration Tool besteht aus der *ScanState.exe*, der *LoadState.exe* sowie den inf-Dateien *Applet.inf*, *Sysfiles.inf* und *Usermig.inf*.

Vor der Installation von Windows 2000/XP wird mithilfe der *ScanState.exe* ein Scan durchgeführt. Dieser Scan erstreckt sich auf die folgenden Einstellungen:

- ▶ Ordneroptionen
- ▶ Netzlaufwerke und Netzwerkdrucker

- Anzeigeeinstellungen
- Einstellungen des Internet Explorers 4.x und 5.x
- Einstellungen der RAS- und Wählverbindungen
- Verbindungseinstellungen von Outlook ab der Version 97
- Dateien aus dem Ordner EIGENE DATEIEN

Zusätzlich zu diesen Informationen können Sie weitere Informationen sichern, indem Sie die drei .inf-Dateien der Migration Rule modifizieren. Hier können Dateien, Ordner und Registry-Schlüssel hinzugefügt oder ausgeschlossen werden. Eine Anleitung dazu finden Sie in der Sektion Migration Rule-Syntax der Datei *usmt_d.htm* im Installationsverzeichnis des Programms.

Nach der Neuinstallation von Windows 2000/XP wird die Datei *LoadState.exe* ausgeführt. Diese spielt die gemäß der inf-Dateien gesicherten Einstellungen zurück.

Das User State Migration Tool ist jedoch *nicht* in der Lage, die folgenden Aufgaben durchzuführen:

- Migration vorhandener Treiber, dlls oder anderer ausführbarer Dateien.
- Migration kompletter Applikationen. Diese müssen neu installiert werden. Nur das Einspielen der benutzerdefinierten Einstellungen ist möglich.
- Es können nur Informationen für Computer eines Microsoft-Netzwerkes gesichert werden.

Für die Ermittlung der Benutzerinformationen wird die *ScanState.exe* ausgeführt. Diese Datei unterstützt die folgenden Parameter (siehe Tabelle 23.20):

Parameter	Beschreibung
Migrationspfad	Gibt den Verzeichnispfad an, in dem die Benutzereinstellungen temporär gespeichert werden sollen. Dieses Verzeichnis muss bereits existieren, es wird nicht neu erstellt.
/i	Gibt den Namen der inf-Datei an. Sollen mehrere inf-Dateien verwendet werden, muss /i vor jeden Dateinamen gesetzt werden. Befindet sich die inf-Datei im selben Verzeichnis wie die <i>scanstate.exe</i> , so müssen Sie .\ dem Dateinamen voranstellen. Befinden sich die Dateien in einem anderen Verzeichnis, ist der komplette Pfad anzugeben.
/l	Optional kann eine Logdatei angegeben werden, in die Fehlermeldungen geschrieben werden. Dieser Parameter muss in diesem Fall vor alle anderen außer /i gesetzt werden.
/v 1-7	Schaltet in den ausführlichen Modus. Der Wert zwischen 1 bis 7 legt die Ausführlichkeit fest. 7 bietet die meisten Informationen.
/c	Erzwingt die weitere Durchführung, auch wenn ein Fehler (fehlende Datei oder zu langer Dateiname) auftritt.

Tabelle 23.20: Die Parameter für die Datei *ScanState.exe* des User State Migration Tool

Allein zum Troubleshooting, nicht aber zur Durchführung eines normalen Scan-Prozesses dienen die Parameter /u und /f. Mit /u werden nur Benutzereinstellungen migriert, mit /f lediglich Dateien.

Um den gesicherten Zustand wieder einzuspielen, wird die Datei LoadState.exe benutzt. Hierbei werden dieselben Parameter verwendet wie bei ScanState.exe. Lediglich der Migrationspfad gibt hier den Zielpfad auf dem Client an, in den die gespeicherten Einstellungen geschrieben werden sollen.

23.1.24 ADCheck (NetIQ)

Das Support-Tool *ADCheck* gehört zwar nicht zu den Windows-Support-Tools, sondern ist von der Firma NetIQ entwickelt worden und kann unter folgender Adresse kostenlos heruntergeladen werden:

<http://www.netiq.com/adcheck/default.asp>

Dieses kompakte Tool führt verschiedene Tests durch und gibt die Ergebnisse in einer html-Datei aus. Diese Tests liefern zwar bei weitem nicht so tiefgehende Ergebnisse wie einige der Windows-Support-Tools, ermöglichen aber dank der leichten Handhabung schnelle Ergebnisse. Die mit ADCheck aufgespürten Probleme können so mit einem anderen Tool behoben werden. Besonders interessant ist dieses Tool für Helpdesk-Mitarbeiter, die bei Active Directory-Problemen einen Hinweis und somit eine Eingrenzung des Problems erhalten, ohne dafür tiefgehendes Hintergrundwissen besitzen zu müssen. Die Ergebnisse werden in eine html-Datei geschrieben, die vom Helpdesk an den Administrator weitergereicht werden kann.

ADCheck ist in der Bedienung selbsterklärend. Die folgenden fünf Tests können für einen Domänencontroller durchgeführt werden:

1. Verbindungstest zum Domänencontroller
2. Anzeige der Betriebsmasterrollen
3. Anzeigen aller Domänencontroller der Domäne
4. Test der Replikation
5. Statusanzeige des Domänencontrollers

Für jeden Test wird eine kurze Zusammenfassung im unteren Fenster ausgegeben (siehe Abbildung 23.13). Die detaillierten Informationen erhalten Sie, indem Sie auf die Schaltfläche DETAILS klicken. Sie erhalten dann eine html-Seite, auf der erläutert wird, welche Tests durchgeführt und ob diese erfolgreich ausgeführt wurden. Sind Probleme ermittelt worden, erhalten Sie einige Hinweise zu deren Behebung.



Abbildung 23.13: ADCheck der Firma NetIQ

23.2 Neue Support-Tools für das Windows 2003 Active Directory

Dieses Kapitel beschäftigt sich mit den Support-Tools, die erstmals für das Windows Server 2003 Active Directory ausgeliefert werden. Alle in Kapitel 10.2 vorgestellten Support-Tools können gleichermaßen unter Windows 2000 und Windows Server 2003 angewendet werden.



Alle in diesem Kapitel beschriebenen Programme sind für das Active Directory unter Windows Server 2003 entwickelt worden. Verwenden Sie diese Programme nicht unter Windows 2000. Die Verwendung unter Windows 2000 kann zu großen unvorhergesehenen Problemen führen.

23.2.1 RENDOM für Windows Server 2003

Das Programm *RENDOM* ist in der Betaphase des Windows Server 2003 als *DOMAIN-RENAME* bezeichnet worden und kursiert teilweise auch noch unter diesem Namen. Der offizielle Name lautet jetzt aber *RENDOM*. Wie es der Name bereits ahnen lässt, lassen sich mithilfe des Kommandozeilenprogramms *RENDOM* sowohl der DNS- als auch

der NetBIOS-Name einer oder mehrerer Domänen in der Gesamtstruktur ändern. Dies war unter Windows 2000 nicht ohne weiteres möglich oder besser gesagt nur auf Umwegen, solange sich die Domäne noch im gemischten Modus befand. Arbeitete die Windows 2000-Domäne bereits im nativen Modus, so gab es keine Chance mehr, die Domäne umzubenennen. Im gemischten Modus musste zunächst ein Windows NT-Server als BDC integriert werden, um auf diesen die Datenbankinhalte zu replizieren. Danach wurden die bestehenden Windows 2000-Domänencontroller zu Mitgliedsservern herabgestuft. Der NT-BDC wurde über den Server-Manager zum PDC heraufgestuft. Danach wurde dieser auf Windows 2000 aktualisiert und erhielt während der Active Directory-Installation den gewünschten Namen. Die Mitgliedsserver konnten nun wieder zu Domänencontrollern heraufgestuft werden. Eine ausführliche Beschreibung des erforderlichen Verfahrens finden Sie in Kapitel 21.11.3.

RENDOM ermöglicht zum einen das Umbenennen von Domänen, zum anderen auch das Erstellen einer neuen Domänenstruktur durch Umstrukturieren der vorhandenen Domänen. Die simpelste Methode besteht darin, eine Domäne von *firma.de* in *neue-firma.de* umzubenennen. Dabei können auch alle untergeordneten Domänen diese Namensänderung übernehmen. Sie können aber auch untergeordnete Domänen wie *vertrieb.firma.de* und *marketing.firma.de* zu neuen Stammdomänen werden lassen, indem Sie diese in *marketing.de* und *vertrieb.de* umbenennen. So entsteht eine neue Struktur.

Mit *RENDOM* wird das Umbenennen und /oder Umstrukturieren in mehreren Schritten durchgeführt. Zunächst wird eine Liste aller Domänen in der Gesamtstruktur erstellt. In dieser Liste legen Sie die Namensänderungen und Umstrukturierungen fest. Danach wird ein Skript generiert, das die erforderlichen Änderungsinformationen für die gewünschten Domänen enthält. Danach wird mit *RENDOM* überprüft, ob in allen Domänen die Voraussetzungen zum Umbenennen erfüllt sind. Abschließend wird das Skript für den eigentlichen Prozess auf jedem Domänencontroller ausgeführt.

Parallel zu allen Schritten, die Sie an der Kommandozeile ausführen, wird das State File generiert. Das State File ist eine XML-Datei, die zunächst nur eine Liste mit allen Domänencontrollern der Gesamtstruktur enthält. Mit jedem Schritt, den Sie über *RENDOM* ausführen, wird das State File dynamisch aktualisiert. So wird nach jedem Schritt der aktuelle Status im Gesamtprozess der Umbenennung der Domänencontroller aufgezeichnet.

Vorbereitungen

Damit das Umbenennen oder Umstrukturieren der Domänen ordnungsgemäß durchgeführt werden kann, müssen die folgenden Punkte erfüllt sein:

- ▶ *RENDOM* kann nur in einem Active Directory ausgeführt werden, in dem der Gesamtstrukturfunktionsmodus Windows Server 2003 ausgeführt wird (siehe Kapitel 10.1.5).
- ▶ Richten Sie DNS-Zonen für die neuen Domänen ein. Für jede neu zu erstellende Domäne richten Sie eine Forward-Lookup-Zone ein und konfigurieren diese für dynamische DNS-Updates (DDNS). Weitere Hinweise dazu finden Sie in Kapitel 16.
- ▶ Verwenden Sie domänenbasierte Ordnerumleitungen, so müssen die DFS-Freigaben als serverbasierte oder allein stehende Freigaben konfiguriert werden. Andernfalls

werden diese Freigaben aufgrund des ungültigen Domänennamens nicht mehr erreichbar sein. Serverbasierte Freigaben können über die entsprechende Gruppenrichtlinie konfiguriert werden. Dasselbe gilt für Benutzerprofile und Home-Shares, deren Verzeichnispfad an den Domänennamen gebunden ist.

- Bezüglich des DNS-Suffixes der Client-Computer brauchen Sie keine Änderungen vorzunehmen, solange die Standardeinstellungen für Windows 2000-/XP-Clients nicht geändert worden sind. Standardmäßig ändert sich das DNS-Suffix automatisch, wenn der Client einer neuen Domäne beitrifft. In der Gruppenrichtlinie sollte den Computern kein spezielles DNS-Suffix zugewiesen worden sein. Bei Domänencontrollern wird das DNS-Suffix nicht automatisch aktualisiert. Dieses muss nach der Namensänderung der Domäne manuell geändert werden. Allerdings müssen Sie bedenken, dass bei den Standardeinstellungen das Suffix automatisch geändert wird, sobald die Client-Computer einen Neustart durchführen. Dies kann zu großer Netzwerkaktivität führen, da diese neuen Informationen nicht nur repliziert werden, sondern die Clients auch im DNS den Host (A)-Eintrag sowie den Zeiger (PTR)-Eintrag aktualisieren.

Dieser erhöhte Netzwerkverkehr muss nicht zwangsläufig zu Problemen führen. Dennoch können Sie vorbeugen, indem Sie über die Gruppenrichtlinien ein neues DNS-Suffix zuweisen, bevor die eigentliche Umbenennung der Domäne erfolgt. So verfügen die Clients zum Zeitpunkt der Umbenennung bereits über das neue DNS-Suffix. Diese Richtlinie kann nach und nach auf alle Clients angewendet werden. Allerdings müssen Sie dafür sorgen, dass das neue DNS-Suffix auch als gültig anerkannt wird. Standardmäßig muss das DNS-Suffix mit dem Namen der Domäne übereinstimmen. Hierzu öffnen Sie z.B. mit *ADSIEDIT* im Objekt *domainDns* das Attribut *msDS-AllowedDNSSuffixes* und fügen das neue Suffix als Wert hinzu. In diesem Attribut werden alle Suffixe gespeichert, die den Domänencomputern zugewiesen werden können. Voraussetzung hierfür ist, dass alle Domänencontroller der Domäne unter Windows Server 2003 laufen und dass für jedes DNS-Suffix eine Subdomäne im DNS existieren muss.

Der Umbenennungsprozess an sich

Im Folgenden werden die einzelnen Schritte beschrieben, die zur Umbenennung notwendig sind. Bis zum Abschluss dieser Operation dürfen Sie in der kompletten Gesamtstruktur keine Aufgaben durchführen, die zu Konflikten führen können. Dazu zählen das Hinzufügen und Entfernen von Domänencontrollern, das Erstellen neuer Domänen oder das Bearbeiten von Vertrauensstellungen. Außerdem sollten Sie von jedem zu bearbeitenden Domänencontroller ein Backup angelegt haben.

Das Umbenennen der Domäne sollte von einem zentralen Computer aus durchgeführt werden. Der Computer muss zu der Gesamtstruktur gehören, in der die Änderungen vorgenommen werden. Es muss sich außerdem um einen Mitgliedsserver mit einer beliebigen Version des Windows Server 2003 als Betriebssystem oder um eine XP Professional-Client handeln. Selbstverständlich müssen Sie für diesen Prozess über Administratorrechte verfügen. Installieren Sie das Tool aus dem Verzeichnis `\VALUEADD\MSFT\MGMT\DOMAINRENAME` der Server-CD sowie zusätzlich die Support-Tools aus dem Verzeichnis `\SUPPORT\TOOLS`. Sie benötigen daraus die Programme *dfsutil.exe* sowie *repadmin.exe*. Auf einem XP-Client müssen Sie zusätzlich die Datei *adminpak.msi* aus dem Verzeichnis `\i386` der Server-CD installieren. Erforderlich ist daraus die Datei *dsquery.exe*.

1. Beschreibung der alten Gesamtstruktur

Starten Sie von dem ausgewählten Computer die Datei *random.exe* mit dem Parameter */list*. Dies generiert im Installationsverzeichnis eine XML-Datei namens *domainlist.xml*. Diese Informationen werden vom DNS-Betriebsmaster der Gesamtstruktur bezogen. Ist dieser nicht erreichbar, erhalten Sie eine Fehlermeldung. Von dieser Datei sichern Sie eine Kopie, da die *domainlist.xml* bearbeitet werden wird. In dieser XML-Datei befinden sich die Informationen als Liste aller Domain-Directory-Partitionen und Application-Directory-Partitionen der Gesamtstruktur. In unserem Beispiel handelt es sich um die Domänen *firma.de* und *sales.firma.de*. Die XML-Datei sieht folgendermaßen aus (siehe Listing 23.1):

```
<Forest>
  <Domain>
    <!-- PartitionType:Application -->
    <Guid>56acc6bd-d4f2-476a-83c8-8baca5a7e19a</Guid>
    <DNSname>DomainDnsZones.sales.firma.de</DNSname>
    <NetBiosName></NetBiosName>
    <DcName></DcName>
  </Domain>
  <Domain>
    <Guid>78ce6ad2-a1a3-432e-bb5c-cb43d74afc32</Guid>
    <DNSname>sales.firma.de</DNSname>
    <NetBiosName>SALES</NetBiosName>
    <DcName></DcName>
  </Domain>
  <Domain>
    <!-- PartitionType:Application -->
    <Guid>e128371d-a999-4345-aaa7-5e247a8d34c6</Guid>
    <DNSname>ForestDnsZones.firma.de</DNSname>
    <NetBiosName></NetBiosName>
    <DcName></DcName>
  </Domain>
  <Domain>
    <!-- PartitionType:Application -->
    <Guid> e128371d-a999-4345-aaa7-5e247a8d34d4</Guid>
    <DNSname>DomainDnsZones.firma.de</DNSname>
    <NetBiosName></NetBiosName>
    <DcName></DcName>
  </Domain>
  <Domain>
    <!-- ForestRoot -->
    <Guid>78ce6b55-a246-33b8-cc4b-6c5d03aa42b5</Guid>
    <DNSname> firma.de</DNSname>
    <NetBiosName>FIRMA</NetBiosName>
    <DcName></DcName>
  </Domain>
</Forest>
```

Listing 23.1: Die Datei *domainlist.xml* mit den Ausgangsinformationen

Für jede einzelne Partition ist die GUID, der DNS-Name sowie der NetBIOS-Name angegeben. Wie Sie sehen, besitzen lediglich die Domänenpartitionen NetBIOS-Namen, die Applikationspartitionen nicht.

2. Beschreibung der neuen Gesamtstruktur

Nun geht es ans Ändern der XML-Datei. Prinzipiell ändern Sie im XML-Code lediglich den alten Domännennamen in den neuen ab. Dabei wird in jeder Sektion zwischen `<Domain>` und `</Domain>` der DNS-Name und der NetBIOS-Name geändert. Sie dürfen jedoch *nicht* die GUID modifizieren. Andernfalls wird die Domäne nicht mehr gefunden. Denken Sie auch daran, den DNS-Namen der untergeordneten Domäne zu ändern. Wird in unserem Beispiel die übergeordnete Domäne *firma.de* in *neuefirma.de* umbenannt, und die untergeordnete Domäne behält den ursprünglichen Namen, so ist diese aus der Gesamtstruktur herausgelöst. Die untergeordnete Domäne kann entweder in *sales.neuefirma.de* umbenannt werden oder in *firma.de*, sodass sie eine neue Root-Domäne wird. Das folgende XML-Beispiel (siehe Listing 23.2) zeigt, wie die Domänenbeschreibung aussieht, wenn in beiden Domänen der Name von *firma* in *neuefirma* geändert wurde. Die Änderungen sind in kursiv hervorgehoben.

```
<Forest>
  <Domain>
    <!-- PartitionType:Application -->
    <Guid>56acc6bd-d4f2-476a-83c8-8baca5a7e19a</Guid>
    <DNSName>DomainDnsZones.neuefirma.de</DNSName>
    <NetBiosName></NetBiosName>
    <DcName></DcName>
  </Domain>
  <Domain>
    <Guid>78ce6ad2-a1a3-432e-bb5c-cb43d74afc32</Guid>
    <DNSName>sales.neuefirma.de</DNSName>
    <NetBiosName>SALES</NetBiosName>
    <DcName></DcName>
  </Domain>
  <Domain>
    <!-- PartitionType:Application -->
    <Guid>e128371d-a999-4345-aaa7-5e247a8d34c6</Guid>
    <DNSName>ForestDnsZones.neuefirma.de</DNSName>
    <NetBiosName></NetBiosName>
    <DcName></DcName>
  </Domain>
  <Domain>
    <!-- PartitionType:Application -->
    <Guid> e128371d-a999-4345-aaa7-5e247a8d34d4</Guid>
    <DNSName>DomainDnsZones.neuefirma.de</DNSName>
    <NetBiosName></NetBiosName>
    <DcName></DcName>
  </Domain>
```

```
<Domain>
  <!-- ForestRoot -->
  <Guid>78ce6b55-a246-33b8-cc4b-6c5d03aa42b5</Guid>
  <DNSname> neuefirma.de</DNSname>
  <NetBiosName>NEUEFIRMA</NetBiosName>
  <DcName></DcName>
</Domain>
</Forest>
```

Listing 23.2: Die Datei domainlist.xml mit dem geänderten Domännennamen

Im Beispiel wurde der DNS-Name und der NetBIOS-Name der Domäne geändert. Es ist jedoch nicht zwangsläufig notwendig, auch den NetBIOS-Namen zu ändern, wenn der DNS-Name geändert wird.

Beachten Sie beim Ändern auch, dass Sie in den Sektionen `<!--Partiton-Type:Application -->` ebenfalls den Namen ändern. Die Applikationspartitionen enthalten die DNS-Zonendaten und auch TAPI-(Telephone API-)Daten. Diese Partitionen können in jeder Hierarchieebene vorkommen bis auf die Root-Ebene. Sie werden automatisch erzeugt, wenn Sie auf einem DNS-Server Active Directory-integrierte Zonen verwenden.

In Schritt 3 stellt *RENDOM* mit einem beliebigen Domänencontroller in jeder Domäne der Gesamtstruktur eine Verbindung her, um Informationen zur Umsetzung der neuen Angaben zu sammeln, die in ein Skript umgesetzt werden. Wollen Sie hierfür bestimmte Domänencontroller festlegen, so geben Sie in jeder Domänensektion zwischen `<DC></DC>` den Namen des Domänencontrollers an, z.B. `<DC>hippokrates.firma.de</DC>`. Denken Sie daran, dass sich der Name des Domänencontrollers nicht automatisch ändert, wenn der Domänenname geändert wird. Deshalb muss hier *firma* und nicht *neuefirma* als Domänenname angegeben werden.

Nun müssen Sie überprüfen, ob die Änderungen zu Ihrer Zufriedenheit ausgefallen sind. Mit dem Befehl *RENDOM /showforest*  wird der Inhalt der modifizierten XML-Datei in einem benutzerfreundlichen Format angezeigt, sodass Sie die Struktur besser erkennen können. Finden sich hier Fehler, müssen Sie die beschriebenen Schritte wiederholen.

3. Generieren des Update-Skripts

In diesem dritten Schritt wird mit der Implementierung der Änderungen begonnen. Als Grundlage dient die XML-Datei mit den von Ihnen eingetragenen Änderungen. Daraus wird ein Skript gebildet, über das in mehreren Stufen nacheinander jeder Domänencontroller in der Gesamtstruktur aktualisiert wird.

Über den Befehl *RENDOM /upload*  wird dieses Skript generiert und auf der Konfiguration-Verzeichnispartition des DNS-Masters abgelegt. Außerdem wird eine Datei namens *dclist.xml* im Installationsverzeichnis von *RENDOM* erstellt. Diese Statusdatei enthält eine Liste aller Domänencontroller. Sie wird während des Updates benutzt, um für jeden Domänencontroller die verbleibenden Schritte verfolgen zu können. In unserem Beispiel sind in jeder der beiden Domänen zwei Domänencontroller vorhanden. Die *dclist.xml* sieht dann folgendermaßen aus (siehe Listing 23.3):

```

<DcList>
  <Hash>zzzzzzzzzz</Hash>
  <Signature>zzzzzzzzzz</Signature>
  <DC>
    <Name>hippocrates.firma.de</Name>
    <State>Initial</State>
    <LastError>0</LastError>
    <Password />
    <LastErrorMsg />
    <FatalErrorMsg />
    <Retry></Retry>
  </DC>
  <DC>
    <Name> archimedes.firma.de </Name>
    <State>Initial</State>
    <LastError>0</LastError>
    <Password />
    <LastErrorMsg />
    <FatalErrorMsg />
    <Retry></Retry>
  </DC>
  <DC>
    <Name> hesiod.sales.firma.de </Name>
    <State>Initial</State>
    <LastError>0</LastError>
    <Password />
    <LastErrorMsg />
    <FatalErrorMsg />
    <Retry></Retry>
  </DC>
  <DC>
    <Name> homer.sales.firma.de </Name>
    <State>Initial</State>
    <LastError>0</LastError>
    <Password />
    <LastErrorMsg />
    <FatalErrorMsg />
    <Retry></Retry>
  </DC>
</DcList>

```

Listing 23.3: Die Datei dclist.xml

Sie sehen, dass auch in dieser Datei die ursprünglichen Namen der Domänencontroller benutzt werden. Der DNS-Name lautet überall *firma.de* statt *neuefirma.de*. Beim Erstellen des Skripts sind die Sektionen `<State>` jeweils auf `Initial` gesetzt. Dieser Wert wird später bei jedem erfolgreich durchlaufenen Schritt angepasst. Auch Fehlermeldungen werden in dieser Statusdatei festgehalten.

4. Replizieren der Änderungen

Als Nächstes müssen nun die im Skript generierten Anweisungen an sämtliche Domänencontroller verteilt werden. Um diesen Prozess zu beschleunigen, können Sie vom DNS-Master aus die Replikation der Namensänderung an alle anderen Domänencontroller erzwingen. Das Erzwingen der Replikation ist optional, Sie können auch das reguläre Replikationsintervall abwarten. Um herauszufinden, welcher Domänencontroller der DNS-Master ist, benutzen Sie den Befehl `dsquery server -hasfsmo name` [↵].

Um die Replikation zu erzwingen, verwenden Sie den Befehl

`repadmin /syncall /d /e /P /q Name des DNS-Masters` [↵].

5. Überprüfen der DNS-Einträge

Nach Abschluss der Replikation müssen Sie die DNS-Ressourceneinträge überprüfen. Benutzen Sie hierzu die DNS-mmc auf einem autorisierenden DNS-Server. Während des Umbenennungsprozesses werden die SRV-Ressourceneinträge für den neuen Domänennamen vom Netlogon-Dienst auf den Domänencontrollern auf den autorisierenden DNS-Servern bereits veröffentlicht. Sind diese Einträge nicht korrekt vorhanden, können vom DC Locator nach der Umbenennung die Domänencontroller nicht mehr gefunden werden. Die folgenden Ressourceneinträge müssen vorhanden sein, ansonsten wird das Active Directory nicht mehr korrekt ausgeführt werden können:

1. Im Container *Domänenname._msdcs* muss auf jedem autorisierenden DNS-Server ein Eintrag für jeden Domänencontroller vorhanden sein (Name = GUID, Typ = Alias). Ansonsten wird von diesem DC aus keine Replikation stattfinden.
2. Im Container *Domänenname._msdcs.pdc.tcp* muss auf jedem autorisierenden DNS-Server ein Eintrag (Name *_ldap*, Typ Dienstidentifizierung) für den PDC-Emulator vorhanden sein. Damit ist die Authentifizierung der Benutzer und Computer sichergestellt.
3. Im Container *Domänenname._msdcs.gc._tcp* muss auf jedem autorisierenden DNS-Server ein Eintrag (Name *_ldap*, Typ Dienstidentifizierung) für mindestens einen globalen Katalogserver vorhanden sein.
4. Im Container *Domänenname._msdcs.dc._tcp* muss auf jedem autorisierenden DNS-Server ein Eintrag (Name *_ldap*, Typ Dienstidentifizierung) für mindestens einen Domänencontroller vorhanden sein.
5. Selbst wenn die Einträge für den Domänencontroller und globalen Katalog korrekt vorhanden sind, prüfen Sie zusätzlich, ob auch folgende Einträge vorhanden sind:
 1. Im Container *Domänenname._msdcs.dc._tcp* muss ein Eintrag (Name *_kerberos*, Typ Dienstidentifizierung) für den KDC vorhanden sein.
 2. Im Container *Domänenname._msdcs.gc* muss ein Eintrag (Typ Host) mit der IP-Adresse des globalen Katalogservers vorhanden sein.

6. Vorbereiten der Domänencontroller

Nun wird mit *RENDOM* eine Überprüfung jedes Domänencontrollers dahingehend durchgeführt, ob die Datenbank für die weiteren im Skript festgelegten Schritte bereit ist. Dazu muss die Replikation der Änderungen (Schritt 4) vollständig abgeschlossen sein. Dieser Schritt wird mit dem Befehl `rendom /prepare` [↵] initialisiert. Mit diesem Befehl wird ein RPC-Aufruf an alle Domänencontroller durchgeführt und der Zustand der

Datenbank geprüft. Wurde dieser Befehl erfolgreich ausgeführt, ist in der *dclist.xml* für jeden DC unter `<State> Prepared` eingetragen. Prüfen Sie, ob dieser Zustand bei sämtlichen Domänencontrollern eingetragen ist. Ist dies nicht der Fall, wiederholen Sie den `rendom /prepare`-Aufruf.

7. Ausführen der Änderungen

Nun werden die im Skript gespeicherten Änderungen auf den Domänencontrollern durchgeführt. Führen Sie dazu den Befehl `rendom /execute`  aus. Auch hier wird wieder ein RPC-Aufruf auf die Domänencontroller durchgeführt, der sie zum Durchführen der Änderungen veranlasst. Wurden alle Schritte erfolgreich abgeschlossen, startet der Domänencontroller automatisch neu.

Prüfen Sie danach in der *dclist.xml*, ob bei allen Domänencontrollern in der Sektion `<State>` der Eintrag `Done` vorhanden ist. Bei diesen Domänencontrollern wurde der Umbenennungsprozess erfolgreich abgeschlossen. Findet sich der Eintrag `Error`, ist es zu Fehlern gekommen. Diese werden in den Sektionen `<LastError>` und `<FatalErrorMsg>` näher spezifiziert. Weitere Hinweise zu Problemen finden Sie in der Logdatei des Skripts. Diese befindet sich in `%SYSTEMROOT%\DEBUG\SCRIPTLOG.LOG`.

Standardmäßig wird auf allen Domänencontrollern, die den Status `Done` oder `Error` tragen, das Skript kein zweites Mal ausgeführt, wenn `rendom /execute`  erneut aufgerufen wird. Haben Sie nun aber auf den Domänencontrollern mit dem Status `Error` den Fehler behoben (z.B. die Verbindung wiederhergestellt), so müssen Sie für diese DCs die *dclist.xml* modifizieren, sodass auf ihnen das Skript ein zweites Mal ausgeführt werden kann. Tragen Sie dazu in der Sektion `<Retry>` den Wert `yes` ein. So wird beim nächsten Aufruf von `rendom /execute`  ein neuer Versuch für den Domänencontroller unternommen.

Lassen sich auf einigen Domänencontrollern die Änderungen nicht erfolgreich durchführen, so müssen Sie auf diesen manuell das Active Directory entfernen, indem Sie den DC zum Mitgliedsserver herabstufen.

8. Umbenennen der Domänencontroller

Wie Sie bereits gesehen haben, werden die DNS-Namen der Domänencontroller nicht automatisch geändert. Diese Änderungen müssen Sie manuell über das Kommandozeilenprogramm *NETDOM* (siehe auch Kapitel 23.1.17) vornehmen. Führen Sie dazu die folgenden Schritte aus:

1. Geben Sie nach dem Aufruf von *NETDOM* folgenden Befehl ein: `netdom computername alter Name /add:neuer Name` . Als `alter Name` kann der Name oder die IP-Adresse des DC angegeben werden.
2. Prüfen Sie, ob nach der Replikation der Host-Eintrag auf allen autorisierenden DNS-Servern vorhanden ist.
3. Geben Sie dann folgenden Befehl ein: `netdom computername alter Name /make-primary: neuer Name` . Damit wird das Konto im Active Directory aktualisiert.
4. Starten Sie den Domänencontroller neu.
5. Prüfen Sie die Einträge der Logdatei *netlogon.dns* im Verzeichnis `%SYSTEMROOT%\SYSTEM32\CONFIG\`. Diese Werte sind im DNS registriert worden.

6. Geben Sie dann folgenden Befehl ein: `netdom computername neuer Name /remove: alter Name` . Damit werden die Host-Einträge des alten Computernamens im DNS gelöscht.
7. Öffnen Sie SYSTEMSTEUERUNG/SYSTEM. Auf der Registerkarte COMPUTERNAMEN klicken Sie auf ÄNDERN und geben den neuen Namen des Domänencontrollers ein. Bestätigen Sie mit OK.

9. Konsolidieren der DFS-Topologie

Nach dem Umbenennen der Domänen müssen die Referenzen in der DFS-Topologie bearbeitet werden, da die Verknüpfungen zu den alten Domänen ins Leere laufen. Hierzu verwenden Sie das Kommandozeilenprogramm `dfsutil.exe` aus den Support-Tools. Zunächst aber starten Sie den Administrationscomputer *zweimal* neu. Damit wird sichergestellt, dass alle laufenden Dienste den neuen Namen der Domäne erfahren.

Öffnen Sie nun die DFS-mmc und überprüfen, welche DFS-Stämme und welche ihrer DFS-Komponenten von den geänderten Domänen betroffen sind. Sehen Sie dabei auch nach, ob die DFS-Stämme über den DNS- oder NetBIOS-Namen referenziert werden. Wie oben beschrieben, müssen Sie den NetBIOS-Namen bei der Änderung nicht auch ändern. Haben Sie den NetBIOS-Namen nicht geändert und werden die DFS-Ressourcen über diesen Namen referenziert, können Sie diesen gesamten Arbeitsschritt überspringen.

Besitzen Sie einen domänenbasierten DFS-Stamm `\\FIRMA.DE\PROJEKT` und wurde die Domäne in *neuefirma.de* umbenannt, so muss der Stamm angepasst werden. Auch die Namen der Server, die die DFS-Replikate besitzen, müssen angepasst werden, wenn sich diese in einer umbenannten Domäne befinden. Dasselbe gilt auch für DFS-Verknüpfungen.

Über `dfsutil.exe` muss nun für jeden DFS-Stamm, bei dem eine der eben genannten Komponenten von der Änderung betroffen ist, der folgende Befehl ausgeführt werden:

```
dfsutil /RenameFtRoot /Root:alter DFSRoot (z.B. \\firma.de\Projekt)
/OldDomain: alter Domänenname
/NewDomain: neuer Domänenname
/verbose 
```

Nun wird ein Scan über die gesamte DFS-Topologie durchgeführt. Dabei werden alle Werte des alten Domänennamens durch den Namen der neuen Domäne ersetzt. Es werden auf jedem Server, der eine DFS-Replik besitzt, die Topologieinformationen aktualisiert, die er lokal in seiner Registry gespeichert hat. Danach müssen Sie jeden dieser DFS-Replik-Server *zweimal* neu starten, damit die DFS-Informationen aktualisiert werden. Die eben beschriebenen Schritte müssen Sie für jede umbenannte Domäne durchführen.

10. Konsolidierung der GPOs

Auch die GPOs verweisen nach dem Umbenennen der Domäne noch auf den alten Namen und müssen angepasst werden. Hierzu verwenden Sie das Kommandozeilenprogramm `gpfixup.exe`. Damit werden auch alle Daten, die für die Softwareverteilung benötigt werden, wie z.B. Pfade zu Softwareverteilungspunkten, automatisch korrigiert. Das Programm muss in jeder umbenannten Domäne einmal ausgeführt werden. Allerdings werden keine GPO-Verknüpfungen zwischen verschiedenen Domänen der Gesamtstruktur

tur sowie keine Pfade zu Softwareverteilungspunkten in externen Domänen automatisch repariert. Diese Verknüpfungen müssen manuell wiederhergestellt werden.

Führen Sie an der Kommandozeile folgende Befehle aus:

```
gpfixup /olddns:alter DNS-Domänenname  
/newdns:neuer DNS-Domänenname  
/oldnb:alter NetBIOS-Domänenname  
/newnb:neuer NetBIOS-Domänenname  
/dc:DNS-Name des DCs mit PDC-Emulatorrolle in der neuen Domäne 
```

Die Parameter `/oldnb` und `/newnb` müssen Sie nur dann setzen, wenn auch der Net-BIOS-Name der Domäne geändert wurde. Um die Replikation der GPO-Änderungen von dem unter `/dc:` angegebenen Domänencontroller auf die übrigen zu erzwingen, verwenden Sie folgenden Befehl:

```
repadmin /syncall /d /e /P /q DNS-DC-Name neuer DNS-Domänenname .
```

11. Bearbeiten der Domänenclients

Nach dem Umbenennen müssen Sie den Domänenclients die Änderungen beibringen, sodass die neuen Namen von Applikationen und Diensten auf den Clients benutzt werden können. Dabei müssen alle Clients und Mitgliedsserver, die Windows 2000, XP oder 2003 als Betriebssystem verwenden, *zweimal* neu gestartet werden. Domänenclients mit Windows NT 4.0 als Betriebssystem müssen aus der alten Domäne entfernt werden und dann der neuen Domäne beitreten. Windows 9x- und ME-Clients wird der neue Domänenname lediglich am Login-Prompt mitgeteilt.

12. Nach dem Umbenennen

Nach dem erfolgreichen Umbenennen der Domäne müssen Sie noch einige Aufgaben in verschiedenen Bereichen durchführen. Dies betrifft Vertrauensstellungen, DNS-Zonen sowie Startmenüeinträge.

Beim Umbenennungsprozess werden automatisch die transitiven Vertrauensstellungen innerhalb der Gesamtstruktur aktualisiert. Verfügen Sie zusätzlich über explizite Vertrauensstellungen zu Domänen einer anderen Gesamtstruktur, so müssen diese manuell neu erstellt werden (siehe Kapitel 12.1.6). Haben Sie nicht nur eine Umbenennung, sondern gleichzeitig auch eine Umstrukturierung der Gesamtstruktur vorgenommen, überprüfen Sie, ob es nicht Vertrauensstellungen gibt, die sich auf ehemalige untergeordnete Domänen beziehen, die nun zu Root-Domänen geworden sind.

Als Nächstes sollten Sie prüfen, ob in der DNS-Konfiguration Zonen eingetragen sind, die nicht mehr benötigt werden. Sollten noch Zonen mit dem alten Namen der Domäne vorhanden sein, so löschen Sie diese Zonen, da in ihnen keine DNS-Records mehr registriert werden müssen.

Als Letztes sollten Sie noch einen Blick auf die Startmenüverknüpfungen unter VERWALTUNG/SICHERHEITSRICHTLINIE FÜR DOMÄNEN und VERWALTUNG/SICHERHEITSRICHTLINIE FÜR DOMÄNENCONTROLLER werfen. Diese Verknüpfungen beziehen sich noch auf den alten Domänennamen. Um dies zu ändern, wählen Sie aus dem Kontextmenü den Eintrag EIGENSCHAFTEN und geben dort unter ZIEL den neuen Namen an.

23.2.2 RedirUsr und RedirComp

Diese beiden Resource Kit Tools haben die Aufgabe, dass neu erstellte Benutzer- und Computerkonten direkt in einer definierten Organisationseinheit angelegt werden. Auf diese Weise wird vermieden, dass die Benutzer und Computer in den Standardcontainern USERS und COMPUTERS der Domäne verbleiben, wie es im Windows 2000 Active Directory der Fall war. Denn für diese Container können keine Gruppenrichtlinienobjekte für die Benutzer angewendet werden – und oftmals liegt der Fehler, dass Gruppenrichtlinien bei bestimmten Benutzern nicht greifen, nur daran, dass sich die Benutzer noch im falschen Container befinden.

Mit den beiden neuen Programmen *redirusr* und *redircmp* können Sie neue OU-Container definieren, in denen die neuen Objekte angelegt werden sollen. Sie legen so Ihre eigenen bevorzugten Ziele für die API-Aufrufe *NetUserAdd*, *NetGroupAdd*, *NetComputerAdd* (Kommandozeilenaufruf) sowie *NetJoinDomain* (GUI unter Windows 2003, XP, 2000 und NT 4.0) fest. Auch Objekte, die mit dem Support-Tool *NETDOM* (siehe Kapitel 23.1.17, Befehl *netdom add*) oder über den Benutzermanager auf Windows NT 4.0-basierten Computern erstellt werden, werden automatisch in den OU-Container verschoben.

Die beiden Programme befinden sich nach der Installation der Windows Server 2003 Resource Kit Tools im Verzeichnis %SYSTEMROOT%\SYSTEM32.

Mit Hilfe des Kommandozeilenprogramms *redirusr* werden Benutzer und Gruppen des Standardcontainers USERS in den Container einer beliebigen OU verschoben, mit *redircmp* die Computerobjekte des Standardcontainers COMPUTERS. Um die beiden Programme benutzen zu können, müssen Sie über Administratorrechte verfügen. Zudem muss der Domänenfunktionslevel auf Windows 2003 eingestellt sein (siehe Kapitel 10.1.4). Erstellen Sie dann einen neuen OU-Container, in den die neu angelegten Benutzer automatisch verschoben werden sollen.

Geben Sie dann folgenden Befehl ein:

```
Redirusr DN=des-Containers ↵
```

Angenommen, die Benutzer sollen nun automatisch im OU-Container BENUTZER der Domäne *firma.de* angelegt werden. In diesem Fall sieht der Befehl folgendermaßen aus:

```
Redirusr ou=Benutzer,dc=firma,dc=de ↵
```

Sobald Sie nun z.B. mit dem Befehl *net user* einen neuen Benutzer erstellen, wird dieser in der OU Benutzer angelegt und nicht mehr im Standardcontainer USER. Soll zudem auch für alle Computer eine bestimmte OU definiert werden, so benutzen Sie mit derselben Syntax den Befehl

```
Redircmp ou=Computer,dc=firma,dc=de ↵
```

Ersetzen der Standardcontainer Users und Computers durch OUs

Sollen die beiden Standardcontainer USERS und COMPUTERS dauerhaft durch zwei spezielle OUs ersetzt werden, so können Sie dies ebenfalls einstellen. Hierzu ist eine Reihe von Schritten erforderlich:

1. Stellen Sie sicher, dass sich die Zieldomäne im Domänenfunktionsmodus Windows 2003 befindet. Melden Sie sich an dieser Domäne mit der Berechtigung des Domänenadministrators an.
2. Erstellen Sie zwei neue OUs, die temporär als Platzhalter für die Container CN=Users sowie CN=Computers dienen sollen. Diese beiden OUs heißen in unserem Beispiel *Usertemp* und *Comptemp* und befinden sich in der Domäne *firma.de*.
3. Als Nächstes werden die beiden ursprünglichen Speichercontainer an die beiden temporären OUs weitergeleitet. Hierzu benutzen Sie die entsprechenden *redirusr*- und *redircmp*-Befehle:

```
redirusr ou=usertemp,dc=firma,dc=de ↵
```

sowie

```
redircmp ou=comptemp,dc=firma,dc=de ↵
```

4. Danach werden die RDNs der ursprünglichen Container USERS und COMPUTERS geändert. Hierzu verwenden Sie das Tool *LDP* (siehe Kapitel 23.1.14). Stellen Sie eine Verbindung zu der Domäne her, deren Container geändert werden sollen. Aus der rechten Spalte wählen Sie aus dem Kontextmenü von CN=Users den Eintrag MODIFY DN. Dort tragen Sie den neuen DN des Containers ein, z.B. CN=Users CN,DC=firma,DC=de.
5. Klicken Sie dann auf RUN und prüfen, ob der neue Name korrekt übernommen wurde. Entsprechend verfahren Sie für den Container CN=Computers. Hier legen Sie über MODIFY DN den neuen DN des Containers fest, z.B. CN=Computers CN,DC=firma,DC=de.
6. Als Nächstes legen Sie die beiden neuen OUs an, die der Standardspeicherort für Benutzer und Computer werden sollen. Hierzu verwenden Sie wahlweise die GUI der mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER, *ADSIEDIT* oder *LDP*.
7. Danach werden diese beiden eben angelegten OUs mit *redirusr* und *redircmp* als Standardspeicherort festgelegt. Verwenden Sie hierzu die Befehle

```
redirusr ou=Benutzer,dc=firma,dc=de ↵
```

und

```
redircmp ou=Computer,dc=firma,dc=de ↵
```

8. Als Letztes löschen Sie die beiden temporären OU-Container USERTEMP sowie COMPTEMP, die Sie in Schritt 2 erstellt haben.

24 Das Active Directory-Schema

Dieses Kapitel gliedert sich in zwei Teile. Zunächst wird die Struktur des Active Directory-Schemas beschrieben. Das Schema enthält eine Reihe von Klassen und Attributen, über die die Objekte definiert werden. Auch weitere theoretische Grundlagen wie das abstrakte Schema und der Zugriff darauf werden vorgestellt.

Nach dieser grundlegenden Betrachtung der Schemaarchitektur wird diskutiert, warum eine Änderung am bestehenden Schema sinnvoll oder in manchen Fällen sogar notwendig sein kann. Bei der Erweiterung des Schemas gibt es allerdings auch gewisse Grenzen, die strikt einzuhalten sind. Sollten Sie sich für eine Änderung des Schemas entschieden haben, ist es wichtig, die internen Abläufe zu verstehen. Eine Schemaänderung umfasst auch Verwaltungsprozesse wie das Festlegen von Verantwortlichkeiten oder das Bereitstellen und Vergeben von OIDs. In einigen Bereichen des Schemas gibt es auch Unterschiede zwischen dem Schema unter Windows 2000 und 2003, auf die auch jeweils eingegangen wird.

An dieser Stelle soll nicht verschwiegen werden, dass Sie mit überstürzten und vor allen Dingen ungetesteten Schemaänderungen sehr schnell ein laufendes Active Directory stark beeinträchtigen, wenn nicht sogar zerstören können. Andererseits bieten sich durch die flexiblen Erweiterungsmöglichkeiten individuelle Anpassungsmöglichkeiten für die verschiedensten Anforderungen. Allerdings sind die Informationen zu diesem Thema sehr spärlich und weit verstreut. Um effektiv mit dem Schema arbeiten zu können, ist ein tiefgehendes Verständnis der Active Directory-Schemaarchitektur unerlässlich. Deshalb geht dieses Kapitel auch auf technische Details ein.

24.1 Allgemeines zum Active Directory-Schema

Das Active Directory-Schema gibt vor, welche Objekte in welcher Form im Verzeichnis gespeichert werden können. Die Objektdefinition wird über Klassen und Attribute geregelt. Diese Attribute und Klassen werden zusammenfassend auch als Schema-Objekte oder Metadaten bezeichnet. Anhand dieser Objektmerkmale identifiziert das Active Directory beispielsweise ein Benutzerobjekt als ein solches und nicht etwa als ein Druckerobjekt.

Das Active Directory-Schema besteht aus einer Liste von Definitionen für sämtliche Klassen und Attribute, die im Directory gespeichert werden können. Diese Attribute müssen dem Directory bekannt sein, damit ein Objekt gespeichert und gefunden werden kann. Das Active Directory-Schema ist für alle Domänen innerhalb einer Gesamtstruktur gültig. Jedes Active Directory-Objekt ist die Instanz einer bestimmten Klasse. Für jede Klasse ist definiert, welche Attribute in ihr enthalten sein müssen und welche optional enthalten sein können. Man spricht dabei von obligatorischen und optionalen Attributen. Zusätzlich wird für jedes Attribut die erlaubte Syntax definiert. Über die Syntax wird vorgegeben, ob ein Attribut z.B. Integer- oder Stringwerte enthalten darf. Jedes Attribut wird im gesamten

Schema nur einmal definiert und kann dann von diversen Klassen genutzt werden. So kommt beispielsweise das Attribut Beschreibung in diversen Klassen vor wie z.B. Computer oder Gruppen. Die Attribute für eine Klasse können sowohl von der übergeordneten Klasse geerbt als auch für jede Klasse direkt definiert werden. Die Zugriffsberechtigungen auf die Klassen- und Attributobjekte werden wie bei herkömmlichen Verzeichnisobjekten auch über Access Control Lists (ACLs) geregelt. In den nächsten beiden Kapiteln werden die Schemaklassen und Schemaattribute genauer erläutert.

Das Active Directory-Schema wird von dem Domänencontroller verwaltet, der die Betriebsmasterrolle des Schemamasters (siehe Kapitel 11.1.1) innehat. An diesem werden Änderungen am Schema vorgenommen und an die übrigen Domänencontroller repliziert.

Das Active Directory-Schema kann dynamisch aktualisiert werden. Sobald bei der Installation einer Applikation neue Attribute und Instanzen hinzugefügt worden sind, können diese neuen Objekte sofort benutzt werden.

Die Standarddefinition des Active Directory-Schemas befindet sich in der Datei *schema.ini* im Verzeichnis %SYSTEMROOT%\SYSTEM32\. Diese ini-Datei beschreibt das anfängliche Aussehen der Datei *NTDS.DIT* (DIT = Directory Information Tree), bevor Änderungen am Schema vorgenommen werden. Bei der Datei handelt es sich um eine Standard-ASCII-Datei, die mit einem beliebigen Texteditor geöffnet werden kann.

Im Active Directory-Schema lassen sich Attribute und Klassen zwar deaktivieren, jedoch nicht löschen. Deshalb sollten Sie sich gut überlegen, wann Sie Änderungen am Schema vornehmen. Die Änderungen am Schema werden innerhalb der Gesamtstruktur repliziert. Im Gegensatz zur Replikation nach der Änderung an Objekten, wobei nur die geänderten Attribute übertragen werden, wird bei der Änderung am Active Directory-Schema unter Windows 2000 die gesamte Klasse und nicht nur das geänderte Attribut übertragen. Die effizientere Übertragung auf Attributebene ist erst unter Windows 2003-Servern durch die Linked-Value Replication (siehe Kapitel 17.1.4) möglich.

24.1.1 Die Active Directory-Klassen

Sämtliche Objektklassen des Active Directory wie z.B. Benutzer oder Domänencontroller sind durch ein classSchema-Objekt im Schema-Container definiert. Jede Objektklasse verfügt dabei über spezielle Attribute, die Angaben über optionale oder obligatorische Attribute, Namens- und ID-Werte oder mögliche übergeordnete Klassen enthalten. Die Klasse beschreibt also die formale Definition. Klasseninstanzen sind mit Werten gefüllte Klassen. Legen Sie in der Klasse Computer einen neuen Computer mit dem Namen Hippokrates an, so haben Sie damit eine Instanz der Klasse Computer erzeugt.

Bevor wir uns diesen Attributen zuwenden, ist zunächst die Einteilung der Klassenobjekte in verschiedene Typen zu erwähnen.

Klassentypen

Jedes Klassenobjekt ist einem bestimmten Klassentyp zugeordnet. Es gibt insgesamt drei verschiedene Klassentypen: strukturelle, abstrakte sowie Erweiterungsklassen. Strukturelle Klassen können von anderen strukturellen oder abstrakten Klassen abstammen. In der Klassendefinition einer strukturellen Klasse können zudem beliebig viele Erweite-

rungsklassen enthalten sein. Strukturelle Klassen sind die einzigen Klassen, aus denen Active Directory-Objekte erstellt werden können. Beispiele für strukturelle Klassen sind container, groupPolicyContainer oder user. Abstrakte Klassen werden auch als zusammenfassende Klassen bezeichnet. Sie sind Vorlagen für Klassen aller drei Typen. Sie können aber nur von abstrakten Klassen hergeleitet werden. Erweiterungsklassen werden auch als zusätzliche Klassen oder Hilfsklassen bezeichnet. Sie sind streng genommen keine Klassen, sondern eher eine Sammlung von Attributen. Diese Erweiterungsklassen können strukturellen und abstrakten Klassen hinzugefügt werden. Damit erhalten diese Klassen auch automatisch die Liste der in der Erweiterungsklasse enthaltenen Attribute. Eine Erweiterungsklasse kann aus einer strukturellen oder einer anderen Erweiterungsklasse hergeleitet werden.

Außer den drei eben beschriebenen Klassentypen gibt es noch den speziellen Typ Klasse 88. Die Einteilung in die drei Klassen beschreibt eine X.500-Spezifikation aus dem Jahre 1988. Allerdings unterliegen alle Klassen, die vor 1993 definiert worden sind, nicht diesem X.500-Standard. Diese alten Klassen werden der Klasse 88 zugerechnet. Dazu gehören die Schema-Objekte country und device.

Die Attribute einer Klasse

Tabelle 24.1 gibt eine Übersicht über die wichtigsten Attribute eines Klassenobjekts. Eine komplette Auflistung aller obligatorischen und optionalen Klassenobjekte finden Sie unter

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/adschema/w2k/C_classSchema.asp

LDAP-Display-Name des Attributes	Beschreibung
CN (Common Name)	Aus diesem Wert wird der relativ definierte Namen (RDN) der Objektklasse gebildet. Der CN der Klasse organizationalUnit lautet Organizational-Unit. Dieser Name erscheint als RDN CN=Organizational-Unit. Der CN muss eindeutig sein im Schema-Container.
IDAPDisplayName	Dieser Name wird von den LDAP-Clients beispielsweise für gefilterte Suchabfragen in ADSI-Skripten benutzt. Auch dieser Name muss eindeutig im Schema-Container sein.
schemaIDGUID	Wird dieser Wert für ein neues Objekt nicht festgelegt, so generiert das Active Directory diese ID. Die ID ist eine Zeichenkette von 8 Bit, die die Klasse eindeutig bestimmt. Die ID wird z.B. in den ACLs benutzt.
governsID	Die OID (Object Identifier) einer Klasse. Weitere Hinweise zum Zuweisen von OIDs finden Sie in Kapitel 24.2.3.
rDNAttId	Identifiziert das Namensattribut dieser Klasse. Das Namensattribut muss mit dem Wert in CN übereinstimmen, allerdings sollten Sie hier die Form CN, DC, OU, O und L verwenden. Diese Schreibweise wird von allen LDAP-Clients der Version 3.0 korrekt verarbeitet.
mustContain, systemMustContain	Gibt die obligatorischen Attribute an, die in den Instanzen dieser Klasse vorhanden sein müssen. Diese Attribute können weder gelöscht noch geändert werden.

LDAP-Display-Name des Attributes	Beschreibung
mayContain, systemMayContain	Gibt die optionalen Attribute an, die in den Instanzen dieser Klasse vorhanden sein können. Die Werte für mayContain können allen Schema-Objekten der Kategorie 1 und 2 (siehe Kapitel 24.2.1) hinzugefügt oder von diesen entfernt werden. Die Eigenschaft systemMayContain kann nach dem Erzeugen einer Klasse nicht mehr geändert werden. Die mustContain und mayContain-Attribute bilden die sog. Content Rules des NTDS für jede Klasse im Schema.
possSuperiors, systemPossSuperiors	Hiermit wird die mögliche Baumstruktur einer Klasse festgelegt. Der Wert gibt die strukturellen Klassen an, die der Klasse übergeordnet sein können. Beide Werte können nicht von den Auxiliary Classes geerbt werden. Die Werte für (system)PossSuperiors können allen Schema-Objekten der Kategorie 1 und 2 (siehe Kapitel 24.2.1) hinzugefügt oder von diesen entfernt werden. Die Eigenschaft systemPossSuperiors kann nach dem Erzeugen einer Klasse nicht mehr geändert werden.
auxiliaryClass, systemAuxiliaryClass	Gibt die Hilfsklassen(n) an, die diese Klasse erbt. Sie können neue Werte für auxiliaryClass hinzufügen, bestehende aber nicht löschen. Der Wert für systemAuxiliaryClass kann nach dem Erstellen einer Klasse nicht mehr geändert werden.
subClassOf	Die OID der unmittelbar übergeordneten Klasse. Existiert die hier angegebene Klasse beim Erstellen einer neuen Klasse nicht, so wird diese nicht in das Schema aufgenommen.
objectClassCategory	Ein Integerwert, der die Klassenkategorie festlegt. Es gibt strukturelle (= 1), abstrakte (= 2) und Hilfsklassen (= 3).
defaultHidingValue	Gibt einen Booleschen Wert als Default-Wert für shownIn-AdvancedViewOnly der neuen Instanzen dieser Klasse an. Ist dieser Wert auf TRUE gesetzt, werden die neuen Objektinstanzen nicht in der Schema-mm und der Windows-Shell angezeigt. Wählen Sie diesen Wert für Objekte, die für den Endbenutzer weniger interessant sind. Die Objektklasse erscheint auch nicht im Wizard zum Erstellen neuer Klassen in der Liste vorhandener Klassen.
systemFlags	Ein Integerwert mit Flags zur Definition zusätzlicher Eigenschaften der Klasse. Der 16-Bit-Wert identifiziert das Objekt als zur Kategorie 1 gehörig. Die Unterschiede zwischen Kategorie 1 und 2 werden in Kapitel 24.2.1 beschrieben.
systemOnly	Der Boolesche Wert bestimmt, ob die Klasse nur vom Directory System Agent (DSA) oder auch manuell erstellt und gelöscht werden kann.
isDefunct	Dieser Boolesche Wert bestimmt, ob die Klasse deaktiviert ist oder nicht. Weitere Hinweise dazu finden Sie in Kapitel 24.3.4.
objectClass	Identifiziert die Objektklasse, von der dieses Objekt eine Instanz bildet.

Tabelle 24.1: Die wichtigsten Attribute einer Objektklasse

Beim Erstellen einer neuen Klasse wird diese automatisch als Subclass / untergeordnete Klasse des Parent- bzw. übergeordneten Objekts definiert. Diese Subclass erbt vom Parent-Objekt sämtliche Attribute sowie die Content Rules (mayContain und mustContain) und Structure Rules (NTDS legt die möglichen Baumstrukturen im Attribut PossSuperiors fest). Damit ist das Parent-Objekt automatisch die Superclass / übergeordnete Klasse der neuen Klasse.

Öffnen Sie in der mmc ACTIVE DIRECTORY-SCHEMA die Eigenschaften eines Klassenobjekts, so finden Sie einen großen Teil der eben beschriebenen Attribute auf den Registerkarten wieder. Das Erstellen eines neuen Objekts wird in Kapitel 24.3.1 beschrieben.

24.1.2 Die Active Directory-Attribute

Jedes mögliche Attribut für ein Active Directory-Objekt wird im Schema-Container als ein attributeSchema-Objekt definiert. Attribute werden zuweilen auch als Properties bzw. Eigenschaften bezeichnet. In den Eigenschaften des attributeSchema-Objekts sind für jedes Attribut Charakteristika wie Attributbezeichnungen und IDs, die erlaubte Syntax oder Speicherung im globalen Katalog hinterlegt. Als Attributinstanz wird jedes Vorkommen eines Attributs bezeichnet. Das Attribut selbst ist die Definition, eine Attributinstanz selbst wird gebildet, wenn Sie einem Attribut einen eigenen Wert zuweisen. So ist im Attribut Common Name (CN) definiert, welche Syntax etc. zu verwenden ist. Legen Sie nun einen Benutzer mit dem CN Peter Mustermann an, so erzeugen Sie damit eine spezielle Instanz des Attributs Common Name.

Tabelle 24.2 gibt einen Überblick über die wichtigsten Attribute. Eine vollständige Auflistung finden Sie unter

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/adschema/w2k/C_attributeSchema.asp

IDAPDisplayName	Beschreibung
CN (Common Name)	Aus diesem Wert wird der relativ definierte Name (RDN) des Objekts gebildet. Der CN des Objekts isSingleValued lautet Is-Single-Valued. Dieser Name erscheint als RDN CN=Is-Single-Valued. Der CN muss eindeutig sein im Schema-Container.
IDAPDisplayName	Dieser Name wird von den LDAP-Clients beispielsweise für gefilterte Suchabfragen in ADSI-Skripten benutzt. Auch dieser Name muss eindeutig im Schema-Container sein.
schemaIDGUID	Wird dieser Wert für ein neues Objekt nicht festgelegt, so generiert das Active Directory diese ID. Die ID ist eine Zeichenkette von 8 Bit, die das Attribut eindeutig bestimmt. Die ID wird z.B. in den ACLs benutzt.
attributeID	Die OID (Object Identifier) des Attributs. Weitere Hinweise zum Zuweisen von OIDs finden Sie in Kapitel 24.2.3.
attributeSecurityGUID	Eine optionale GUID, die ebenfalls in ACLs benutzt werden kann.

IDAPDisplayName	Beschreibung
attributeSyntax	Zusammen mit der Eigenschaft oMSyntax wird die Syntax des Attributs vorgegeben. Die Syntax beschreibt, ob es ein String- oder Integerwert usw. ist. Eine Auflistung der gültigen Syntaxwerte finden Sie unter http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/ad/syntaxes_for_active_directory_attributes.asp
oMSyntax	Integerwert zur Kennzeichnung der Syntax. Eine Auflistung aller oMSyntax-Werte finden Sie unter http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/ad/syntaxes_for_active_directory_attributes.asp
oObjectClass	Dieser Wert muss nur für Attribute mit der oMSyntax 127 gesetzt werden (siehe oMSyntax). Bei allen anderen oMSyntax-Werten stimmt die oObjectClass mit dem Wert der attributeSyntax überein.
rangeLower, rangeUpper	Diese beiden Werte geben den erlaubten Minimal- und Maximalwert des Attributs an. Die gültigen Werte müssen sich innerhalb dieses Bereichs befinden.
isSingleValued	Dieser Wert wird auf TRUE gesetzt, wenn das Attribut nur einen einzigen Wert besitzen darf. Dies ist die Standardeinstellung.
searchFlags	Über die Flags wird bestimmt, ob ein Attribut für Abfragen indiziert wird oder nicht. Weiteres dazu siehe das Kapitel „Indizierte Attribute“.
isMemberOfPartial-AttributeSet	Ist der Wert auf TRUE gesetzt, wird das Attribut in den globalen Katalog repliziert, bei FALSE erfolgt keine Replikation. Weiteres dazu siehe das Kapitel „Attribute im globalen Katalog“.
systemFlags	Diese Flags legen zusätzliche Eigenschaften von Attributen fest. Einige Systemflags können nicht geändert werden, z.B. das Flag zum Kennzeichnen eines Kategorie 1-Objekts. Eine Aufstellung dieser Flags finden Sie unter http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/ad/syntaxes_for_active_directory_attributes.asp
mAPIID	Integerwert, über den MAPI-Clients das Attribut identifizieren können.
systemOnly	Der Boolesche Wert bestimmt, ob das Attribut nur vom Directory System Agent (DSA) oder auch manuell erstellt und gelöscht werden kann.
isDefunct	Dieser Boolesche Wert bestimmt, ob das Attribut deaktiviert ist oder nicht. Weitere Hinweise dazu siehe Kapitel 24.3.4.
objectClass	Identifiziert die Objektklasse, von der dieses Objekt eine Instanz bildet.

Tabelle 24.2: Die wichtigsten Attributdefinitionen

Indizierte Attribute

In Tabelle 24.2 ist vermerkt, dass über den Wert von `searchFlags` geregelt wird, ob und wie Attribute indiziert werden können, um bei Suchabfragen schneller verfügbar zu sein. Es werden dabei die folgenden Flags benutzt (siehe Tabelle 24.3):

Flag	Beschreibung
1	Nur das Attribut selbst wird indiziert.
2	Das Attribut und sein Container werden indiziert.
4	Das Attribut wird zur Ambiguous Name Resolution (ANR) gesetzt. Weitere Hinweise siehe http://msdn.microsoft.com/library/default.asp?url=/library/en-us/cdo/html/_olemsg_ambiguousnames_property_recipient_object_.asp
8	Das Attribut wird im Tombstone-Objekt (siehe Kapitel 21.4) der gelöschten Objekte geschützt.
16	Die Attributwerte werden kopiert, wenn das zugehörige Objekt als Vorlage kopiert wird. Diese Option ist sinnvoll, wenn Sie z.B. Attributwerte für Firma oder Abteilung eines Benutzers als Vorlage für das neue Benutzerobjekt übernehmen möchten, aber andere Attribute, z.B. den Namen, nicht.

Tabelle 24.3: Die Flags zur Attributindizierung

Sobald der Wert für `searchFlag` auf mindestens den Wert 1 gesetzt wird, wird der Index automatisch auf dem Domänencontroller gebildet. Setzen Sie das Flag auf 0, wird der Index für dieses Attribut wieder gelöscht. Es ist nur möglich, Attribute zu indizieren, nicht jedoch komplette Klassen. Werden bestimmte Attribute indiziert, so werden sämtliche Instanzen des Attributs dem Index hinzugefügt und nicht nur die Instanzen, die zu einer bestimmten Klasse gehören.

Damit die Suchabfragen korrekt durchgeführt werden können, muss auf den Servern unter Umständen der Registry-Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\Current Control Set\Services\NTDS\Diagnostics\9 Internal Processing` angepasst werden. Setzen Sie hier den Wert von 0 auf 4. Im Ereignisprotokoll des Directory Service finden sich nun nach einer Abfrage Informationen über die Indizes.

Um Abfragen so performant wie möglich zu gestalten, sollten Sie Eigenschaften von Attributen indizieren, die nur einen einzigen Wert besitzen, der zudem eindeutig ist und in vielen Instanzen vorkommt. Eigenschaften mit Mehrfach-Werten können zwar auch indiziert werden, allerdings nimmt das Bilden eines solchen Index mehr Zeit für Suchabfragen und Aktualisierungen in Anspruch. Außerdem dauert es länger, neue Instanzen einer Klasse zu bilden, je mehr indizierte Attribute in dieser Klasse enthalten sind.

Attribute im globalen Katalog

Der globale Katalog umfasst ein Teilreplikat der am häufigsten benutzten Attribute jedes Active Directory-Objekts. Gehört ein `attributeSchema`-Objekt zum globalen Katalog, so ist dort das Attribut `isMemberOfPartialAttributeSet` auf `TRUE` gesetzt. Um zu entscheiden, welche Attribute in den globalen Katalog aufgenommen werden sollten, beachten Sie die folgenden Kriterien.

An dem Attribut sollten nur selten Änderungen vorgenommen werden. Jede Änderung an einem Wert wird an sämtliche globalen Katalogserver der Gesamtstruktur repliziert. Die Attribute sollten natürlich auch von allgemeinem Interesse sein. So können Attribute wie Mitarbeitername, Mail-Adresse oder Telefonnummern in den globalen Katalog aufgenommen werden, sodass diese Informationen bezogen werden können, ohne dass der Zugriff auf ein vollständiges Replikat des Benutzerobjekts erfolgen muss. Generell gilt, je mehr Attribute Sie dem globalen Katalog hinzufügen, desto mehr Replikationsverkehr und Speicherbedarf entsteht auf dem Katalogserver. Wird ein Attribut nicht im globalen Katalog gefunden, so wird die Suchanfrage an einen anderen Server weitergeleitet, der ein vollständiges Replikat des Objekts enthält. Dabei wird der definierte Name (DN) des Objekts aus dem globalen Katalog ausgelesen und dann über den DN eine Verbindung zu einem vollständigen Replikat des Objekts hergestellt.

24.1.3 Das abstrakte Schema

In dem Container des Active Directory-Schemas `CN=Schema,CN=Configuration,DC=xxx,DC=xx` befindet sich neben den eben beschriebenen Klassen- und Attributobjekten auch ein Objekt *Aggregate* in der Klasse `subSchema`. Sie sehen dieses Objekt nicht in der mmc `ACTIVE DIRECTORY-SCHEMA`, sondern müssen die Tools *ADSIEDIT* oder *LDP* benutzen. Dieses spezielle Objekt wird auch als das abstrakte Schema bezeichnet.

Das abstrakte Schema beinhaltet eine bestimmte Untermenge an Informationen der Objekte *classSchema* und *attributeSchema*. Über den Mechanismus des abstrakten Schemas können die am häufigsten benutzten Teile der Klassen- und Attributdefinitionen besonders schnell und effektiv abgerufen werden. Um von einer bestimmten Objektklasse die obligatorischen und optionalen Attribute zu erhalten, müsste theoretisch der Zugriff auf diverse Objekte erfolgen, um alle Werte für `mayContain`, `mustContain`, `systemMayContain` sowie `systemMustContain` für diese Klasse, deren übergeordnete Klassen und Hilfsklassen sowie deren übergeordnete Klassen zu erhalten. Über das abstrakte Schema werden alle diese Informationen in dem einzelnen `subSchema`-Objekt zusammengefasst. Auf dieses Objekt können Sie wie auf alle anderen Schema-Objekte auch zugreifen.

Da die Aufgabe des abstrakten Schemas in der Optimierung von Abfragen besteht, können über das abstrakte Schema auch keine Änderungen am eigentlichen Schema vorgenommen werden. Das abstrakte Schema ist schreibgeschützt. Lesender Zugriff auf das abstrakte Schema kann über die ADSI-Methode `IADsContainer` erfolgen (siehe Kapitel 32.1.3).

24.1.4 Die mmc Active Directory-Schema

Um mit dem Active Directory-Schema effektiv arbeiten zu können, muss zuerst die mmc `ACTIVE DIRECTORY-SCHEMA` installiert werden. Standardmäßig befindet sich diese Konsole nicht in der Windows-Verwaltung eines Domänencontrollers. Sie müssen zunächst die Datei *schmmgmt.dll* für das Konsolen-Snap-In unter Windows registrieren, bevor Sie das Snap-In einer Konsole hinzufügen können. Diese Registrierung erfolgt an der Kommandozeile mit dem Befehl `regsvr32.exe schmmgmt.dll`.

Um die Verwaltungskonsolle auf einem Mitgliedsserver oder auf Clients zu erstellen, müssen Sie zunächst die Datei *adminpak.msi* aus dem i386-Verzeichnis der Server-CD installieren.

Öffnen Sie dann eine leere mmc und fügen das Snap-In ACTIVE DIRECTORY-SCHEMA hinzu. Speichern Sie diese neue Konsole. Die mmc ACTIVE DIRECTORY-SCHEMA sieht folgendermaßen aus (siehe Abbildung 24.1):

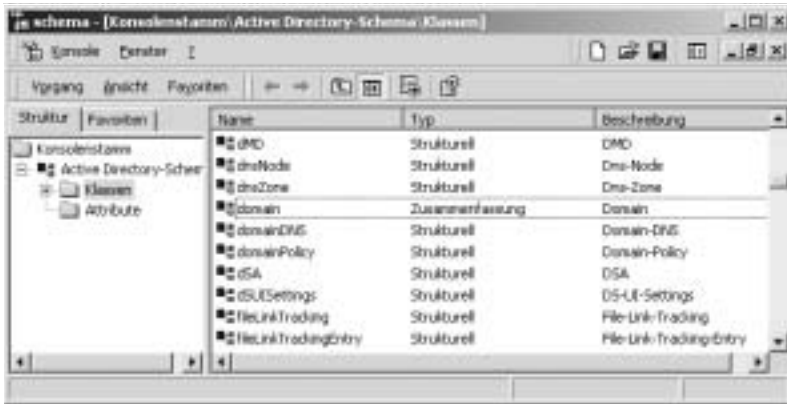


Abbildung 24.1: Die mmc Active Directory-Schema

Im Bereichsabschnitt links sehen Sie die beiden Untercontainer des Schemas, nämlich die Klassen und Attribute. Markieren Sie die Klassen, so sehen Sie im Ergebnisabschnitt rechts sämtliche Objektklassen, deren Klassentyp sowie eine kurze Beschreibung. Für die Attribute wird statt des Typs die definierte Syntax angegeben. Über die mmc können Sie über das Kontextmenü des Knotens ACTIVE DIRECTORY-SCHEMA die Berechtigungen für den Schemazugriff konfigurieren, den Betriebsmaster ändern sowie die Verbindung zu einem anderen Domänencontroller herstellen. Das Erstellen neuer Klassen und Attribute wird in Kapitel 24.3.1 beschrieben.

24.2 Warum Änderungen durchführen?

Eine der Stärken von Active Directory ist die Erweiterbarkeit des Schemas. Damit haben Sie die Möglichkeit, unternehmensspezifische Attribute zu den Objekten hinzuzufügen. Active Directory bietet zwar schon eine große Menge an vorhandenen Attributen, doch diese Attribute sind erweiterungsfähig. Sie können z.B. eigene Attribute für Qualifikationen der Mitarbeiter, ihr Alter, gesprochene Sprachen, Angaben zu Dienstwagen, Inventarnummern, Kostenstellen usw. anlegen.

Das Ändern des Schemas ist jedoch ein tiefgreifender Einschnitt in das Active Directory. Er sollte auch nur nach gründlicher Planung und Überlegung durchgeführt werden. Bevor Sie wirklich an die Änderung des Schemas gehen, überlegen Sie sich, ob es für Ihre Zwecke nicht ausreichend ist, ein bereits vorhandenes Attribut zu finden, das Sie garantiert nicht benutzen werden und das die gewünschten neuen Informationen aufnehmen kann. Jedoch müssen Sie hierbei bedenken, dass das Attribut, das Sie sich für die neue

Funktion hernehmen, leider nicht den Namen des Attributs trägt, das Sie neu festlegen. Sie müssen also die Umfunktionierung des gewählten Attributs auf Administratorebene dokumentieren und auch den Verzeichnisbenutzern mitteilen, unter welchem alten Attribut die neuen Werte gefunden werden können. Sie sehen, dass dies nicht gerade ein eleganter Weg ist, um zusätzliche Informationen im Verzeichnis aufzunehmen, aber Sie sparen sich in diesem Fall den Umweg, das Schema bearbeiten zu müssen. Es kann an dieser Stelle auch nicht generell zwischen richtig und falsch entschieden werden, wann eine Schemaänderung durchgeführt werden muss und wann die eben beschriebene Hilfsmethode völlig ausreichend ist.

Bei der Neuinstallation des Active Directory sollten Sie bereits in der Planungsphase des Projekts darüber nachdenken, welche zusätzlichen Attribute Sie in das Verzeichnis aufnehmen möchten. Bei einer Migration von Windows NT auf Windows 2000 oder 2003 können alle unter NT vorhandenen Attribute ins Active Directory übernommen werden. Die im Vergleich zu Windows 2000 recht wenigen Attribute sind dem Active Directory-Schema vollständig bekannt.

Zur Änderung des Schemas stehen Ihnen mehrere Möglichkeiten offen. So können Sie zum einen sämtliche Änderungen über die mmc ACTIVE DIRECTORY-SCHEMA vornehmen. Zum anderen können auch die Schemadaten mit ADSI-Skripten bearbeitet werden. Diese Methode wird jedoch erst in Kapitel 32.4 vorgestellt, da Sie zuvor einen Einblick in die Funktionsweise von ADSI- und ADSI-Skripten erhalten sollten. Die dritte, wenn auch wahrscheinlich am wenigsten praktizierte Möglichkeit besteht darin, Schemaänderungen über Microsoft Visio vorzunehmen und die Änderungen via *LDIFDE* wieder zu importieren. Dieses Verfahren wird kurz in Kapitel 26.1.3 vorgestellt.

Zur Erweiterung des Schemas stehen Ihnen grundsätzlich zwei Möglichkeiten offen. Sie können zum einen eine neue Klasse von einer bereits vorhandenen ableiten und dieser neben den bereits von der übergeordneten Klasse geerbten Attributen noch zusätzliche eigene hinzufügen. Die andere Möglichkeit besteht darin, einer bereits vorhandenen Klasse neue Attribute oder eine Hilfsklasse (Auxiliary Class) hinzuzufügen oder für eine Klasse sogar eine neue übergeordnete Klasse zu erstellen. Die erste Möglichkeit sollten Sie immer dann verwenden, wenn eine bereits vorhandene Klasse bereits die meisten gewünschten Attribute umfasst und diese nur noch ergänzt werden soll. Dieser Weg ist beispielsweise zu empfehlen, wenn Sie für Benutzerobjekte zusätzliche Attributinformationen wie besondere Qualifikationen oder gesprochene Sprachen hinzufügen möchten. Sie sollten es auch nach Möglichkeit vermeiden, bereits vorhandene Klassen zu modifizieren. Bedenken Sie für Ihre weitere Arbeit mit den neuen Attributen auch, dass Sie zur Anzeige und Verwaltung dieser neuen Objekte mmcs wie ACTIVE DIRECTORY-BENUTZER UND -COMPUTER anpassen müssen. Die neuen Attribute erscheinen nicht einfach durch das bloße Hinzufügen im Schema auch in der mmc. Hier muss schon mit einem kleinen ADSI-Skript nachgeholfen werden. Ein praktisches Beispiel dafür finden Sie in Kapitel 32.4.3. Die Verwaltungsinstrumente unter Windows sind "out of the box" lediglich für das standardmäßige Schema ausgelegt.

24.2.1 Einschränkungen bei der Schemaerweiterung

Bei allen Möglichkeiten zur Erweiterung des Schemas gibt es jedoch auch einige Einschränkungen. Diese Begrenzungen haben ihren guten Grund, um nicht die Konsistenz des Schemas zu gefährden oder durch Änderungen, die eine Applikation am Schema vornehmen könnte, die Funktion einer anderen zu beeinträchtigen.

Um zu verstehen, worauf sich die Einschränkungen beziehen, muss zunächst die Kategorieneinteilung des Schemas erläutert werden. Das komplette Active Directory-Schema wird in zwei Kategorien unterteilt. Sämtliche Schema-Objekte, die mit Windows ausgeliefert wurden, bilden die Kategorie 1. Zur Kategorie 2 gehören folglich alle Objekte, die später manuell durch den Schema-Administrator oder bei der Installation einer Applikation als Erweiterung hinzugefügt worden sind. Um zu ermitteln, ob ein Objekt zur Kategorie 1 oder 2 gehört, überprüfen Sie das Attribut `systemFlags`. Dieses Attribut hat ausschließlich bei Objekten der Kategorie 1 einen 16-Bit-Wert, der nicht geändert werden kann. Außerdem wird über dieses Attribut geregelt, ob ein Objekt gelöscht, verschoben oder umbenannt werden kann. So wird sichergestellt, dass keine Objekte in einer Form modifiziert werden, die für die Funktionsweise des Active Directory erforderlich sind.

An Objekten der Kategorie 1 können die Attribute `attributeSecurityGuid` sowie `rangeLower` und `rangeUpper` nicht geändert werden. Die `range`-Attribute geben den Bereich an, innerhalb dessen die Werte liegen müssen. Über die `attributeSecurityGuid` wird bestimmt, zu welchem Satz von Eigenschaften das Attribut gehört. Weiterhin können keine Klassen und Attribute der Kategorie 1 umbenannt werden. Auch die Werte für `defaultObjectCategory` einer Kategorie 1-Klasse oder einer deren Instanzen sowie für `ldapDisplayName` einer Kategorie 1-Klasse oder eines Kategorie 1-Attributs können nicht geändert werden. Weiterhin können auch kein Attribut und keine Klasse der Kategorie 1 als deaktiviert (`isDefunct=TRUE`, siehe Kapitel 24.3.3) gesetzt werden. Schließlich können Sie auch kein neues `mustContain` zu einer Klasse, auch zu keiner geerbten Klasse, neu hinzufügen oder ein `mustContain` einer Klasse löschen. Diese Vorgabe gilt gleichermaßen für Objekte der Kategorie 1 und 2.

24.2.2 Der Schema-Cache

Auf jeden Domänencontroller wird vom Schemamaster ausgehend das gesamte Active Directory-Schema repliziert. Dabei ist auf jedem Domänencontroller neben diesem Schemareplikat auch eine komplette Kopie des Schemas im Arbeitsspeicher vorhanden. Diese Kopie wird auch Schema-Cache genannt. Im Schema-Cache sind sämtliche Klassen- und Attributobjekte des Schemas in Tabellen indiziert, damit Suchoperationen schneller durchgeführt werden können. Bei den Klassenobjekten sind der `ldapDisplayName`, die `guid` sowie die `mapID` indiziert, bei den Attributobjekten die `attributeID` sowie der `ldapDisplayName`. Standardmäßig sind die Tabellen so ausgelegt, dass sie 1024 Klassen und 2048 Attribute aufnehmen können. Die Größe ist aber dynamisch und hängt von der Größe des vorhandenen Arbeitsspeichers ab.

Der Schema-Cache wird automatisch bei jedem Start des Domänencontrollers erstellt. Wurden Aktualisierungen am Schema vorgenommen, so wird der Cache mit fünf Minuten Verzögerung ebenfalls neu geladen. Werden innerhalb dieser fünf Minuten immer noch Änderungen am Schema vorgenommen – man denke an eine zeitintensive Exchange 2000-

Installation – so werden die geänderten Schema-Objekte wiederum mit fünf Minuten Verspätung in den Schema-Cache geladen. Innerhalb dieser fünf Minuten ist es nicht möglich, neue Instanzen der geänderten oder neu erstellten Objektklassen zu erstellen. Versuchen Sie dieses, so erhalten Sie eine Fehlermeldung. Dies liegt darin begründet, dass für das Neuerstellen der Objekte der Schema-Cache und nicht das eigentliche Schemareplikat verwendet wird. Lediglich neue Klassen und Attribute können innerhalb dieser fünf Minuten bereits den frisch erstellten Klassen hinzugefügt werden.

Bis die Replikation der Schemaänderungen auf allen Domänencontrollern abgeschlossen ist, kann das Schema temporär inkonsistent sein. Werden beispielsweise zeitgleich eine neue Klasse im Schema erstellt und für diese Klasse auch neue Objekte, so können die neuen Objekte unter Umständen auf einige Domänencontroller repliziert werden, bevor diese Informationen über die neue Schemaklasse erhalten haben. Um diesem Problem vorzubeugen, benutzt das Active Directory einen speziellen Mechanismus. Wird das Objekt von DC1 an DC2 gesendet und DC2 kann das Objekt nicht verarbeiten, weil ihm noch die entsprechenden Schemainformationen fehlen, so fordert DC2 von DC1 das Schema-Containerobjekt an. Das Schema-Objekt wird dann sofort von DC1 auf DC2 repliziert, gleichzeitig wird auf DC2 der Schema-Cache aktualisiert. Dann wird wieder das neue Objekt repliziert und kann nun von DC2 verarbeitet werden, da ihm nun die entsprechenden Schemainformationen vorliegen.

Es gibt auch Möglichkeiten, den Schema-Cache direkt nach einer Änderung des Schemas upzudaten und nicht auf das automatische Update zu warten. Dies ist sinnvoll, wenn Sie neue Attribute und Klassen erstellen möchten und nach der Erstellung der Attribute nicht die obligatorischen fünf Minuten abwarten möchten, bevor Sie die neuen Klassen erstellen können. Hierzu verwenden Sie entweder die mmc ACTIVE DIRECTORY-SCHEMA oder ein LDIF-Skript. In der mmc wählen Sie aus dem Kontextmenü von ACTIVE DIRECTORY-SCHEMA den Eintrag SCHEMA NEU LADEN.

Alternativ können Sie in einem LDIF-Skript den Wert `schemaUpdateNow` am RootDSE auf 1 ändern. Der RootDSE ist die oberste Wurzel des Directory Information Tree (DIT) auf dem Verzeichnisserver. Da der RootDSE nicht Bestandteil des Namensraums ist, verfügt er auch über keinen definierten Namen (DN). Wird das Skript ohne Fehler ausgeführt, ist der Schema-Cache upgedatet, und Sie können mit dem Erstellen der Klassen fortfahren. Im Folgenden sehen Sie ein LDIF-Skript, das den Schema-Cache aktualisiert. Weitere Hinweise zu LDIF sowie der Ausführung von LDIF-Skripten finden Sie in Kapitel 25.1 und 25.2.

```
dn:
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
```

Listing 24.1: LDIF-Skript zur Aktualisierung des Schema-Cache

24.2.3 Festlegen und Zuweisen von Object Identifiern (OIDs)

Beim Erstellen von Klassen und Attributen müssen Sie Werte für den Object Identifier (OID) angeben. OIDs sind wie GUIDs eindeutige numerische Werte, um Daten verteilter Applikationen, z.B. in X.500-Verzeichnissen oder SNMP, eindeutig zu beschreiben. Die Struktur der OIDs basiert auf einer Baumstruktur. Eine übergeordnete Autorität gibt dabei untergeord-

nete OIDs weiter. Eine OID ist folgendermaßen strukturiert: 1.2.840.113556.1.5.4. Dabei haben die einzelnen Werte folgende Bedeutung:

1 = ISO

2 = ANSI

840 = USA

113556 = Microsoft

1 = MS Active Directory

5 = MS Active Directory, Classes

4 = MS Active Directory, Classes, Built-In-Domain

In diesem Beispiel ist 1 = ISO die Root-Autorität. Diese gibt den Wert 1.2 an ANSI weiter. Die Autorität ANSI weist ihrerseits den Wert 1.2.840 dem Staat USA zu und dieser wiederum die OID 1.2.840.113556 an die Firma Microsoft.

Um für die eigenen Klassen und Attribute OIDs zu erstellen, können Sie entweder selbst OIDs beantragen oder auch selbst OIDs generieren. Das Beantragen eigener OIDs ist ein aufwändiger und teilweise auch kostenpflichtiger Prozess. Im Resource Kit für Windows 2000 befindet sich zum Generieren eigener OIDs das Tool `oidgen.exe`. Mit diesem Programm können Sie eigene OIDs für eigene Objekte innerhalb des von Microsoft bereitgestellten OID-Raums generieren. Sie erhalten zwei Root-OIDs, die Sie für Schemaerweiterungen benutzen können. Diese OIDs sind jedoch nicht öffentlich verwendbar. Rufen Sie das Programm an der Kommandozeile mit `oidgen.exe /?`  auf, um weitere Hinweise zu erhalten.

Auf welche Weise auch immer Sie Ihre OIDs beziehen, so müssen Sie eine verantwortliche Person benennen, die sich um die Vergabe und Zuweisung der OIDs kümmert. In der Regel wird dies der Schema-Administrator sein, der auch für die Bedarfsplanung neuer Klassen und Attribute zuständig ist. Diese Rollen können aber auch getrennt vergeben werden.

24.3 Das Ändern des Schemas

Das Active Directory-Schema kann auf zwei verschiedene Arten geändert werden. Zum einen haben Sie die Möglichkeit, selbst manuell Änderungen vorzunehmen. Eine andere Möglichkeit besteht darin, dass Sie eine Applikation, wie etwa Exchange 2000, installieren, die im Rahmen der Installation das Schema ändert. Die Änderungen am Schema haben immer die folgenden Konsequenzen:

1. Alle globalen Katalogserver der Gesamtstruktur bilden ihren Katalog neu. Dies kann in einer großen Umgebung mehrere Stunden dauern. Verlegen Sie nach Möglichkeit das Ändern des Schemas auf Zeiträume mit geringer Netzwerkauslastung, z.B. in die Nachtstunden oder auf ein Wochenende.
2. Die Änderungen am Schema wirken sich auf die Gesamtstruktur aus, sodass die Änderungen an alle Domänencontroller repliziert werden müssen.

3. Die Änderungen am Schema lassen sich nicht mehr rückgängig machen. Selbst wenn eine Applikation bei ihrer Installation Änderungen am Schema vorgenommen hat, so werden die Änderungen durch die Deinstallation der Applikation nicht entfernt. Sie haben lediglich die Möglichkeit, Klassen und Attribute zu deaktivieren (siehe Kapitel 24.3.3).

Vor dem Ändern des Schemas in der produktiven Umgebung sollten Sie immer ein Backup durchführen. Stellen Sie ebenfalls sicher, dass während der Änderungen am Schema keine Änderungen an anderen Objekten durchgeführt werden. So können Sie sicherstellen, dass keine Änderungen an Objekten verloren gehen, wenn Sie eine autorisierende Wiederherstellung (siehe Kapitel 21.7.2) des Active Directory durchführen müssen, wenn beim Ändern des Schemas Probleme aufgetreten sind.

Idealerweise testen Sie die Änderungen des Schemas zuvor an einer Testdomäne, die nicht mit dem produktiven Netz – auch nicht über Vertrauensstellungen – verbunden ist. Auch wenn eine Applikation das Schema ändert, installieren Sie diese zuerst in der Testdomäne.

Bevor Sie die Änderungen am Schema durchführen, müssen Sie die folgenden Punkte überprüfen und vorbereiten:

1. Der Domänencontroller mit der Betriebsmasterrolle des Schemamasters muss aktiv sein. In Kapitel 11.1.4 wurde erklärt, wie Sie ermitteln können, welcher Domänencontroller diese Rolle innehat. Ist der Schemamaster nicht verfügbar, können Sie dessen Rolle an einen anderen Domänencontroller übertragen. Weitere Hinweise dazu finden Sie in Kapitel 11.1.5. Die Schemaänderungen können immer nur auf dem Domänencontroller durchgeführt werden, der die Betriebsmasterrolle des Schemamasters innehat. Damit ist das Schema geschützt, sodass nicht zur gleichen Zeit von zwei verschiedenen Punkten in modifizierender Weise auf das Schema zugegriffen werden kann.
2. Weiterhin darf das Schema nicht im schreibgeschützten Modus sein. Um den Schreibschutz aufzuheben, öffnen Sie die mmc ACTIVE DIRECTORY-SCHEMA und wählen aus dem Kontextmenü von ACTIVE DIRECTORY-SCHEMA den Eintrag BETRIEBSMASTER. Aktivieren Sie die Checkbox SCHEMA KANN AUF DIESEM DOMÄNENCONTROLLER GEÄNDERT WERDEN. Alternativ dazu können Sie auf dem Domänencontroller auch in der Registry im Schlüssel HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters einen neuen Wert Update-Allowed (REG-DWORD) mit dem Wert 1 erstellen.
3. Zum Ändern des Schemas ist standardmäßig nur die Gruppe „Schema-Admins“ berechtigt. Sie müssen Mitglied dieser Gruppe sein, wenn Sie das Schema ändern, oder eine Applikation installieren, die das Schema ändert. In der mmc ACTIVE DIRECTORY-SCHEMA haben Sie die Möglichkeit, Benutzerkonten Berechtigungen zum Bearbeiten des Schemas zuzuweisen. Wählen Sie hierzu aus dem Kontextmenü des Knotens ACTIVE DIRECTORY-SCHEMA den Eintrag BERECHTIGUNGEN. Auf keinen Fall sollten Sie sich bei der täglichen Arbeit mit einem Benutzerkonto anmelden, das Mitglied der Gruppe „Schema-Admins“ ist. Die Gefahr dabei ist zu groß, dass unbeabsichtigt Änderungen am Schema durchgeführt werden. Nachdem Sie die Änderungen durchgeführt haben, sollten Sie dem Schema seinen Schreibschutz wiedergeben. Deaktivieren Sie dazu einfach wieder die Checkbox SCHEMA KANN AUF DIESEM DOMÄNENCONTROLLER GEÄNDERT WERDEN.

24.3.1 Hinzufügen neuer Klassen und Attribute

Sobald Sie alle eben beschriebenen Schritte vorbereitet haben, können Sie mit dem Erstellen neuer Klassen und Attribute beginnen. Wollen Sie nur neue Klassen oder nur neue Attribute hinzufügen, sind keine weiteren Schritte in der Reihenfolge zu bedenken. Wollen Sie jedoch eine neue Klasse mit neuen Attributen definieren, so müssen Sie folgende Reihenfolge einhalten:

1. Definieren Sie die neuen Attribute.
2. Führen Sie ein Update des Schema-Cache durch (siehe Kapitel 24.2.2).
3. Definieren Sie die neuen Klassen.
4. Fügen Sie den neuen Klassen die Attribute hinzu.
5. Führen Sie nochmals ein Update des Schema-Cache durch.

In unserem Beispiel sollen einige zusätzliche Benutzerinformationen dem Schema hinzugefügt werden. Um über eingesetzte Dienstwagen einen besseren Überblick zu behalten, werden für jeden Mitarbeiter als zusätzliche Attribute das KFZ-Kennzeichen, KFZ-Typ sowie der monatliche Kilometerstand gespeichert. Diese Informationen werden in einer Hilfsklasse DienstwagenBenutzer zur Klasse User hinzugefügt.

1. Um die neuen Attribute zu erstellen, wählen Sie aus dem Kontextmenü der Attribute den Eintrag **ATTRIBUT ERSTELLEN**. Sie erhalten zunächst eine Warnung, dass Schema-Objekte zwar deaktiviert, aber nicht gelöscht werden können und deshalb immer im Schema verbleiben werden.
2. Mit **WEITER** gelangen Sie zum Fenster **NEUES ATTRIBUT ERSTELLEN**. Dort werden für jedes Attribut der gemeinsame Name (CN), der LDAP-Anzeigename, die OID sowie die Syntax festgelegt (siehe Abbildung 24.2).

Abbildung 24.2: Erstellen eines neuen Attributs

Für die drei neuen Attribute werden die folgenden Werte festgelegt:

Name	OID	Syntax
kfzKennzeichen	1.2.840.113556.1.4.7000.141	Groß-/Kleinschreibung beachten
kfzTyp	1.2.840.113556.1.4.7000.142	Groß-/Kleinschreibung nicht beachten
KilometerBis-LetzterMonat	1.2.840.113556.1.4.7000.143	Numerisch

Tabelle 24.4: Beispielwerte für die neuen Attribute

Beim Erstellen eines neuen Attributs müssen Sie die folgenden Attribute (siehe Tabelle 24.4) mit Werten füllen: Gemeinsamer Name (CN), LDAP-Anzeigename (LDAPDisplayName), X500-OID (attributeID), Syntax (attributeSyntax) sowie mehrwertig (isSingleValued). Die folgenden Attribute erhalten ihre Werte automatisch vom Betriebssystem: Schema-ID-GUID, Attribute-Security-GUID, Extended-Chars-Allowed, System-only, NT-Security-Descriptor, Instance-Type und Object-Class.

- 3. Sobald Sie diese neuen Attribute hinzugefügt haben, erscheinen diese in der mmc in der Liste der Attribute. Dort können Sie über die Eigenschaften des Attributs noch weitere Einstellungen vornehmen. Es kann eine Beschreibung angegeben werden, das Attribut kann deaktiviert werden, es kann in den Active Directory-Index (siehe Kapitel 24.1.2) oder den globalen Katalog aufgenommen werden. Zusätzlich können noch der minimale und maximale Bereichswert (rangeUpper und rangeLower) für das Attribut festgelegt werden (siehe Abbildung 24.3).



Abbildung 24.3: Die Eigenschaften eines Attributs

- 4. Nachdem Sie die Attribute erstellt haben und der Schema-Cache aktualisiert worden ist, erstellen Sie nun die neue Hilfsklasse DienstwagenBenutzer. Wählen Sie hierzu aus dem Kontextmenü der Klassen den Eintrag KLASSE ERSTELLEN. Sie erhalten wieder die Warnmeldung, dass die Objekte nur deaktiviert, nicht aber gelöscht werden können. Klicken Sie auf WEITER.
- 5. Sie erhalten das Fenster NEUE SCHEMAKLASSE ERSTELLEN (siehe Abbildung 24.4). Dort werden für die neue Klasse die folgenden Werte (siehe Tabelle 24.5) eingetragen:

Wert	Eingabe
Gemeinsamer Name	DienstwagenBenutzer
LDAP-Anzeigename	dienstwagenBenutzer
OID	1.2.840.113556.1.4.7000.20
Übergeordnete Klasse	Kein Eintrag
Klassentyp	Zusätzliche Klasse

Tabelle 24.5: Beispielwerte für die neue Klasse

Beim Erstellen einer neuen Klasse müssen Sie die folgenden Attribute mit Werten füllen: Gemeinsamer Name (CN), LDAP-Anzeigename (LDAPDisplayName), X500-OID (governsID), übergeordnete Klasse (subClassOf) sowie Klassentyp (objectClassCategory). Die Attribute Schema-ID-GUID, Instance-Type, NT-Security-Descriptor und Object-Class werden automatisch vom Betriebssystem mit Werten gefüllt.



Abbildung 24.4: Erstellen einer neuen Klasse

- Klicken Sie auf WEITER. Sie können nun bereits die verbindlichen und optionalen Attribute für diese Klasse hinzufügen oder dies in einem eigenen späteren Schritt tun (siehe Abbildung 24.5).



Abbildung 24.5: Die Attribute für eine Klasse auswählen

- Wählen Sie aus dem Bereich der verbindlichen Attribute die drei eben erstellten Attribute aus und klicken dann auf FERTIG STELLEN. Die Klasse erscheint in der Liste der vorhandenen Klassen.

Für jede Klasse können auch erweiterte Eigenschaften konfiguriert werden. Die Eigenschaften einer Klasse umfassen vier Registerkarten: ALLGEMEIN, BEZIEHUNG, ATTRIBUTE und SICHERHEITSEINSTELLUNGEN. Unter ALLGEMEIN finden Sie die der Klasse zugewiesenen Werte und können eine Beschreibung hinzufügen sowie die Klasse deaktivieren. Auf der Registerkarte BEZIEHUNG können Sie zusätzliche Erweiterungsklassen bestimmen und erlaubte Oberklassen hinzufügen. Da Sie keinen Wert für die übergeordnete Klasse angegeben haben, ist die Klasse selbst vom Typ top. Um weitere Attribute hinzuzufügen, wählen Sie die Registerkarte ATTRIBUTE. Sie erhalten hier dieselbe Eingabemaske wie in Abbildung 24.5.



Wird ein bestimmtes Attribut aus der Liste der optionalen Attribute (may-Contain) gelöscht, können sämtliche Klassenobjekte ungültig werden, die dieses Attribut in ihrer Klassendefinition enthalten. Das Objekt wird vom Active Directory als ungültig erklärt, aber dennoch nicht gelöscht. Es wird lediglich dafür gesorgt, dass keine Konflikte im Schema entstehen.

Unter SICHERHEITSEINSTELLUNGEN werden die Berechtigungen für das Klassenobjekt festgelegt. Diese Berechtigungen werden in der Access Control List des Klassenobjekts gespeichert.

- Schließlich müssen Sie noch die neue Hilfsklasse der Klasse USER hinzufügen. Öffnen Sie dazu die Eigenschaften der Klasse User und wählen die Registerkarte BEZIEHUNG. Im Bereich ERWEITERUNGSKLASSEN fügen Sie die neue Klasse hinzu (siehe Abbildung 24.6).



Abbildung 24.6: Hinzufügen von Erweiterungsklassen

Damit ist das Erstellen neuer Klassen und Attribute abgeschlossen. Um die neuen Werte jedoch anzeigen zu können, müssen Sie die Ansicht der mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER oder die Shell-Erweiterungen bearbeiten. Diese Aufgaben müssen per Skript erledigt werden. Die Anleitungen dazu finden Sie in Kapitel 32.4.

24.3.2 Namensregeln für Schema-Objekte

Bei der Namensgebung für die Klassen und Attribute müssen einige Regeln eingehalten werden. Diese Regeln gelten für den LDAP-Anzeigenamen (ldapDisplayName) sowie den allgemeinen Namen. In der mmc ACTIVE DIRECTORY-SCHEMA wird Ihnen für jedes Objekt der eindeutige LDAP-Anzeigename gezeigt. Dieser kann auch verwendet werden, um über ADSI-Skripte auf ein Objekt zuzugreifen. Alle LDAP-Anzeigenamen umfassen mindestens zwei Wörter. Dabei wird das erste Wort in Kleinbuchstaben angegeben, während alle folgenden Wörter mit einem Großbuchstaben beginnen müssen, z.B. domainPolicy oder licensingSiteSettings. Der LDAP-Anzeigename darf keine Leerzeichen enthalten.

Der allgemeine Name entspricht dem LDAP-Anzeigenamen, allerdings wird eine benutzerfreundlichere Schreibweise benutzt. Der allgemeine Name für die beiden eben erwähnten Klassen lautet Domain-Policy und Licensing-Site-Settings. Auch über den allgemeinen Namen kann ein Zugriff auf die Objekte per Skript erfolgen. Die dritte Möglichkeit für den Objektzugriff ist die eindeutige OID eines Objekts.

24.3.3 Klassen- und Attributprüfung bei Schemaänderungen

Jedes Mal, wenn Sie eine neue Klasse oder ein neues Attribut im Schema erstellen, wird in einem ersten Schritt das Schema geändert. In einem zweiten Schritt wird ein festgelegter Prüfmechanismus vom Active Directory in Gang gesetzt, der die Änderungen auf ihre Gültigkeit hin überprüft. Verläuft die Prüfung erfolgreich, wird die Änderung endgültig übernommen. Derselbe Prüfmechanismus wird auch durchgeführt, wenn die Installationsroutine einer Applikation Änderungen am Schema vorgenommen hat. Die Prüfung wird an einer fest definierten Reihe von Attributen durchgeführt. Die überprüften Attribute sind unterschiedlich, je nachdem, ob Sie eine Klasse oder ein Attribut neu erstellt haben. Dabei werden an den Klassen folgende Gültigkeitsprüfungen vollzogen:

1. Die Attribute `ldapDisplayName` und `governsID` müssen im gesamten Active Directory eindeutig sein.
2. Sämtliche Klassen, die in den Attributen `mustContain`, `mayContain`, `systemMustContain` und `systemMayContain` sowie `auxiliaryClass`, `systemAuxiliaryClass`, `possSuperiors` und `systemPossSuperiors` definiert sind, müssen bereits vorhanden sein.
3. Das Attribut `rdnAttId` muss eine Unicode-Zeichenkette als Syntax definiert haben.
4. Die Einträge in `subClassOf` werden überprüft, ob kein Verstoß gegen X.500-Spezifikationen begangen wurde.

Bei neu erstellten oder geänderten Attributen werden die folgenden Merkmale auf ihre Gültigkeit hin untersucht:

1. Die Attribute `ldapDisplayName`, `schemaIDGUID`, `attributeID` sowie `mapID` müssen im gesamten Active Directory eindeutig sein.
2. Die Werte für `attributeSyntax` und `omSyntax` müssen zusammenpassen.
3. Die Werte für `rangeUpper` und `rangeLower` müssen so gesetzt sein, dass der Wert für `rangeUpper` größer ist als der für `rangeLower`.

24.3.4 Deaktivieren von Klassen und Attributen

Alle Schema-Objekte, die manuell oder durch eine Applikation zum Standardschema hinzugefügt werden, bleiben permanent in diesem enthalten. Sie können weder Klassen noch Attribute aus dem Schema löschen. Hierbei handelt es sich um einen Schutzmechanismus. Beim Löschen würden auch alle Instanzen der Klasse oder des Attributs gelöscht werden, sodass unvorhersehbare Probleme auftreten. Die einzige Alternative zum Löschen ist das Deaktivieren bestehender Klassen und Attribute. In diesem Fall werden die bestehenden Instanzen der deaktivierten Klasse nicht in ihrer Funktion beeinträchtigt. Es wird lediglich verhindert, dass neue Instanzen dieser Klasse angelegt werden können. Klassen und Attribute werden als deaktiviert gekennzeichnet, wenn der Wert `isDefunct` im `attributeSchema` oder `classSchema` auf `TRUE` gesetzt ist. Um die Klasse oder das Objekt wieder zu aktivieren, setzen Sie den `isDefunct`-Wert auf `FALSE`. Das (De-)Aktivieren von Klassen und Attributen können Sie auch über die GUI der mmc vornehmen. In den Eigenschaften der Klassen und Attribute können Sie das entsprechende Häkchen setzen. Dabei wird der Wert `TRUE` oder `FALSE` automatisch zugewiesen. Allerdings können keine Klassen und Attribute der Kategorie 1 deaktiviert werden. Es können auch keine Attribute deaktiviert werden, die zu einer Klasse gehören, die nicht auch

deaktiviert ist. Enthält die Klasse einen mustHave-Verweis auf ein deaktiviertes Attribut, so kann diese Klasse keine neuen Instanzen mehr anlegen.

Das Deaktivieren von Schema-Objekten kann aus verschiedenen Gründen sinnvoll sein. Auf jeden Fall müssen Sie zuvor das Deaktivieren in einer Testumgebung nachstellen, um so unvorhersehbare Probleme von der produktiven Umgebung abzuwenden. Wenn Sie eine bestimmte Schemaerweiterung nicht mehr benötigen und diese Deaktivierung keine Probleme nach sich zieht, können Sie diese selbst in einer produktiven Umgebung einfach deaktivieren. Sollten Sie diese Erweiterung später doch wieder benötigen oder auch aus Versehen ein falsches Schema-Objekt deaktiviert haben, so können Sie dieses ebenso einfach auch wieder aktivieren. Wäre das Objekt gelöscht, hätten Sie nun möglicherweise ein ernsthaftes Problem. Um negative Auswirkungen der Deaktivierung so gering wie möglich zu halten, sollten Sie aus einer deaktivierten Klasse alle Werte des Attributs mayHave löschen sowie die Größe der mustHave Attributwerte beschränken. Zusätzlich sollten alle deaktivierten Attribute aus dem globalen Katalog gelöscht und auch von der Indexierung ausgeschlossen werden (siehe Kapitel 24.1.2).

Eine wichtige Neuerung beim Deaktivieren von Klassen bringt der Windows Server 2003 mit sich. Während unter Windows 2000 auch deaktivierte Objekte in der mmc ACTIVE DIRECTORY-SCHEMA sichtbar waren und deren isDefunct-Attribut dort wieder auf FALSE gesetzt werden konnte, sind nun die deaktivierten Objekte dort nicht mehr sichtbar. Dies heißt jedoch nicht, dass die deaktivierte Klasse oder das deaktivierte Attribut nicht wieder aktiviert werden können. Sie müssen hierzu jedoch den kleinen Umweg über ein LDIF-Skript nehmen. Das Dateiformat LDIF sowie LDIF-Skripte lernen Sie in Kapitel 25 kennen.

Allerdings bringt dieser Mechanismus des Windows Server 2003 den Vorteil, dass Sie die Werte ldapDisplayName, schemaIDGUID, OID sowie mapID einer deaktivierten Klasse oder eines Attributs sofort neu vergeben können. Damit wird das deaktivierte Objekt komplett ersetzt. Unter Windows 2000 mussten Sie komplett neue Werte festlegen, um ein deaktiviertes Attribut wieder zu erstellen. Soll unter Windows 2003 das deaktivierte Objekt doch wieder aktiviert werden, so müssen Sie nicht nur den isDefunct-Wert umsetzen, sondern auch den RDN-Wert (relativ definierter Name) ändern. Andernfalls würden zwei Objekte, nämlich das ursprünglich deaktivierte sowie das aktivierte, mit demselben RDN innerhalb desselben Containers existieren, was eindeutig gegen die Namenskonvention verstößt.

24.3.5 Dokumentieren der Änderungen

Neben den Änderungen, die Sie selbst am Schema vornehmen, dürfen auch nicht die Modifikationen verschwiegen werden, die bei der Installation einer Applikation vorgenommen werden können. Ein klassisches Beispiel ist die Installation des Exchange 2000 Servers, der weitgehende Schemaänderungen vornimmt. Gerade bei den Änderungen, die von einer Applikation durchgeführt werden, stellt sich oftmals die Frage, was genau geändert worden ist. Oftmals sind die Applikationen selbst nicht sehr auskunftsfreudig, welche Schemaänderungen durch sie ausgelöst wurden.

Um an einem unbekannten oder unsauber dokumentierten Schema zu ermitteln, ob Änderungen vorgenommen worden sind, können Sie z.B. das Programm LDP (siehe Kapitel 23.1.14) benutzen. Bei allen Schema-Objekten sollte der Wert whenChanged das

Datum der Forest-Erstellung (whenCreated) tragen. Treten Abweichungen auf, wurden Änderungen vorgenommen. Leider ist aber auf diese Weise nicht zu ermitteln, von welcher Applikation diese Änderungen vorgenommen wurden.

Komfortabler ist das Programm *ERDisk* for Active Directory von Aelita Software. Hiermit können Sie direkt nach der Installation einer Applikation ermitteln, ob und, wenn ja, welche Schemaänderungen vorgenommen worden sind. Stellen Sie hierzu einen eigenen Domänencontroller bereit, der nicht mit dem produktiven Netzwerk verbunden ist und auch keine Vertrauensstellungen zu diesem besitzen darf. Führen Sie mit *ERDisk* zunächst ein Backup des Systemstatus durch. Installieren Sie dann die Applikation. Danach lassen Sie den Online Restore Wizard von *ERDisk* im Vergleichsmodus laufen. Dieser Wizard generiert einen Report, der alle Änderungen am Schema und an den Active Directory-Objekten zwischen dem gesicherten Zustand sowie dem aktuellen Zustand auflistet.

Eine weitere, wenn auch aufwändigere Alternative besteht darin, die Änderungen am Schema über ein VBScript auszulesen.

24.4 Dokumentation von Änderungen mit Schemadocfile.exe

Dieses Kapitel wendet sich hauptsächlich an Anwendungsentwickler, deren Programme bei der Installation Modifikationen am Active Directory-Schema vornehmen. Um für eigenentwickelte Applikationen übersichtlich darzustellen, welche Änderungen diese am Schema vornehmen, sollten Sie das Programm *Schemadocfile.exe* benutzen. Dieses Programm wurde von Microsoft herausgegeben und kann unter folgender Adresse heruntergeladen werden:

<http://msdn.microsoft.com/downloads/default.asp?URL=/downloads/sample.asp?url=/msdn-files/027/001/989/msdncompositedoc.xml>

Schemadocfile durchsucht das Active Directory nach einem bestimmten Präfix. Um ein gültiges Präfix zu erhalten, müssen Sie sich auf der Webseite für Active Directory Naming Registration registrieren (<http://msdn.microsoft.com/certification/ADReg.asp>). Diese Registrierung ist zwingend erforderlich, wenn eine selbst geschriebene Applikation das Schema modifiziert und die Zertifizierung für das Windows 2000 Logo-Programm bestehen soll. Für jede Klasse und jedes Attribut, das das Präfix enthält, werden die Änderungen in eine XML-Datei kopiert.

Bevor Sie mit dem Programm arbeiten können, müssen Sie die Datei *xmlschema.dll* ins Verzeichnis %SYSTEMROOT%\SYSTEM32 kopieren und mit dem Befehl `regsvr32 xmlschema.dll`  registrieren.

1. Beim Programmstart von *Schemadocfile* müssen Sie die folgenden Angaben machen (siehe Abbildung 24.7): DIRECTORY PATH gibt den Pfad zum Schema an, z.B. LDAP://CN=Schema,CN=Configuration,DC=Firma,DC=DE. Unter NAMING PREFIX tragen Sie das registrierte Präfix ein, das den Klassen und Attributen vorangehen soll, die im Schema geändert worden sind. Bestimmen Sie auch den Pfad der XML-Ausgabedatei (OUTPUT FILE). Weiterhin müssen Sie ein gültiges Benutzerkonto für die Domäne angeben. Klicken Sie dann auf NEXT.

The screenshot shows the 'Schema Documentation Program' dialog box. It has a title bar with 'Schema Documentation Program' and standard window controls. The dialog contains several input fields: 'Directory path' with the value 'LDAP://CN=Schemas,CN=Configuration,DC=', 'Naming profile' with the value 'Firma', and 'Output file' with the value 'c:\test.xml'. Below these is a 'Credentials' section with 'User name' set to 'Administrator', an empty 'Password' field, and 'Domain' set to 'firma.de'. At the bottom are 'Exit' and '< Next >' buttons.

Abbildung 24.7: Dokumentation von Schemaänderungen mit Schemadocfile.exe

2. In dem nächsten Fenster **VENDOR INFORMATION** (siehe Abbildung 24.8) können Sie einige Angaben über Ihr Unternehmen eintragen. Diese Daten werden in einer Konfigurationsdatei gespeichert, sodass der Endbenutzer die Möglichkeit hat, mit Ihnen Kontakt aufzunehmen, wenn Fragen zu den durch Ihre Applikation durchgeführten Schemaänderungen auftreten sollten. Klicken Sie dann auf **NEXT**.

The screenshot shows the 'Vendor Information' dialog box. It has a title bar with 'Vendor Information' and standard window controls. The dialog contains several input fields for company information: 'Name', 'Address', 'City', 'State/Province', 'Postal code', 'Country', 'Telephone', and 'Support email'. At the bottom are 'Exit', '< Prev', and 'Next >' buttons.

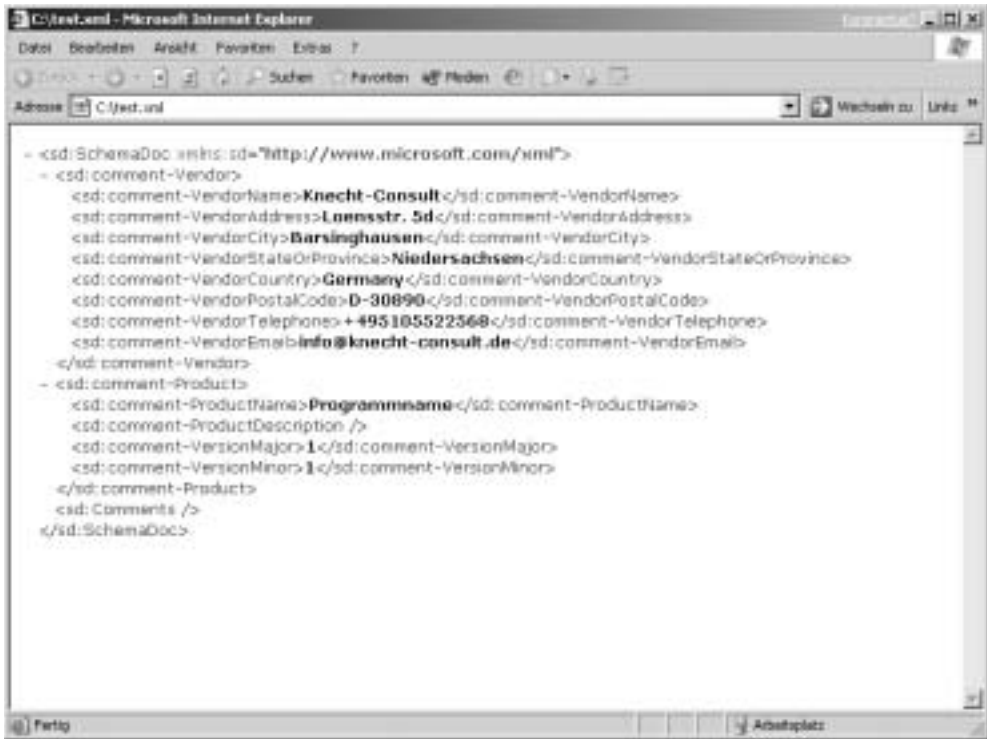
Abbildung 24.8: Angabe von Herstellerinformationen

3. Schließlich geben Sie im Fenster **PRODUCT INFORMATION** den Namen, eine Beschreibung sowie die Versionsnummer der Applikation an (siehe Abbildung 24.9). Klicken Sie dann auf **EXECUTE**. Damit wird die XML-Ausgabedatei erstellt.



Abbildung 24.9: Eingabe von Produktinformationen

Die XML-Ausgabedatei ist in insgesamt vier Sektionen gegliedert (siehe Abbildung 24.10).



```
<?xml version='1.0' encoding='utf-8' ?>
<!-- Schemadoc -->
<!-- Vendor -->
<!-- Product -->
<!-- Comments -->
```

Abbildung 24.10: Die XML-Ausgabedatei von Schemadocfile

In den Bereichen Vendor und Product befinden sich die Informationen, die Sie eben eingegeben haben. In den Sektionen Class und Attribute finden Sie eine Auflistung aller Klassen und Attribute, die mit dem festgelegten Präfix übereinstimmen. Dazu werden auch die Eigenschaften der Klassen und Attribute angegeben. Sämtliche Klassen und Attribute werden unter dem LDAP-Anzeigenamen aufgeführt. Zu sämtlichen Klassen und Attributen können Sie in der XML-Datei zusätzliche Kommentare einpflegen, die verdeutlichen, aus welchem Grund bestimmte Objekte geändert worden sind.

24.5 Schemaänderungen als potenzielle Fehlerquelle

So komfortabel und sinnvoll eine Änderung am Schema auch sein mag, so darf jedoch nicht vergessen werden, wie schnell Ihr Active Directory dadurch auch dauerhaften Schaden nehmen kann.

Wie bereits erwähnt, soll durch die Betriebsmasterrolle des Schemamasters verhindert werden, dass zeitgleich von mehreren Personen Änderungen am Schema vorgenommen werden. Dieser Schutzmechanismus greift jedoch nicht mehr, wenn mehrere Mitglieder, die zur Gruppe der Schema-Administratoren gehören, gleichzeitig von verschiedenen Orten aus Applikationen ausführen, die das Schema verändern. Dabei verbindet sich jede Applikation mit dem Schemamaster. Wird gerade auf das Schema in ändernder Weise zugegriffen, so wird ein Systemattribut gesetzt. Dieses Attribut wird aber wieder entfernt, sobald der Schreibvorgang beendet ist. Und genau hier liegt das Problem: Erfolgt bei einer Installation oder einer Skriptausführung eine Änderung des Schemas, so dauert der entsprechende Schreibvorgang nur kurze Zeit. Hat beispielsweise gerade eine Installation von Computer A ausgehend eine Änderung vorgenommen, wird das Systemattribut wieder entfernt. Damit hat ein Skript, das von Computer B ausgeführt wird, freie Bahn, um die nächste Änderung durchzuführen. Danach greift wieder Computer A auf das Schema zu und möchte die nächste Änderung schreiben. Dabei kann es passieren, dass die Änderung von Computer B aus schwerwiegende Fehler verursachen kann, da sie mit der neuerlichen Änderung von Computer A inkompatibel ist. Eine Fehlermeldung erscheint auch, wenn von beiden Computern gleichzeitig der schreibende Zugriff erfolgt. Eine der beiden Applikationen muss dabei neu gestartet werden. Abhilfe schafft hier nur eine Absprache und Koordination der Aufgaben für die Schema-Administratoren. Erstellen Sie Zeitpläne, wann welcher Administrator Änderungen am Schema vornehmen darf und wann nicht. Relativ unkritisch ist dieses Problem, wenn Sie nur über einen Schema-Administrator verfügen.

Ein Problem kann auch entstehen, wenn der Schema-Betriebsmaster ausfällt und Sie sofort einen neuen Domänencontroller auswählen, der die Rolle übernehmen soll. War der Ausfall des alten Betriebsmasters nur temporär und wird dieser wieder online geschaltet, so haben Sie zwei Schemamaster im Netzwerk. Beide Schemamaster sind dabei der Ansicht, dass sie Änderungen am Schema zulassen dürfen. Dabei können widersprüchliche Schemaeinstellungen in der Gesamtstruktur repliziert werden. Sie sollten also immer prüfen, ob der alte Schemamaster kurzfristig, längerfristig oder für immer ausfallen wird. Lediglich im letzten Fall können Sie ohne weitere Überlegungen

einen neuen Schemamaster einrichten. Fällt der Schemamaster nur für einen begrenzten Zeitraum aus, so sollten Sie überlegen, ob Sie für die Zwischenzeit wirklich einen neuen Schemamaster benötigen oder ob Sie weitere Änderungen am Schema erst dann wieder vornehmen, wenn der alte Master wieder im Netzwerk verfügbar ist.

Weitere große Probleme können entstehen, wenn Sie unbedacht Klassen und Attribute aus dem Schema löschen. Sobald verbindliche und /oder optionale Attribute aus einer Klasse entfernt werden, kann es passieren, dass Instanzen dieser Klasse nicht mehr existierende Attribute besitzen. Denselben Effekt können Sie auch erzielen, wenn Sie von bestehenden Klassen Erweiterungsklassen entfernen. Ebenso sollten Sie auch Vorsicht walten lassen, wenn Sie übergeordnete Klassen entfernen. Ist die übergeordnete Klasse entfernt, sind damit alle Instanzen dieser Klasse ungültig.

25 Import und Export der Active Directory-Umgebung

In diesem Kapitel wird Ihnen der Import und Export von Active Directory-Objekten vorgestellt. Dieser Austausch von Daten findet in der Regel dann statt, wenn eine große Menge an Verzeichnisdaten mit einem Schlag geändert werden soll. Die Grundlage dazu ist ein Einblick in LDIF. Dies ist das Format, in dem die Im- und Exportdateien erstellt werden. Ein umfangreiches nützliches Hilfsmittel für den Im- und Export ist das Kommandozeilenprogramm *LDIFDE*, dessen Handhabung Sie ebenfalls kennen lernen werden.

25.1 Das Format LDIF und LDIF-Dateien

Die Abkürzung LDIF steht für LDAP Data Interchange Format. LDIF ist ein Standardformat für Dateien in LDAP-konformen Verzeichnissen. In diesem Standard ist festgelegt, wie der Import und Export von Dateien zwischen LDAP-Verzeichnisservern erfolgt. LDIF-Dateien vereinfachen das Management von großen Mengen an Daten, die auf einen Schlag im Verzeichnis geändert werden müssen. Das LDIF-Format ist dafür optimiert, Verzeichnisinformationen oder die Beschreibung von Änderungen an Verzeichnisdaten zwischen LDAP-Servern auszutauschen.

Eine LDIF-Datei enthält diverse Einträge zu den Objekten des Verzeichnisses. Für jedes Objekt gibt es dabei eine Reihe von Einträgen. Jeder Eintrag besteht aus einer Zeile, die jeweils den Wert für eine Eigenschaft des Objekts enthält. Anstelle der Einträge kann eine LDIF-Datei auch Aufzeichnungen über Änderungen an bestimmten Objekten enthalten. Allerdings kann eine LDIF-Datei entweder nur Einträge oder nur Änderungen enthalten. Eine LDIF-Datei kann mit jedem beliebigen Texteditor geöffnet werden. Es handelt sich dabei um eine Standard-ASCII-Textdatei.

Um sich eine bessere Vorstellung von einer LDIF-Datei machen zu können, sehen Sie in Abbildung 25.1 einen Ausschnitt aus einer solchen Datei. In der abgebildeten Sektion sind Eigenschaften und Werte eines Drucker-Objekts angegeben. Sie finden dort Werte wie den definierten Namen (DN) sowie den Common Name (CN), die Objektkategorie, USN-Werte, die Treiberversion, Angaben zur Druckauflösung usw. Kurz gesagt enthält die LDIF-Datei die Werte aller Eigenschaften des Drucker-Objekts, die im Schema für diese Objektklasse definiert sind.

Eine LDIF-Datei kann neben ASCII-Daten auch Binärdaten enthalten. Allerdings können diese nur nach der Base64-Kodierung kodiert enthalten sein. Base64-kodierte Daten werden in der Datei durch zwei aufeinander folgende Doppelpunkte gekennzeichnet (::). Ein Beispiel für Binärdaten als Eigenschaftswert ist ein Foto im JPEG-Format, das Sie als zusätzliche Information dem Benutzerobjekt mitgeben. Dieses sieht in einer LDIF-Datei folgendermaßen aus: `jpegPhoto:: <kodierte Daten>`. Diese Kodierung wird bei allen Eigenschaftswerten verwendet, die keine ASCII-Daten enthalten oder deren Wert mit

einem Leerzeichen bzw. Semikolon (;) beginnt. Weitere Informationen zur Base64-Kodierung finden Sie in RFC 2045 in der Sektion 6.8.

```
dn: cn=HIPPOKRATES-Epson EPL-N1200,cn=HIPPOKRATES,ou=Domain Controllers,dc=firma,dc=de
objectClass: top
objectClass: leaf
objectClass: connectionPoint
objectClass: printQueue
objectCategory: CN=Print-Queue,CN=Schema,CN=Configuration,DC=firma,DC=de
instanceType: 4
cn: HIPPOKRATES-Epson EPL-N1200
versionNumber: 4
ucnName: \\hippokrates.firma.de\Epson EPL-N1200
shortServerName: HIPPOKRATES
serverName: hippokrates.firma.de
printerName: Epson EPL-N1200
url: http://hippokrates.firma.de/Epson
whenCreated: 23.08.2002 09:49:25
whenChanged: 23.08.2002 09:49:25
ucnCreated: 4175
ucnChanged: 4177
name: HIPPOKRATES-Epson EPL-N1200
distinguishedName: CN=HIPPOKRATES-Epson EPL-N1200,CN=HIPPOKRATES,OU=Domain Controllers,DC=firma,DC=de
flags: 0
portName: LPT1
driverName: Epson EPL-N1200/A4 EPSOMScript
priority: 1
printStartTime: 0
printEndTime: 0
printBinNames: Option Lower Cassette2
printBinNames: Option Lower Cassette1
printBinNames: HP Tray
printBinNames: Manual Feed
printBinNames: Printer's Automatic
printBinNames: Automatisch eusehnen
printMaxResolutionSupported: 600
printOrientationsSupported: LANDSCAPE
printOrientationsSupported: PORTRAIT
printCollate: True
printColor: False
printLanguage: PostScript
printShareName: Epson
printSpooling: PrintAfterSpooled
printKeepPrintedJobs: False
driverVersion: 1025
```

Abbildung 25.1: Auszug aus einer LDIF-Datei

Der Standardmodus für den Export von LDIF-Dateien ist ANSI. Die Unicode-Inhalte werden automatisch in das Base 64-Format kodiert. Wollen Sie eine Datei im Unicode-Format exportieren, so müssen Sie LDIFDE mit dem Parameter `-u` (siehe Tabelle 25.1) verwenden.

25.2 Das Tool LDIFDE

Nachdem Sie nun bereits eine LDIF-Datei gesehen haben, wird Ihnen das Tool *LDIFDE* vorgestellt, mit dem Sie diese Dateien erstellen können. *LDIFDE* (LDAP Data Interchange Format Data Exchange) ist ein Kommandozeilenprogramm, mit dem Sie Objekte aus dem Active Directory exportieren und auch wieder importieren können. Dieses Tool kooperiert mit dem LDIF-Dateiformat. Dabei werden die Daten als LDIF-Dateien exportiert und Daten aus diesem Format wieder importiert. Zusätzlich können bestehende Objekte auch modifiziert werden. Dies ist der große Vorteil von *LDIFDE* gegenüber dem Programm *CSVDE*. Mit *CSVDE* können Sie zwar auch Daten im kommaseparierten For-

mat im- und exportieren, aber es können keine bestehenden Objekte geändert werden, lediglich das Hinzufügen neuer Objekte ist möglich.

LDIFDE eignet sich ideal zur Verwendung in Batchdateien, wenn eine große Anzahl von Objekten neu erstellt oder bearbeitet werden soll. Außerdem können Sie mit LDIFDE Filter setzen, um nur nach bestimmten Verzeichnisobjekten zu suchen und diese anzuzeigen.

Das Programm ist standardmäßig auf allen Windows 2000- und Windows 2003-Domänencontrollern installiert. Sie können das Programm aber auch auf Windows 2000- und XP-Clients kopieren und eine Verbindung zum Domänencontroller herstellen.

LDIFDE bietet Ihnen eine Reihe von Parametern. Deren Bedeutung wird Ihnen in Tabelle 25.1 erklärt, bevor in den nächsten Kapiteln einige praktische Beispiele für den Einsatz des Programms folgen.

LDIFDE-Parameter	Beschreibung
Generelle Parameter	
-i	Schaltet vom standardmäßigen Export- in den Importmodus.
-f Dateiname	Dateiname der Im- oder Exportdatei.
-s Servername	Name des Servers, mit dem die Verbindung erfolgen soll. Standard ist der Domänencontroller der aktuellen Domäne. In diesem Fall muss der Parameter nicht gesetzt werden.
-c fromDN toDN	Ersetzt alle vorkommenden Einträge von vonDN durch zuDN. Wird benutzt, wenn die Daten in eine andere Domäne importiert werden und dabei der DN der Exportdomäne durch den DN der Importdomäne ersetzt werden muss.
-v	Schaltet den ausführlichen Modus ein.
-j	Pfad zur Protokolldatei
-t	Angabe des Ports. Muss nur angegeben werden, wenn nicht der Standardport 389 benutzt werden soll.
-u	Benutzt das Unicode-Format.
Exportspezifische Parameter	
-d RootDN	Stamm der LDAP-Suche. Ist nichts definiert, wird der Namenskontext benutzt.
-r Filter	Gibt den LDAP-Suchfilter an. Der Standardfilter lautet: "(object-Class=*)"
-p SearchScope	Gibt den Suchbereich an. Gültige Werte sind subtree (durchsucht alles unterhalb des unter -d angegebenen Startpunkts), base (sucht nur im angegebenen Startpunkt) und onelevel (sucht nur einen Level unter dem Startpunkt).
-l list	Listet die Attribute kommasepariert auf, nach denen bei der LDAP-Suche gesucht werden soll.

LDIFDE-Parameter	Beschreibung
-o list	Listet die Attribute kommasepariert auf, die bei dem Export ausgelassen werden sollen. Diese Option ist sinnvoll, wenn Sie die Objekte in einen anderen Verzeichnisdienst importieren möchten, der nicht alle Active Directory-Attribute unterstützt.
-g	Deaktivierung der seitenweisen Suche.
-m	Übergeht eine Reihe sicherheitsbezogener Attribute wie Object-GUID, ObjectSID, pwdLastSet oder samAccountType.
-n	Es werden keine Binärwerte exportiert.
Importspezifische Parameter	
-k	Die Fehler „Beschränkungsverletzung“ sowie „Objekt ist bereits vorhanden“ werden beim Import ignoriert.
-y	Der Import wird mit der Option Lazy Commit ausgeführt, um eine bessere Systemleistung zu erzielen.
Parameter zur Verbindungsherstellung	
Werden keine Parameter angegeben, wird das aktuell angemeldete Benutzerkonto für die Verbindungsherstellung benutzt.	
-a	-a DN des Benutzers [Passwort *] führt eine einfache Authentifizierung durch.
-b	-b Benutzername Domäne [Passwort *] stellt die Verbindung über die SSPI-Bindungsmethode her.

Tabelle 25.1: Die Parameter für LDIFDE

Um die aktuelle Domäne vollständig zu exportieren, verwenden Sie den Befehl `ldifde -f Export.ldf` .

Um einen vollständigen Import durchzuführen, benutzen Sie den Befehl `ldif -i -f Import.ldf` .

Weitere ausführliche Beispiele für verschiedene LDIFDE-Einsatzgebiete finden Sie in den folgenden Kapiteln.

25.2.1 Im- und Export von Active Directory-Objekten zwischen Domänen

Im folgenden Beispiel werden OUs und Benutzerkonten zwischen zwei Domänen ausgetauscht. Die Domäne, aus der die Daten exportiert werden, heißt *firma.de*, die Domäne, die die Objekte importiert, *filiale.de*.

1. Hierzu verwenden Sie folgenden Befehl:

```
ldifde -f Ouexport.ldf -s Hippokrates -d "dc=firma,dc=de" -p subtree  
-r "(objectClass=organizationalUnit)" -l "cn,objectclass,ou" 
```

Über den Parameter `-p` geben Sie den Bereich an, in dem die Objekte gesucht werden sollen. OUs befinden sich immer in dem Subtree einer Domäne. Über `-r` setzen Sie

einen Filter, der in den Subtrees lediglich nach Objekten sucht, deren Objektklasse `organizationalUnit` lautet. Dabei werden alle OUs bis auf die spezielle OU `Domain-controllers` exportiert. Der Parameter `-l` listet die Attribute auf, nach denen innerhalb der angegebenen Objekte gesucht werden soll.

2. Nach dem Export der OUs müssen Sie nun die Benutzerkonten aus der Domäne *firma.de* exportieren. Dazu verwenden Sie den folgenden Befehl:

```
ldifde -f Userexport.ldf -s Hippokrates -d "dc=firma,dc=de" -p subtree
-r "(&(ObjectCategory=person)(ObjectClass=User)(givenname=*))" -l
"cn,givenName,objectClass,sAMAccountName" ↵
```

Die Parameter werden hier wie bei dem Export der OUs verwendet. Der Filter über `-r` sucht nun nach mehreren Objekten. Wie Sie sehen, kann der Filter dabei auch Wildcards verwenden. Vordefinierte Benutzerkonten wie z.B. der Administrator besitzen keinen `givenName`. Also werden bei Verwendung des hier gesetzten Filters die vordefinierten Benutzerkonten nicht exportiert. Außerdem können Sie mit *LDIFDE* nicht die Passwörter der Benutzerkonten exportieren. Unter `-l` werden wiederum die Attribute aufgelistet, nach denen gesucht werden soll. In jedem Fall sind hier auch die Attribute `objectClass` sowie `sAMAccountName` zwingend erforderlich. Ansonsten wird der Import der Objekte fehlschlagen. Wenn Sie nicht sicher sind, welche Attribute zu setzen sind, können Sie im Zweifelsfall lieber einige Attribute zu viel angeben.

3. Nach den beiden Exportvorgängen geht es nun an den Import. Hierbei ist zu beachten, dass Sie immer erst die übergeordneten Container, in diesem Fall also die OUs, importieren, bevor Sie die darin befindlichen Untercontainer oder Endknotenobjekte, hier also die Benutzer, importieren können.

Öffnen Sie nun mit einem beliebigen Texteditor die Datei *Ouexport.ldf*. In dieser Datei wird nun der Name der Export-Domäne *firma.de* mit dem der Import-Domäne *filiale.de* ersetzt. Über die Funktion `FINDEN UND ERSETZEN` des Texteditors suchen Sie nach dem String *firma.de* und ersetzen ihn durch *filiale.de*. Speichern Sie anschließend die Datei.

4. An der Kommandozeile geben Sie nun folgenden Befehl ein:

```
Ldifde -i -f Ouexport.ldf -s Sokrates ↵
```

Der Parameter `-s` gibt hier den Servernamen eines Domänencontrollers in der Domäne *filiale.de* an. Sie erhalten dann eine Statusmeldung, wie viele Einträge insgesamt abgearbeitet wurden und ob der Vorgang erfolgreich abgeschlossen wurde.

5. Verfahren Sie nun analog mit der Datei *Userexport* und ersetzen in dieser auch den Namen der Export-Domäne durch den Namen der Import-Domäne. An der Eingabeaufforderung geben Sie dann den Befehl

```
Ldifde -i -f Userexport.ldf -s Sokrates ↵
```

ein. Überprüfen Sie an der mmc `ACTIVE DIRECTORY-BENUTZER UND -COMPUTER`, ob alle Benutzer korrekt importiert worden sind. Dabei werden Sie feststellen, dass die neuen Benutzerkonten zunächst deaktiviert sind und kein Passwort gesetzt ist, sondern die Checkbox `BENUTZER MUSS KENNWORT BEI DER NÄCHSTEN ANMELDUNG ÄNDERN` aktiviert ist. Dies liegt darin begründet, dass *LDIFDE* aus Sicherheitsgründen die Passwörter nicht exportieren kann.

25.2.2 Export von Objekten aus einer Gesamtstruktur

Im letzten Beispiel haben Sie gesehen, wie man Objekte aus einer einzelnen Domäne exportiert. Nehmen wir aber nun an, dass Sie Objekte aus allen Domänen einer Gesamtstruktur exportieren müssen. Sie könnten zwar auch das eben beschriebene Verfahren anwenden und auf diese Weise eine Domäne nach der anderen exportieren, aber diese Methode kann sehr langwierig werden. Deshalb können Sie die LDAP-Abfrage auch am globalen Katalog durchführen.

1. Hierbei müssen Sie sicherstellen, dass Sie die Verbindung für die LDAP-Abfrage mit dem globalen Katalogserver der Domäne herstellen. Um zu ermitteln, ob ein Domänencontroller die Rolle des Katalogservers innehat, sehen Sie in der mmc ACTIVE DIRECTORY-STANDORTE UND -DIENSTE in den Eigenschaften der NTDS-Settings nach. Zusätzlich müssen Sie den Port des globalen Katalogservers (3268) angeben.
2. Um beispielsweise die Organisationseinheiten der kompletten Gesamtstruktur zu exportieren, verwenden Sie folgenden Befehl:

```
Ldifde -f Ouexport.ldf -s Archimedes -t 3268 -d "dc=firma,dc=de", -p subtree -r "(objectClass=OrganizationalUnit)" -l "cn,objectclass,ou"
```



Sie sehen, dass sich der Exportbefehl gegenüber dem ersten Beispiel nur geringfügig unterscheidet. Es ist jetzt statt des Domänencontrollers der globale Katalogserver angegeben sowie mit `-t` zusätzlich der Port 3268.

25.2.3 Ändern von Benutzerattributen

Nachdem Sie erfahren haben, wie man mit *LDIFDE* Objekte ex- und importiert, zeigt Ihnen dieses Kapitel, wie Sie die LDIF-Dateien bearbeiten können und welche Punkte dabei zu beachten sind. Stellen Sie sich dabei folgendes Szenario vor: Bei einer Gruppe von Benutzern, die sich an einem Standort in einer Organisationseinheit Vertrieb befinden, hat sich die Faxnummer geändert. Diese Änderung soll nun an allen Benutzerkonten durchgeführt werden. Führen Sie dazu die folgenden Schritte aus:

1. Zunächst einmal müssen Sie aus den Benutzerobjekten der OU über einen entsprechenden Filter die Faxnummern exportieren. Dazu verwenden Sie folgenden Befehl:

```
Ldifde -f fax.ldf -s Hippokrates -d "ou=vertrieb,dc=firma,dc=de" -p subtree -r "(objectCategory=cn=Person,CN=Schema,CN=Configuration,DC=firma,dc=de)" -l "FaxNumber" 
```

2. Für jeden Benutzer sollten Sie dort die folgenden Einträge sehen:

```
dn: cn=pmustermann,cn=Users,dc=firma,dc=de
changetype: add
FaxNumber: 123456
```

- Über die Funktion SUCHEN/ERSETZEN des Texteditors müssen nun die Werte für `changetype` und `FaxNumber` geändert sowie eine zusätzliche `replace`-Anweisung eingefügt werden. Danach sollten die folgenden Einträge in der LDIF-Datei enthalten sein:

```
dn: cn=pmustermann,cn=Users,dc=firma,dc=de
changetype: modify
replace: FaxNumber
FaxNumber: 998877
```



Wenn Sie Änderungen vornehmen, achten Sie unbedingt darauf, dass Sie bei den Attributen die korrekte Groß- und Kleinschreibung verwenden. Andernfalls können die Änderungen nicht durchgeführt werden. Wenn Sie nicht wissen, wie ein Attributname im Active Directory korrekt lautet, führen Sie einen Export der gewünschten Objekte durch und lassen dabei den Parameter `-l` weg. Sie erhalten so sämtliche Attribute des Objekts, sofern die Attribute einen Wert besitzen.

- Speichern Sie die Änderungen und importieren die Datei. Überprüfen Sie dann, ob die Änderungen übernommen worden sind.

Außer dem Bearbeiten einer LDIF-Datei zum Ändern von Benutzerattributen können Sie auch ADSI-Skripte verwenden. Möglicherweise sehen Sie im Moment eher den Vorteil darin, eine LDIF-Datei komfortabel zu bearbeiten. Aber ADSI-Skripte können Sie jederzeit wieder benutzen oder auch schnell geringfügig modifizieren. In Kapitel 32.2.4 finden Sie ein Skriptbeispiel, mit dem Sie ebenfalls die Faxnummern der Benutzer ändern können.

Neben dem eben benutzten Befehl `replace` werden in LDIF-Dateien auch die Befehle `add` zum Hinzufügen neuer Objekte sowie `delete` zum endgültigen Löschen eines Objekts unterstützt.

Wollen Sie auf einen Schlag mehrere Attribute an einem Objekt ändern, so müssen Sie die Befehlszeilen jeweils durch einen Bindestrich in einer eigenen Zeile voneinander trennen, und auf diese Zeile muss eine Leerzeile folgen. Wollen Sie also neben der Faxnummer auch noch die Telefonnummer und weitere Attribute ändern, so müssen folgende Einträge in der LDIF-Datei stehen:

```
dn: cn=pmustermann,cn=Users,dc=firma,dc=de
changetype: modify
replace: FaxNumber
FaxNumber: 998877
-
replace: TelephoneNumber
TelephoneNumber: 112233
-
replace: ..
```

Listing 25.1: LDIF-Datei zum gleichzeitigen Ändern mehrerer Attribute

25.2.4 Anlegen und Löschen von Benutzern

In diesem Kapitel erfahren Sie, wie Sie mit LDIF neue Benutzerkonten anlegen und diese zu einer Organisationseinheit hinzufügen können und wie bestehende Benutzerkonten gelöscht werden.

1. Um neue Benutzer anzulegen, erstellen Sie zunächst mit einem Texteditor eine neue Datei, die Sie unter der Dateiendung `.ldf` abspeichern. Für jeden neuen Benutzer müssen Sie folgende Einträge vornehmen: den DN des Benutzers, den `changetype`, hier also `add`, den CN und `sAMAccountName` des Benutzers sowie die `objectClass`. Selbstverständlich können Sie auch weitere Attribute definieren. Abbildung 25.2 zeigt die erforderlichen Einträge.

```
dn:CN=PeterMustermann,OU=Vertrieb,DC=Firma,DC=De
changetype: add
cn: Peter Mustermann
objectClass: user
sAMAccountName: PeterM
```

Listing 25.2: LDIF-Datei zum Anlegen eines neuen Benutzerkontos

2. Speichern Sie die Änderungen und importieren die `.ldf`-Datei wie weiter oben beschrieben.

Über LDIF können Sie bestehende Benutzer auch wieder löschen.

Erstellen Sie hierzu eine neue `.ldf`-Datei und geben für jedes zu löschende Konto den DN sowie den `changetype delete` an. Anschließend importieren Sie diese Datei. Mit folgendem Befehl wird ein Benutzer gelöscht:

```
dn: CN=PeterMustermann,OU=Vertrieb,DC=Firma,DC=De
changetype: delete
```

Listing 25.3: LDIF-Datei zum Löschen eines Benutzerkontos

Zum Erstellen und Löschen von Benutzerkonten können Sie auch ADSI-Skripte verwenden. In Kapitel 32.2.1 finden Sie Beispielskripte, die dieselbe Aufgabe erfüllen wie die eben beschriebenen LDIF-Aktionen.

25.2.5 Setzen von Passwörtern

In diesem Kapitel geht es um passwortspezifische Bearbeitungsmöglichkeiten über LDIF. Wie bereits in Kapitel 25.2.1 beschrieben, können über LDIF keine Passwörter exportiert werden. Importieren Sie die Benutzerdaten, so ist kein Passwort gesetzt, und der Benutzer muss bei der nächsten Anmeldung sein Kennwort ändern. Dies liegt darin begründet, dass das Passwort-Attribut `unicodePwd`, bei LDAP-Abfragen nicht gelesen und, da es eben nicht auslesbar ist, auch nicht zu einem Benutzerobjekt hinzugefügt werden kann. Unter bestimmten Voraussetzungen jedoch ist es möglich, auf dieses Attribut schreibend zuzugreifen.

Für den schreibenden Attributzugriff muss zwischen dem Client und dem Server eine 128-Bit-verschlüsselte SSL-Verbindung bestehen. Zusätzlich muss auf dem Server und den Clients das High Encryption Pack installiert sein. Sind diese Voraussetzungen erfüllt, gibt es zwei Möglichkeiten, das Passwort zu ändern.

Die erste Möglichkeit funktioniert analog zu einer benutzerseitigen Passwortänderung, bei der das alte und neue Passwort angegeben werden muss. Der changetype-Befehl unter LDIF enthält hierbei zunächst eine delete-Anweisung für das alte Passwort. Dieses muss in Anführungszeichen Base64-kodiert angegeben werden. Dann folgt eine add-Anweisung, die das neue Passwort setzt. Auch hier muss das Passwort Base64-kodiert in Anführungszeichen angegeben werden.

Auf dem zweiten Weg wird das Passwort so abgeändert, als würde der Administrator das Benutzerkennwort zurücksetzen. Voraussetzung hierfür ist, dass die Operation unter einem Benutzerkonto durchgeführt wird, das über Administratorrechte verfügt. Der changetype-Befehl enthält hier nur eine einzige modify-Anweisung für das Attribut unicodePwd. Auch hier wird das neue Passwort in Anführungszeichen gesetzt und Base64-kodiert angegeben. Dieses neue Passwort wird übernommen, ohne dass das alte bekannt sein muss.

Wollen Sie die Benutzer dazu zwingen, bei der nächsten Anmeldung das Kennwort zu ändern, müssen Sie das Attribut pwdLastSet bearbeiten. Exportieren Sie dazu das Attribut, indem Sie den Parameter `-l pwdLastSet` setzen. Setzen Sie dann in der Exportdatei den Wert des Attributs pwdLastSet über `changetype: modify` auf 0.

26 Visualisierung und Design der Active Directory-Umgebung in Microsoft Visio

In diesem Kapitel geht es um die weniger bekannten Funktionalitäten des Programms Microsoft Visio im Zusammenhang mit Active Directory. Neben der klassischen Funktion der Visualisierung können Sie mit Visio Daten aus einem bestehenden Active Directory importieren, diese Daten sowie das Active Directory-Schema modifizieren und schließlich wieder als LDIF-Datei in das Verzeichnis exportieren.

26.1 Microsoft Visio und Active Directory

Microsoft Visio ist in zweierlei Hinsicht für das Active Directory von Interesse. Zum einen können Sie eine neue Active Directory-Umgebung quasi am Reißbrett planen, zum anderen eine bereits bestehende Struktur des Active Directory oder Teile daraus importieren, visualisieren und weiterbearbeiten. Über die Windows-mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER können Sie zwar die Objekte anzeigen, aber die Struktur der Objekte ist darin nicht zu erkennen. Außerdem ist die Verzeichnisansicht in der mmc nicht ausdrückbar. Visio bietet Ihnen die Möglichkeit zur strukturellen Visualisierung, die zur Dokumentation bestehender Verzeichnisse oder aber auch zur Migrationsplanung genutzt werden kann. Zusätzlich haben Sie die Möglichkeit, über Visio neue Active Directory-Objekte zu erstellen und zu bearbeiten sowie das Active Directory-Schema zu erweitern und modifizieren und diese geänderten Objekte als LDIF-Datei zu exportieren und dann wieder ins Active Directory zu importieren.

Das Importieren, Bearbeiten und Exportieren von Objekten funktioniert unter Visio nicht nur für ein Active Directory, sondern auch für beliebige andere LDAP-Verzeichnisse und den Novell-Verzeichnisdienst NDS.

Tabelle 26.1 gibt Ihnen eine Übersicht darüber, welche Visio-Version Sie für welchen Zweck verwenden müssen. Der Einsatz von Standardversionen des Produkts ist weder mit Visio 2000 noch mit Visio 2002 möglich, da diese nicht die erforderlichen Netzwerk-Schablonen besitzen.

Aufgabe	Benötigte Visio-Version
Design einer Active Directory-Umgebung	Visio 2002 Professional Visio 2000 Professional/Enterprise
Import von Objekten aus einer vorhandenen Active Directory-Umgebung	Visio 2002 Professional + Add-On Enterprise Network Tools (VENT), Visio 2000 Enterprise
Export der neuen Objekte ins LDIF-Format	Visio 2002 Professional + VENT Visio 2000 Enterprise

Tabelle 26.1: Erforderliche Microsoft Visio-Versionen für die Bearbeitung des Active Directory

Für Visio 2002 Professional ergibt sich dabei leider das Problem, dass Microsoft das Add-On Enterprise Network Tools am 01.07.2002 vom deutschen Markt genommen hat. Als Grundlage für die folgenden Beispiele in diesem Buch wird die Visio 2000 Enterprise-Version verwendet.

In diesem Kapitel wird beschrieben, wie Sie ein bestehendes Verzeichnis einlesen, darin Objekte modifizieren und neu anlegen und diese Daten schließlich im LDIF-Format wieder exportieren. Dabei wird ein Grundlagenwissen in Visio vorausgesetzt. Sie sollten mit Begrifflichkeiten wie Schablonen, Shapes sowie der allgemeinen Benutzung vertraut sein.

26.1.1 Importieren von Active Directory-Objekten

Um eine Netzwerkverbindung mit dem Verzeichnis herstellen zu können, ist die ADSI-Schnittstelle (Active Directory Services Interface, siehe Kapitel 32.1) erforderlich. Diese ist unter Windows 2000 und XP automatisch installiert. Wollen Sie von einem Windows NT- oder 98-Client aus die Verbindung herstellen, so müssen Sie zunächst das ADSI-Paket downloaden. Zusätzlich müssen Sie auf dem Active Directory-Server über Administratorrechte verfügen.

Um eine bestehende Umgebung einzulesen und zu bearbeiten, führen Sie unter Visio die folgenden Schritte aus:

1. Wählen Sie über das Menü DATEI/NEU/NETZWERKDIAGRAMM/ACTIVE DIRECTORY. Bevor Sie das Fenster MIT VERZEICHNIS VERBINDEN (siehe Abbildung 26.1) erhalten, sehen Sie, wie im Hintergrund das Standard-Active Directory-Schema geladen wird.
2. Als Erstes müssen Sie entscheiden, ob Sie online oder offline arbeiten möchten. Entscheiden Sie sich für die Online-Variante, klicken Sie auf DURCHSUCHEN und geben den Servernamen, Benutzernamen und das Kennwort für den Server an, von dem Sie die Active Directory-Inhalte einlesen möchten.

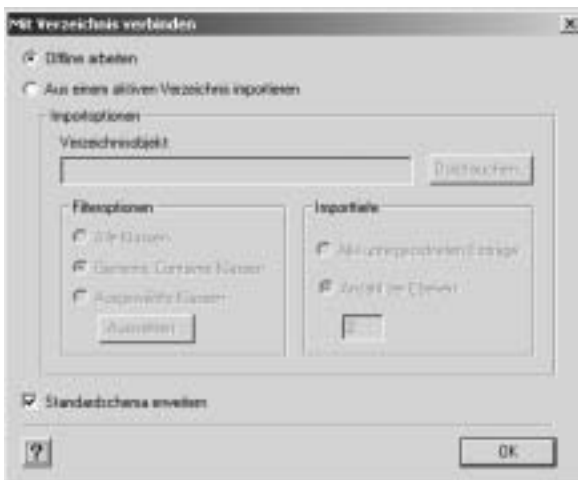


Abbildung 26.1: Die Verbindung zwischen Visio und dem Active Directory wird hergestellt.

3. Sie erhalten dann das Fenster VERZEICHNIS-BROWSER (siehe Abbildung 26.2). In diesem Fenster können Sie auswählen, welche Strukturebenen in Visio geladen werden sollen. Sie können die Struktur im Verzeichnisbaum erweitern. Die nicht zu importierenden Objekte werden durch Anklicken abgewählt. Klicken Sie dann auf OK.



Abbildung 26.2: Der Verzeichnis-Browser

4. Haben Sie hier die gewünschten Objekte ausgewählt, können Sie die Filteroptionen und die Importtiefe für die Objekte angeben (siehe Abbildung 26.1). Die Filteroptionen beziehen sich auf die Schemaklassen. Wählen Sie unter FILTEROPTIONEN die Auswahl AUSGEWÄHLTE KLASSEN, erhalten Sie ein weiteres Fenster, in dem Sie die gewünschten Klassen der Auswahl hinzufügen können. Mit der Importtiefe wird die Anzahl der zu importierenden Ebenen – gerechnet von der Stammebene – bestimmt. Bedenken Sie bei den Auswahlen, dass mit sämtlichen gewählten Objekten auch deren Eigenschaften importiert werden. In einer großen Umgebung kann dieser Vorgang den Importprozess verlängern, und auch die Größe der Importdatei nimmt zu.
5. Nachdem die Objekte in Visio importiert worden sind, werden diese in einer Baumstruktur im Verzeichnisnavigator dargestellt (siehe Abbildung 26.3). Um die Active Directory-Umgebung auf dem Zeichenblatt zu visualisieren, ziehen Sie einfach die Objekte aus dem Verzeichnisnavigator per Drag&Drop auf das Zeichenblatt. Sie können dabei einen beliebigen Container als das übergeordnete Objekt auswählen. Dabei werden Sie gefragt, ob Sie nur das Zeichenobjekt (Shape) selbst oder dieses mit einer wählbaren Anzahl von untergeordneten Shapes darstellen möchten.
6. Haben Sie sich für den Offline-Betrieb von Visio entschieden, so entfallen alle eben genannten Schritte. Sie erhalten direkt den Verzeichnisnavigator, in dem sich lediglich das Symbol SUBTREE befindet, sowie das Standardschema mit seinen Klassen und Eigenschaften. Weitere Objekte sind nicht vorhanden.

Um die Übersichtlichkeit zu verbessern, sollten Sie zu den Objekten im Verzeichnisnavigator die Einträge wie `dc=firma`, `cn=Computers`, `ou=Marketing` usw. einblenden. Wählen Sie dazu aus dem Menü **VERZEICHNISDIENSTE** die **OPTIONEN**. Dort aktivieren Sie die Checkbox **QUALIFIZIERTE NAMEN ANZEIGEN**.



Abbildung 26.3: Der Verzeichnisnavigator

26.1.2 Bearbeiten und Neuerstellen von Objekten

Das Neuerstellen und Bearbeiten von Objekten ist sowohl im Online- als auch im Offline-Betrieb von Visio möglich. Um ein neues Objekt zu erstellen, wählen Sie das gewünschte Zeichnungsobjekt aus der Schablone auf der linken Seite aus und ziehen es auf das Zeichenblatt. Alternativ dazu können Sie auch im Verzeichnisnavigator auf das übergeordnete Objekt klicken und aus dem Kontextmenü den Eintrag **EINTRAG HINZUFÜGEN** wählen. Sie erhalten dann eine Liste aller verfügbaren Klassen. Um in einer neuen Umgebung die erste Domäne anzulegen, wählen Sie aus dem Kontextmenü **SubTree** den Eintrag **EINTRAG HINZUFÜGEN**. Für eine Domäne wählen Sie die Eintragsklasse **domainDNS**. Im Feld **EINTRAGSNAME** geben Sie dem Objekt den gewünschten Namen.



Wenn Sie ein Objekt später umbenennen, dürfen Sie nach der Eingabe des neuen Namens die Eingabe nicht mit Enter abschließen. Die Eingabe von Enter kann unvorhersehbare Schäden am LDIF-Dateiformat hervorrufen. Sofern Sie nicht planen, die Daten zu exportieren, ist dieser Hinweis nicht weiter wichtig. Wollen Sie aber die Daten ex- und wieder importieren, so kann es beim Import zu Problemen kommen.

Haben Sie das Domänen-Objekt hingegen per Drag and Drop eingefügt, wird es im Verzeichnisnavigator platziert. Sie können dort aus dem Kontextmenü des Objekts **EIGENSCHAFTEN BEARBEITEN** wählen und den Namen im Feld **DC** ändern (siehe Abbildung 26.4).

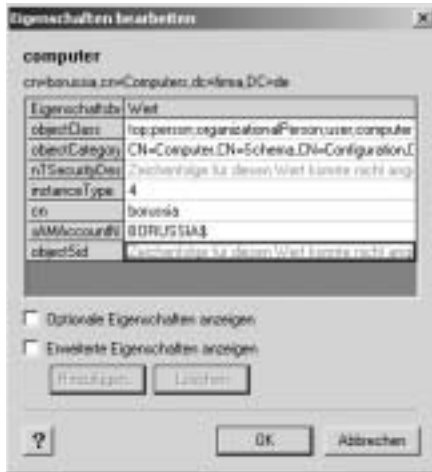


Abbildung 26.4: Hinzufügen von weiteren Objekten

Um dem eben erstellten Domänenobjekt untergeordnete Container hinzuzufügen, können Sie im Verzeichnisnavigator und auf dem Zeichenblatt aus dem Kontextmenü des Objekts **EINTRAG HINZUFÜGEN** auswählen. Wählen Sie nun als Eintragsklasse **organizationalUnit** aus und legen die gewünschte Anzahl der Einträge fest. So können Sie auf einen Schlag mehrere untergeordnete Container desselben Typs anlegen und mit einem Namen versehen.

Die dritte Methode zum Hinzufügen von untergeordneten Objekten besteht darin, das gewünschte Objekt aus der Schablone links zu wählen und im Zeichenblatt auf das übergeordnete Objekt zu ziehen. Diese Methode bietet sich an, um in die eben erstellten OUs Benutzer und Computer oder weitere Container einzufügen.

Ein weiteres Feature von Visio besteht darin, die Eigenschaften von Objekten zu bearbeiten sowie neue Eigenschaften zu definieren, mit denen das Standardschema erweitert werden kann. Wenn Sie für ein Objekt aus dem Kontextmenü **EIGENSCHAFTEN BEARBEITEN** wählen, erhalten Sie das gleichnamige Fenster (siehe Abbildung 26.5). Standardmäßig werden nur die Eigenschaften angezeigt, die für die jeweilige Objektklasse unbedingt anzugeben sind. Um alle weiteren optionalen Eigenschaften aufzulisten, die für die Objektklasse definiert sind, markieren Sie die Checkbox **OPTIONALE EIGENSCHAFTEN ANZEIGEN**. Für sämtliche Eigenschaften können Sie hier Werte festlegen. Sind für eine Eigenschaft mehrere Werte erforderlich, so müssen Sie diese durch ein Semikolon (;) voneinander trennen.

Beim Anzeigen der Eigenschaftswerte sehen Sie, dass bei einem neu hinzugefügten Objekt lediglich die Eigenschaft **CN** (Common Name) einen Wert besitzt. Bei importierten Objekten sind bereits weitere Eigenschaften mit Werten gefüllt. Abbildung 26.5 zeigt ein aus dem Active Directory importiertes Computerobjekt.

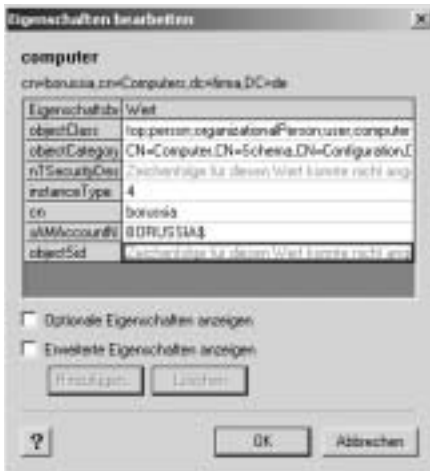


Abbildung 26.5: Die Eigenschaften eines Objekts unter Visio bearbeiten

Wenn Sie ein Objekt löschen möchten, so können Sie dieses im Verzeichnisnavigator oder im Zeichenblatt löschen. Löschen Sie es im Navigator, wird es auch automatisch vom Zeichenblatt entfernt, dieser Vorgang funktioniert jedoch nicht umgekehrt. So haben Sie die Möglichkeit, aus Gründen der Übersichtlichkeit jederzeit Objekte vom Zeichenblatt zu entfernen, ohne dass dabei die Gefahr besteht, diese Objekte aus dem Verzeichnis zu entfernen. Außerdem erhalten Sie eine Fehlermeldung, wenn Sie versuchen, ein Shape auf das Zeichenblatt zu ziehen, das sich bereits auf diesem befindet. Dies liegt darin begründet, dass auch im Active Directory ein Objekt desselben Namens nicht doppelt existieren darf.

Das Hinzufügen und Bearbeiten von Objekten und deren Eigenschaften in einer importierten Active Directory-Umgebung funktioniert genauso wie eben für eine neue, leere Umgebung beschrieben.

Mit Visio haben Sie auch die Möglichkeit, die Active Directory-Struktur-Ansicht mit ihren Objekten auszudrucken. Diese Möglichkeit ist in der mmc unter Windows nicht gegeben.

26.1.3 Bearbeiten des Active Directory-Schemas

Wie bereits erwähnt, können Sie unter Visio neben den standardmäßigen Schemaklassen auch selbstdefinierte Klassen erstellen sowie eigene Eigenschaften für die Objektklassen definieren. In Kapitel 24 haben Sie bereits eine Einführung in die Funktionsweise des Schemas sowie Möglichkeiten zu dessen Änderung erhalten. Deshalb werden die Grundbegriffe an dieser Stelle vorausgesetzt.

Um eine neue Eigenschaft dem Schema hinzuzufügen, gehen Sie im Verzeichnisnavigator auf den Knoten KLASSEN/EIGENSCHAFTEN und wählen aus dem Kontextmenü EIGENSCHAFTSKLASSE HINZUFÜGEN. Für die neue Klasse müssen Sie mehrere Eigenschaften und Werte festlegen. Dazu zählen der Klassenname, Klassenkennzeichner, zwingende und optionale Eigenschaften sowie eventuell vorhandene Oberklassen (siehe Abbildung 26.6).



Abbildung 26.6: Hinzufügen neuer Schemaklassen über Visio

Um eine neue Eigenschaft hinzuzufügen, gehen Sie im Verzeichnisnavigator auf den Knoten SCHEMA/EIGENSCHAFTEN und wählen dort aus dem Kontextmenü EIGENSCHAFTSKLASSE HINZUFÜGEN. Für die Eigenschaft müssen Sie einen Namen und Kennzeichner sowie die Syntax (z.B. Integer, Boolean oder CaseSensitiveString) und Maximalgröße festlegen (siehe Abbildung 26.7).

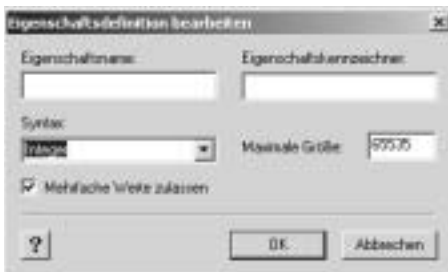


Abbildung 26.7: Hinzufügen neuer Eigenschaften

Sofern Sie sich beim Erstellen neuer Klassen und Eigenschaften im reinen Designmodus befinden und die Änderungen nicht in ein Verzeichnis exportieren möchten, müssen Sie darauf achten, dass diese neuen Klassen und Eigenschaften auch im realen Active Directory-Schema angelegt werden.

Um bestehende Klassen und Eigenschaften zu ändern, wählen Sie den entsprechenden Kontextmenüeintrag und führen dann die Änderungen durch. So haben Sie die Möglichkeit, neu definierte Eigenschaften zu bereits bestehenden Klassen als optionale oder zwingende Eigenschaft hinzuzufügen oder eine neue Klasse mit neuen Eigenschaften zu erstellen.

26.1.4 Exportieren von Objekten ins Active Directory

Eine sehr nützliche Funktion ist der Export von geänderten Objekten bzw. nur von den Änderungen im LDIF-Format. Diese LDIF-Exportdatei kann in ein bestehendes Active Directory eingelesen werden. Es handelt sich um eine Textdatei im ASCII-Format. In dieser Datei werden sämtliche Objekte, Klassen und Eigenschaften gespeichert, die unter Visio dargestellt worden sind.

Um die Dateien zu exportieren, wählen Sie aus dem Menü VERZEICHNISDIENSTE den Eintrag IN LDIF EXPORTIEREN. Dabei können Sie entscheiden, ob Sie sämtliche Einträge exportieren möchten oder lediglich die Änderungen. In beiden Fällen wird das Dialogfeld SPEICHERN UNTER geöffnet. Geben Sie hier den Speicherort der .ldf-Datei an.

Da es sich bei den LDIF-Dateien um ASCII-Textdateien handelt, können diese mit jedem beliebigen Texteditor geöffnet werden. In den Dateien wird eine spezielle Syntax benutzt, die für Verzeichnisdienste benutzt wird. Diese LDIF-Datei können Sie nun in ein Active Directory importieren. Dieses ist nützlich, wenn Sie unter Visio quasi am Zeichentisch eine Umgebung designed haben und diese nun real testen möchten.

26.1.5 Strukturdesign der Active Directory-Umgebung

Wie Sie bei der Arbeit mit den Active Directory-Objekten vielleicht bemerkt haben, steht Ihnen neben der Schablone ACTIVE DIRECTORY-OBJEKTE auch noch die Schablone ACTIVE DIRECTORY-STANDORTE UND -DIENSTE zur Verfügung. In dieser Schablone finden Sie verschiedene Shapes, mit denen Sie die physische Struktur der Umgebung visualisieren können. Hierzu zählen Shapes wie Standorte, Standortverknüpfungen und Standortverknüpfungsbrücken, Domänen, Domänencontroller sowie WAN- und DFÜ-Verbindungen und Replikationspfade. Die Shapes dieser Schablone dienen der reinen Visualisierung und Dokumentation. Sie haben mit diesen Shapes nicht die Möglichkeit, diesen Eigenschaften zu vergeben oder zu ändern bzw. die Strukturobjekte als LDIF-Datei zu exportieren.

27 Migration und Update von Windows NT zu Active Directory

Dieses Kapitel beschäftigt sich mit der Migration und dem Update von Windows NT auf Active Directory. Es wird zunächst begründet, warum ein nicht unerheblicher Aufwand für die Migration von NT zu Windows 2000 oder 2003 betrieben werden soll. Hierzu wird ein Überblick über die Vorteile einer Directory-Struktur gegeben.

Nach diesem theoretischen Teil folgt eine Beschreibung darüber, welche Prozesse beim Aktualisieren auf einem NT-Domänencontroller ablaufen. Weiterhin werden auch verschiedene Möglichkeiten für die Planung eines DNS-Modells angegeben. Diese Überlegung muss der eigentlichen Migration vorausgehen. Hieran anknüpfend werden verschiedene Vorgehensweisen zur Erstellung einer neuen Domänenstruktur vorgestellt. Hier werden alle erforderlichen Schritte beschrieben, die Sie von der Migration der ersten Masterdomäne bis hin zur letzten Ressourcendomäne durchführen müssen. Abschließend folgt ein Überblick über die Aufgaben, die nach einer erfolgreichen Migration durchgeführt werden können. Hierzu zählen beispielsweise das Zusammenfassen und Löschen nicht mehr benötigter Domänen sowie auch das Umsortieren von Gruppen oder Computern innerhalb der Domänen.

27.1 Warum auf Windows 2000 oder 2003 aktualisieren?

„Warum soll eine bestehende NT-Landschaft unbedingt auf Windows 2000 oder 2003 aktualisiert werden? Es funktioniert doch alles.“ Diese oder eine ähnliche Frage ist durchaus berechtigt. Denn vor einem funktionierenden Active Directory steht ein nicht unerheblich langer Weg des Planens, Installierens und Anpassens der neuen Domänenstruktur. Hierzu zählt auch die Aktualisierung der Clients auf Windows 2000 oder XP. Dieses alles sind Kriterien, die viel Zeit in Anspruch nehmen und nebenbei auch nicht unerhebliche Kosten verursachen. Dem gegenüber sollte dann selbstverständlich auch eine lange Liste von Vorteilen und neuen Features einer Active Directory-Struktur gegenüber dem NT-Domänenmodell stehen, die die Investition von Zeit und Geld rechtfertigt. Und dieses ist in der Tat der Fall.

Unter Windows 2000/2003 werden wesentlich weniger Domänen benötigt als unter NT, da die Datenbank eine Größe von bis zu 70 Tbyte umfassen kann, während unter NT die Grenze für die Kontendatenbank mit 40 MB empfohlen war. Eine Windows 2000/2003-Domänen-Gesamtstruktur kann bis 10 Millionen Objekte umfassen, eine einzelne Domäne 1 bis 2 Millionen Objekte. Hierdurch ist ein wesentlich geringerer Verwaltungsaufwand erforderlich. Das Active Directory-Schema ist außerdem individuell anpassbar, um auch speziellste Informationen zu Objekten im Directory speichern zu können. Auch

die unter NT nicht gegebene Zusammenarbeit von Active Directory mit anderen Verzeichnisdiensten, etwa NDS von Novell NetWare, darf in keinem Fall vergessen werden.

Da keine PDCs und BDCs mehr benötigt werden, sondern nur noch gleichrangige Domänencontroller eingesetzt werden, kann die Netzwerkbandbreite reduziert werden, da erstens die Clients ihre Domänencontroller effektiver nutzen und zweitens die Domänencontroller über ihre Multimaster'-Replikation schneller und zuverlässiger arbeiten als die Replikation unter Windows NT von nur einem PDC aus. Auch der Zugriff auf andere Rechner oder beliebige Netzwerkressourcen ist im Active Directory im einheitlichen Modus wesentlich schneller als in einem NT-Netzwerk.

Durch das Erstellen eines durchdachten DNS-Namespaces sowie von OUs kann man ein Unternehmen sehr präzise abbilden. Hierbei ist es möglich, sowohl nach geografischen als auch nach organisatorischen Strukturen ein Abbild zu erstellen. Die Objekte im Active Directory können übersichtlich in den einzelnen OUs organisiert werden.

Weiterhin haben Sie die Möglichkeit, effektiv Berechtigungen über Gruppenrichtlinien für Benutzergruppen festzulegen. Für jedes einzelne Objekt im Active Directory wird ein ACL erstellt. Hierdurch wird eine sehr präzise Kontrolle über den Objektzugriff erreicht. Auch beim Delegieren von Verwaltungsaufgaben an bestimmte Benutzer oder Gruppen stehen mit Windows 2000/2003 genauer definierbare Lösungen bereit.

Weiterhin werden typische Komponenten eines Windows NT-Netzwerkes überflüssig. Hierzu zählen zum einen die BDCs, da im Active Directory nur noch gleichrangige Domänencontroller verwendet werden. Zum anderen werden auch Netzwerkdienste wie WINS oder LMHOSTS-Einträge überflüssig, da die Clients ihre Kommunikation im TCP/IP-Netzwerk über den DNS-Dienst ausüben. Hierbei ist natürlich zu bedenken, dass nach der Migration auch im Client-/Server-Bereich nur solche Software verwendet werden sollte, die nicht noch veraltete Netzwerkdienste erfordert. Die separate Pflege von WINS- oder LMHOSTS-Tabellen entfällt somit.

27.1.1 Die Entscheidung: Migration oder Update

Ob ein Update oder eine Migration einer bestehenden Windows NT-Umgebung durchgeführt werden soll, ist eine gut zu durchdenkende Entscheidung. Ist hierüber die Entscheidung gefallen, können Sie mit allen weiteren Schritten der Planung und Durchführung beginnen. Bei einem Update bleibt die bestehende NT-Domäne bestehen. Ihr PDC wird auf Windows 2000 oder 2003 aktualisiert. Dabei bleiben sämtliche Benutzerkonten in der Domäne erhalten. Bei einer Migration richten Sie eine völlig neue Domäne ein. In diese neue Domäne müssen Sie sämtliche Benutzer und Gruppen verschieben. Nach dem erfolgreichen Abschluss der Migration kann die alte NT-Domäne endgültig aufgelöst werden. Für beide Verfahrensweisen gibt es Pro- und Contra-Argumente.

Vorteile der Migration

Für eine Migration spricht, dass Sie nur so von Grund auf eine neue Domänenstruktur designen und aufbauen können. Eine neue Domänenstruktur ist meistens sinnvoll, wenn unter NT zahlreiche Ressourcendomänen lediglich deshalb entstanden sind, weil die Obergrenze der möglichen Objekte erreicht wurde, diese Domänen aber keiner logischen Struktur unterworfen sind. Weiterhin besteht bei einem Update die Gefahr, dass in

die neue Domäne zu viele Objekte als Ballast mitgeschleppt werden könnten, die veraltet sind und nicht mehr benötigt werden. Dabei entsteht jedoch ein nicht unerheblicher Aufwand durch den Import ausgewählter Objekte in die neue Domäne. Soll im Rahmen des Migrationsprojekts auch die Server-Hardware erneuert werden, so muss ohnehin eine Neuinstallation erfolgen.

Vorteile des Updates

Das Hauptargument gegen eine Migration ist, dass der Arbeitsaufwand gewaltig werden kann, da bei einer Migration sämtliche Objekte, Berechtigungen und Einstellungen aus der alten Domäne exportiert oder komplett neu erstellt werden müssen. Bei einem Update bleiben die Objekte erhalten, und der Update-Prozess an sich dauert nicht länger als eine herkömmliche Windows 2000/2003-Installation. Auch weitere Programme, die auf dem Domänencontroller ausgeführt werden, müssen nicht neu installiert werden, sofern sie Windows 2000/2003-kompatibel sind. Weiterhin wird es nicht zu großen Problemen mit den Security-IDs (SIDs), insbesondere der SID-History der Objekte kommen. Über eine SID wird unter Windows NT und 2000 jeder Benutzer und jede Gruppe eindeutig identifiziert. Bei jedem Zugriff auf eine Datei wird nicht überprüft, ob der Benutzername einen Eintrag in der Zugriffsliste (ACL) enthält, sondern ob die SID in der ACL der Datei enthalten ist.

Fazit

Es wäre vermessen zu sagen, eine Migration sei besser als ein Upgrade oder umgekehrt. Jedes Unternehmen wird seine eigenen Präferenzen setzen und danach entscheiden, welcher Weg eingeschlagen werden soll. Verfügen Sie lediglich über eine einzelne NT-Domäne, die in einer einzelnen Active Directory-Domäne münden soll, so ist ein Update anzuraten. Andererseits kann aber auch eine Migration sinnvoll sein, um alles von Grund auf zu erneuern. Auf der anderen Seite müssen Sie eine Migration durchführen, wenn mehrere Domänen zu einer einzelnen Active Directory-Domäne werden sollen. Auch wenn Sie zunächst sämtliche NT-Domänen in mehrere Active Directory-Domänen updaten und diese dann konsolidieren, sodass nur eine Domäne übrig bleibt, spricht man von einer Migration. Gerade dies wird das Ziel vieler Unternehmen sein. Sicherlich ist eine Migration aufwändiger und risikoreicher als ein Update, aber dennoch oft der einzige Weg.

27.2 Allgemeine Planung einer Migration

Dieses Kapitel führt Sie schrittweise durch die nötigen Vorbereitungen und Überlegungen, die bei der Planung einer Migration und eines Updates betrieben werden müssen. Insgesamt sind sechs Schritte erforderlich.

27.2.1 Vorbereitung der Domänenstruktur

Entscheidend für den Erfolg des Active Directory ist die Planung und Strukturierung der Domänen. Der Aufwand für diesen Arbeitsschritt ist stark abhängig von der Größe und Architektur des bestehenden Netzwerks. Sofern Sie nur über eine einzelne Domäne mit mehreren BDCs an verschiedenen Standorten verfügen und diese Struktur beibehalten

werden soll, so sind Migration oder Update kein großes Problem. Anders sieht es aber aus, wenn Sie über ein komplexes Multi-Domänenmodell verfügen. Aufgrund der Objektbeschränkungen in NT-Domänen spiegeln die Domänen möglicherweise nur die administrative Struktur oder die funktionelle Struktur wider. Das Active Directory-Domänenmodell ist wesentlich flexibler. Sie können nun die geografische Struktur oder die organisatorische Struktur oder eine Kombination aus beiden abbilden. Benutzerkonten können endlich in die Domänen verschoben werden, in die sie korrekterweise gehören. Die Verwaltung ist im Active Directory nicht mehr an bestimmte Benutzergruppen wie Administratoren oder Server-Operatoren gebunden, sondern kann an jeden beliebigen Benutzer delegiert werden. Damit entfällt die Notwendigkeit zentraler Administration, da ausgewählte Benutzer lokal ihre Standorte im Rahmen der zugewiesenen Rechte verwalten können. Mit der Implementierung von Organisationseinheiten im Active Directory entfällt die Notwendigkeit, mehrere Domänen anzulegen, um die Unterabteilungen abzubilden. Innerhalb einer Domäne können Sie beliebig viele Organisationseinheiten anlegen. Das Bilden von Organisationseinheiten sollte an erster Stelle bei der Konsolidierung der alten Domänenstruktur stehen.

Bei einem Multi-Domänenmodell besteht der erste Schritt in der Planung, wie Domänen sinnvoll zusammengelegt und nicht mehr benötigte Domänen aufgelöst werden. Dabei müssen bestehende Benutzer- und Computerkonten nicht manuell in die neuen Domänen aufgenommen werden. Hierfür stehen Ihnen verschiedene Programme zur Verfügung (siehe Kapitel 27.5.).

Auch wenn die bestehende Multi-Domänenstruktur beibehalten werden soll, vereinfachen die transitiven Vertrauensstellungen im Active Directory die Verwaltung. Wenn Domäne 1 eine Vertrauensstellung zu Domäne 2 besitzt und Domäne 2 zu Domäne 3, so vertraut automatisch Domäne 1 auch Domäne 3. Diese Möglichkeit war unter Windows NT noch nicht verfügbar.

Wichtig ist auch die Konzeption von Forest (Gesamtstruktur) und Tree (Domänenstruktur). So können die Domänen *firma.de* und *filiale.de* in einer Active Directory-Gesamtstruktur existieren. Beide bilden je eine separate Domänenstruktur, da sie einen unterschiedlichen Namensraum besitzen. Dennoch benutzen beide Domänen dasselbe Schema und denselben globalen Katalog. Zusätzlich vertrauen sämtliche Domänen einer Domänenstruktur den Domänen der anderen Domänenstruktur.

27.2.2 Standardisierung des Netzwerks auf TCP/IP

Ein weiterer wichtiger Schritt zur Vorbereitung der Active Directory-Implementierung ist die Standardisierung des Netzwerks auf TCP/IP. Das TCP/IP-Protokoll ist das einzige Protokoll, das bei einer Neuinstallation von Windows 2000 und höher standardmäßig installiert wird. Das TCP/IP-Protokoll ist zwingend erforderlich für die Verwendung von LDAP. Windows 2000 unterstützt zwar auch weiterhin das IPX/SPX- und NetBEUI-Protokoll, aber dennoch sollten Sie die Vorteile von TCP/IP nutzen. NetBEUI kann im Gegensatz zu TCP/IP nicht geroutet werden, IPX/SPX lässt sich zwar routen, besitzt aber einen wesentlich größeren Overhead in WAN-Umgebungen. Zur Namensauflösung der NetBIOS-Namen in IP-Adressen werden DNS-Server eingerichtet. Zusätzlich können auch WINS-Server installiert werden, falls einige Anwendungen auf WINS zurückgreifen müssen.

27.2.3 Die DNS-Struktur

Neben der Standardisierung des Netzwerks auf TCP/IP ist die Implementierung einer DNS-Struktur zur Namensauflösung eine wichtige Aufgabe. In zahlreichen NT-Netzwerken ist möglicherweise noch kein DNS implementiert, und die Namensauflösung wird über WINS-Server oder LMHOSTS-Dateien geregelt. Active Directory benötigt jedoch zwingend DNS. Es verwendet die spezielle Form des dynamischen DNS. Dabei führen die DHCP-Server die Registrierung und Deregistrierung der Clients im DNS-Namensraum aus. Damit entfällt die Pflege der DNS-Zonendaten. Da diese Daten im Active Directory gespeichert werden können, bietet diese Methode eine hohe Fehlertoleranz. Trotzdem können unter Windows 2000/2003 auch weiterhin WINS-Server betrieben werden, sofern einige Applikationen WINS erfordern.

Um DNS einzusetzen, stellen Sie sicher, dass alle Clients über DNS-konforme Namen verfügen. Dabei dürfen die Zeichen A–Z, a–z, 0–9 sowie der Bindestrich (-) enthalten sein. Danach muss entschieden werden, wie die Domäne des Unternehmens heißen soll. Überlegungen zu diesem Thema finden Sie in Kapitel 6.1.2.

27.2.4 Die SID-Probleme

Eine weitere Hürde bei der Migration ist das SID-Problem. Zu jedem Benutzer-, Gruppen- und Computerobjekt existiert eine SID von 32 Bit Länge. Die Computer-SID wird bei der Installation des Betriebssystems dem Computer automatisch zugewiesen. Wurden die Computer eines Unternehmens über eine Clone-Prozedur erstellt, so tragen alle Computer dieselbe SID wie das Quellsystem. Unter NT stellte dies im Gegensatz zum Active Directory noch kein Problem dar. Das Active Directory verwendet die SIDs jedoch für das Auslesen von Berechtigungen. Dabei ist es fatal, wenn mehrere Computer dieselbe SID besitzen. Benutzen Sie also auf keinen Fall Cloning-Methoden für die Installation von Windows 2000/2003. Ist dieses Verfahren erforderlich, so muss die Duplizierung nach Abschluss der textbasierten Installation und vor Beginn des GUI-geführten Setups erfolgen.

Zusätzlich gibt es zwei Programme, die die Eindeutigkeit von SIDs sicherstellen. So haben Sie zum einen mit Microsofts *SysPrep* die Möglichkeit, eine SID festzulegen, bevor Sie mit einem Image-Programm ein Abbild des Systems erstellen. Danach kann das System gefahrlos geclost werden. Zum anderen können Sie auch das Programm *SIDchanger* von PowerQuest benutzen. Mit diesem Programm können Sie automatisch die doppelten SIDs der NT-Computer in eindeutige Werte umwandeln.

Das zweite SID-Problem bei einer Migration sind die SID-Histories bei Benutzern und Gruppen. Sobald die entsprechenden Konten in die Active Directory-Domäne migriert und damit neu angelegt werden, erhalten Sie eine neue SID. Mit dieser neuen SID hätten die Benutzer jedoch keinen Zugriff mehr auf die Ressourcen, für die ihnen der Zugriff unter der SID der ursprünglichen Domäne gestattet war. Deshalb werden die ursprünglichen SIDs im Active Directory in ein Attribut namens SID History kopiert. Damit haben die Benutzer auch weiterhin Zugriff auf ihre Ressourcen. Migrationsprogramme wie *ADMT* (siehe Abbildung 27.5) kopieren die SIDs automatisch in die SID-History. Mit *ADMT* besteht auch die Möglichkeit, bestehende Ressourcen auf einem Dateiserver nach SIDs zu scannen und die SIDs in allen ACLs durch die neuen SIDs des Active Directory

zu ersetzen. Danach kann die SID-History aus dem Active Directory entfernt werden, da sie nicht länger benötigt wird. Bedenken Sie aber auch, dass diese Aufgabe langwierig wird, wenn sich Tausende von Dateien auf dem Dateiserver befinden, und dass im Falle eines Fehlschlags die Daten für keinen Benutzer mehr zugänglich sind.

27.3 Welches DNS-Modell ist das Beste?

Vor der Betrachtung verschiedener Migrations- und Update-Konzepte darf auch die Planung der DNS-Architektur nicht vernachlässigt werden. Eine durchdachte DNS-Implementierung ist die Grundlage für ein funktionierendes Active Directory. Sofern in Ihrem Unternehmen bereits ein laufendes DNS-Modell vorhanden ist, müssen Sie sich vor der Migration auch Gedanken darüber machen, in welcher Form Sie DNS nach der Migration betreiben möchten. In diesem Kapitel werden drei mögliche Szenarien vorgestellt. Jede der drei Methoden erfordert ein anderes Maß an Vorbereitung und gegebenenfalls auch Umstellung der bisherigen DNS-Landschaft. Dafür bietet aber auch nicht unbedingt jede Methode die Unterstützung für alle Features im Zusammenspiel zwischen Windows 2000 und DNS. Für die Grundlagen zum Thema DNS sei auf Kapitel 16 verwiesen.

Für ein DNS-Modell gibt es drei verschiedene Ansätze. Zwei davon beruhen darauf, dass DNS unter Windows 2000/2003 ausgeführt wird; die dritte Möglichkeit sieht die Verwendung eines nicht von Windows verwalteten DNS-Servers vor. Diese drei Ansätze sollen nun genauer betrachtet werden.

27.3.1 Windows 2000/2003 beinhaltet den kompletten DNS-Stamm

Diese Möglichkeit bietet am ehesten die komplette Nutzung aller Features von DNS mit Windows 2000/2003 wie der dynamischen DNS-Aktualisierung, der Integration von DNS in das Active Directory, was mehrere primäre DNS-Server zulässt, sowie die Unterstützung von Unicode-DNS-Namen. Allerdings bringt diese Methode auch eine komplette Umstellung der bisherigen DNS-Serverlandschaft mit sich, da alle DNS-Server neu unter Windows 2000/2003 eingerichtet werden müssen. Es wird eine komplette Migration aller DNS-Server mit den möglicherweise umfangreichen DNS-Einträgen sowie eventuell verknüpfter Skripte und Programme erforderlich. Auch an das Zusammenspiel von DNS mit anderen Diensten und Betriebssystemen ist zu denken, wenn Sie die Umstrukturierung in Betracht ziehen.

Dieser Weg dürfte am einfachsten für ein kleines Unternehmen zu praktizieren sein, bei dem lediglich eine noch relativ überschaubare Menge an Aufgaben durchzuführen ist. Jedoch sollte auch ein größeres Unternehmen über diese Methode nachdenken und abwägen, ob die Nutzung der Features von DNS und Windows 2000/2003 eine möglicherweise komplette Umstellung der vorhandenen DNS-Infrastruktur rechtfertigt. Da bereits die Installation von Active Directory ein tiefgreifender Schnitt ist, sollte getrost auch an diesen zweiten tiefen Einschnitt der IT-Landschaft gedacht werden.

27.3.2 Windows 2000/2003 beinhaltet eine untergeordnete Zone

Auch mit dieser Methode können Sie adäquat die Features von Windows 2000/2003 und DNS wie dynamische Aktualisierung und Active Directory-Integration nutzen. Hierbei behalten die vorhandenen primären DNS-Server weiterhin die Haupt-DNS-Zone des Unternehmens und delegieren eine untergeordnete DNS-Zone als Stamm des Windows 2000/2003 DNS-Dienstes. So kann z.B. die Hauptzone *firma.de* die ihr untergeordnete Zone *dns.firma.de* zur Verwaltung delegieren. Ein DNS-Server unter Windows 2000/2003 ist für alle Anfragen an die untergeordnete Zone autorisiert, die er beherbergt.

Allerdings hat diese Methode drei kleinere Nachteile. Erstens werden auf diese Art und Weise die Namen der einzelnen Domänen länger. Zweitens benötigen Sie mehr DNS-Server als vorher, nämlich mindestens einen für jede delegierte Zone. Dadurch steigt natürlich der Verwaltungsaufwand, es sei denn, Sie planen die dynamische Aktualisierung von DNS. Ist diese nach einmal durchdachter Planung eingeführt, geht Ihr Verwaltungsaufwand fast gegen null. Als dritter Nachteil ist zu sehen, dass die Clients nicht in der neu delegierten Zone, sondern in der bestehenden Zone registriert werden könnten.

Diese Nachteile sind jedoch für Ihr Unternehmen möglicherweise nicht so groß, dass eine wie in Methode 1 beschriebene komplette Umstrukturierung der DNS-Landschaft durchgeführt werden muss. Diese Methode bietet sich an, wenn Sie sowohl die Features von Windows 2000/2003 und DNS nutzen möchten, aber dabei gleichzeitig nicht einen Neuaufbau einer bestehenden DNS-Umgebung durchführen möchten.

27.3.3 Ein Unix-Server beinhaltet den Windows 2000/2003-Stamm

Diese Lösung sollte natürlich nur dann angewandt werden, wenn bereits vor der anstehenden Migration der DNS-Dienst auf Unix-Servern ausgeführt wird. Allerdings müssen Sie hierbei im Vorfeld zwei Punkte überprüfen:

Damit Ihr DNS-Server überhaupt eine Windows 2000/2003-Domäne beinhalten kann, muss er SRV-Ressourceneinträge unterstützen. Ressourceneinträge sind Verknüpfungen zwischen DNS-Domännennamen und den Daten für bestimmte Netzwerkressourcen. Über den Eintragstyp SRV wird bei einer DNS-Anfrage ermittelt, welche Server bestimmte TCP/IP-Dienste ausführen. Nähere Informationen hierzu finden Sie in Kapitel 29.8 sowie RFC 2052. Sollte Ihr DNS-Server diese Funktion nicht unterstützen, kann der Windows 2000/2003-Stamm nicht auf dem DNS-Server liegen.

Dann sollten Sie herausfinden, ob Ihr DNS-Server dynamische Aktualisierungen zulässt. Eine genaue Spezifikation der hierfür verwendeten Technik würde den Umfang dieses Buches übertreffen. Deshalb sei auf die Beschreibung in RFC 2136 verwiesen. Die dynamische Aktualisierung ist zwar nicht zwingend notwendig, verringert aber Ihren Verwaltungsaufwand enorm. Sie müssen ansonsten für jeden neuen DNS-Server die Daten manuell einpflegen. Weiterhin sollten Sie in diesem Fall darauf achten, dass alle Clients so konfiguriert werden, dass sie keine dynamischen Aktualisierungen an ihre DNS-Server senden. Da die Server diese Informationen ohnehin nicht verarbeiten können, würde nur unnötiger Netzwerkverkehr entstehen.

Sollten Ihre DNS-Server in der Lage sein, einen Windows 2000/2003-Domänenstamm zu beherbergen, und darüber hinaus auch noch dynamische Aktualisierungen zulassen, so steht dieser Methode nichts im Wege. Sollten keine Windows 2000/2003-Domänen unterstützt werden, müssen Sie sich ohnehin ein anderes DNS-Konzept ausdenken. Solange nur die dynamischen Aktualisierungen nicht unterstützt werden, müssen Sie abwägen, ob ein erhöhter Verwaltungsaufwand durch manuelles Pflegen der DNS-Einträge rechtfertigt, die DNS-Infrastruktur komplett auf Windows 2000 zu ändern. Dies dürfte in den meisten Fällen wohl nicht der Fall sein.

Als Fazit der Beschreibung dieser drei Konzepte lässt sich Folgendes sagen: Am einfachsten dürfte die dritte Methode entweder von vornherein auszuschließen sein, falls Sie keine Nicht-Windows-Server in Ihrer bisherigen Umgebung verwenden, oder aber zumindest zu überprüfen sein, ob die Unterstützung für Windows 2000/2003-Domänen gewährleistet ist, falls bisher der DNS-Dienst auf Nicht-Windows-Rechnern ausgeführt wird. Sollte dies nicht der Fall sein, müssen Sie sich für eines der anderen beiden Modelle entscheiden, bei denen DNS unter Windows 2000/2003 ausgeführt wird. In beiden Fällen werden dieselben Features unterstützt, sodass zu entscheiden ist, ob eine komplette existierende DNS-Infrastruktur umgebaut werden soll oder ob einige kleine Nachteile in Kauf genommen werden können, ohne die Infrastruktur neu aufbauen zu müssen. In diesem Fall kann die zweite Methode auch als der „goldene Mittelweg“ angesehen werden.

27.4 Migrationsmodelle für NT-Domänen

Dieses Kapitel beschreibt drei verschiedene Wege der Migration von Windows NT zur Active Directory-Domäne. Jeder dieser Wege hat seine Vor- und Nachteile. Bevor Sie jedoch mit der Migration beginnen, sollten Sie einige Dinge im Vorfeld bedenken und vorbereiten. Andernfalls könnten Sie statt einer Migration eher ein großes Fiasko erleben.

27.4.1 Vorbereiten der Migration

Das Wichtigste vorweg: Seien Sie sich stets darüber bewusst, dass eine Migration von Windows NT zu Windows 2000/2003-Active Directory ein sehr komplexer Prozess ist. Dabei liegt es in der Natur der Sache, dass nicht alles auf einen Schlag reibungslos ohne Probleme nach Ihren Wünschen ablaufen wird. Deshalb sollten Sie sich von Beginn an einen Fallback-Plan überlegen, falls Schwierigkeiten während der Migration auftreten sollten, sodass Sie immer noch auf den NT-PDC zurückgreifen und die Domäne weiterhin unter NT betreiben können. Separieren Sie deshalb während der Migration mindestens einen BDC vom Netzwerk, sodass Sie diesen bei einem Fehlschlag wieder zum PDC heraufstufen können.

Weiterhin sollten Sie vor der Migration überflüssige und veraltete Konten aus der NT-Domäne entfernen, die nicht in die neue Domäne übernommen werden sollen. Dies gilt auch für das Update einer Domäne. Neben der manuellen Selektion veralteter Konten können Sie auch skriptgesteuert nach Benutzerkonten suchen, die seit einer bestimmten Anzahl von Tagen – ein guter Wert sind 90 Tage – nicht mehr benutzt wurden.

Sie sollten auch sicherstellen, dass die Zeitsynchronisierung übereinstimmt. Die Clients beziehen ihre Zeitangabe vom Domänencontroller, und sämtliche Domänencontroller

synchronisieren sich mit dem PDC-Emulator-Betriebsmaster. Damit keine Replikationsprobleme durch Asynchronitäten auftreten, überprüfen Sie die Systemzeiten der Rechner. Ansonsten könnte es dazu führen, dass sich Benutzer nicht an der Domäne anmelden können.

Die Migrationsprogramme sollten immer direkt auf einem Domänencontroller der Zieldomäne ausgeführt werden und nicht auf einer beliebigen Workstation. So ersparen Sie sich den unnötigen Netzwerktransfer zwischen der Workstation und der Quell- sowie der Zieldomäne. Stellen Sie zudem sicher, dass zwischen der Quell- und Zieldomäne eine ausreichende Netzwerkverbindung besteht.

Bevor Sie sich nach Abschluss einer Testmigration der ersten zu aktualisierenden produktiven Domäne zuwenden, müssen Sie Folgendes bedenken: Der Auswahl der ersten zu migrierenden Domäne kommt eine besondere Bedeutung zu. Diese Domäne wird die Stammdomäne der neuen Gesamtstruktur und kann nach der Migration nicht mehr gelöscht werden. Sie sollten sich also im Vorfeld genaueste Gedanken machen, mit welcher Domäne Sie beginnen. Bei der neuen Stammdomäne kann es sich entweder um eine komplett neu erstellte Domäne handeln oder um die erste zu migrierende Domäne Ihrer bestehenden Umgebung.



In keinem Fall ist es möglich, dass Sie zuerst eine neue Domäne etwa mit dem Namen *test.firma.de* einrichten, dann eine nicht zusammenhängende Struktur, etwa *firma.de*, zu der Gesamtstruktur hinzufügen und danach die zuerst erstellte Domäne *test.firma.de* löschen.

27.4.2 Vorbereiten des Updates

Auch beim Update der NT-Domänencontroller sind einige Punkte zu bedenken und auszuführen. Eine Selbstverständlichkeit sollte vor der Aktualisierung ein vollständiges Sichern der SAM-Datenbank des PDCs sowie weiterer wichtiger Daten sein. Aber gerade das Backup wird oft genug gern vernachlässigt, was sich dann im unpassendsten Moment bitter rächen kann. Außerdem sollten Sie sich eine Methode überlegen, wie Sie im Notfall am schnellsten wieder Ihr altes System herstellen können. Hierzu gibt es außer einem Backup des PDC, z.B. auf Band, zwei verschiedene schnellere Möglichkeiten der Wiederherstellung:

1. Überprüfen Sie, welcher BDC in Ihrem zum Test ausgewählten Netzwerksegment über die aktuellen Einträge der SAM-Datenbank verfügt. Über den NT Server-Manager können Sie die Replikation erzwingen, sodass der BDC auf dem aktuellen Stand ist. Separieren Sie diesen BDC aus dem Netzwerk. Sollte nun der Aktualisierungsversuch auf dem PDC fehlschlagen, können Sie den BDC wieder ins Netzwerk bringen und zum PDC heraufstufen.
2. Entfernen Sie den aktuellen PDC aus Ihrem Netzwerk, und stufen Sie anschließend einen der BDCs zum PDC herauf. Achten Sie darauf, ob noch Dienste statisch auf den alten PDC verweisen. Konfigurieren Sie diese entsprechend um. Sollte nun die Migration nicht den gewünschten Erfolg haben, können Sie Ihren ursprünglichen PDC wieder ins Netzwerk integrieren.

Es ist nicht universell zu entscheiden, welcher der beiden Wege der bessere ist. Mit der ersten Methode haben Sie zwar weniger Vorbereitungen und können schneller mit der Migration beginnen, aber im Falle eines Fehlschlags dürfte dann die Arbeit zur Reintegration größer sein als beim zweiten Weg. Bei diesem ist zwar etwas mehr Vorarbeit erforderlich, aber dafür haben Sie den PDC nach einem Problem bei der Migration wieder schneller in die produktive Umgebung gebracht. Im Einzelfall ist abzuwägen, ob die Vorbereitung mehr Zeit in Anspruch nehmen darf oder eher schnell mit dem Test begonnen werden soll, in der Hoffnung, dass alles gut läuft und nur im Worst-Case-Szenario Wiederherstellungsarbeiten zu leisten sind.

Außerdem müssen noch die folgenden Punkte auf dem PDC/BDC, der aktualisiert werden soll, sichergestellt sein:

1. Sofern Sie komprimierte Laufwerke verwenden, die mit *DriveSpace* oder *DoubleSpace* komprimiert worden sind, müssen Sie die Komprimierung aufheben. Unter Windows 2000/2003 ist zwar auch eine Komprimierung möglich, aber diese muss mit dem betriebssystemimmanenten Komprimierungsprogramm für NTFS-Laufwerke neu erstellt werden.
2. Falls der Computer über die serielle Schnittstelle mit einer unterbrechungsfreien Stromversorgung (USV) verbunden ist, sollte diese während der Aktualisierung entfernt werden. Da die Setup-Routine von Windows 2000/2003 die Geräte an den seriellen Schnittstellen versucht automatisch zu erkennen, kann dies u.U. zu Problemen führen.
3. Wenn Sie die Spiegelung von Datenträgern einsetzen, muss die Spiegelung vor Beginn der Aktualisierung aufgehoben werden. Ist das Windows 2000/2003-Setup abgeschlossen, können Sie die Datenträgerspiegelung wieder aktivieren.
4. Auf allen PDCs und BDCs muss mindestens das NT Servicepack 4 oder höher installiert sein.

27.4.3 Was geschieht beim Update auf dem PDC?

Das Update eines NT-PDC auf einen Windows 2000/2003-Domänencontroller ist ein recht komplexer Prozess, der im Folgenden näher beschrieben werden soll.

Die Installation von Active Directory erfolgt nach dem Update eines NT-PDC von NT4.0-Server auf einen Windows 2000/2003 Server durch den Aufruf von DCPROMO. Hierbei werden folgende Dinge durchgeführt:

1. Aus der Registry des PDC werden alle bestehenden SAM-Einträge in die neue Datenbank kopiert. Hierbei handelt es sich um die Einträge der Benutzerkonten und Computerkonten sowie der lokalen und globalen Gruppen.
2. Es wird das Kerberos V5-Protokoll installiert. Hierbei handelt es sich um das primäre Sicherheitsprotokoll für die Authentifizierung innerhalb der Windows 2000/2003-Domäne, bei dem die gegenseitige Authentifizierung (Überprüfung des Benutzers und der Netzwerkdienste) angewendet wird. Durch die Installation des Kerberos-Protokolls werden der Authentifizierungsdienst und der ticketgenehmigende Dienst auf dem Domänencontroller gestartet.

3. Haben Sie im Menü des Installations-Assistenten für Active Directory das Erstellen einer untergeordneten Domäne ausgewählt, wird automatisch eine transitive Vertrauensstellung zur übergeordneten Domäne hergestellt.
4. Auf diese neue untergeordnete Domäne werden alle Informationen bezüglich des Schemas und der Konfiguration vom Domänencontroller kopiert.
5. Wenn für die neu erstellte Domäne kein autorisierender DNS-Server gefunden wird oder aber ein autorisierender DNS-Server keine dynamische DNS-Aktualisierung unterstützt, müssen Sie einen DNS-Server installieren. Auch dies geschieht über einen Assistenten.

Hiermit sind die von der Active Directory-Installation durchgeführten Prozesse abgeschlossen. Nach einem Neustart des aktualisierten Rechners ist dieser ein neues funktionsfähiges Mitglied an seinem Platz in der Domänen- und Standortstruktur in der Active Directory-Gesamtstruktur. Die übrigen Domänencontroller erhalten gemäß der von Ihnen festgelegten Replikationstopologie Kenntnis über den neuen Domänencontroller in der Gesamtstruktur.

Der neue Domänencontroller wird nach seiner Aktualisierung von den noch bestehenden Windows NT-BDCs als Domänenmaster angesehen. Client-Computer mit einer früheren Version als Windows 2000 greifen auf den neuen Domänencontroller wie auf einen NT-Domänencontroller zu. Allerdings können diese Clients im gemischten Modus nur noch auf die Ressourcen in Domänen zugreifen, die explizite Windows NT-Vertrauensstellungen zu der neu erstellten Domäne besitzen.

Sie können nun in Ihrer Domäne sukzessive weitere BDCs zu Domänencontrollern heraufstufen. Während der Aktualisierung können die SAM-Einträge nur auf einem Domänencontroller unter Windows 2000/2003 erfolgen. Damit die noch vorhandenen BDCs mit dem Domänencontroller zusammenarbeiten können, übernimmt dieser die Rolle des PDC-Emulator-Betriebsmasters (siehe Kapitel 11.1.2). Dadurch sehen die BDCs den Domänencontroller als herkömmlichen Windows NT-PDC an. Der PDC-Emulator muss somit zwei Authentifizierungsprotokolle unterstützen, nämlich das NTLM-Protokoll für die Kommunikation mit den NT-Rechnern und das Kerberos V5-Protokoll für die Authentifizierung innerhalb der Windows 2000/2003-Domäne.

27.4.4 Verschiedene Wege zur neuen Gesamtstruktur

Den einfachsten Weg der Aktualisierung der NT-Domänenstruktur können Sie beschreiben, wenn Ihr Unternehmen entweder nur eine einzelne Domäne umfasst oder sämtliche Domänen gegenseitige Vertrauensstellungen untereinander besitzen. Bei einer einzelnen Domäne müssen Sie nur einmalig den Active Directory-Installationsassistenten starten und die bestehende Domäne ins Active Directory konvertieren. Auch gegenseitige Vertrauensstellungen von Domänen bleiben während der Migration erhalten und werden übernommen. Die Modelle dieser beiden Szenarien sind zwar am einfachsten zu aktualisieren, aber leider wird in den wenigsten Unternehmen eine der beiden simplen Strukturen vorhanden sein.

Viel eher wird es der Fall sein, dass Sie ein Domänenmodell mit einer oder mehreren Masterdomänen und untergeordneten Ressourcendomänen im Einsatz haben. Die verschiedenen NT-Domänenmodelle wurden bereits in Kapitel 2.1 ausführlich beschrieben.

Als Erstes müssen Sie entscheiden, ob Sie als neue Stammdomäne der Gesamtstruktur eine neue Domäne erstellen möchten und dieser dann die vorhandenen Domänen hinzufügen wollen oder ob eine bestimmte vorhandene Domäne die neue Stammdomäne werden soll. Es gibt dann drei verschiedene Wege, eine neue Struktur zu erstellen. Diese werden nun erläutert:

1. Erstellen einer neuen Stammdomäne
2. Migration einer bestehenden Domäne als Stammdomäne
3. Getrennte Domänenstruktur in gemeinsamer Gesamtstruktur

Für die drei Methoden zur Erstellung einer neuen Struktur soll die folgende Ausgangskonstellation der NT-Domänen gelten (siehe Abbildung 27.1):

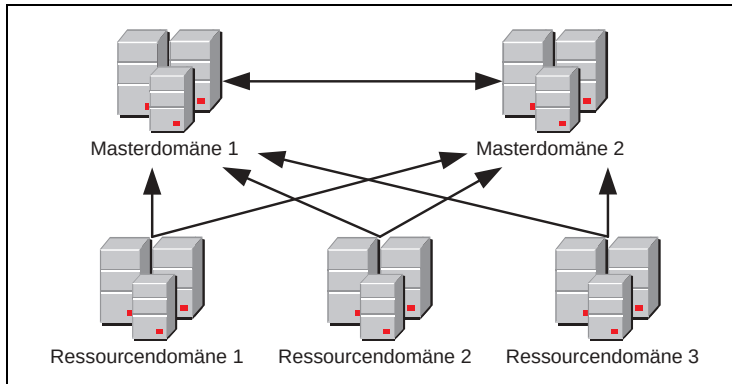


Abbildung 27.1: Die NT-Domänen vor der Aktualisierung

Die beiden Masterdomänen enthalten die Benutzerkonten und vertrauen sich gegenseitig. Die drei Ressourcendomänen haben je eine einseitige Vertrauensstellung zu den beiden Masterdomänen. Damit ist gewährleistet, dass sich die Benutzer an den Ressourcendomänen anmelden und auf die Ressourcen dieser drei Domänen zugreifen können.

Erstellen einer neuen Stammdomäne

Bei dieser Methode erstellen Sie eine komplett neue Stammdomäne im Active Directory. Jede der beiden Masterdomänen repräsentiert nun eine eigene Domänenstruktur unterhalb der Stammdomäne. Die Ressourcendomänen werden als untergeordnete Domänen der Masterdomänen hinzugefügt. Dabei ist es sowohl möglich, eine oder mehrere Ressourcendomänen direkt unterhalb einer Masterdomäne (wie dargestellt) als auch eine Ressourcendomäne unterhalb einer anderen Ressourcendomäne anzusiedeln. Nach Durchführung dieser Methode bietet sich folgendes Bild (siehe Abbildung 27.2):

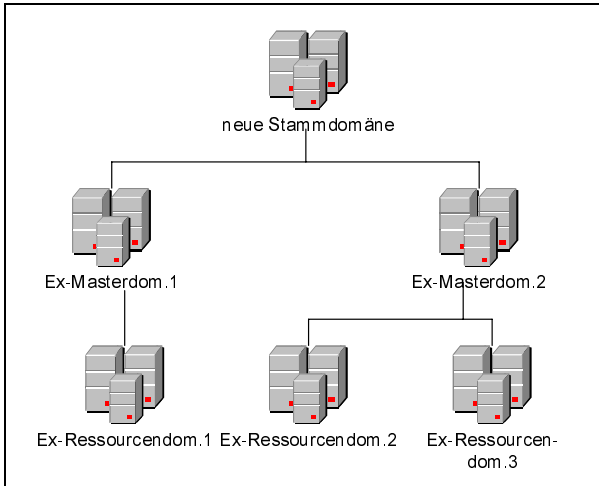


Abbildung 27.2: Die Masterdomänen als Teilstruktur einer Stammdomäne

Migration einer bestehenden Domäne als Stammdomäne

In diesem Fall müssen Sie eine der beiden Masterdomänen auswählen, die die neue Stammdomäne der Gesamtstruktur repräsentieren soll. Die andere Masterdomäne wird der neuen Stammdomäne untergeordnet. Die Ressourcendomänen können nun entweder alle gleichrangig der ehemaligen Masterdomäne 2 untergeordnet werden (im Bild Ressourcendomäne 2). Es kann aber auch eine der Ressourcendomänen direkt der neuen Stammdomäne untergeordnet werden (im Bild Ressourcendomäne 1), oder die Ressourcendomänen werden unterhalb einer anderen Ressourcendomäne angesiedelt (im Bild Ressourcendomäne 3). Nach Durchführung dieser Migrationsmethode kann sich beispielsweise das folgende Bild ergeben (siehe Abbildung 27.3):

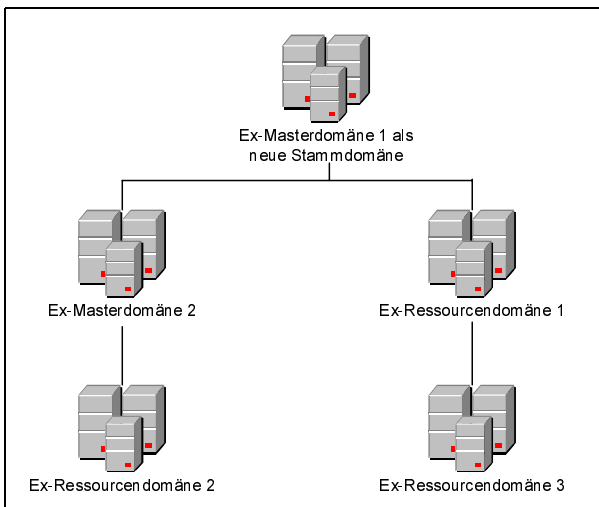


Abbildung 27.3: Eine Masterdomäne wird zur Stammdomäne der Gesamtstruktur

Getrennte Domänenstruktur in gemeinsamer Gesamtstruktur

Bei der dritten Methode wird jede Domäne zu einer eigenen Domänenstruktur. Die erste migrierte Masterdomäne wird zur Stammdomäne der Gesamtstruktur. Die übrigen Masterdomänen werden zu Stammdomänen ihrer eigenen Domänenstruktur. Diesen Masterdomänen können die Ressourcendomänen beliebig untergeordnet werden.

Egal für welches der drei Modelle Sie sich auch entschieden haben, für die praktische Umsetzung ist für alle Modelle Folgendes zu bedenken und durchzuführen:

1. Zuerst müssen immer die übergeordneten Masterdomänen aktualisiert werden, weil die Ressourcendomänen von ihnen abhängig sind.
2. Aktualisieren Sie den PDC der gewünschten Masterdomäne auf Windows 2000/2003. Damit haben Sie die neue Stammdomäne eingerichtet.
3. Prüfen Sie, ob durch die Migration Vertrauensstellungen zwischen der neuen Domäne und bestehenden Master- oder Ressourcendomänen verloren gegangen sind. Sollte dies der Fall sein, stellen Sie die Vertrauensstellungen wieder her.
4. Nach der Migration des PDC der neuen Domäne können Sie die vorhandenen BDCs oder einen Teil davon auf Windows 2000/2003 aktualisieren.
5. Aktualisieren Sie nun in der eben genannten Reihenfolge die übrigen Masterdomänen.
6. Überprüfen Sie, ob die Vertrauensstellungen zu den noch bestehenden NT-Ressourcendomänen noch vorhanden sind. Stellen Sie diese bei Bedarf wieder her. Dabei handelt es sich um explizite Vertrauensstellungen. Die neu erstellten Windows 2000/2003-Domänen besitzen automatisch untereinander implizite transitive Vertrauensstellungen.
7. Wenn Sie alle Masterdomänen aktualisiert haben, können Sie entweder damit beginnen, diese Domänen zusammenzufassen, oder aber Sie setzen die Aktualisierung auf Windows 2000/2003 mit den Ressourcendomänen fort. Die Ressourcendomänen müssen auch auf Windows 2000/2003 aktualisiert sein, damit diese später zu Organisationseinheiten (OUs) konvertiert werden können.

27.4.5 Domänenstruktur und Verwaltungsvorgaben

Gerade bei der Migration eines NT-Multi-Domänenmodells in eine einzelne Active Directory-Domäne kann oftmals der Einwand kommen, dass in einer einzelnen Domäne nicht die Sicherheit bei der Verwaltung garantiert ist wie bei mehreren Domänen. In jeder Domäne gibt es die vordefinierte Gruppe der Domänenadministratoren. Diese Gruppe hat vollen Zugriff auf alle Objekte der Domäne. Dieser Zugriff besteht auch, wenn die Verwaltung bestimmter Objekte an andere Personen der Domäne delegiert ist. Soll der Gruppe der Domänenadministratoren nicht der Zugriff auf alle Ressourcen ermöglicht werden, so hilft lediglich das Einrichten mehrerer Domänen.

Prüfen Sie die folgenden Fragen, um herauszufinden, ob ein Einzeldomänen-Modell den Anforderungen des Unternehmens entspricht. Sind die folgend aufgeführten Punkte erfüllt, können Sie eine einzelne Domäne verwenden. Sind einige Punkte nicht erfüllt, sollten Sie ein Multi-Domänenmodell implementieren.

1. Wird von einer zentralen Stelle aus die Verantwortlichkeit für alle Clients und Server sowie Benutzer und Benutzergruppen der Domäne übernommen? Ist dies nicht der

Fall, verwenden Sie mehrere Domänen, deren jeweilige Domänenadministratoren die volle Verantwortung für die entsprechenden Objekte der Domäne tragen.

2. Sofern nur eine Domäne implementiert ist, gelten für sämtliche Benutzer identische Bestimmungen bezüglich der Passwortlänge, -komplexität und -gültigkeitsdauer. Sind in bestimmten Bereichen höhere Sicherheitsanforderungen an Passwörter notwendig, so müssen für diese Unternehmensbereiche separate Domänen erstellt werden.
3. Darf aus Sicherheitsaspekten eine einzelne Person oder eine Abteilung das Recht zum Ändern aller Active Directory-Objekte besitzen, oder soll diese Aufgabe unter den Domänenadministratoren der einzelnen Domänen aufgeteilt werden?

Ist die Administration der einzelnen Domänen bereits erfolgreich implementiert, sodass die Administratoren lediglich für eine Domäne zuständig sind, besteht keine Notwendigkeit, dieses Prinzip zu ändern. In diesem Fall ist eine leere Stammdomäne zu empfehlen, unter der alle Domänen angeordnet werden, die jeweils vor Ort verwaltet werden. Die leere Stammdomäne erfüllt lediglich den Zweck, eine Basis für alle untergeordneten Domänen zu sein. In diesem Modell ergibt sich jedoch – je nach Sicht der Dinge – das Problem oder die Chance, dass die Administratoren einer Domäne Benutzern einer anderen Domäne Zugriffsrechte für ihre Ressourcen einräumen können. Da die untergeordneten Domänen automatisch zur Stammdomäne eine transitive Vertrauensstellung aufbauen, vertrauen sich auch alle untergeordneten Domänen untereinander. So hat ein Administrator der Domäne *vertrieb.firma.de* die Möglichkeit, Benutzern der Domäne *marketing.firma.de* Zugriffsrechte für Dateiserver in seiner Domäne zu gewähren.

Um auch die Vertrauensstellungen der Domänen innerhalb der Gesamtstruktur zu unterbinden, hilft nur die Einrichtung separater Gesamtstrukturen. Dies ist auch notwendig, wenn aus firmenpolitischen Gründen verschiedene Geschäftsbereiche unabhängig voneinander bleiben müssen. In besonderen Fällen bleibt die Möglichkeit, manuell Vertrauensstellungen zwischen den Gesamtstrukturen zu erstellen. Der Datenaustausch zwischen den separaten Gesamtstrukturen kann jedoch auch völlig ohne Vertrauensstellungen erfolgen. E-Mails können ohnehin verschickt werden, und der Datenaustausch ist via FTP oder den Einsatz eines Microsoft Share Point Portal Servers dennoch möglich.

27.5 Das Active Directory Migration Tool (ADMT)

Das Active Directory Migration Tool (ADMT) wird benötigt, wenn Sie sich für die Migration entschieden haben und Sie aus den alten NT-Domänen die Daten in die neue Domäne importieren möchten. ADMT kann direkt von Microsoft unter folgendem Link heruntergeladen werden: (<http://www.microsoft.com/windows2000/downloads/tools/admt/default.asp>).

Die Version 1.0. des ADMT wurde für die Migration von Windows NT auf Windows 2000 benutzt. Mit der aktuellen Version 2.0, die zeitgleich mit Windows Server 2003 ausgeliefert wird, sind Migrationen auf Windows 2000 und Windows 2003 möglich. ADMT besteht aus einem Satz von Wizards, die für die Migration von Benutzerkonten, Computerkonten usw. zuständig sind. Nach der Installation können die Wizards aus der mmc ACTIVE DIRECTORY MIGRATIONSPROGRAMM heraus gestartet werden (siehe Abbildung 27.4).

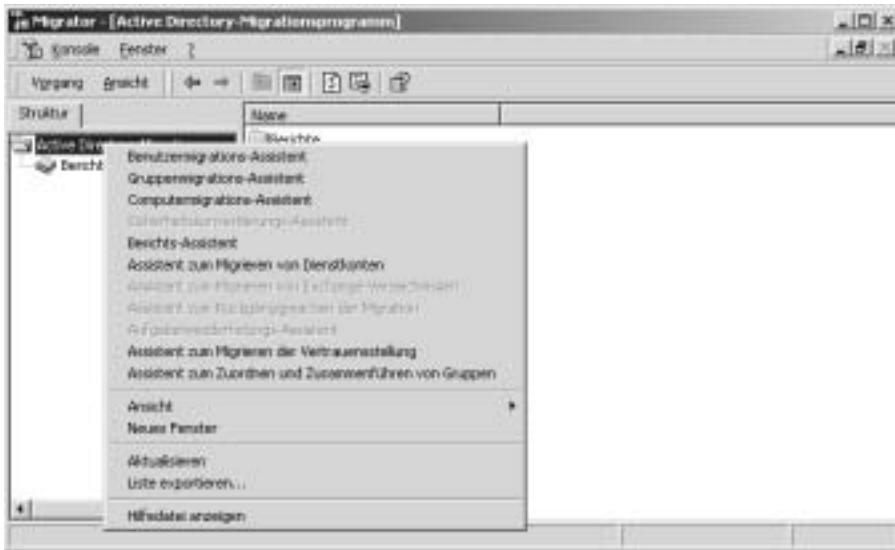


Abbildung 27.4: Die mmc des Active Directory-Migrationsprogrammes (ADMT)

27.5.1 Features

Dieses Kapitel zeigt, welche Daten über ADMT in die Active Directory-Domäne importiert werden können und welche Einschränkungen und Möglichkeiten dabei bestehen.

Benutzerkonten

Über den BENUTZERMIGRATIONS-ASSISTENT können Sie die Benutzerkonten mit sämtlichen Einstellungen importieren. Besonders wichtig ist in diesem Zusammenhang die Möglichkeit, die SID-History-Informationen des Benutzerkontos ebenfalls zu migrieren. Damit wird sichergestellt, dass die Benutzer als Mitglied der Active Directory-Domäne noch auf ihre alten Ressourcen auf Dateiservern oder auch auf Exchange 5.5-Postfächer zugreifen können. Allerdings gilt für die Version 1.0, dass das Benutzerpasswort nicht migriert werden kann. Sie haben lediglich die Wahl, das Passwort dem Benutzernamen gleichzusetzen oder ein zufälliges Passwort zu erstellen. Die ursprünglichen Passwörter können erst mit ADMT 2.0 migriert werden. Außerdem können Sie entscheiden, ob das Benutzerkonto in der NT-Domäne oder in der Active Directory-Domäne deaktiviert werden soll oder ob beide Konten aktiviert bleiben sollen.

Benutzergruppen

Über den GRUPPENMIGRATIONS-ASSISTENT werden die Gruppeninformationen in die Zieldomäne kopiert. Zusätzlich können Sie den ASSISTENT ZUM ZUORDNEN UND ZUSAMMENFÜHREN VON GRUPPEN benutzen, um eine Gruppe in der Quelldomäne einer neuen oder bereits bestehenden Gruppe in der Zieldomäne zuzuweisen. Werden die Gruppeninformationen vor den Benutzerinformationen in die Zieldomäne importiert, so können Sie danach wahlweise die Benutzerkonten migrieren oder lediglich die Informationen zur Gruppenmitgliedschaft dieser Gruppe.

Computer

Mit dem COMPUTERMIGRATIONS-ASSISTENT erstellen Sie nicht nur die Computerkonten an sich in der neuen Domäne. Es besteht auch die Möglichkeit, alle bestehenden lokalen Benutzerprofile sowie deren Einstellungen auf den Windows 2000-Computer zu migrieren. Beim Ausführen dieses Assistenten werden automatisch die Agenten auf den Zielcomputern installiert.

Bei der Migration von Benutzern, Gruppen und Computern besteht die Möglichkeit, diese aus den Ressourcendomänen direkt in OU-Container der Active Directory-Domäne zu importieren.

Dienstkonten

Über den ASSISTENT ZUM MIGRIEREN VON DIENSTKONTEN werden sämtliche Dienstkonten migriert, die von Applikationen benutzt werden, z.B. Exchange oder SQL.

Vertrauensstellungen

Mit dem ASSISTENT ZUM MIGRIEREN DER VERTRAUENSSTELLUNG werden in der Zieldomäne alle Vertrauensstellungen zu den Domänen hergestellt, zu denen die Quelldomäne bereits Vertrauensstellungen besaß.

Die Migration rückgängig machen

Mit dem ASSISTENT ZUM RÜCKGÄNGIGMACHEN DER MIGRATION können Sie bereits durchgeführte Migrationsschritte wieder zurücknehmen. Es wird der ursprüngliche Zustand wiederhergestellt.

Zusätzlich stehen noch einige weitere Wizards zur Verfügung, so z.B. der ASSISTENT ZUM MIGRIEREN VON EXCHANGE-VERZEICHNISSEN. Diese können jedoch nur angewählt werden, wenn die entsprechenden Komponenten in der Domäne vorhanden sind.

Jeder Migrationsassistent kann zunächst im Testmodus gestartet werden. Dabei werden noch keine Änderungen vorgenommen. Lesen Sie die Logdateien und Berichte, um zu sehen, ob es beim Test zu Problemen gekommen ist. Dennoch sollten Sie sämtliche Migrationaufgaben zunächst in einer Testumgebung durchführen. Erst wenn hier alle Schritte einwandfrei ausgeführt wurden, wenden Sie *ADMT* in der produktiven Umgebung an.

In der Version 1.0 kann *ADMT* nur über die GUI ausgeführt werden. Erst ab der Version 2.0 ist auch die Ausführung der Befehle via Skript möglich.

Ausführliche Anleitungen und Konzepte für die Benutzung des *ADMT* finden Sie unter dem Link

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/deploy/cookbook/cookintr.asp>

27.5.2 Voraussetzungen

Um mit *ADMT* arbeiten zu können, müssen einige Voraussetzungen aufseiten der NT-Domäne und der Active Directory-Domäne erfüllt sein.

NT-Quelldomäne

1. Installieren Sie auf dem PDC der NT-Quelldomäne Servicepack 4 oder höher.
2. Der *ADMT*-Agent, der von *ADMT* auf den zu migrierenden Quellcomputern installiert wird, kann nur unter Windows 2000, NT 4.0 SP4 oder NT 3.51 SP5 ausgeführt werden.
3. Für die Kontenverwaltung muss das Auditing aktiviert sein (erfolgreiche und fehlgeschlagene Ereignisse).
4. Es muss eine Vertrauensstellung zur Zieldomäne existieren.
5. Auf dem PDC muss in der Registry unter `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA` der Schlüssel `TcpipClientSupport` mit dem Wert `REG_DWORD 0x1` hinzugefügt werden.
6. Die globale Gruppe der Domänen-Admins der Quelldomäne muss Mitglied der lokalen Gruppe der Administratoren der Zieldomäne sein. Zusätzlich muss eine neue lokale Gruppe namens *Source Domain\$\$\$* erstellt werden, die aber keine Mitglieder enthalten soll.

Active Directory-Zieldomäne

1. Die Zieldomäne muss im einheitlichen Betriebsmodus laufen. Eine Migration in eine 2000/2003-Domäne im gemischten Modus ist nicht möglich. Dies liegt darin begründet, dass das SID-History-Attribut für die Benutzer- und Gruppenkonten nur im einheitlichen Modus verfügbar ist und mit Werten gefüllt werden kann. Wäre dieses Attribut auch im gemischten Modus verfügbar, würde die Replikation mit den NT-BDCs nicht funktionieren, da diese das Attribut nicht kennen.
2. Für die Kontenverwaltung muss das Auditing aktiviert sein (erfolgreiche und fehlgeschlagene Ereignisse).
3. Es muss eine Vertrauensstellung zur Quelldomäne existieren.
4. Die lokale Gruppe der Administratoren der Zieldomäne muss Mitglied der globalen Gruppe der Domänen-Admins der Quelldomäne sein.
5. Führen Sie *ADMT* auf dem Domänencontroller aus, der die Betriebsmasterrolle des PDC-Emulators innehat.
6. In der Zieldomäne sowie auf allen Computern, auf denen der *ADMT*-Agent ausgeführt wird, müssen administrative Freigaben vorhanden sein.

Auf dem Server, auf dem *ADMT* ausgeführt wird, müssen Sie sich mit einem Benutzerkonto anmelden, das die folgenden Eigenschaften erfüllt: Der Benutzer muss Mitglied der Administratoren-Gruppe in der NT-Quelldomäne, Mitglied der globalen Gruppe der Domänenadministratoren in der Zieldomäne sein sowie über Administratorrechte auf jedem Computer verfügen, der migriert werden soll.

27.5.3 Features des ADMT Version 2.0

Die Version ADMT 2.0 (enthalten auf der Windows 2003 Server-CD) wird zeitgleich mit dem Windows 2003 Server fertig gestellt. Neben der Migration von NT zu 2000 können Sie mit der Version 2.0 auch eine Migration von 2000 auf 2003 durchführen. Die neue Version muss nicht ausschließlich über die GUI bedient werden, sondern kann auch per Skript gesteuert werden. Dazu wird das Beispielskript *TemplateScript.vbs* mitinstalliert, aus dem die verschiedenen Optionen ersichtlich sind.

Eine weitere Neuerung besteht darin, dass nun auch Passwörter von Benutzerkonten bei der Migration zwischen zwei Gesamtstrukturen übernommen werden können. Dabei wird ein Password Export Server (PES) in der Quelldomäne benutzt. Auch die Überwachung und Sicherheit wurde verbessert. So wird für jeden neuen ADMT-Arbeitsschritt eine neue Logdatei angelegt. Bei der Computerkonten-Migration müssen Sie nicht mehr bei jeder Verteilung des ADMT-Agents ein Benutzerkonto und Kennwort angeben.

27.5.4 Weitere Migrationstools

Neben dem eben beschriebenen Active Directory Migration Tool von Microsoft gibt es noch eine Reihe weiterer Programme von Drittanbietern zur Vereinfachung und Automatisierung der Migration. Diese haben z.T. sogar ein weiteres Funktionsspektrum als ADMT.

- ▶ Die Firma NetIQ bietet für die Migration den *Domain Migration Administrator* an (<http://www.netiq.com/products/dma/default.asp#>). Mit diesem Programm kann im Gegensatz zu ADMT sogar eine Migration durchgeführt werden, wenn sich die Zieldomäne noch im gemischten Modus befindet. Gerade die ADMT-Anforderung an eine Zieldomäne im einheitlichen Modus stellt für viele Unternehmen die größte Hürde dar, wenn ein Umstieg in den einheitlichen Modus nicht praktikabel ist.
- ▶ Ein weiteres Produkt ist der *FastLane Migrator* der Firma QuestSoftware (<http://www.quest.com/fastlane/migrator/>). Dieses Produkt versammelt in einer mmc alle Assistenten, die der Reihe nach für eine Migration von Windows NT zum Active Directory aufgerufen werden können.
- ▶ Weitere Programme sind der *bv-Admin for Windows 2000 Migration* der Firma Bind-View (<http://www.bindview.com/products/admin/winmig.cfm>) oder der *Domain Migration Wizard* von Aelita Software (<http://www.aelita.com/products/DMW.htm>).

Diese Auflistung erhebt keinen Anspruch auf Vollständigkeit. Es ist ferner nicht Sinn dieses Buches, die Programme miteinander zu vergleichen oder zu bewerten. Es wird sich jedes Unternehmen seine eigenen Gedanken zu den Tools machen und danach entscheiden, ob überhaupt eines davon eingesetzt werden soll oder nicht, zumal von den meisten Programmen Demo-Versionen bezogen werden können.

27.6 Die Migration gleichnamiger NT-Benutzergruppen

Eine Herausforderung bei der Migration ist auch das Zusammenführen von mehreren gleichnamigen Gruppen der NT-Domänen zu einer einzigen Gruppe diesen Namens im Active Directory. Angenommen, Sie verfügen in drei verschiedenen NT-Domänen über die Benutzergruppe „Manager“ und wollen diese drei Gruppen in einer einzelnen Active Directory-Domäne zu einer Gruppe zusammenführen, die alle Mitglieder der einzelnen Gruppen umfasst. Auch in dieser Konstellation muss wieder besonderes Augenmerk auf die SID-History geworfen werden.

Die Mitglieder der Gruppe „Manager“ in der Domäne A können nur auf die Ressourcen zugreifen, in deren ACL die SID ihrer Gruppe eingetragen ist, dasselbe gilt auch für die Gruppenmitglieder in den Domänen B und C. Dabei ist es unwichtig, ob die Domänen über Vertrauensstellungen untereinander verfügen oder nicht.

Sobald Sie nun mit *ADMT* oder einem anderen Programm die Domänen A, B und C migrieren, werden die gleichnamigen Gruppen in einer neuen globalen Gruppe vereint und dieser die Mitglieder der alten Gruppen hinzugefügt. Dabei werden die SIDs der drei ursprünglichen Gruppen in die SID-History der neuen Gruppe im Active Directory geschrieben. Jedes Mitglied der neuen Gruppe verfügt nun über eine Reihe von SIDs, nämlich der SID des alten und neuen Benutzerkontos sowie der SID der neuen Benutzergruppe sowie aller SIDs der drei alten Benutzergruppen „Manager“. Dies führt dazu, dass ein Benutzer, der zuvor Mitglied der Gruppe „Manager“ in Domäne A war und nur auf Ressourcen seiner Domäne zugreifen konnte, nun auch auf die Ressourcen Zugriff hat, die zuvor den Manager-Mitgliedern der Domänen B und C vorbehalten waren. Ist die durch die Migration entstandene Erweiterung der Zugriffsberechtigung erwünscht, können Sie dieses Verfahren auch für weitere Gruppen anwenden.

Sollen dem Benutzer nach der Migration auch weiterhin nur die Ressourcen seiner alten Domäne zur Verfügung stehen, dürfen Sie die NT-Benutzergruppen nur migrieren, wenn sie in der Active Directory-Domäne verschiedene Namen bekommen. So wäre es denkbar, die neuen Benutzergruppen „ManagerA“, „ManagerB“ und „ManagerC“ einzurichten.

Verwenden Sie für die Migration den *Domain Migration Wizard* von Aelita Software, haben Sie die Möglichkeit, den Gruppennamen spezielle Präfixe oder Suffixe mitzugeben. In diesem Fall werden die einzelnen Gruppen beibehalten, und die Benutzer erhalten nur Zugriff auf die Objekte, auf die sie schon vor der Migration Zugriff hatten.

27.7 Die manuelle Migration

Selbstverständlich müssen Sie für die Migration nicht *ADMT* oder eines der anderen Programme benutzen. Sie können auch die neuen Domänen erstellen und manuell die Benutzer, Gruppen, Computer und Mitgliedsserver einpflegen sowie anschließend die überflüssigen Domänen löschen. Für diesen komplexen Vorgang müssen Sie auf verschiedene Programme des Ressource-Kits und der Support-Tools zurückgreifen.

27.7.1 Verschieben von Benutzern

Für das Verschieben der Benutzer zwischen den Domänen müssen diese im einheitlichen Modus betrieben werden. Zum Verschieben von Benutzern müssen Sie die folgenden Schritte ausführen:

1. Übertragen Sie zuerst sämtliche globalen Gruppen, in denen die zu verschiebenden Benutzer Mitglied sind, in die Zieldomäne. Die bestehenden Verknüpfungen in der Quelldomäne bleiben auch beim Verschieben der Gruppe selbst erhalten.
2. Jetzt können die einzelnen Benutzer in die Zieldomäne verschoben werden. Dabei erhalten die globalen Gruppen in der neuen Domäne aktualisierte Informationen über die Mitgliedschaften, da die Benutzer jetzt denselben Gruppen nur in der neuen statt in der alten Domäne angehören.

Für das Verschieben von Benutzern zwischen der alten und neuen Domäne sollten Sie die Windows 2000 Resource Kit Tools *MOVETREE* (siehe Kapitel 23.1.15) oder *SIDWALK* benutzen. Mit *MOVETREE* können Sie Container von einem Teil einer Struktur einer Domäne in eine andere Domäne verschieben.

SIDWALK sollten Sie anschließend benutzen, um die ACLs zu überprüfen und anzupassen. Auch dieses Tool können Sie an der Kommandozeile über `sidwalk.exe`  aufrufen. Bevorzugen Sie hingegen die Arbeit an der grafischen Oberfläche, so rufen Sie an der Kommandozeile `sidwalk.msc`  auf.

SIDWALK arbeitet in drei Stufen. Im ersten Schritt müssen Sie ermitteln, welche Benutzer Zugriff auf Ressourcen wie freigegebene Ordner, Drucker usw. auf einem beliebigen Computer haben. Danach müssen Sie sich entscheiden, ob die alten ermittelten Sicherheitsidentitäten gelöscht oder z.B. durch neue Sicherheitsgruppen ersetzt werden sollen. Im dritten Schritt werden dann die ACLs anhand der ermittelten Ergebnisse und Planungen konvertiert. Dieser Arbeitsvorgang ist komplexer, als er auf den ersten Blick scheinen mag. Auf jeden Fall ist das Tool *SIDWALK* sehr ressourcenintensiv.

27.7.2 Verschieben von Benutzergruppen

Erst mit der Ausführung der Domäne im einheitlichen Modus haben Sie die Möglichkeit, bestehende Gruppen in universelle Gruppen zu konvertieren. Mitglieder universeller Gruppen können Gruppen aus verschiedenen Domänen sein. Diese Mitglieder haben Zugriff auf Ressourcen verschiedener Domänen (vgl. hierzu Kapitel 18.5).

Für die Einrichtung der Gruppen gibt es zwei verschiedene Verfahren. So können Sie eine neue parallele Gruppe einrichten. Hierbei werden alle Mitglieder der einzelnen Gruppen zu der neuen Gruppe hinzugefügt. Diese Personen sind nun vorübergehend sowohl Mitglied der alten Gruppe(n) als auch der neu eingerichteten universellen Gruppe. Die alten Gruppen können gelöscht werden. Der andere Weg besteht darin, die bestehenden Gruppen zu verschieben. Allerdings sind dabei einige Punkte zu beachten.

Angenommen, Sie haben drei gleichnamige globale Gruppen in drei verschiedenen Domänen: Die Gruppe „Mitarbeiter“ in den Domänen *vertrieb.firma.de*, *buchhaltung.firma.de* und *marketing.firma.de*. Die globalen Gruppen sollen zur universellen

Gruppe „Mitarbeiter“ der Domäne *firma.de* werden. Führen Sie dazu die folgenden Schritte durch:

1. Zunächst müssen die globalen Gruppen „Mitarbeiter“ in ihrer jeweiligen Domäne zu universellen Gruppen konvertiert werden.
2. Die eben erstellten universellen Gruppen müssen unterschiedliche Namen bekommen, damit sie in einer Domäne vorhanden sein können. Die neuen Namen könnten etwa so aussehen: *vertrieb\vertrieb_mitarbeiter*, *buchhaltung\buchhaltung_mitarbeiter* und *marketing\marketing_mitarbeiter*.
3. Jetzt können Sie die drei Gruppen verschieben. Bringen Sie die drei im letzten Schritt erstellten Gruppen in die Domäne *firma.de*.
4. Jetzt müssen Sie in der Domäne *firma.de* eine neue universelle Gruppe erstellen. Diese Gruppe könnte dann „Mitarbeiter“ heißen.
5. Fügen Sie zu der neuen universellen Gruppe „Mitarbeiter“ die Mitglieder der drei Gruppen „vertrieb“_mitarbeiter, „buchhaltung“_mitarbeiter und „marketing_mitarbeiter“ hinzu.

Der erste Weg ist sicherlich einfacher, insbesondere dann, wenn die zu konvertierenden Gruppen von Applikationen oder Servern benötigt werden. Folgen Sie dem zweiten Weg, müssen Sie die Gruppen einmal nach dem Umbenennen anpassen und zum zweiten Mal nach dem Verschieben der Gruppe. Alternativ dazu könnten Sie auch die entsprechend verweisenden Applikationen und Server anpassen. Benutzen Sie jedoch die erste Methode, müssen die Gruppen nur einmal angepasst werden, was deutlich weniger Arbeit bedeutet.

27.7.3 Verschieben von Computern

Das Verschieben von Computern ist einfacher als das von Benutzern und Gruppen. Um Computerkonten zwischen Domänen zu verschieben, muss die Domäne – im Gegensatz zum Verschieben von Benutzern und Benutzergruppen – nicht im einheitlichen Modus ausgeführt werden. Ein Computerkonto unter Windows NT war nur in einer Domäne vorhanden, damit der Benutzer sich von diesem Rechner aus anmelden konnte. Es lag nur eine einseitige Vertrauensstellung zwischen Computer und Domäne vor.

Um Computer zu verschieben, verwenden Sie das Kommandozeilentool *NETDOM* (siehe Kapitel 23.1.17). Beim Verschieben von Computern wird das Ursprungs-konto in der Quelldomäne nicht gelöscht, sondern nur deaktiviert. Im Gegensatz zu NT können einzelne Computer unter 2000 zu Mitgliedern einer Gruppe werden.

27.7.4 Verschieben von Mitgliedsservern

Mitgliedsserver können entweder in andere Domänen verschoben oder sogar zum neuen Domänencontroller werden. Um einen Mitgliedsserver zwischen zwei Domänen zu verschieben, müssen die folgenden Punkte gewährleistet sein:

1. Die Ziel- und die Quelldomäne des Mitgliedsservers müssen im einheitlichen Modus betrieben werden.

2. Verschieben Sie alle Gruppen des Mitgliedsservers in die Zieldomäne. Damit werden die Gruppenmitgliedschaften beibehalten.
3. Verschieben Sie dann den Mitgliedsserver selbst in die Zieldomäne. Alternativ dazu können Sie auch den Mitgliedsserver zu einem neuen Domänencontroller heraufstufen.

27.7.5 Löschen von Domänen

Wenn Sie aus einer Domäne sämtliche Benutzer, Gruppen, Computer und Mitgliedsserver entfernt haben, steht dem Löschen der dann überflüssigen Domäne nichts mehr im Wege. Zum Löschen der nicht mehr benötigten Domänen können Sie das Programm *ADSIEDIT* (siehe Kapitel 23.1.2) benutzen.

27.8 Nach der Migration

Sobald Sie die Migration entweder mithilfe von *ADMT* oder eines anderen Programms oder aber auch manuell durchgeführt haben, können Sie der neuen Domäne quasi den letzten Feinschliff geben. Dazu zählen das Löschen der SID-History sowie die Eliminierung von NetBIOS aus dem TCP/IP-Netzwerk. Beide Schritte sind optional, sollten aber zur Verbesserung der Active Directory-Leistung angedacht werden.

27.8.1 Aktualisieren der ACLs und Löschen der SID-History

Nach der erfolgreichen Migration haben Sie die Möglichkeit, die ACLs der Ressourcen z.B. auf Dateiservern so anzupassen, dass lediglich die SIDs des Active Directory benutzt werden. Als logische Konsequenz kann danach die SID-History im Active Directory gelöscht werden. Die Zuweisung der neuen SIDs zu den ACLs darf jedoch erst dann erfolgen, wenn sämtliche Benutzer und Gruppen migriert worden sind. Diese Aufgabe kann beispielsweise mit *ADMT* erledigt werden.

ADMT durchsucht die SIDs in den ACLs sämtlicher Ordner und Dateien auf einem zu spezifizierenden Computer. Findet sich dabei eine Übereinstimmung zwischen der SID der Ressource und einer SID aus der SID-History, so ersetzt *ADMT* die SID mit der neuen SID des Active Directory-Benutzer- oder Gruppenkontos. Ist dieser Vorgang abgeschlossen, werden in den ACLs der Ressourcen ausschließlich die neuen SIDs benutzt. Für diesen Prozess installiert *ADMT* Wizards auf den zu migrierenden Computern, die den Scan- und Änderungsvorgang im Hintergrund ausführen.

Komfortabler als *ADMT* ist die Server Consolidation Wizard-Komponente des *Domain Migration Wizard* von Aelita Software. Dieser verwendet wie *ADMT* Agents, die die ACLs scannen und modifizieren. Das anschließende Verschieben der geänderten Daten auf einen neuen Dateiserver kann sogar durchgeführt werden, wenn die Dateien gerade benutzt werden. Dasselbe gilt auch für Freigaben. Es ist also nicht notwendig, den Dateiserver offline zu schalten. Zusätzlich können Sie den Agents eine bestimmte Priorität zuweisen. So verhindern Sie, dass der Server mit der Umsetzung der SIDs so ausgelastet wird, dass er keine anderen Aufgaben mehr übernehmen kann.

27.8.2 Ein Netzwerk ohne NetBIOS

Mit der Implementierung von Active Directory kann NetBIOS im TCP/IP-Netzwerk theoretisch entfernt werden, da das Namenskonzept auf DNS und nicht mehr auf NetBIOS beruht. Damit kann der komplette NetBIOS-Verkehr aus dem Netzwerk eliminiert werden. Allerdings gibt es zahlreiche Applikationen und Windows-eigene Befehle, die zwangsläufig NetBIOS erfordern, da sie einen NetBIOS API-Layer für ihre Funktion verwenden. Ein Beispiel dafür sind sämtliche Windows Net-Befehle wie `net use` usw.

Ein erster Schritt zur Eliminierung von NetBIOS besteht darin, alle Computer, die NetBIOS für die Namensauflösung verwenden, ins Active Directory aufzunehmen. Damit ist sichergestellt, dass für die Namensauflösung ausschließlich DNS benutzt wird.

Überprüfen Sie dann alle verwendeten Applikationen dahingehend, ob sie zwangsläufig NetBIOS erfordern. Möglicherweise müssen Applikationen in einer neueren Version installiert werden. In jedem Fall müssen Sie die Applikationen in einer Testumgebung gründlich auf Probleme durch das Ausschalten von NetBIOS prüfen.

27.8.3 Aktualisierte Domänencontroller und die Client-Anmeldung

Sobald in der NT-Domäne ein PDC oder BDC auf Windows Server 2000 oder Windows Server 2003 aktualisiert wurde, verwenden sämtliche Clients der Betriebssysteme Windows XP und Windows 2000 ausschließlich diesen aktualisierten Domänencontroller für die Anmeldung. Dies liegt darin begründet, dass die Clients an einem Domänencontroller unter Windows Server 2000/2003 die Kerberos-Authentifizierung durchführen können. Dies ist das standardmäßige Authentifizierungsverfahren dieser Clients. Da an einem Windows NT-PDC bzw. -BDC lediglich die unsichere NTLM-Authentifizierung möglich war, wird nun ausschließlich der Domänencontroller verwendet, der die Kerberos-Authentifizierung beherrscht. Aufgrund dieses Verhaltens der Clients kann es jedoch schnell zu einer Überlastung des aktualisierten Domänencontrollers kommen. Um dieses Problem zu umgehen, können Sie entweder auf einen Schlag mehrere Domänencontroller auf Windows Server 2000/2003 aktualisieren oder aber den Clients die Information vorenthalten, dass sich in der Domäne ein Domänencontroller befindet, der die Kerberos-Authentifizierung beherrscht.

Hierzu müssen Sie auf dem aktualisierten Domänencontroller, bevor Sie den Active Directory-Installations-Assistenten über DCPROMO aufrufen, in der Registry im Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Netlogon\Parameters` einen neuen Eintrag mit dem Namen `NT4Emulator` vom Typ `DWORD` mit dem Wert `1` erstellen. Damit ist sichergestellt, dass die Clients den Domänencontroller nicht als Windows 2000/2003-Domänencontroller identifizieren und allein an diesem die Authentifizierung durchführen.

Das eben beschriebene Verfahren sollten Sie selbstverständlich nur so lange anwenden, bis eine ausreichende Anzahl an Domänencontrollern auf Windows Server 2000/2003 aktualisiert ist. Ab diesem Zeitpunkt sollten die Clients an den Domänencontrollern die sicherere Kerberos-Authentifizierung durchführen. Dazu ist es erforderlich, dass Sie den erstellten Registry-Schlüssel von sämtlichen Domänencontrollern wieder entfernen.

Solange der neue Registry-Schlüssel auf den Domänencontrollern aktiv ist, ergibt sich das Problem, dass Domänencontroller unter Windows Server 2000/2003, die der Domäne neu hinzugefügt werden, die bereits vorhandenen aktualisierten Domänencontroller nicht als solche erkennen. Somit ist es nicht möglich, einen dieser Domänencontroller als zusätzlichen Domänencontroller zu der Domäne hinzuzufügen. Um dieses Problem zu beheben, aber gleichzeitig den Clients die Informationen über den Windows 2000/2003-Domänencontroller vorzuenthalten, ist ebenfalls eine Änderung an der Registry notwendig.

Fügen Sie auf allen aktualisierten Domänencontrollern vor der Installation des Active Directory im Registry-Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Netlogon\Parameters` den Eintrag `NeutralizeNT4Emulator` vom Typ `DWORD` mit dem Wert `1` hinzu.

28 Der Active Directory-Anwendungsmodus (AD/AM) des Windows Server 2003

Windows Server 2003 unterstützt gegenüber Windows Server 2000 noch besser die vielfältigen Möglichkeiten von LDAP. Die wichtigste Option hierbei ist der Anwendungsmodus des Active Directory, der zuweilen auch als AD/AM bzw. ADAM bezeichnet wird. Dieser Anwendungsmodus ist insbesondere für Softwareentwickler und -anbieter nützlich, da nun Applikationen direkt in den Verzeichnisdienst integriert werden können. Der Zugriff auf das Active Directory kann somit verbessert für Single Sign-on-Verfahren, die gemeinsame Nutzung von verschiedenen Netzwerkbetriebssystemen oder auch die Benutzung öffentlicher Schlüssel benutzt werden. Über den AD/AM wird das Active Directory als Lightweight-Verzeichnisdienst genutzt, sodass den Applikationen ein flexibler Verzeichnisdienst bereitgestellt werden kann.

28.1 Überblick über den AD/AM

In der Realität werden oftmals mehrere Verzeichnisse parallel betrieben, die jeweils für unterschiedliche Aufgaben zuständig sind, wie z.B. Authentifizierung, Remote-Zugriff oder Verwaltung öffentlicher Schlüssel. Unter Umständen werden von den verschiedenen Verzeichnissen auch noch unterschiedliche Technologien verwendet, sodass parallel z.B. ein Active Directory, ein X.500-kompatibler Verzeichnisdienst oder ein Novell Directory benutzt werden. Da alle diese Verzeichnisdienste auf LDAP basieren, stellt sich die Frage, ob diese verschiedenen Verzeichnisse nicht auch in einer einzigen Technologie aufgehen können.

Gründe für die Benutzung nur einer Technologie können mangelhafte oder nicht vollständige Interoperabilität zwischen den Verzeichnisdiensten sein. Auch besteht die Möglichkeit, dass bestimmte Applikationen lediglich mit einem bestimmten Verzeichnisdienst zusammenarbeiten. Soll diese Applikation in einem Unternehmen eingesetzt werden, so muss zwangsläufig auch der dazugehörige Verzeichnisdienst implementiert werden, unabhängig davon, ob dieser mit dem bereits bestehenden vollständig kompatibel ist oder nicht. Neben dem Aufwand von Test, Implementierung, Pflege und Wartung der parallel betriebenen Verzeichnisdienste darf hierbei auch der Mehraufwand an Kosten nicht übersehen werden. So werden zur Administration jedes Dienstes unterschiedlich ausgebildete Personen benötigt. Zudem entstehen höhere Lizenzkosten und Supportkosten für die verschiedenen Systeme. Besonders bei Lizenzmodellen, die nach der Anzahl der Objekte gestaffelt sind, können schnell sehr hohe Gesamtkosten entstehen. Auch der Verwaltungsaufwand für die Synchronisation von Objekten muss betrachtet

werden. Sofern die Synchronisation nicht automatisiert werden kann, können schnell inkonsistente Daten vorliegen, sobald Objekte zwischen Verzeichnisdiensten verschoben oder aktualisiert werden müssen.

Ein Wunsch wäre also ein Verzeichnis, das gleichzeitig für das Netzwerkbetriebssystem an sich sowie verschiedene Anwendungen verwendet werden kann. Wichtig ist hierbei, die Sicherheitsimplementierung des Netzwerkbetriebssystems gleichzeitig auch für die Anwendungen nutzen zu können.

Der Anwendungsmodus des Active Directory des Windows Server 2003 stellt genau diese Ziele bereit, ohne dass dabei zusätzliche Kosten für Lizenzen, Personalschulungen oder doppelten Verwaltungsaufwand fällig werden.

28.1.1 Funktionsweise und Architektur des AD/AM

Die Informationen einer Anwendung werden in einem separaten Anwendungsverzeichnis gespeichert und nicht innerhalb der Daten des Netzwerkbetriebssystems, also etwa des Active Directory. Dieser quasi lokale Verzeichnisdienst kann auf demselben Server wie die Anwendung an sich betrieben werden, ohne dass der Verzeichnisdienst des Netzwerkbetriebssystems, also das Active Directory, für die Aufnahme dieser Daten, z.B. durch eine Schemaänderung, separat konfiguriert werden muss. Die gespeicherten Anwendungsdaten benötigen nicht unbedingt dasselbe hohe Replikationsintervall wie die Daten des Netzwerkbetriebssystems. Zudem würden diese Daten bei häufigen Änderungen hohen Replikationsverkehr verursachen. Außerdem sind die Daten der Anwendung auch nicht von einem so globalen Interesse, dass sie im gesamten Verzeichnis zur Verfügung gestellt werden müssen. Über den AD/AM wird für die Anwendungen ein spezieller Speicherort angeboten, in dem sich lediglich die Informationen der Applikation befinden.

Die Replikation des AD/AM folgt denselben Prinzipien wie das Multimaster-Replikationsmodell des Active Directory. Die AD/AM-Replikation greift auf dieselben Standorte zurück wie das Active Directory. Somit stehen auch hier die Replikationsoptionen wie zeitgesteuert usw. zur Verfügung. Die Verwaltung und Kontrolle der AD/AM-Replikation erfolgt auch mithilfe derselben Programme wie die herkömmliche Replikation, z.B. kann auch das Tool *REPADMIN* (siehe Kapitel 23.1.20) eingesetzt werden. Werden Anwendungsdaten im Rahmen der Active Directory-Replikation innerhalb der Anwendungspartitionen repliziert, so muss für das Replikationsintervall ein Kompromiss gefunden werden, der die Daten aller darin enthaltenen Anwendungen zufrieden stellend repliziert. Verwenden Sie hingegen AD/AM, so kann für jede Applikation separat ein Intervall bestimmt werden. Bei der Replikation von Anwendungsdaten zwischen verschiedenen AD/AM-Instanzen müssen die Server, die die Instanzen beherbergen, nicht zwangsläufig Mitglied derselben Gesamtstruktur sein. AD/AM-Instanzen können sich auf Servern in verschiedenen Gesamtstrukturen oder auch auf Mitgliedern einer Arbeitsgruppe befinden.

Sie sehen also, dass die Architektur des AD/AM der Architektur des Active Directory selbst entspricht. Beide Komponenten speichern ihre Daten hierarchisch. Das Active Directory verwendet die Datenbankdatei *NTDS.DIT*, AD/AM die Datei *adamntds.dit*. Zur Verwaltung des Verzeichnissespeichers benutzt AD/AM wie auch das AD die Extensible Storage Engine (ESE). Die Anfragen von Verzeichnisdienstclients sowie -diensten

werden im Active Directory über die *ntdsa.dll* (wird in der *lsass.exe* ausgeführt), im AD/AM von der *dsamain.exe* bearbeitet. Als Verzeichnisdienst-Interface benutzen das AD sowie AD/AM LDAP sowie die Replikation. Das AD verwendet zusätzlich noch MAPI. Die Festlegung der optimalen Replikationstopologie geschieht wie im AD auch über den Knowledge Consistency Checker (KCC).

Die Installation des Anwendungsmodus kann wahlweise über einen Assistenten oder auch skriptgesteuert erfolgen. Letzteres ist für unbeaufsichtigte oder Silent-Installationen von Applikationen von Bedeutung. Mithilfe des Installations-Assistenten können auch einzelne Instanzen bzw. Replikate einer bereits vorhandenen Instanz angelegt werden. Bei der Deinstallation kann ausgewählt werden, ob Instanzen, die mit den Instanzen verbundenen Partitionen oder Dateien mit Konfigurationsdaten entfernt werden sollen.

Der Anwendungsmodus wird als Dienst ausgeführt. Auf einem Computer können parallel mehrere Instanzen des AD/AM installiert und ausgeführt werden. Jede Instanz ist eine separat installierte Datei und verfügt über einen eindeutigen Namen sowie Port. Die einzelnen Instanzen werden einer automatischen Online-Sicherung unterzogen. Zusätzlich kann jederzeit ein Online-Backup sowie eine Offline-Wiederherstellung durchgeführt werden.

Parallel unabhängig voneinander vorhandene Instanzen stellen sicher, dass z.B. in der Testphase verschiedene, voneinander unabhängig konfigurierte Szenarien parallel betrieben und zwischen diesen gewechselt werden kann, ohne jedes Mal das Verzeichnis neu installieren zu müssen. Auch die Deinstallation einzelner Instanzen ist problemlos möglich. Weder bei der Installation noch bei der Konfiguration oder Deinstallation werden Neustarts erforderlich. Ein Entwickler kann so mit mehreren lokalen Instanzen arbeiten und diese später in das laufende Active Directory integrieren. Zudem kann der AD/AM installiert und jederzeit wieder deinstalliert werden. Dieses ist besonders für Testszenarien sowie Entwicklungsabteilungen von Interesse.

Da AD/AM nicht zwangsläufig auf einem Server oder gar Domänencontroller ausgeführt werden muss, ersparen Sie sich für die Entwicklungs- und Testphase die Bereitstellung und Administration eines zusätzlichen Servers. Stattdessen erfolgt die lokale Installation und Administration auf einem Windows XP-Client. Weiterhin kann der AD/AM unter Windows Server 2003 Standard, Enterprise und Datacenter-Edition installiert und betrieben werden.

Da der AD/AM unabhängig vom Verzeichnisdienst des Unternehmens ausgeführt wird, ist er auch nicht unternehmensweiten Änderungen wie z.B. den Änderungen am Schema unterworfen. Jede der AD/AM-Instanzen besitzt ein eigenes Schema. Somit kann für jede Instanz flexibel den Anforderungen der jeweiligen Applikation entsprochen werden. Das AD/AM-Schema kann mit denselben Programmen bearbeitet werden, mit denen auch das Active Directory-Schema modifiziert werden kann. Dazu zählen etwa *ADSIEDIT* (siehe Kapitel 23.1.2) oder *LDIFDE* (siehe Kapitel 25.2). Die Planungen und Erweiterungen des Schemas für eine Instanz werden somit gegenüber der Planung des Gesamtschemas wesentlich vereinfacht.

Innerhalb jeder Instanz können sich mehrere Datenpartitionen befinden. Damit ist eine flexible Zuweisung von Speicher und Replikationseinstellungen möglich. Zudem können für die Partitionsdaten sowohl DNS-Namen als auch X.500 Distinguished Names benutzt werden. Beide Namensräume sind gleichberechtigt verfügbar.

Für den Zugriff auf Objekte innerhalb des AD/AM können Benutzer des Verzeichnisses, Benutzer einer Windows NT 4.0-Domänenstruktur sowie auch Benutzer des lokalen Computers, auf dem AD/AM ausgeführt wird, bestimmt werden. Im AD/AM können auch direkt Benutzerkonten angelegt werden. Die jeweilige Anwendung fragt die Berechtigungen des Benutzers dann direkt aus dem AD/AM ab. Hierbei spricht man vom LDAP-Simple-Bind-Verfahren. Der Zugriff auf die Objekte innerhalb des AD/AM wird wie der Zugriff auf Active Directory-Objekte über ACLs (Access Control Lists) gesteuert.

Das Active Directory kann innerhalb eines Unternehmens zahlreiche verschiedene Rollen übernehmen. Beginnend bei der Administration eines Windows basierten Client-Server-Netzwerks über die Verwaltung der Sicherheit bis hin zu E-Commerce-Applikationen oder Anwendungen wie Exchange, die auf einen Verzeichnisdienst zugreifen, finden sich die Einsatzgebiete des Active Directory.

Sofern in einem Unternehmen bereits ein Verzeichnis implementiert ist, jedoch noch kein Verzeichnisdienst benutzt wird, so stellen sich umfangreiche Aufgaben für Entwickler und Softwareanbieter: Soll eine verzeichnishaftige Anwendung in diesem Unternehmen eingesetzt werden, so muss der Softwareanbieter abwarten, bis das Unternehmen einen Verzeichnisdienst implementiert hat, oder aber das Unternehmen entscheidet sich für ein anderes Produkt, das nicht ein Verzeichnis zum Speichern der Applikationsinformationen benutzt. Auch wenn ein Unternehmen bereits einen Verzeichnisdienst verwendet, so bedeutet es für die Entwickler einen nicht unerheblichen Aufwand, eine Anwendung in das bestehende Verzeichnis zu integrieren. Bei einem Einsatz des Verzeichnisdienstes innerhalb des gesamten Unternehmens bleibt unter Umständen die Flexibilität auf der Strecke, wenn je nach Geschäftsbereich unterschiedliche Änderungen am Verzeichnisschema erforderlich werden.

Nach dieser allgemeinen Beschreibung werden nun in den folgenden Kapiteln einige spezielle Einsatzszenarien für den Anwendungsmodus des Active Directory vorgestellt.

28.1.2 Einsatzmöglichkeiten des AD/AM

Angenommen, in einem Unternehmen wird eine Portalanwendung benutzt. Diese Anwendung erfordert bestimmte Daten der Benutzer, die sich am Active Directory authentifiziert haben. Das Speichern dieser Daten innerhalb des Active Directory wäre nur nach der Modifikation des Active Directory-Schemas möglich, diese Schemaänderung darf jedoch aus unternehmenstechnischen Gründen nicht durchgeführt werden. Aus diesem Grund wird der AD/AM eingesetzt. Im separaten Speicherort des AD/AM werden die speziellen Benutzerdaten abgelegt. Da diese Daten lediglich für die Portalanwendung relevant sind, müssen sie nicht im Active Directory hinterlegt sein. Somit erfolgt auch keine Replikation dieser Daten zwischen den Domänencontrollern. Über AD/AM wird das Active Directory von der Portalanwendung benutzt, um Benutzer zu authentifizieren und applikationsspezifische Dienste zu veröffentlichen.

Die Vermeidung der Replikation spezieller Anwendungsdaten ist besonders dann von Interesse, wenn eine Anwendung lediglich von einer einzigen Abteilung oder einem Bereich benutzt wird. Würden die Daten im Active Directory vorgehalten, so würden diese Daten automatisch an sämtliche Domänencontroller des gesamten Unternehmens repliziert werden, was zu einer völlig unnötigen Belastung des gesamten Netzwerks führt. Bei der Speicherung im lokalen AD/AM-Verzeichnis erfolgt keine unnötige Replikation der Daten.

Selbstverständlich können die Daten der Applikation auch im Active Directory gespeichert und sogar in den globalen Katalog aufgenommen werden. Der Speicherort im AD/AM ist nicht zwingend. Sinnvoll ist meistens eine Kombination. Damit nicht für jeden AD/AM-Speicherort eine separate Benutzerdatenbank mit eigenen Passwörtern und Benutzer-IDs gepflegt werden muss, sollten Sie die Sicherheitsprincipals des Active Directory für den Zugriff auf Daten im AD/AM-Speicherort benutzen. Im AD/AM werden dann lediglich spezielle Daten der Portalanwendung, z.B. Richtlinien dieser Applikation, hinterlegt.

Auch in Windows NT 4.0-Domänen können verzeichnisbasierte Applikationen mit AD/AM verwendet werden. Windows NT-Benutzer können ebenfalls authentifiziert werden, da AD/AM auch die Windows-integrierte Sicherheit verwendet. Die Installation von AD/AM erfolgt auf einem Windows 2003 Server, der dann als Mitgliedsserver in die NT 4.0-Domäne aufgenommen wird.

Weiterhin können im AD/AM Daten gespeichert werden, die bei der Speicherung im Active Directory eine Änderung des Schemas erfordern würden. Soll eine Applikation, die diese speziellen Daten erfordert, lediglich von einem bestimmten Geschäftsbereich eingesetzt werden, so wäre die unternehmensweite Modifikation des Schemas eigentlich überflüssig, bei der Speicherung dieser Daten im AD aber erforderlich, da das Schema für alle Domänen der Gesamtstruktur identisch ist. Werden diese Daten im AD/AM abgelegt, kann dieses Verzeichnis ein abweichendes Schema vom Schema des gesamten Active Directory besitzen. Diese Daten werden dann via LDAP den Clients der Portalapplikation zur Verfügung gestellt. Auch die Gefahr von Konflikten innerhalb des Active Directory-Schemas beim Einsatz mehrerer Applikationen wird so gebannt, da jede Applikation im AD/AM ihr eigenes Schema im eigenen Verzeichnis besitzt.

Wie bereits erwähnt, können auf einem Computer mehrere Instanzen von AD/AM parallel betrieben werden. Diese Instanzen können von unterschiedlichen Applikationen verwendet werden. Jede dieser Instanzen kann dabei unabhängig von den anderen eine Replikation ihrer Daten mit anderen Replikaten durchführen.

Auch für die Verwaltung von Extranet-Zugriffen kann AD/AM optimal verwendet werden. Diese Konstellation ist beispielsweise bei der Verwendung eines Webportals gegeben, wobei die Portalanwendung das Verzeichnis lediglich zur Authentifizierung benutzt und die einzelnen Anmeldeinformationen darin speichert. In dem AD/AM-Verzeichnis werden in diesem Fall Benutzerinformationen gespeichert, die nicht den standardmäßigen Windows-Sicherheitsprincipals entsprechen. Da die Authentifizierung der Web-Clients am Webportal über LDAP-Binds erfolgt, werden die dafür notwendigen Benutzerdaten sowie Berechtigungen im AD/AM-Speicher abgelegt. Die Webportal-Applikation benutzt den AD/AM-Speicher als simplen LDAP-Speicher. Dabei ist es

gleichgültig, ob die Applikation auf einer Windows-basierten Plattform oder einer beliebigen anderen LDAP-fähigen Plattform betrieben wird. Der Einsatz des Active Directory ist in dieser Konstellation nicht erforderlich.

Auch bei der Umstellung eines Verzeichnisses, das dem X.500-Standard entspricht, auf Active Directory oder den parallelen Betrieb dieser beiden Verzeichnisse kann AD / AM sinnvoll eingesetzt werden. Sobald das Active Directory als Netzwerkbetriebssystem implementiert worden ist, stellt AD / AM den alten Anwendungen des X.500-Standards weiterhin ein Verzeichnis bereit. Besteht das Ziel darin, sämtliche Anwendungsdaten im Active Directory zu hinterlegen, so sollte ein Metadirectory eingesetzt werden, damit die bestehenden Daten im AD / AM und im Active Directory synchronisiert werden können. Hierfür bieten sich die Microsoft Metadirectory Services an (siehe Kapitel 30). Damit kann die Synchronisation automatisch vollzogen werden.

28.1.3 Installation des AD/AM

Dieses Kapitel beschreibt die Installation des AD / AM.

1. Durch den Installationsvorgang leitet Sie ein Installations-Assistent. Nach der Willkommensmeldung (siehe Abbildung 28.1) klicken Sie auf WEITER.



Abbildung 28.1: Der AD/AM-Installations-Assistent

2. Nachdem Sie den Lizenzbedingungen zugestimmt haben, müssen Sie entscheiden, ob Sie AD / AM mit den zugehörigen AD / AM-Verwaltungstools oder lediglich die Tools installieren möchten (siehe Abbildung 28.2). Mit den Verwaltungstools können Sie auf anderen Computern installierte AD / AM-Instanzen per Remote-Zugriff verwalten. Klicken Sie dann auf WEITER.



Abbildung 28.2: Die Auswahl der zu installierenden Komponenten

3. Wenn Sie sich in Schritt 2 für die Installation des AD / AM entschieden haben, müssen Sie nun bestimmen, ob eine neue AD / AM-Instanz angelegt werden soll (A UNIQUE INSTANCE) oder ob die Partition zu einem bestehenden Set hinzugefügt werden soll (JOIN A CONFIGURATION SET, siehe Abbildung 28.3). Im ersten Fall wird eine vollständig neue Instanz angelegt, die sich nicht mit bereits vorhandenen Instanzen repliziert. Soll die anzulegende Instanz hingegen dieselben Konfigurations- und Schemapartitionen wie eine bereits bestehende AD / AM-Instanz benutzen, so wählen Sie die zweite Option. Klicken Sie dann auf WEITER.



Abbildung 28.3: Erstellen einer neuen Instanz bzw. die Instanz zu einer bestehenden Instanz hinzufügen

4. Als Nächstes legen Sie im Feld INSTANCE NAME einen aussagekräftigen Namen für die Instanz fest (siehe Abbildung 28.4). Daraus wird auch automatisch der Name für den AD / AM-Windows-Dienst gebildet. Klicken Sie dann auf WEITER.



Abbildung 28.4: Einen Namen für die AD/AM-Instanz vergeben

5. Danach bestimmen Sie den Port für LDAP und SSL (siehe Abbildung 28.5). Abhängig davon, ob auf dem Computer Active Directory-Dienste ausgeführt werden, werden die Ports vergeben. Handelt es sich um einen Domänencontroller, so darf für AD/AM-LDAP nicht Port 389 und für AD/AM-SSL nicht Port 636 benutzt werden, da diese für den Active Directory-Verkehr reserviert sind. In diesem Fall müssen zwei Ports aus dem Bereich zwischen 1025 und 65535 gewählt werden. Klicken Sie dann auf WEITER.



Abbildung 28.5: Auswahl der AD/AM-Ports für LDAP und SSL

6. Im nächsten Schritt müssen Sie entscheiden, ob Sie eine Applikationspartition anlegen möchten oder nicht (siehe Abbildung 28.6). Sofern die Anwendung, die Sie verwenden möchten, selbst eine Partition anlegt, ist das manuelle Anlegen nicht erforderlich. Wählen Sie die Option NO, DO NOT CREATE AN APPLICATION DIRECTORY PARTITION. Benötigt

die Anwendung hingegen eine Partition, so wählen Sie die Option YES, CREATE AN APPLICATION DIRECTORY PARTITION und geben einen für diese Instanz noch nicht benutzten Partitionsnamen im Format CN=Partitionsname,DC=,DC= an. Klicken Sie dann auf WEITER.

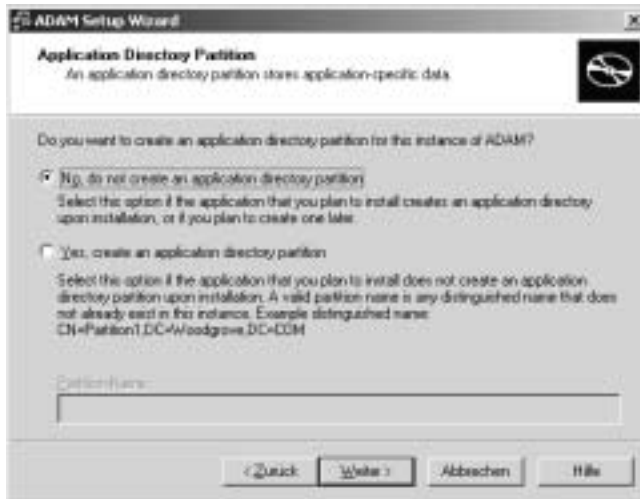


Abbildung 28.6: Die Entscheidung, ob eine Applikationspartition zu erstellen ist oder nicht

7. Dann können Sie den Installationspfad für AD/AM bestimmen (siehe Abbildung 28.7). Sie können unterschiedliche Pfade für die Programmdateien sowie die Wiederherstellungsdaten auswählen. Standardmäßig erfolgt die Installation ins Verzeichnis PROGRAMME\MICROSOFT\ADAM\<NAME DER INSTANZ>\DATA der Systempartition. Die Verwaltungswerkzeuge werden in das Verzeichnis %SYSTEMROOT%\ADAM installiert. Klicken Sie dann auf WEITER.

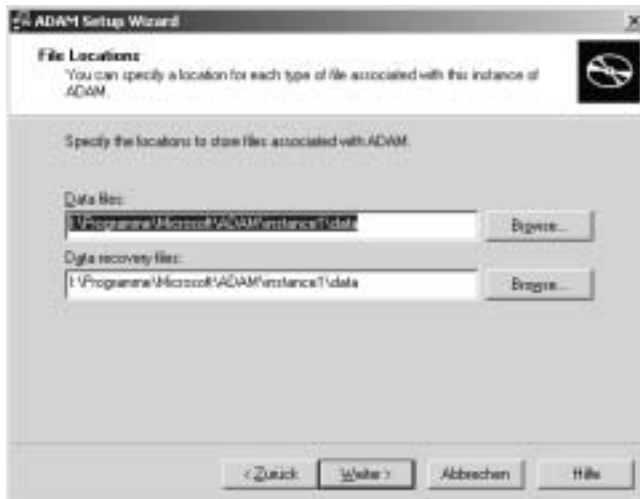


Abbildung 28.7: Auswahl des AD/AM-Installationsverzeichnis

8. Als Nächstes wird ein Konto ausgewählt, mit dessen Berechtigungen AD/AM ausgeführt wird (siehe Abbildung 28.8). Handelt es sich bei dem Installationsrechner um einen Domänencontroller, so kann das Standardkonto des Netzwerkdienstes nicht benutzt werden. Die Checkbox NETWORK SERVICE ACCOUNT ist in diesem Fall nicht anwählbar. Wählen Sie stattdessen ein anderes Konto aus. Stellen Sie dabei sicher, dass das gewählte Konto als Dienst ausgeführt werden kann. Ist dies nicht der Fall, erhalten Sie einen kurzen Hinweis. Bestätigen Sie diesen mit OK, und AD/AM kann diese Berechtigung dem Konto hinzufügen. Klicken Sie dann auf WEITER.



Abbildung 28.8: Auswahl eines Dienstkontos, unter dem AD/AM ausgeführt werden soll

9. Dann müssen Sie ein Konto bestimmen, das administrative Berechtigungen zur Verwaltung des AD/AM besitzen soll (siehe Abbildung 28.9). Sie haben die Wahl zwischen dem aktuell verwendeten Benutzerkonto oder einem beliebigen anderen. Klicken Sie dann auf WEITER.



Abbildung 28.9: Auswahl der Benutzer, die administrative Berechtigungen für die AD/AM-Verwaltung besitzen sollen

10. Abschließend werden sämtliche Einstellungen in der Zusammenfassung angezeigt (siehe Abbildung 28.10). Sofern Sie keine Änderungen mehr vornehmen möchten, kann nun die Installation erfolgen. Klicken Sie dazu auf WEITER und dann auf FERTIG STELLEN.



Abbildung 28.10: Die Zusammenfassung der Installationsangaben

Nach der Installation der AD/AM-Verwaltungstools befinden sich im Startmenü die Einträge ADAM ADSIEDIT, ADAM HELP, ADAM TOOLS COMMAND PROMPT sowie LDP. Unter den Tools befinden sich Programme wie *ldifde*, *dsdiag.exe*, *dsadmin.exe* und *csvde.exe*. Die AD/AM-Instanz selbst erzeugt keine Einträge im Startmenü.

Um eine AD/AM-Instanz wieder zu deinstallieren, wählen Sie die gewünschte Instanz unter SYSTEMSTEUERUNG/SOFTWARE aus und wählen ENTFERNEN (siehe Abbildung 28.11).



Abbildung 28.11: Deinstallieren einer AD/AM-Instanz

Die Installation kann auch als Unattended Installation durchgeführt werden. Eine ausführliche Anleitung sowie ein Beispiel dazu findet sich in der AD / AM-Hilfe.

28.2 Die Verwaltungswerkzeuge des AD/AM

Sofern Sie bei der Installation die AD / AM-Verwaltungswerkzeuge ausgewählt haben, steht Ihnen ein Satz von Programmen zur Verfügung. Mit diesen Programmen können Sie sowohl eine lokale AD / AM-Instanz als auch Instanzen auf Remote-Computern verwalten. Die Programme *ADAM ADSIEDIT* sowie *LDP* entsprechen den Windows Support-Tools *ADSIEDIT* sowie *LDP*. Hinweise zu diesen beiden Programmen finden Sie in Kapitel 23.1.2 sowie Kapitel 23.1.14. Auch die Programme *DSACLS* (siehe Kapitel 23.1.7), *DCDIAG* (siehe Kapitel 23.1.4), *LDIFDE* (siehe Kapitel 25.2) sowie *REPADMIN* (siehe Kapitel 23.1.20) sind bereits vorgestellt worden.

28.2.1 ADAMSetup

ADAMSetup ist ein Kommandozeilenprogramm, das Sie für die Unattended Installation benutzen können. Hierzu müssen Sie eine Antwortdatei erstellt haben, die sämtliche Werte für die AD / AM-Installation enthält. *ADAMSetup* benutzt die folgende Syntax:

```
Adamsetup /c:"adaminstall.exe /answer:Dateiname" 
```

Unter */answer:* müssen Sie den Dateinamen der Antwortdatei angeben. Hinweise zum Erstellen einer Antwortdatei finden Sie in der AD / AM-Hilfe.

28.2.2 Adamuninstall

Das Kommandozeilenprogramm *Adamuninstall* wird zur Deinstallation einer AD / AM-Instanz verwendet. Das Programm verwendet die folgenden Parameter (siehe Tabelle 28.1):

Parameter	Beschreibung
/q	Führt die Deinstallation aus, ohne den Fortschritt des Prozesses anzuzeigen.
/i:Name der Instanz	Mit diesem Parameter werden die angegebene AD/AM-Instanz sowie die AD/AM-Verwaltungsprogramme deinstalliert.
/i:Tools	Mit diesem Parameter werden lediglich die AD/AM-Verwaltungsprogramme deinstalliert.

Tabelle 28.1: Die Parameter des Programms *Adamuninstall*

Um also eine Instanz namens „Instanz1“ sowie die Verwaltungsprogramme zu deinstallieren, verwenden Sie den Befehl:

```
Adamuninstall /i:Instanz1 
```

28.3 Verwalten einer AD/AM-Instanz

Um eine vorhandene AD / AM-Instanz zu verwalten, müssen Sie zunächst eine Verbindung zu dem Computer herstellen, auf dem sich die Instanz befindet. Hierzu können Sie die Programme *ADAM ADSIEDIT* oder *LDP* benutzen. Im Folgenden wird die Verbindungsherstellung unter *ADAM ADSIEDIT* beschrieben.

1. Starten Sie das Programm *ADAM ADSIEDIT* und wählen das Menü *AKTION/SETTINGS*. Sie erhalten das Fenster *CONNECTION SETTINGS* (siehe Abbildung 28.12).



Abbildung 28.12: Die Herstellung einer Verbindung zu einer ADAM-Instanz auf einem Computer

2. Tragen Sie im Feld *CONNECTION NAME* den Namen der Verbindung ein. Unter *SERVER NAME* geben Sie den DNS- oder NetBIOS-Namen des Computers oder dessen IP-Adresse an. Handelt es sich um den lokalen Computer, so geben Sie *localhost* ein. Geben Sie auch den Port (LDAP oder SSL) an, über den die Kommunikation erfolgen soll. Sie müssen hier denselben Port eintragen, den Sie bei der Installation der Instanz festgelegt haben. Unter *CONNECT TO THE FOLLOWING NODE* können Sie entweder die Verbindung zu einem bestimmten Namenskontext angeben oder unter *WELL-KNOWN NAMING CONTEXT* aus der Drop-down-Liste *CONFIGURATION*, *SCHEMA* oder *ROOTDSE* auswählen. Im Bereich *CONNECT USING THIS CREDENTIALS* wählen Sie ein Benutzerkonto für die Verbindung aus.
3. Sobald Sie die Verbindung hergestellt haben, können Sie in der *mmc ADAM ADSIEDIT* den Verbindungsnamen doppelklicken und sehen darunter die übergeordneten Container der Verzeichnispartition (siehe Abbildung 28.13). Sie können dann aus dem Container bzw. dessen Untercontainern das gewünschte Objekt auswählen und per Doppelklick öffnen und bearbeiten.

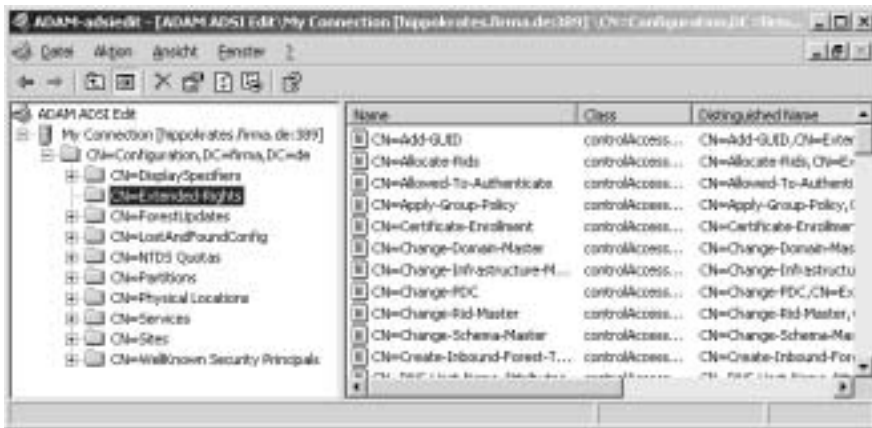


Abbildung 28.13: Die Instanzenverwaltung mit ADAM ADSIEDIT

28.3.1 Auflisten der Verzeichnispartitionen und Namensräume einer AD/AM-Instanz

Um die in einer AD/AM-Instanz enthaltenen Verzeichnispartitionen und Namensräume aufzulisten, verwenden Sie das Support-Tool *DCADMIN*. Geben Sie dazu an der Eingabeaufforderung nacheinander folgende Befehle ein:

```
dcadmin ↵
domain management ↵
connections ↵
```

Sie erhalten den Prompt `server connections`: Dort geben Sie den folgenden Befehl ein:

```
connect to server Computername:Portnummer ↵
```

Danach beenden Sie den Prompt `server connections` mit `quit` ↵.

Sie gelangen wieder an den Prompt `domain management`. Geben Sie hier `list` ↵ ein. Sie erhalten nun eine Liste der in der AD/AM-Instanz enthaltenen Daten.

28.3.2 Den Dienst der AD/AM-Instanz verwalten

Der Dienst einer AD/AM-Instanz kann wie jeder andere Windows-Dienst auch gestartet, beendet, unterbrochen und wieder neu gestartet werden. Dies können Sie sowohl GUI-basiert über *VERWALTUNG/DIENSTE* als auch an der Kommandozeile mit dem Befehl `net` ausführen.

Um den Dienst zu starten, verwenden Sie den Befehl `net start Name der Instanz` ↵, um den Dienst zu beenden den Befehl `net stop Name der Instanz` ↵.

28.3.3 Den Port der AD/AM-Instanz ändern

Standardmäßig benutzt AD/AM den LDAP-Port 389 und den SSL-Port 636, sofern die Instanz nicht auf einem Domänencontroller ausgeführt wird. Da dort die beiden Ports nicht für AD/AM verfügbar sind, müssen Sie bei der Installation einen Port zwischen 1025 und 65535 festlegen. Die bei der Installation festgelegten Ports können später wieder geändert werden. Dazu können Sie entweder an der Kommandozeile das Programm *dsutil* verwenden oder eine Änderung an der Registry vornehmen.

Ändern des Ports über dsutil

1. Öffnen Sie über STARTMENÜ / PROGRAMME / ADAM den Eintrag ADAM TOOLS COMMAND PROMPT.
2. Wechseln Sie an der Eingabeaufforderung in das Verzeichnis \BIN der AD/AM-Instanz.
3. Beenden Sie den Dienst der AD/AM-Instanz, deren Port Sie ändern möchten.
4. Geben Sie `dsutil` ein und danach `activate instance Dienstname der Instanz` .
5. Um den LDAP-Port zu ändern, verwenden Sie den Befehl `LDAP port Portnummer` , um den SSL-Port zu ändern den Befehl `SSL port Portnummer` .
6. Um `dsutil` zu beenden, geben Sie `quit` ein.
7. Starten Sie danach wieder den Dienst der AD/AM-Instanz.

Ändern des Ports über die Registry

Um den Port über die Registry zu ändern, öffnen Sie den Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Name der ADAM-Instanz\Parameters`. Um den LDAP-Port zu ändern, modifizieren Sie den Wert `Port LDAP`, um den SSL-Port zu ändern den Wert `Port SSL`.

29 Koexistenz mit Unix, Linux und MacOS

Eine reine Windows-Umgebung – idealerweise nur Windows 2000 und neuer – ist für die Erstellung eines Active Directory zwar die unkomplizierteste Lösung, in vielen Umgebungen aber nicht praktikabel. Man denke dabei z.B. an MacOS-Clients, die in weiten Bereichen des Desktop Publishings oder im Grafikbereich eingesetzt werden oder an Linux-Clients, deren Anzahl zwar sehr langsam, aber stetig zunimmt. Dieses Kapitel beschäftigt sich mit der Anbindung dieser Nicht-Microsoft-Betriebssysteme an ein Active Directory. Hierzu erhalten Sie für die Bereiche Linux / Unix sowie MacOS einen Einblick in verschiedene Konfigurationsmöglichkeiten. Zusätzlich werden einige Zusatzprogramme und Tools von Drittanbietern vorgestellt, die Sie bei der Integration dieser Clients ins Active Directory unterstützen.

29.1 Die Benutzerverwaltung unter Unix

Vor der Integration von Linux- oder Unix-Clients in das Active Directory steht ein langer Weg. Dennoch ist es am Ende möglich, dass Benutzerdaten für Linux-Clients wie Passwörter oder Gruppenzugehörigkeit zentral über das Active Directory verwaltet werden. Dabei muss aufseiten der Administration sichergestellt werden, dass die Benutzerpflege zentral an einer Stelle erfolgen kann, für die Benutzer muss gewährleistet werden, dass sie für sämtliche Daten unter Unix und Windows nur eine einzige Authentifizierung benötigen. Dennoch dürfen die Passwortinformationen von außen nicht zugreifbar sein. Zum besseren Verständnis wird nun kurz auf die standardmäßigen Mechanismen der Benutzerverwaltung unter Unix eingegangen, um daraus die Probleme, aber auch Chancen herzuleiten, die sich bei der Integration ins Active Directory ergeben.

Unix ist ein bereits sehr altes Betriebssystem. Die Benutzerverwaltung erfolgt nicht zentral an einer Stelle, da dies zu Zeiten von Mainframes und Terminals nicht erforderlich war. Clients waren damals noch nicht untereinander im Netzwerk verbunden. Auf jedem Unix-Client befinden sich mehrere Dateien mit Benutzerinformationen. Diese sind die */etc/passwd*, die */etc/shadow* sowie die */etc/group*. Die Datei */etc/passwd* enthält der Reihe nach die Informationen Login-Name, das verschlüsselte Passwort, die UID (numerische Benutzernummer) und GID (Gruppennummer), den Benutzernamen, das Homeverzeichnis sowie der Pfad zur Benutzer-Shell.

Sobald sich ein Benutzer an einem Terminal oder einer Mainframe anmeldet, wird beim Login über z.B. *getpwent* der Name des Benutzers ausgelesen. Sobald er das Kennwort eingegeben hat, wird dieses über *crypt* verschlüsselt und mit dem entsprechenden Eintrag in der Datei */etc/passwd* verglichen.

Das in */etc/passwd* enthaltene verschlüsselte Passwort bietet einen einfachen Angriffspunkt, um dieses auszuspionieren. Deshalb wurde unter Sicherheitsaspekten das Passwort in die Datei */etc/shadow* verlegt. Auf diese Datei hat nur noch der Benutzer root Zugriff. Das in der Datei */etc/group* enthaltene Passwort wurde in die Datei */etc/gshadow* verlegt und kann nur noch von der Gruppe selbst gelesen werden.

Da allmählich der Zugriff mehrerer Clients auf eine zentrale Instanz wichtiger wurde, wobei die Informationen aus */etc/passwd* und */etc/group* benutzt werden sollten, wurde NIS von der Firma Sun erfunden. NIS bedeutet Network Information System. Es beruht auf dem Prinzip, die Informationen der */etc/passwd* und */etc/group* im selben Format in einer zentralen Datenbank vorzuhalten. Auf diese Datenbank wird von allen anderen Rechnern via RPC zugegriffen, um die gewünschten Informationen zu erhalten. Dieses Verfahren wurde von Sun weiterentwickelt zu NSS (Name Service Switch). Hierbei werden in der Konfigurationsdatei */etc/nsswitch* die Quellen verschiedener Informationen vorgehalten, z.B. Benutzerinformationen aus */etc/passwd* oder Hostinformationen aus */etc/hosts*. Diese Konfigurationsdatei wird über die C-Library ausgelesen. Danach wird entschieden, ob die Informationen z.B. aus NIS bezogen werden sollen.

Allerdings ergab sich bei all diesen Implementierungen das Problem, dass Passwörter nur über das allmählich veraltete Crypt-Verfahren verschlüsselt werden konnten. Um dieser Sicherheitslücke abzuhelpen, wurde PAM (Pluggable Authentication Module) erfunden. PAM ist zwar in der Lage, erweiterte Authentifizierungsmaßnahmen wie Smartcards bereitzustellen, allerdings ist damit auch die Änderung der Applikationen zur Authentifizierung erforderlich geworden. Diese müssen nun die PAM-Library benutzen, anstatt auf die gewohnten *getpwent*- und *crypt*-Mechanismen zurückzugreifen. Zwischenzeitlich ist jedoch für alle Authentifizierungsapplikationen auch eine PAM-Library vorhanden.

Um eine Authentifizierung der Unix-Clients am Active Directory zu ermöglichen, wird die LDAP-Fähigkeit des Verzeichnisdienstes ausgenutzt. Im LDAP ergeben sich für Unix zwei verschiedene Authentifizierungsmethoden, nämlich *pam_ldap* und *nss_ldap*. Diese beiden Libraries sind für diverse Unix- und Linux-Systeme erhältlich. Voraussetzung dafür ist jedoch, dass das Active Directory-Schema entsprechend erweitert wird, damit die Informationen von *pam_ldap* und *nss_ldap* gelesen werden können. Hierzu bieten sich die Services for Unix (SFU) oder das Freeware-Tool *AD4Unix* an. Die Kommunikation zwischen Unix und dem LDAP-Server kann zusätzlich über SSL abgesichert werden.

29.2 Die Windows Services for Unix (SFU)

An erster Stelle der Programme für die Integration von Unix/Linux in eine Windows 2000/2003-Umgebung stehen die Windows Services for Unix (SFU). Aktuell ist die Version 3.0. Die Vorgängerversion 2.0 war bereits für Windows NT verfügbar. Sie kann aber auch unter Windows 2000 und 2003 installiert werden. Bei der Installation der SFU wird auch das Active Directory-Schema um Klassen und Attribute erweitert, die für die Kommunikation zwischen Windows und Unix erforderlich sind. Dabei unterscheiden sich die Schemaänderungen der SFU 2.0 in SFU 3.0. Es existiert nach der Installation eine

Reihe neuer Schema-Objekte, von denen die meisten mit *msSFU30...* beginnen. Offiziell benennt Microsoft die folgenden Unix-Versionen, die mit SFU 3.0 zusammenarbeiten:

- ▶ Solaris 2.7
- ▶ HP-UX 11
- ▶ AIX 4.3.3
- ▶ Red Hat Linux 7.0

Die SFU umfassen einen großen Satz an Komponenten. Diese reichen von der Passwort-synchronisation über NFS-Clients, Server und Gateways bis hin zu einer Interix-Entwicklungsumgebung, um Unix-Anwendungen Windows-kompatibel zu machen. Hier wird jedoch nur auf die Komponenten der SFU 3.0 eingegangen, die Active Directory-relevante Themen wie Benutzerverwaltung, Passwortsynchronisation oder Dateifreigaben betreffen.

Die Verwaltung der SFU erfolgt über eine zentrale mmc, über die alle installierten Komponenten administriert werden können (siehe Abbildung 29.1). Diese mmc finden Sie unter **STARTMENÜ/PROGRAMME/WINDOWS SERVICES FOR UNIX/SERVICES FOR UNIX ADMINISTRATION**. Nach der Installation der SFU muss der Server neu gestartet werden. Die Installation muss auf jedem Server der Domäne durchgeführt werden, der als Server for NFS dienen soll.

29.2.1 Server/Client/Gateway for NFS

- ▶ **SERVER FOR NFS** (siehe Abbildung 29.1). Mit dieser Komponente kann der Windows-Administrator Verzeichnisse als exportierte NFS-Shares freigeben. Die Unix-Clients können dieses Verzeichnis wie ein NFS-Share eines Unix-Servers mounten. Über das User Name Mapping wird sichergestellt, dass die UID und GID des Unix-Clients dem Windows-Benutzerkonto zugemappt werden. Damit gelten für den Unix-Benutzer die unter Windows definierten Berechtigungen.

Als weitere Optionen können Sie festlegen, welche Ereignisse protokolliert werden sollen. Neben den Ereignissen wie Lesen, Schreiben und Löschen können auch die Mountvorgänge überwacht werden. Auf der Registerkarte **LOCKING** wird festgelegt, wie lange ein Client auf die Wiederherstellung der Verbindung zum NFS-Share warten muss, wenn diese unterbrochen worden ist. Unter **CLIENT GROUPS** können Sie bestimmen, welche Benutzergruppen Zugriff auf ein NFS-Share haben. Auf der letzten Registerkarte können verschiedene Servereinstellungen vorgenommen werden. So können Sie für die Windows-Dateisysteme FAT, NTFS und CDFS einzeln bestimmen, ob die Dateinamen in Groß- oder Kleinbuchstaben ausgegeben oder das Format beibehalten werden soll. Unix-Dateien, die mit "." beginnen, können als versteckte Dateien gekennzeichnet werden. Auch die Größe für den Directory-Cache kann hier eingestellt werden.

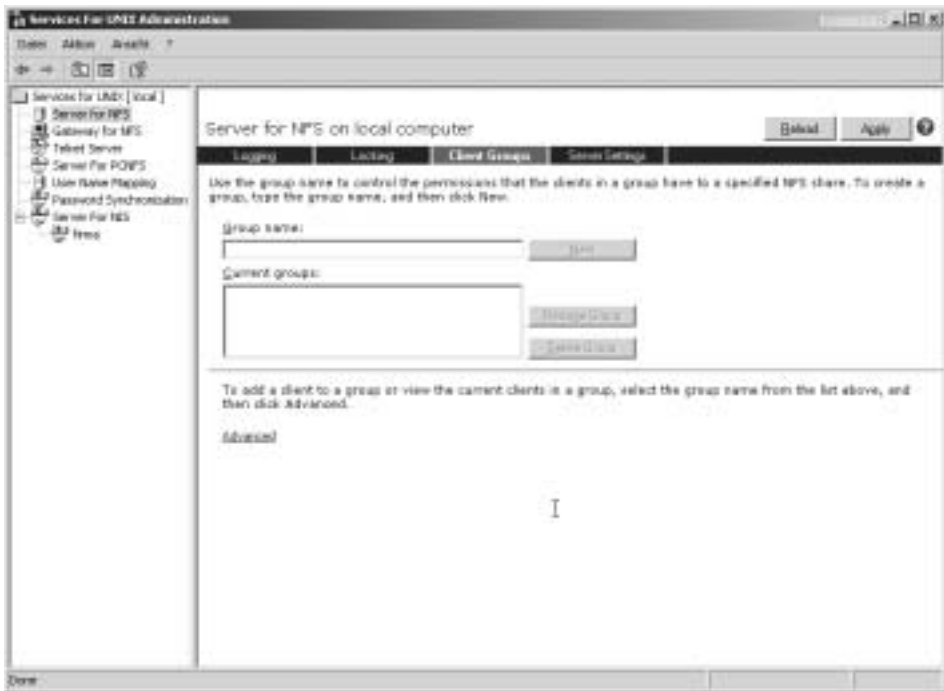


Abbildung 29.1: Die Verwaltungskonsolle der SFU 3.0, Server for NFS

- ▶ **CLIENT FOR NFS:** Mit dem Client for NFS kann auf Windows-Computers ein exportiertes NFS-Share einem Laufwerksbuchstaben zugemappt werden. Zur Verbindungsherstellung können UNC-Namen benutzt werden. Die Unix-Authentifizierungsinformationen können über User Name Mapping oder einen PCNFS-Server bezogen werden.
- ▶ **GATEWAY FOR NFS:** Über das Gateway for NFS können Windows-Benutzer ohne weitere zusätzliche Software auf die NFS-Shares zugreifen. Die NFS-Shares sieht der Benutzer als herkömmliche Windows-Netzwerkfreigaben. Sie können für alle neu auf dem NFS-Server erstellten Dateien und Ordner bereits im Voraus die Berechtigungen im Unix-Format über Checkboxes festlegen (write, read, execute für Benutzer, Gruppe und Andere).

29.2.2 Server for PCNFS

Windows-Clients, auf denen der SERVER FOR NFS oder CLIENT FOR NFS ausgeführt wird, können auf das NFS-Dateisystem zugreifen, wobei die notwendigen Authentifizierungsinformationen für Unix bereitgestellt werden. Werden ein Benutzername und Passwort an einer PCNFS-Server gesendet, werden diese mit der Passwort-Datei verglichen. Stimmen die Werte überein, gibt der SERVER FOR PCNFS (siehe Abbildung 29.2) die UID und GID des Benutzers aus, die zur Verbindung mit dem NFS-Server benötigt werden.



Abbildung 29.2: Der Server for PCNFS

Auf den Registerkarten USERS und GROUPS können Sie neue Benutzer und Gruppen anlegen und diesen die Unix-Informationen UID, GID, Login-Name und Passwort mitgeben. Bestehende Benutzer und Gruppen können auch bearbeitet werden.

29.2.3 User Name Mapping

Dies ist das zentrale Werkzeug zur Verbindungsherstellung zwischen den Benutzerkonten unter Windows und den Unix-Konten der Benutzer und Gruppen. Somit können Windows- und Unix-Benutzer wechselseitig auf ihre Dateien auf dem anderen Betriebssystem zugreifen.

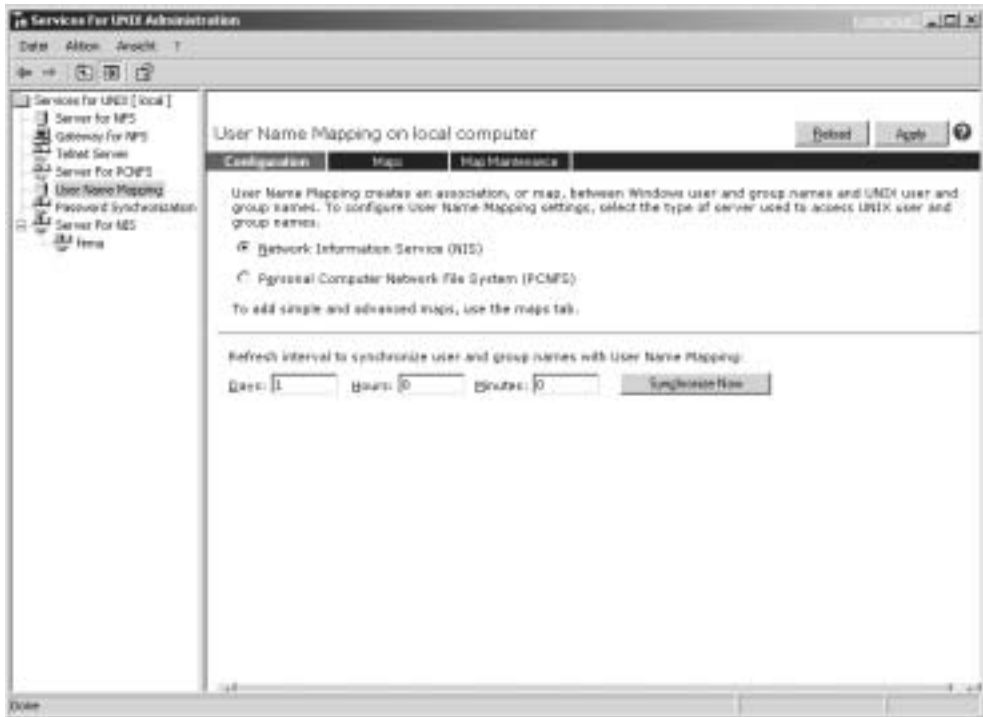


Abbildung 29.3: Die Konfiguration des User Name Mapping

Auf der Registerkarte CONFIGURATION (siehe Abbildung 29.3) bestimmen Sie, ob auf die Unix-Konten von PCNFS- oder NIS-Servern aus zugegriffen werden soll. Auch das Synchronisationsintervall kann bestimmt werden. Über MAPS wird die Art der Verbindungen festgelegt. Verwenden die Windows- und Unix-Benutzer denselben Namen, wählen Sie SIMPLE MAPS. Zur Konfiguration der ADVANCED MAPS werden die gewünschten Einträge aus den bestehenden User- und Group-Maps gewählt. Weiterhin können Sie unter MAP MAINTENANCE Pfade festlegen, an denen ein Backup der User Name Mapping-Daten angelegt werden soll bzw. von wo aus Daten wiederhergestellt werden sollen.

29.2.4 Password-Synchronisation

Über diese Komponente (siehe Abbildung 29.4) wird sichergestellt, dass bei der Passwortänderung eines Benutzers unter Windows dieses auch unter Unix geändert wird oder nur umgekehrt oder in beiden Fällen. Damit muss nur ein Benutzerpasswort für beide Systeme gepflegt werden. Weiterhin wird auf der Registerkarte DEFAULT festgelegt, welcher Schlüssel für die Verschlüsselung der Passwörter benutzt werden soll. Auch der Port sowie erweitertes Logging und Intervalle zur Synchronisation werden hier eingestellt. Auf der Registerkarte ADVANCED können Sie zusätzliche Computer angeben, zwischen denen eine Passwort-Synchronisation mit den Unix-Rechnern stattfinden soll.

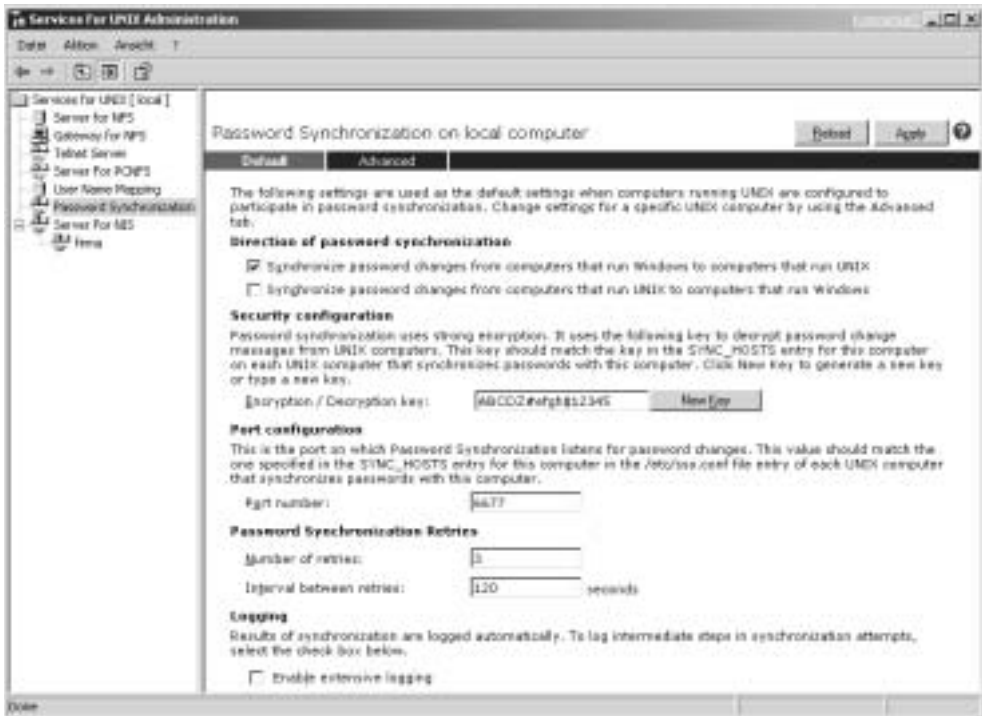


Abbildung 29.4: Die Konfiguration der Password-Synchronisation

29.2.5 Server for NIS

Mit dieser Komponente wird über einen Windows-Domänencontroller die Administration eines Unix-Netzwerks ermöglicht. Auf der Unix-Seite wird Unix Network Information System (NIS) benutzt, auf Windows-Seite das Active Directory. Der Server for NIS ist für die Übersetzung der beiden Umgebungen zuständig. Über einen Wizard können NIS-Domänen-Maps als Active Directory-Einträge exportiert werden. Somit wird der Domänencontroller, der die SFU ausführt, zum Master-Server für die NIS-Domäne. Die

aktuelle Version unterstützt md5-Verschlüsselung sowie bis zu 64000 Benutzer. Über das Snap-In SERVER FOR NIS (siehe Abbildung 29.5) wird allgemein das Intervall festgelegt, in dem der Server in den NIS-Domänen, für die er als Master zuständig ist, nach Aktualisierungen der Maps suchen soll, um diese Daten an die untergeordneten (Slave) Master weiterzugeben.



Abbildung 29.5: Konfiguration des Servers for NIS

Für jede einzelne NIS-Domäne können Sie über die Registerkarte SERVERS zusätzliche NIS-Slave-Server hinzufügen. Es darf aber nur einen Master geben. Auf der Registerkarte MAPS können Sie aus einer Reihe von Maps (z.B. hosts, passwd, netid usw.) wählen, welche davon vom Master an die Slave-Server weitergegeben werden sollen. Slave-Server können lediglich diese vom Master weitergereichten Maps erhalten.

Durch die Installation der SFU erhalten Sie nicht nur die zusätzliche mmc, sondern sämtliche Active Directory-Benutzer bekommen in den Eigenschaften die zusätzliche Registerkarte UNIX ATTRIBUTES (siehe Abbildung 29.6). Hier tragen Sie für die Benutzer Unix-spezifische Angaben wie NIS-Domäne, UID, Login-Shell, Home-Directory und GID ein.

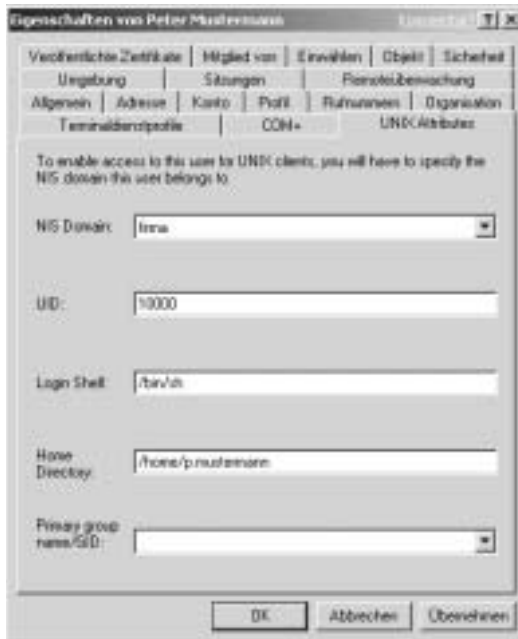


Abbildung 29.6: Die erweiterten Benutzereigenschaften nach der Installation der SFU

29.2.6 Konfiguration des NFS-Servers

Dieses Kapitel beschreibt, wie Sie nach der Installation der SFU den NFS-Server konfigurieren. Die Konfiguration ist Voraussetzung für alle weiteren Einstellungen. Markieren Sie dazu in der SFU-mmc das übergeordnete Snap-In SERVICES FOR UNIX und wählen im Detailbereich die Registerkarte SETTINGS. Hier müssen Sie den Namen des User Name Mapping-Servers angeben.

Als Nächstes legen Sie unter SERVER FOR NFS auf der Registerkarte LOGGING die gewünschten Einstellungen fest. Sie können die gewählten Ereignisse entweder ins Ereignisprotokoll aufnehmen und/oder in eine separate Logdatei schreiben lassen. Legen Sie auch die Maximalgröße der Logdatei fest. Auch die Locking-Einstellungen müssen konfiguriert werden. Zum Schluss müssen noch Einstellungen auf der Registerkarte SERVER SETTINGS vorgenommen werden. Hier wählen Sie das Verbindungsprotokoll. Standardmäßig ist NFS Version 3 aktiviert, es ist aber auch möglich, parallel TCP zu aktivieren. NFS V3 arbeitet mit TCP- und UDP-Protokollen.

Bei der Einstellung des Verzeichnis-Cache bedenken Sie die folgenden Punkte: Ist der Cache aktiviert, wird die Performance gesteigert. Je größer der Cache, desto schneller können die Clients im Speicher-Cache suchen, desto weniger Speicher bleibt aber auch für andere Zwecke.

Weiterhin können Sie den Zeitraum bestimmen, nach dem sich ein Benutzer neu authentifizieren muss, wenn die Verbindung zwischen Client und Server nur im Leerlauf bestand. Diese erneute Authentifizierung kann auch komplett abgeschaltet werden.

Auf der linken Seite der Registerkarte werden die Einstellungen getroffen, wie die Dateinamen zwischen Windows und Unix gehandhabt werden sollen. Dieses ist wichtig, da für NTFS und das Unix-Dateisystem unterschiedliche Zeichen in Dateinamen ungültig sind. So dürfen z.B. Dateinamen unter Windows keinen Doppelpunkt (:) enthalten, unter Unix ist dies gestattet. Sie können hier nun die entsprechenden Übersetzungsregeln konfigurieren. Unix-Dateien, die mit einem Punkt (.) beginnen, können unter Windows als versteckte Datei dargestellt werden. Zusätzlich legen Sie fest, wie die Groß- und Kleinschreibung der Windows-Dateien gehandhabt werden soll. Diese Übersetzungsregeln werden in einer Datei gespeichert. Stellen Sie unbedingt sicher, dass lediglich der Administrator und das System Vollzugriff auf diese Datei haben, die Benutzer nur lesenden Zugriff.

Nachdem der Server konfiguriert worden ist, müssen Client Groups angelegt werden. Über die Client Groups wird bestimmt, welche Zugriffsberechtigungen für welche Computer gelten. Öffnen Sie die Registerkarte CLIENT GROUPS im Container SERVER FOR NFS. Geben Sie der Gruppe einen Namen und klicken auf NEW. Um dieser Gruppe Computer hinzuzufügen, klicken Sie auf ADVANCED und geben die IP-Adressen der gewünschten Computer an.

Im letzten Schritt müssen Sie den Ordner auswählen, auf den die Unix-Clients zugreifen dürfen. Sobald Sie aus dem Kontextmenü des Ordners FREIGABE gewählt haben, sehen Sie, dass durch die Installation der SFU eine neue Registerkarte namens NFS-SHARING (siehe Abbildung 29.7) hinzugekommen ist. Auf dieser Registerkarte werden lediglich Einstellungen für die Unix-Clients vorgenommen. Umgekehrt sind die Unix-Clients nicht von den Einstellungen auf der Karte FREIGABE betroffen. Geben Sie wie gewohnt einen Namen für die Freigabe an. Als Kodierungstyp wird standardmäßig ANSI vorgeschlagen. Schließlich müssen Sie noch festlegen, ob Sie den anonymen Zugriff auf den Ordner zulassen möchten. Um die Zugriffsberechtigungen detaillierter festzulegen, klicken Sie auf PERMISSIONS.



Abbildung 29.7: Die zusätzliche Registerkarte NFS-Sharing nach der Installation der SFU

Standardmäßig verfügen alle Computer nur über die Leseberechtigung für den Ordner. Sie können nun bestimmte Clients Groups hinzufügen, für die Sie andere Berechtigungen festlegen. Markieren Sie die Checkbox ALLOW ROOT ACCESS, so besteht die Zugriffsberechtigung nicht nur für den gewählten Ordner, sondern für den gesamten Verzeichnisbaum, in dem sich der Ordner befindet. Dabei werden für andere Freigaben möglicherweise eingeschränkte Berechtigungen ignoriert.

Stellen Sie unbedingt sicher, dass Sie auf allen Domänencontrollern die Server for NFS-Authentifizierung aktiviert ist, die Konten enthalten, denen der Zugriff auf die Freigaben gestattet ist. Ist diese Authentifizierung nicht aktiviert, wird lediglich der anonyme Zugriff zugelassen. Außerdem sollten sich die Freigaben lediglich auf NTFS-Laufwerken befinden. Hier können Sie die NTFS-Berechtigungen zusätzlich zu den NFS-Rechten konfigurieren.

Um vom Windows-Domänencontroller aus die Unix-Clients mit ihren Freigaben zu sehen, öffnen Sie in der Netzwerkumgebung das gesamte Netzwerk und darin das NFS-Network. Dort sind die Clients mit ihren Freigaben aufgelistet.

29.3 Das Freeware-Tool AD4Unix

Das Freeware-Tool *AD4Unix* bietet wie die SFU Erweiterungsmöglichkeiten für die Interoperabilität zwischen Linux-/Unix-Clients und dem Active Directory. Der Schwerpunkt liegt hier auf einer gemeinsamen Benutzerkontendatenbank für Windows- und Unix-Benutzer im Active Directory, damit eine gegenseitige Authentifizierung erfolgen kann. Die .msi-Datei wird als Erweiterungs-Plug-In auf den Domänencontrollern des Active Directory installiert. Es nimmt ebenso wie die SFU Änderungen am Schema vor. Dabei entsprechen die Modifikationen eher denen der SFU in der Version 2.0. Weiterhin werden auch die Benutzer- und Gruppeneigenschaften um eine Registerkarte für die Unix-Einstellungen erweitert.

Das Programm kann kostenlos unter der Adresse <http://www.css-solutions.ca/ad4unix/> heruntergeladen werden.



Während der Installation kommt es des Öfteren zu Fehlermeldungen bezüglich der DisplaySpecifizer und der verwendeten Sprachversion des Betriebssystems, die aber die Funktionsweise nicht beeinflussen. Es ist empfohlen, unter Windows 2000 mindestens das Servicepack 2 zu installieren.

Da bei der Installation Änderungen am Schema vorgenommen werden, muss zuvor auf dem Schemamaster das Zulassen von Änderungen aktiviert werden. Während der Installation müssen Sie einen NIS-Namen angeben. Dies kann der Name der Windows-Domäne sein. Wird die Benutzerpflege nicht auf dem Domänencontroller, sondern von einer Workstation aus vorgenommen, so müssen Sie *AD4Unix* auch auf diesem Computer installieren.

Nach der Installation können Sie über die mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER die erweiterten Unix-Eigenschaften der Benutzer festlegen. Bei der Installation wurde die Registerkarte UNIX-SETTINGS hinzugefügt. Hier legen Sie die Werte für die NIS-Domäne, die UID und GID fest. Die Einträge im Feld DESCRIPTION ersetzen die Sektion COMMENT der Datei */etc/passwd*. Unter HOME-FOLDER geben Sie den Pfad zum Homeverzeichnis des Benutzers an. Die Spezifizierung der Shell hängt davon ab, ob dem Benutzer die interaktive Anmeldung gestattet werden soll oder nicht. Sind interaktive Anmeldungen erforderlich, so geben Sie z.B. */bin/bash* an. Sind interaktive Anmeldungen untersagt, behalten Sie */bin/false* bei. Diese Einstellungen repräsentieren den Inhalt der Datei */etc/passwd*.

Auch in den Eigenschaften der Benutzergruppen ist eine zusätzliche Registerkarte namens UNIX-SETTINGS hinzugekommen (siehe Abbildung 29.8). Hier werden der Unix-Gruppenname sowie die GID festgelegt. Das Hinzufügen von Benutzern zu Unix-Gruppen geschieht genauso wie das Hinzufügen von Benutzern zu einer Windows-Benutzergruppe.



Abbildung 29.8: Die erweiterten Benutzereigenschaften nach der Installation von AD4Unix

Nachdem Sie entweder die SFU oder AD4Unix installiert, konfiguriert und Benutzer angelegt haben, ist die Einrichtung auf der Windows-Seite abgeschlossen. In den folgenden Kapiteln erfahren Sie, welche Einstellungen aufseiten der Unix-Clients getroffen werden müssen. Sie lernen die Konfiguration verschiedener Authentifizierungsmethoden (*pam_ldap* und *nss_ldap*), den OpenLDAP-Client sowie die Konfiguration des Samba-Servers kennen.

29.4 Der OpenLDAP-Client

Für die Konfiguration ist in unserem Fall lediglich der OpenLDAP-Client interessant. Es gibt jedoch im Rahmen des OpenLDAP-Projekts auch einen Server sowie verschiedene Clientkomponenten. In den aktuellen Linux-Distributionen ist der Client bereits enthalten. Aktuelle Versionen können unter <http://www.openldap.org> heruntergeladen werden. Sie sollten mindestens die Version 2.0.12 oder höher verwenden.

Nach der Installation des OpenLDAP-Clients muss dessen Konfigurationsdatei `/etc/openldap/ldap.conf` angepasst werden. Die Einträge `HOST` und `BASE` müssen gültige Werte erhalten. Unter `HOST` tragen Sie die IP-Adresse oder den DNS-Namen des Windows-LDAP-Servers ein. Benutzen Sie die IP-Adresse, kann der Zugriff selbst bei DNS-Problemen erfolgen. Unter `Searchbase` geben Sie den Namen der Windows-Domäne an, also z.B. `dc=firma,dc=de`. Ein vollständiger Eintrag sieht folgendermaßen aus:

```
HOST 172.20.20.177
BASE dc=firma,dc=de
```

Um die Einträge zu prüfen, verwenden Sie das Programm `ldapsearch`. Es gehört zum Installationsumfang des OpenLDAP-Clients. Eine einfache LDAP-Suche starten Sie mit `ldapsearch -x ""`. Allerdings können mit `ldapsearch` keine anonymen Suchaufträge gestartet werden. Sie müssen ein gültiges Benutzerkonto angeben, z.B.

```
ldapsearch -x -D
"cn=administrator,cn=Users,dc=firma,dc=de"
-W/
"sAMAccountName=del"
```

In diesem Beispiel werden Sie zur Eingabe des Passworts aufgefordert.

29.5 Unix-Authentifizierung am Active Directory über `pam_ldap`

Da das Active Directory auf LDAP beruht, können sich Unix-Clients gegenüber dem Active Directory-LDAP-Server über `pam_ldap` (LDAP Pluggable Authentication Module) bei der Anmeldung authentifizieren. Das `pam_ldap`-Modul unterstützt die folgenden Unix-Versionen:

- ▶ beliebige Linux-Versionen mit Linux-PAM
- ▶ Solaris ab Version 2.6
- ▶ HP-UX 11
- ▶ FreeBSD 3.x und höher
- ▶ Mac OS 10.2

Im Folgenden sehen Sie ein Beispiel für die Konfiguration einer Linux RedHat 8.0-Standardinstallation. Aufseiten des Domänencontrollers müssen lediglich die Benutzerkonten erstellt werden. Auf der Linux-Seite ist die Konfiguration aufwändiger. Dort müssen verschiedene Optionen eingestellt und die Dateien `/etc/ldap.conf` und `/etc/pam.d/login`

angepasst werden. Über die erste Datei wird das `pam_ldap`-Modul konfiguriert, die zweite bestimmt, wie die Benutzerlogins gehandelt werden sollen.

Zuvor müssen Sie sicherstellen, dass eine Netzwerkverbindung zum LDAP-Server besteht. Er kann über die IP-Adresse oder den Hostnamen angegeben werden. Im zweiten Fall prüfen Sie, ob der Name korrekt über den DNS-Server aufgelöst wird. Als DNS-Server sollte der DNS-Server des Active Directory eingetragen sein. Überprüfen Sie den Eintrag in der `/etc/resolv.conf`. Außerdem müssen Sie sämtliche Konten, die sich über LDAP authentifizieren sollen, auch lokal unter Linux einrichten.

29.5.1 Konfiguration der Datei `/etc/ldap.conf`

Als Erstes wird in der Datei `ldap.conf` der Name oder die IP-Adresse eines oder mehrerer LDAP-Server eingetragen. Die entsprechende Sektion der Datei sollte folgendermaßen aussehen:

```
# Your LDAP server. Must be resolvable without using LDAP.
host 172.20.20.175
```

Als Nächstes wird die Sektion `search base` konfiguriert. Geben Sie hier die Domäne an, in der sich der LDAP-Server befindet:

```
# The distinguished name of the search base.
base dc=filiale,dc=de
```

Überprüfen Sie dann, ob in der Sektion `LDAP-Version` der Eintrag `ldap_version 3` vorhanden ist.

Nun muss die User-ID angegeben werden, mit der sich die Benutzer am Domänencontroller anmelden können. Dieses Benutzerkonto muss im Active Directory ebenfalls vorhanden sein. Aus Sicherheitsgründen sollte nicht das Administratorkonto benutzt werden, da das Passwort unverschlüsselt übertragen wird. Konfigurieren Sie dazu Folgendes:

```
# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
binddn cn=Linuxuser,cn=Users,dc=filiale,dc=de
```

Geben Sie als Nächstes das Kennwort für das Konto an:

```
# The credentials to bind with.
# Optional: default is no credential.
bindpw kennwort
```

Legen Sie dann in der Sektion `Port` den Port für die Verbindung fest. Der LDAP-Standardport ist 389. Setzen Sie danach im Bereich `Search Scope` den Wert `scope sub` als aktiv, da der Suchbereich `filiale.de` die oberste Hierarchieebene darstellt.

```
# The search scope.
scope sub
#scope one
#scope base
```


Als Nächstes müssen Sie das `pam_login`-Attribut auf den Wert `sAMAccountName` setzen. Standardmäßig wird die UID benutzt, und diese Information kann das Active Directory nicht bereitstellen.

```
# The user ID attribute (defaults to uid)
pam_login_attribute sAMAccountName
```

Legen Sie dann die Hash-Methode für das Kennwort fest. Vom Active Directory werden die Methoden `clear text`, `unix cipher` sowie `md5` akzeptiert. Die sicherste Methode ist `md5`.

```
# Do not hash the password at all; presume
# the directory server will do it, if
# necessary. This is the default.
pam_password md5
```

In der `ldap.conf` kann noch eine Reihe von weiteren Parametern konfiguriert werden. Sie benutzen diese, wenn Sie eine SSL-Verschlüsselung und Zertifikatsprüfung für die LDAP-Authentifizierung benutzen möchten. Auch Gruppenmitgliedschaften des Benutzers sind dort einstellbar. Mit diesen Änderungen ist die Konfiguration der `ldap.conf` abgeschlossen.

29.5.2 Authconfig

Wenn Sie die `ldap.conf` nicht komplett manuell editieren möchten, können Sie unter Red-Hat-Linux auch das Konfigurationsprogramm `authconfig` als Root in der Konsole aufrufen. Hier können Sie nacheinander die Werte für den LDAP-Server, den Namensraum usw. angeben. Achten Sie unbedingt darauf, dass die Auswahl `USE LDAP-AUTHENTICATION` markiert ist.

Bedenken Sie jedoch, dass `authconfig` dafür entwickelt wurde, das System für eine Authentifizierung an einem OpenLDAP-Server vorzubereiten. Deshalb werden auch nicht alle Informationen abgefragt, die zur Authentifizierung am Active Directory erforderlich sind. Vergleichen Sie nach Abschluss von `authconfig` die Einträge der `ldap.conf` mit den im letzten Kapitel beschriebenen. Fehlende oder nicht korrekte Angaben müssen Sie noch manuell anpassen.

29.5.3 Konfiguration der Datei `/etc/pam.d/login`

Als Nächstes wird nun die Datei `/etc/pam.d/login` bearbeitet. In diesem Verzeichnis befinden sich mehrere Dateien zur Konfiguration von PAM. In der `/login`-Datei wird festgelegt, wie die Authentifizierung bei der Anmeldung gehandhabt wird. Diese Datei kann etwa folgendermaßen aussehen:

```
##%PAM-1.0
auth      required    /lib/security/pam_securetty.so
auth      required    /lib/security/pam_nologin.so
auth      required    /lib/security/pam_ldap.so try_first_pass_debug
auth      sufficient  /lib/security/pam_unix_auth.so
account   sufficient  /lib/security/pam_ldap.so
account   required    /lib/security/pam_unix_acct.so
```

```
password required /lib/security/pam_cracklib.so
password sufficient /lib/security/pam_ldap.so
password required /lib/security/pam_unix_passwd.so
use_first_pass md5 shadow
session required /lib/security/pam_unix_session.so
```

Dabei wird über die folgende Zeile sichergestellt, dass zuerst das Kennwort gegenüber Unix überprüft wird. Damit wird der Zugang zum System gewährleistet.

```
auth sufficient /lib/security/pam_unix_auth.so
```

Über diese Zeile wird sichergestellt, dass dasselbe Passwort für die LDAP-Authentifizierung benutzt wird: Sollte dieses nicht funktionieren, so wird nach dem LDAP-Passwort gefragt.

```
auth required /lib/security/pam_ldap.so try_first_pass_debug
```

Alternativ zu der eben beschriebenen Konfiguration der Datei */etc/pam.d/login* können Sie auch die von allen Applikationen benutzte PAM-Konfigurationsdatei */etc/pam.conf* editieren. Die dort eingetragenen Werte gelten für alle Applikationen, die auf PAM zurückgreifen und nicht nur für das Login.

29.5.4 Authentifizierung über pam_ldap und SSL

Bei jeder Authentifizierung verbindet sich *pam_ldap* mit LDAP und sendet dabei Passwörter im Klartext. Dasselbe gilt auch für die *nss_ldap*-Authentifizierung. Um die *pam_ldap/nss_ldap*-Authentifizierung zusätzlich abzusichern, können Sie die SSL-Verschlüsselung aktivieren. Hierzu müssen Sie auf dem Domänencontroller zunächst das Windows 2000 High Encryption Pack sowie einen Zertifikatsserver installieren. Sie benötigen eine autorisierende CA.

Aufseiten des Linux-Clients müssen Sie nun noch einige Änderungen an der *ldap.conf* vornehmen. In der Sektion *Host* muss als LDAP-Server ein Zertifikatsserver eingetragen werden. Im Bereich *Port* müssen Sie nun 636 eintragen. Dies ist der Port für SSL-gesicherte LDAP-Verbindungen. Zum Schluss muss noch unter *SSL* der Wert *ssl=on* eingetragen werden. Damit sind die nötigen Änderungen durchgeführt.

Um die Konfiguration zu testen, sollten Sie wiederum das Programm *ldapsearch* ausführen.

29.5.5 Authentifizierung über stunnel

Als Alternative kann auch die Authentifizierung über *stunnel* eingesetzt werden. Auch hierbei handelt es sich um eine SSL-Verbindung. Dabei wird ein Tunnel zwischen der gesicherten Verbindung zum LDAP-Server und der ungesicherten *pam_ldap*- oder auch *nss_ldap*-Verbindung hergestellt. Bei dieser Methode benötigen Sie keine Zertifikate. Dieses Verfahren ist damit besonders für Umgebungen interessant, in denen noch keine Zertifikatsarchitektur vorhanden ist. Es wird aufseiten des Clients lediglich ein freier Port benötigt. Sollte auf der Client-Seite ebenfalls ein LDAP-Server laufen, so müssen Sie in der *ldap.conf* einen anderen Port als den Standard-LDAP-Port 389 festlegen.

Um *stunnel* auf dem Unix-Client zu starten, verwenden Sie den folgenden Befehl:

```
stunnel -c -d localhost:389 -r hippokrates.firma.de:636 
```

In diesem Beispiel benutzt der Client den Standardport 389. Die Anfrage an den Windows-Server (der Name wird als DNS-Name angegeben) erfolgt über den Port 636. Dies ist der Port für SSL-gesicherte LDAP-Verbindungen.

29.6 Unix-Authentifizierung am Active Directory über *nss_ldap*

Alternativ zur *pam_ldap*-Authentifizierung können Sie auch die *nss_ldap*-Authentifizierung anwenden. *nss* steht für Name Service Switch. Die *nss_ldap*-Module stehen für die folgenden Unix-Versionen zur Verfügung:

- ▶ alle Linux-Distributionen mit Linux-PAM
- ▶ Solaris Version 2.6 und höher
- ▶ HP-UX 11
- ▶ AIX 4.3.3 und höher

Aktuelle Versionen können über *ftp.padl.com* bezogen werden.



Die Erweiterung des Active Directory-Schemas zum Einsatz von *nss_ldap* darf nur über die Services for Unix in der Version 2.0, nicht jedoch in der Version 3.0 erfolgen. Diese Version wird offiziell von der Firma padl noch nicht unterstützt. Alternativ können Sie das Freeware-Tool *AD4Unix* benutzen.

Um die *nss_ldap*-Libraries korrekt zu konfigurieren, müssen über *autoconf* die Optionen *-enable-rfc2307bis* sowie *-enable-schema-mapping* angegeben werden. Dies gilt jedoch nur für Versionen ab 172.

Auch für die Benutzung der *nss_ldap*-Authentifizierung muss die Datei */etc/ldap.conf* editiert werden. *nss_ldap* verwendet nämlich dieselbe Konfigurationsdatei wie *pam_ldap*. Dabei können Sie die im Kapitel *pam_ldap* beschriebenen Änderungen übernehmen. Zusätzlich müssen Sie die Sektion *RFC2307bis naming contexts* anpassen. Diese sollte etwa folgendermaßen aussehen:

```
nss_base_passwd CN=Users,DC=firma,DC=de
nss_base_shadow CN=Users,DC=firma,DC=de
nss_base_group  CN=Group,DC=firma,DC=de
```

In der Sektion *For MSSFU now do* aktivieren Sie die folgenden Einträge:

```
nss_map_objectclass posixAccount user
nss_map_attribute   uid msSFUName
nss_map_attribute   homeDirectory msSFUHomeDirectory
nss_map_objectclass posixGroup Group
nss_map_attribute   cn msSFUName
nss_map_attribute   userPassword msSFUPassword
nss_map_attribute   uniqueMember member
```

Zusätzlich müssen die folgenden Einträge aktiviert bzw. geändert werden:

```
pam_filter objectclass=user
pam_login_attribute sAMAccountName
pam_password ad
```

Als Nächstes wird die Datei */etc/nsswitch.conf* bearbeitet. In dieser Datei wird die Reihenfolge bestimmt, aus welchen Quellen Informationen zu den Services wie *passwd* oder *shadow* bezogen werden sollen. Als Quellen können Sie *files* angeben. Damit werden zuerst lokale Einstellungen, z.B. für den lokalen Root, ausgelesen, dann erst die im LDAP hinterlegten. Die Datei */etc/nsswitch.conf* sollte etwa folgendermaßen aussehen:

```
passwd: files ldap
shadow: files ldap
group: files ldap
```



Änderungen an dieser Datei werden sofort übernommen. Es besteht dabei die Gefahr, dass Sie sich selbst unter Linux aussperren, wenn die spezifizierte Verbindung zum Active Directory noch nicht funktioniert. Um ungewollte Änderungen dennoch rückgängig machen zu können, sollte immer eine Root-Shell geöffnet sein.

29.7 Samba 3.0 und Active Directory

Eine weitere Möglichkeit für den gemeinsamen Dateizugriff von Windows- und Unix-Client ist die Konfiguration des Samba-Servers. Samba ist ein SMB-(Server Message Block-)Server für Dateidienste und Authentifizierung. Die Integration in eine Windows 2000 Active Directory-Domäne ist jedoch etwas komplizierter geworden als das Zusammenspiel zwischen einer NT-Domäne und Samba in der Version 2.2.x. Samba kann jedoch im Active Directory nur in einer Domäne im gemischten Betriebsmodus betrieben werden, in der sich noch Windows NT-Domänencontroller befinden.

Ab Windows 2000 wird zudem im Active Directory Kerberos als das primäre Authentifizierungsprotokoll verwendet. Diese Tatsache sowie der Wunsch einer Domäne im einheitlichen Betriebsmodus stellt neue Herausforderungen an den Samba-Server, sofern dieser auch weiterhin eingesetzt werden soll. Ermöglicht wird dieses in der Samba-Version 3.0. Momentan befindet sich diese jedoch noch im Beta-Stadium. Aufgrund dieser Tatsache erhalten Sie des Öfteren Fehlermeldungen, obwohl die Befehle letztendlich korrekt ausgeführt werden. An den Konfigurationseinstellungen sollten zwischen der Beta- und der endgültigen Version keine großen Unterschiede vorhanden sein.

Zur Installation benötigen Sie die folgenden Komponenten:

- ▶ Den aktuellen Code der Samba-Version 3.0
- ▶ Die aktuellen OpenLDAP Development Libraries
- ▶ Die MIT Kerberos Development Libraries (krb5-devel, krb5-workstation und krb5-libs)

Überprüfen Sie zunächst, ob die Zeit zwischen dem Active Directory-Server und dem Unix-Rechner synchronisiert ist. Dies ist für die Funktionsweise von Kerberos entscheidend. Weichen die Systemzeiten beider Rechner um mehr als fünf Minuten voneinander ab, so kann zwar weiterhin eine Kommunikation stattfinden, aber die Ticketinformationen verlieren ihre Gültigkeit.

Nach der Installation müssen Sie Samba konfigurieren, damit Kerberos weiß, wie der Active Directory-Server zu handhaben ist. Diese Konfiguration wird in `/etc/krb5.conf` vorgenommen. Die Konfigurationsdatei sollte folgendermaßen aussehen. Beachten Sie, dass bei der Schreibweise zwischen *firma.de* und *FIRMA.DE* unterschieden wird.

```
[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
ticket_lifetime = 24000
default_realm = FIRMA.DE
dns_lookup_realm = false
dns_lookup_kdc = false

[realms]
FIRMA.DE = {
    kdc = 172.20.20.177
    default_domain = firma.de
}

[domain_realm]
.firma.de = FIRMA.DE
firma.de = FIRMA.DE

[kdc]
profile = /var/kerberos/krb5kdc/kdc.conf

[appdefaults]
pam = {
    debug = false
    ticket_lifetime = 36000
    renew_lifetime = 36000
    forwardable = true
    krb4_convert = false
}
```

Listing 29.1: Die Konfigurationsdatei `etc/krb5.conf`

Zum Testen der Verbindung benutzen Sie den Befehl `/usr/kerberos/bin/kinit user@REALM`. Dabei wird *REALM* durch den Domänennamen *FIRMA.DE* (**unbedingt in Großbuchstaben!**) ersetzt. Funktioniert die Verbindung, werden Sie nach dem Kennwort gefragt. Wurde dieses korrekt angegeben, gelangen Sie wieder an den Prompt.

Nun muss die Konfigurationsdatei des Samba-Servers, die *smb.conf* angepasst werden. Für eine Minimalkonfiguration müssen die folgenden Werte eingetragen werden:

```
realm = FIRMA.DE
ads server = 172.20.20.177
security = ADS
encrypt passwords = yes
```

Als Nächstes muss im Active Directory ein Computerkonto für den Samba-Server erstellt werden. Dieses können Sie entweder über die mmc unter Windows vornehmen oder von Linux aus über den Befehl

```
/usr/kerberos/bin/kinit administrator@FIRMA.DE 
```

Geben Sie nun das gültige Passwort an und fügen mit dem Befehl

```
/usr/local/samba/bin/net ads join 
```

das Computerkonto für den Samba-Server namens Archimedes hinzu. Sie sollten dann die Meldung `Joines 'SOKRATES' to realm 'FIRMA.DE'` erhalten.

Vom Unix-Rechner aus sollten Sie nun in der Lage sein, ohne Angabe eines Passworts – da ja Kerberos verwendet wird – eine Verbindung zu einer Windows-Freigabe herstellen zu können. In der Beta-Version funktioniert jedoch noch nicht der Zugriff von Windows 2000 auf die Unix-Freigaben. Dieser Fehler ist aber in der Endversion behoben. Für das Upgrade der Konfigurationsdateien der Samba-Version 2.x werden entsprechende Wizards bereitgestellt.

29.8 Unix-basierte DNS-Server im Active Directory

Dieses Kapitel beschäftigt sich mit Unix-basierten DNS-Servern für das Active Directory. Auf den ersten Blick mag die DNS-Implementierung unter Windows wesentlich einfacher erscheinen, und in einer reinen Windows-Umgebung wird ohnehin niemand auf die Idee kommen, einen Unix-basierten DNS-Server aufzusetzen. Wird nun aber das Active Directory in einer gemischten Umgebung implementiert, in der bereits ein Unix-Server die DNS-Dienste innehat, so gibt es nicht unbedingt einen Grund, ihm diese Rolle zu entziehen oder einen Unix- und einen Windows-DNS-Server parallel zu betreiben. Allerdings müssen zwei Punkte erfüllt sein, damit dieser DNS-Server mit Active Directory zusammenarbeitet. Zum einen muss er SRV-Einträge (Diensteanträge) zulassen (siehe RFC 2052), idealerweise sollte er auch dynamische Updates (DDNS, siehe RFC 2136) unterstützen. Für die BIND-Version ist die erste Option ab der Version 4.9.7 sichergestellt, die dynamischen Updates werden ab der Version 8.2.1 unterstützt.

Sollen für eine Active Directory-Umgebung Unix-basierte DNS-Server eingesetzt werden, so sind folgende Schritte nacheinander auszuführen oder zu prüfen:

1. Stellen Sie sicher, dass die Unix-DNS-Server über die RFC-Spezifikationen verfügen. Aktualisieren Sie gegebenenfalls die Server.
2. Richten Sie nun auf dem Unix-Server die DNS-Zone ein, die später vom Active Directory benutzt werden soll. Da diese Zone von Windows übernommen wird, muss sie bereits vor der Active Directory-Implementierung existieren.

3. Passen Sie die Zone für dynamische Aktualisierungen an (siehe Kapitel 29.8.1).
4. Auf dem Windows 2000 Server, der zum Domänencontroller werden soll, tragen Sie in der TCP/IP-Konfiguration als DNS-Server den Unix-basierten Server ein.
5. Installieren Sie das Active Directory. Geben Sie als Zonennamen den in Schritt 2 festgelegten Zonennamen an.
6. Nach Abschluss der Active Directory-Installation prüfen Sie die Konfiguration mithilfe des Programms `nslookup`.

29.8.1 Dynamische Aktualisierungen zulassen

Ist der DNS-Server nicht in der Lage, dynamische Updates durchzuführen, so müssen alle Clients eine statische IP-Adresse besitzen, und diese Einträge müssen manuell im DNS-Server eingetragen werden. Unterstützt der DNS-Server dynamische Updates, so wird über die Datei `/etc/named.conf` festgelegt, für welche Zonen die dynamischen Updates angewendet werden sollen. Diese Einträge müssen nur auf dem (primären) Master-DNS-Server für die entsprechende Zone vorgenommen werden. Alle dynamischen Updates werden auf diesem Server durchgeführt. Ein solcher Eintrag sieht folgendermaßen aus:

```
zone "filiale.de" {  
    type master;  
    file "zone1.test";  
    allow update {172.20.20/24};  
}
```

Unter `type` und `file` ist angegeben, dass es sich um einen Master-DNS-Server handelt. `File` gibt den Namen der Datenbankdatei an. Zum Eintrag `allow update` müssen Sie den IP-Adressbereich für die Hosts angeben, die Updates am DNS-Server vornehmen dürfen. Dabei bedeutet `/24`, dass es sich um ein 24-Bit-Subnetz (255.255.255.0) handelt. Nach Hinzufügen dieses Eintrags muss der DNS-Server neu gestartet werden.

Um die dynamischen Updates zu testen, benutzen Sie am besten das Kommandozeilenprogramm `nsupdate`. `nsupdate` ist vergleichbar mit dem Windows-Kommandozeilenprogramm `dnscmd`.

```
$ nsupdate  
> update add archimedes.firma.de. 3600 IN A 172.20.20.172  
> update add _ldap._tcp.dc._msdcs.firma.de. 600 IN SRV 0 100 389  
Windows archimedes.firma.de.  
>
```

Über den Befehl `update add` wird der Hosteintrag (A) für den Rechner `archimedes` in der Domäne `firma.de` vorgenommen. In der nächsten Zeile wird ein SRV-Eintrag hinzugefügt. Dabei wird angegeben, dass der LDAP-Dienst über das TCP-Protokoll für den Domänencontroller der Domäne `firma.de` zur Verfügung steht.

29.8.2 Inkrementelle Zonenübertragungen

Optional ist auch die Fähigkeit des Servers, inkrementelle Zonenübertragungen durchzuführen. Diese Option wird jedoch erst dann wichtig, wenn es innerhalb derselben Zone einen primären und einen sekundären DNS-Server gibt, die untereinander die Zonendaten austauschen. Weitere Spezifikationen dazu finden Sie in RFC 1995. Diese Variante ist nur interessant, wenn Sie in einem großen Netzwerk über mehrere DNS-Server für dieselbe Zone verfügen. In diesem Fall ist der Einsatz von Zonenübertragungen zu empfehlen. Bei nur einem DNS-Server werden logischerweise keine Zonendaten übertragen. Um Zonenübertragungen zuzulassen, müssen Sie ebenfalls die Datei `/etc/named.conf` editieren. Fügen Sie die beiden folgenden Zeilen zur Zonenbeschreibung hinzu:

```
allow-transfer {172.20.20.177};
allow-update {any};
```

Unter `allow-transfer` geben Sie die IP-Adresse(n) der DNS-Server an, an die Zonenübertragungen stattfinden dürfen. In der zweiten Zeile wird spezifiziert, dass beliebige Zonenübertragungen stattfinden dürfen.

29.8.3 Überprüfen der DNS-Einstellungen mit Dlint

Bei der DNS-Konfiguration unter Linux reichen bereits kleine Syntaxfehler wie ein vergessenes Semikolon oder eine zu viel gesetzte Klammer aus, um Probleme bei DNS-Abfragen zu verursachen. Um diesem vorzubeugen, sollten Sie das Programm *Dlint* verwenden. Dies kann unter <http://www.domtools.com/dlint/> heruntergeladen werden. *Dlint* benutzt DiG (Domain Information Groper) und eine Kombination aus shell- und Perl-Script, um DNS-Informationen aus der DNS-Datenbank zu sammeln und analysieren. Sie können also bereits im Vorfeld die Informationen prüfen, bevor Sie später im laufenden Betrieb auf Fehlersuche gehen müssen. Die Fehlersuche über *Dlint* ist wesentlich tiefergehend als die in BIND integrierte Syntaxprüfung.

Dlint überprüft die DNS-Einträge für die Domäne, indem Syntaxfehler, unvollständige Domännennamen sowie die Beziehungen zwischen Host- und Pointer-Ressourceneinträgen untersucht werden. Zusätzlich werden diese Informationen auch für alle Unterdomänen geprüft.

29.9 MacOS-Clients im Active Directory

Neben den Unix-/Linux-Clients sind Macintosh-Computer die häufigsten Clients, die in einer gemischten Umgebung mit Windows oder sogar im Active Directory vorkommen. Da es aber auch für Macintosh keinen Active Directory-Client gibt, ist die Einbindung nicht sehr einfach. Der große und für die Konfiguration entscheidende Entwicklungsschritt erfolgte zwischen der Version MacOS 9.x und MacOS X. Da MacOS X sowie auch die aktuelle Version 10.2 (Jaguar) auf einem Unix-Kern basieren, ist es einfacher, diese Versionen zu integrieren, da MacOS wie ein Unix behandelt werden kann. Ein Beispiel dafür sind die *nss_ldap*-Module, die neben den "klassischen" Unix-Versionen auch für MacOS 10.2 bereitgestellt werden. Ab der Version X unterstützt MacOS jedoch LDAP. So kann zumindest für diese Clients über eine Modifikation des Schemas eine Verbindung

zum Active Directory hergestellt werden. Dieses Kapitel zeigt Ihnen, wie Sie mit Windows-"Bordmitteln" den Datenaustausch zwischen den Macintosh- und Windows-Clients und die Anmeldung an Windows-Servern bewerkstelligen. Hierzu werden die Services for Macintosh benutzt. Außerdem erhalten Sie eine Anleitung zur Modifikation des Active Directory-Schemas für die Verbindung zwischen MacOS X und Windows.

29.9.1 Die Services for Macintosh (SFM)

Die Services for Macintosh (SFM) stellen einige Komponenten bereit, die den Datei- und Druckerzugriff von Macintosh-Clients auf Windows ermöglichen. Die SFM müssen im Gegensatz zu den Services for Unix nicht separat bezogen werden, sondern sind im Lieferumfang des Windows 2000/2003 Servers enthalten.

Sobald die SFM auf einem Windows-Server installiert worden sind, kann dieser als Datei- und Druckserver, RAS-Server sowie als Apple-Talk-Router fungieren. Der Vorteil für die Macintosh-Clients besteht darin, dass auf ihnen keine zusätzliche Software installiert werden muss. Weiterhin können Sie für den Client die MS-UAM (Microsoft User Authentication Module) verwenden, sodass sich dieser beim Start automatisch am Windows-Server anmeldet.

Der in den SFM enthaltene File Server – auch als MacFile – bezeichnet – erstellt auf dem Windows-Server, nicht auf Windows-Clients, eine für den Mac zugängliche Freigabe, organisiert die Berechtigungen und stellt sicher, dass die Macintosh-Dateinamen auch für das Dateisystem NTFS gültige Namen sind. Für das AFP (Apple Filing Protocol) bietet MacFile TCP/IP-Unterstützung an. Sie können somit das Apple-Talk-Protokoll komplett aus dem Netzwerk entfernen, sofern die Mac-Clients ebenfalls auf TCP/IP eingestellt sind. Mac-Clients unterstützen TCP/IP nativ ab der Version 8.x. Für ältere Versionen müssen Sie Zusatzsoftware wie z.B. MacTCP benutzen.

Über den Print-Server MacPrint können die Mac-Clients Druckaufträge an die Drucker eines Windows-Servers schicken. Die Druckaufträge werden direkt weitergeleitet, der Mac-Client kann seine Arbeit fortsetzen, bevor der Druckauftrag beendet wurde.

Außerdem werden den Macintosh-Clients weitere Features von Windows 2000 und höher zuteil. Dazu zählen die Unterstützung von Dateisystem-Filtern, wie z.B. dem EFS- (Encrypted File System-)Filter. Es werden alle vom Macintosh-Client in die Freigabe geschriebenen Daten sofort verschlüsselt und beim Abrufen wieder entschlüsselt. Damit ist auch für die Macintosh-Daten auf einem Windows-Server hohe Sicherheit gewährleistet. Außerdem können auch für die Macintosh-Clients auf Benutzerbasis Datenträgerkontingente eingerichtet werden, um den verfügbaren Speicherplatz zu begrenzen.

Um die SFM auf einem Windows-Server zu installieren, führen Sie die folgenden Schritte aus, sofern diese nicht bereits bei der Erstinstallation mitinstalliert worden sind:

1. Öffnen Sie die SYSTEMSTEUERUNG / SOFTWARE / WINDOWS-KOMPONENTEN HINZUFÜGEN / ENTFERNEN. Dort wählen Sie den Menüpunkt WEITERE DATEI- UND DRUCKDIENSTE FÜR DAS NETZWERK.
2. Über die Details werden dann die Komponenten DATEIDIENSTE FÜR MACINTOSH und DRUCKDIENSTE FÜR MACINTOSH ausgewählt. Nach der Installation laufen die Dienste Dateiserver für Macintosh und SFM Druckserver zusätzlich auf dem Windows-Server.

29.9.2 Freigaben für Macintosh-Clients

Freigaben für Macintosh-Clients können lediglich auf Windows-Servern, nicht jedoch auf Windows 2000- oder XP Professional-Clients eingerichtet werden. Deshalb können die Windows-Clients auch nicht direkt mit den Macintosh-Clients im Netzwerk kommunizieren, selbst wenn beide Seiten ausschließlich TCP/IP verwenden. Ein Client kann nur per FTP oder Telnet auf den Macintosh-Computer zugreifen.

Eine weitere Voraussetzung für die Macintosh-Freigabe auf dem Server ist, dass sie sich auf einem Laufwerk mit NTFS5 befinden muss. Außerdem kann auf CDs (CDFS-Format) zugegriffen werden. Zur Erstellung einer Freigabe für Macintosh-Clients führen Sie die folgenden Schritte aus:

1. Öffnen Sie aus dem Kontextmenü des Arbeitsplatzes den Menüpunkt VERWALTEN. Navigieren Sie zum Snap-In FREIGELEGEBENE ORDNER.
2. Wählen Sie dort aus dem Kontextmenü von FREIGABEN den Eintrag NEUE DATEIFREIGABE. In der Eingabemaske (siehe Abbildung 29.9) wählen Sie den freizugebenden Ordner. Standardmäßig ist nur die Checkbox FOLGENDEN CLIENTS ZUGRIFF GEWÄHREN für Microsoft Windows aktiviert. Aktivieren Sie auch die Checkbox APPLE MACINTOSH und geben einen Freigabenamen für die Mac-Freigabe an.
3. Klicken Sie dann auf WEITER. Sie können nun die Freigabeberechtigungen konfigurieren. Haben Sie die Berechtigung nur für Macintosh-Clients eingerichtet, steht nur die Option FREIGABE- UND ORDNERBERECHTIGUNGEN ANPASSEN zur Verfügung. Da mit den Freigabeberechtigungen nur der Netzwerkzugriff gesteuert wird, sollten Sie lieber die Berechtigungen auf Datei- oder Ordnersebene festlegen.

Damit der Macintosh-Client die Größe des Volumes korrekt erkennt, muss auf ihm der AppleShare-Client in mindestens der Version 3.8 installiert sein. Andernfalls wird die Größe als 2 oder 4 GB angegeben, auch wenn ein freigegebenes Laufwerk größer ist. Serverseitig ist in den SFM zur Behebung dieses Problems die AFP-Spezifikation 2.2 implementiert.



Abbildung 29.9: Erstellen einer Macintosh-Freigabe unter Windows

Unter den vorhandenen Freigaben erscheinen diese Verzeichnisse dann mit Typ MACINTOSH. Das Einrichten von Macintosh-Freigaben kann auch an der Kommandozeile über *macfile* vorgenommen werden. Dazu bietet Windows eine ausführliche Hilfe.

Standardmäßig ist immer die Macintosh-Freigabe MICROSOFT UAM-DATENTRÄGER vorhanden. Diese Freigabe enthält das Installationsprogramm für die UAM-Authentifizierung.

Sobald ein Macintosh-Client auf eine Freigabe zugegriffen hat, befinden sich darin zwei zusätzliche Objekte, die vom Apple-Finder angelegt werden. In dem Ordner NETWORK TRASH FOLDER werden alle Dateien der Freigabe abgelegt, die vom Mac-Client in den Papierkorb verschoben worden sind. Außerdem wird eine Datei namens ICON angelegt.

29.9.3 Authentifizierung der Macintosh-Clients an der Domäne

Sobald auf einem Domänencontroller die SFM ausgeführt werden, können sich die Macintosh-Clients an diesem authentifizieren. Zuerst sollten Sie am Server jedoch die akzeptierten Anmeldearten konfigurieren. Wählen Sie hierzu aus dem Kontextmenü von FREIGABEN in der mmc COMPUTERVERWALTUNG den Eintrag DATEISERVER FÜR MACINTOSH KONFIGURIEREN. Auf der Registerkarte KONFIGURATION können Sie den Servernamen bestimmen, der den Mac-Clients angezeigt werden soll. Optional können Sie einen Anmeldetext verfassen. In der Sektion SICHERHEIT können Sie bestimmen, ob der Macintosh-Client die Kennwörter lokal speichern darf oder nicht. Werden die Passwörter lokal gespeichert, muss der Benutzer diese nicht jedes Mal angeben, wenn die Freigaben beim Start automatisch verbunden werden. Dann müssen Sie eine der Authentifizierungsmethoden wählen. Standardmäßig ist die Option APPLE-KLARTEXT ODER MICROSOFT aktiviert. Bei dieser Einstellung kann der Benutzer selbst entscheiden, ob er die Standard-Macintosh-Anmeldung oder die Microsoft-UAM-Authentifizierung (siehe Kapitel 29.9.5) verwenden möchte. Weitere Möglichkeiten sind APPLE VERSCHLÜSSELT ODER MICROSOFT, NUR MICROSOFT, APPLE KLARTEXT und APPLE VERSCHLÜSSELT. Außerdem können Sie die Anzahl der gleichzeitigen Sitzungen zu diesem Server beschränken (siehe Abbildung 29.10).



Richten Sie die reine Microsoft-Authentifizierung erst ein, wenn auf allen Mac-Clients der MS-UAM-Installer (siehe Kapitel 29.9.5) ausgeführt wurde. Die Clients benötigen für den Zugriff auf den Installer noch eine Standard-Apple-Authentifizierungsmöglichkeit. Ansonsten sind sie von der Installation ausgesperrt.



Abbildung 29.10: Auswahl der Apple-Authentifizierung

Selbstverständlich müssen auf dem Windows-Server die Benutzerkonten für die Macintosh-Benutzer angelegt sein. Damit ist die serverseitige Konfiguration abgeschlossen.

29.9.4 Die standardmäßige Apple-Authentifizierung

Ein Macintosh-Client muss sich nicht zwangsläufig am Windows-Netzwerk anmelden. Solange er nur auf Ressourcen anderer Macintosh-Computer zugreift, kann dies nicht vom Domänencontroller kontrolliert werden. Um den Mac-Client für den Zugriff auf den Server über die standardmäßige Apple-Authentifizierung zu konfigurieren, führen Sie die folgenden Schritte aus. Die Beschreibung bezieht sich auf MacOS 9.1.

1. Öffnen Sie das Apfel-Menü und öffnen das Dienstprogramm AUSWAHL. Markieren Sie das Objekt APPLESARE.
2. Sie sehen im rechten Fenster eine Liste aller verfügbaren Windows-Server, auf denen die SFM installiert sind.
3. Wird die Verbindung jedoch nur über TCP/IP hergestellt, klicken Sie auf SERVER IP-ADRESSE und geben die Adresse des Servers an. Klicken Sie dann auf VERBINDEN.
4. Nun müssen Sie noch ein gültiges Benutzerkonto und Kennwort für die Anmeldung am Server angeben. Bei der standardmäßigen Apple-Authentifizierung wird das Passwort unverschlüsselt gesendet, zudem darf es maximal acht Zeichen umfassen. Sie sehen also, dass diese Methode bestenfalls für sehr kleine Netzwerke geeignet ist, in denen das interne Sicherheitsrisiko nicht sehr hoch ist.
5. Sie sehen nun alle Macintosh-Freigaben, die auf dem Server vorhanden sind. Aktivieren Sie die Checkboxes der Freigaben, mit denen beim Start eine Verbindung automatisch hergestellt werden soll. Diese werden automatisch als Volume gemountet (siehe Abbildung 29.11).

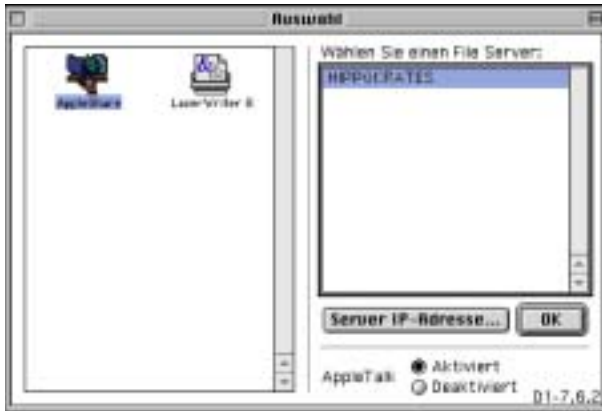


Abbildung 29.11: Das Apple-Menü Auswahl

Da diese Anmeldung insbesondere in großen Netzwerken erhebliche Sicherheitsrisiken birgt, sollten Sie lieber die MS-UAM-Authentifizierung einrichten.

29.9.5 Die Microsoft UAM-Authentifizierung

Um diese Authentifizierung zu ermöglichen, muss auf dem Macintosh-Client zunächst das Programm Microsoft UAM (User Authentication Method) installiert werden. Dieses befindet sich in der Freigabe MICROSOFT UAM-DATENTRÄGER jedes Servers mit SFM. Stellen Sie über den NETZWERKBROWSER/MIT SERVER VERBINDEN eine Verbindung zu einem Server her. Dort sehen Sie alle Freigaben des Servers. Starten Sie aus der Freigabe das MS-UAM-Installationsprogramm (siehe Abbildung 29.12).



Abbildung 29.12: Das UAM-Installationsprogramm

Die Installation dauert nur sehr kurze Zeit. Sie sollten dann eine Meldung erhalten, dass die Systemerweiterung erfolgreich installiert wurde. Starten Sie danach den Macintosh-Client neu. Wählen Sie nun aus dem Apfel-Menü den Eintrag AUSWAHL. Klicken Sie auf APPLESHARE und den gewünschten Server. Sie sehen, dass Ihnen nun die Apple-Standardauthentifizierung sowie die UAM-Authentifizierung zur Wahl stehen. Wählen Sie letztere und geben gültige Benutzerinformationen an. Sie sehen nun alle Macintosh-Freigaben auf diesem Server.

Allerdings hat diese sichere Authentifizierungsmethode einen kleinen Nachteil gegenüber der Standard-Apple-Authentifizierung. Bei der Microsoft-Authentifizierung ist es leider nicht möglich, Laufwerke beim Start automatisch als Volumes zu mounten. Verwenden Sie die Apple-Authentifizierung, werden Sie, bevor der Finder erscheint, nach den gültigen Benutzerdaten für die Windows-Freigaben gefragt. Ist das Passwort lokal gespeichert, erfolgt die Anmeldung am Server automatisch. Dieses Verhalten ist bei der Microsoft-Anmeldung aus Sicherheitsgründen nicht möglich. So soll vermieden werden, dass automatisch auf Windows-Daten zugegriffen werden könnte. Versuchen Sie die Datenträger für den automatischen Start zu konfigurieren, erhalten Sie eine entsprechende Fehlermeldung.

Wollen Sie die sichere Authentifizierung verwenden, müssen Sie nach jedem Start über das APFEL-MENÜ / AUSWAHL eine neue Verbindung zum Windows-Server herstellen.

29.10 Die Anmeldung am Active Directory über MacAdministrator

Wie Sie eben gesehen haben, kann mit Bordmitteln keine gesicherte Authentifizierung in Kombination mit automatischem Mounten der Macintosh-Freigaben erfolgen. Abhilfe schafft hier das Programm *MacAdministrator* der Firma Hi Resolution (www.hi-resolution.com). Mit diesem Programm können sich Macintosh-Clients an beliebigen Betriebssystemen anmelden. Neben der Anmeldung am Active Directory ist auch eine Anmeldung unter Novell Netware sowie anderen AFP- und AFP/IP-fähigen Systemen wie Windows NT 4 oder AFP-fähigen Unix-Versionen möglich.

Auch für die Authentifizierung steht ein breites Spektrum an unterstützten Servern bereit. Diese kann an LDAP-Servern, Kerberos-Servern, Radius-Servern sowie Novell-Servern erfolgen.

MacAdministrator wird zentral auf einem Server in einer Macintosh-Freigabe installiert. In dieser Freigabe befinden sich sämtliche Konfigurationsdateien sowie der *MacAdministrator*-Client. Dieser Client wird einmalig auf dem Macintosh-Clients installiert und authentifiziert sich beim Start am angegebenen Server. Dabei werden auch automatisch die zugewiesenen Volumes gemountet.

Weiterhin unterstützt der *MacAdministrator*, dass ein Macintosh-Benutzer das Passwort für seine Volumes ändern kann. Diese Änderungen werden direkt an den Server weitergeleitet und von diesem übernommen.

Selbstverständlich können auch diverse Macintosh-spezifische Einstellungen für die Clients vorgenommen und diesen zugewiesen werden. Diese Zuweisungen sind in Ansätzen vergleichbar mit den Gruppenrichtlinien unter Windows.

Aktuell liegt der *MacAdministrator* in der Version 2.5 vor. Diese Version unterstützt alle Macintosh-Clients der Version MacOS 7.1 bis 9.x. Die Version 3.0 befindet sich momentan noch im Beta-Stadium. Sie wird dieselben Clients sowie zusätzlich MacOS X unterstützen.

29.11 Verbindung von MacOS X-Clients mit dem Active Directory

Wie bereits erwähnt, bietet das Betriebssystem keine Unterstützung der ADSI-Schnittstelle. Allerdings unterstützt MacOS X aufgrund des Unix-Kerns LDAP. Somit ist es möglich, über LDAP-Aufrufe auf das Active Directory zuzugreifen. Hierfür sind jedoch einige Modifikationen am Active Directory-Schema notwendig.

Eine zentrale Authentifizierung am Active Directory kann selbst dann erfolgen, wenn die Macintosh-Clients in einer Netzwerkumgebung auf Ressourcen zugreifen, die sich auf MacOS X-Servern befinden, während die Windows-Clients Ressourcen der Windows-Server benutzen. Das Active Directory soll in die Lage versetzt werden, die Homeverzeichnisse der Macintosh-Clients auf den MacOS X-Servern zu spezifizieren. Sobald ein Macintosh-Benutzer eine Verbindung zum Mac-Server herstellt, um auf eine Ressource in einer Freigabe zuzugreifen, wird er vom Server aufgefordert, einen Benutzernamen und ein Kennwort anzugeben. In diesem Moment sendet der Mac-Server die Informationen an einen Domänencontroller, der diese mit den Benutzerinformationen im Active Directory vergleicht. Wurde der Benutzer erfolgreich authentifiziert, werden diese Informationen für den Zugriff auf die Freigabe auch vom Mac-Server als gültig angesehen.

Neben der Authentifizierung an den Freigaben auf den Mac-Servern kann über das Active Directory auch die Zuweisung des Homeverzeichnisses erfolgen. Während der Authentifizierung erhält der Mac-Server die Benutzerinformationen aus dem Active Directory. Neben dem Benutzernamen und Kennwort sind hier auch die Angaben über das Homeverzeichnis, das Dateisystem des Homeverzeichnisses sowie das Zugriffsprotokoll dafür enthalten. Der Mac-Server gibt diese Informationen an den Client weiter, sodass sich dieser mit seinem Homeverzeichnis verbinden kann.

Damit im Active Directory die zusätzlichen Informationen für das Homeverzeichnis speichern kann, müssen Sie drei neue Attribute anlegen. Diese Attribute verknüpfen Sie mit einer ebenfalls neu zu erstellenden Klasse. Bevor Sie diese Änderungen am Schema-master der Domäne vornehmen, stellen Sie sicher, dass mindestens Windows 2000 SP2 installiert ist und das Änderungen am Schema auf diesem Server gestattet sind. Außerdem müssen für die neuen Schema-Objekte gültige OIDs bereitstehen.

1. Zunächst legen Sie drei Attribute mit den Namen *vfmdir* (Verzeichnispfad), *vfstype* (Dateisystem) und *vfsopts* (Zugriffsprotokoll) an. Diese Attribute müssen folgende Einträge besitzen (siehe Tabelle 29.1):

Eintrag	vfmdir	vfstype	vfsopts
Gemeinsamer Name	vfmdir	vfstype	vfsopts
LDAP-Anzeigenname	vfmdir	vfstype	vfsopts
Syntax	Groß-/Kleinschreibung beachten	Groß-/Kleinschreibung beachten	Groß-/Kleinschreibung beachten
Mehrwertig	nein	ja	ja

Tabelle 29.1: Schemaeinträge für die neuen Attribute

- Nach dem Erstellen dieser Attribute führen Sie zunächst ein Update des Schema-Cache durch (siehe Kapitel 24.2.2). Dann müssen Sie eine neue Klasse erstellen, der die Attribute zugewiesen werden. Diese Klasse erhält die folgenden Werte (siehe Kapitel 29.2):

Eintrag	Wert
Gemeinsamer Name	mounts
LDAP-Anzeigename	mounts
Übergeordnete Klasse	top
Klassentyp	strukturell

Tabelle 29.2: Schemaeinträge für die neue Klasse

- Klicken Sie dann auf NEXT und fügen die drei eben erstellten Attribute als optionale Attribute hinzu. Nach dem Erstellen der Klasse wählen Sie aus deren Kontextmenü EIGENSCHAFTEN und überprüfen nochmals die Einträge. Achten Sie darauf, dass auf der Registerkarte BEZIEHUNG als einzige zugelassene Oberklasse ORGANIZATIONAL-UNIT eingetragen ist.
- Danach starten Sie das Support-Tool *ADSIEDIT*. Wählen Sie aus dem Kontextmenü des Containers DC=, DC=, der ein Untercontainer von DOMAIN NC ist, den Eintrag NEU/OBJECT. In der dann erscheinenden Dialogbox CREATE OBJECT wählen Sie aus der Liste der Klassen ORGANIZATIONALUNIT und klicken auf NEXT. Geben Sie dann als Wert MOUNTS ein. Klicken Sie auf WEITER und schließen den Vorgang ab. Sie sehen, dass nun in der Liste ein neues Objekt OU=mounts vorhanden ist.
- Jetzt müssen Sie mount-Objekte erstellen, die sich auf die verschiedenen Lokationen der Homeverzeichnisse der Macintosh-Benutzer beziehen. Legen Sie dann Benutzerkonten für die Mac-Benutzer an und verbinden die Benutzerobjekte mit den mounts-Objekten.

30 Metadirectory-Services

Dieses Kapitel beschreibt die Microsoft Metadirectory-Services. Diese Dienste werden benötigt, wenn neben dem Active Directory noch weitere Verzeichnisdienste in einem Unternehmen zum Einsatz kommen und die Einträge der verschiedenen Verzeichnisse synchronisiert werden sollen, um die Administration und Pflege der Datenquellen zu vereinfachen. Das aktuelle Metadirectory-Service-Produkt von Microsoft ist der Microsoft Identity Integration Server (MIIS) 2003. Dieser ist der Nachfolger der Microsoft Metadirectory Services (MMS) 2.2. Die Version 1.0 der MMS wurde noch von der Firma Zoomit entwickelt. Diese wurde jedoch 1999 von Microsoft übernommen, sodass die Version 2.x direkt von Microsoft entwickelt wurde.

30.1 Der Zweck eines Metadirectories

Ein Unternehmen verfügt nicht zwangsläufig nur über ein einziges Verzeichnis, in dem sämtliche Daten gespeichert sind. Verschiedene Datenquellen können auf der Fusion und Zusammenlegung von Unternehmen beruhen, die unterschiedliche Produkte verwenden und auch nach der Zusammenlegung weiterbenutzen. Eine Erforderlichkeit für verschiedene Datenquellen kann auch darin liegen, dass für bestimmte Erfordernisse eines Unternehmens nicht die benötigten Produkte von ein und demselben Hersteller geliefert werden können, sodass der Einsatz verschiedener Applikationen mit unterschiedlichen Speicherorten erforderlich wird. Durch die Zusammenlegungen sind zwar die einzelnen IT-Umgebungen zusammengeführt und vereinigt worden, eine wirkliche Integration hat aber meist nie stattgefunden. So kommt es, dass Daten wie Benutzerprofile, Einstellungen oder berechtigungsbezogene Daten an diversen Speicherorten hinterlegt sind und oftmals der Überblick über die Daten fehlt, was im schlimmsten Fall zu Sicherheitsrisiken führen kann.

30.2 Microsoft Identity Integration Server 2003 (MIIS)

Der MIIS ist die neueste Version der Microsoft Metadirectory Services und seit Juli 2003 erhältlich. Während der Entwicklungsphase trug das Produkt noch den Namen MMS 2003. MIIS ist in der Standard- und Enterprise-Version verfügbar. In der Standardversion befinden sich lediglich Managements Agents für die Synchronisation von Active Directory und Exchange 2000, sodass Active Directory-Gesamtstrukturen untereinander verbunden und synchronisiert werden können. In der Enterprise-Version befindet sich eine Reihe weiterer Agents für die Synchronisation unterschiedlichster Verzeichnisse wie z.B. Novell e-Directory, SunOne Directory, Microsoft SQL, Oracle oder Lotus Notes. Eine

detaillierte Auflistung finden Sie in Kapitel 30.3.1. Auch eine Passwort-Management-Funktion ist nur in die Enterprise-Version integriert. Die Standardversion ist frei verfügbar und kann bei Microsoft heruntergeladen werden. Bei der Enterprise-Version wird eine prozessorbasierte Lizenzstruktur verwendet.

30.2.1 Die Architektur des MIIS 2003

In diesem Kapitel wird Ihnen zunächst der Aufbau und die Architektur des MIIS 2003 mit seinen Komponenten vorgestellt.

Datenquelle und Management Agents

Eine *verbundene Datenquelle* ist eine Datenbank oder ein Verzeichnis mit Identitätsdaten. Dabei kann es sich um eine Verzeichnisdatenbank, ein E-Mail-Verzeichnis oder aber auch Dateien im LDIF-Format oder in XML handeln. Diese Datenquelle wird über einen *Management Agent* mit dem Metadirectory verbunden. Über diesen Agent wird das Verschieben und Synchronisieren von Daten geregelt. Dies geschieht mithilfe von Regeln, die vorgeben, wann Objekte erstellt oder gelöscht werden, wie die Attribute eines Objekts verbunden werden und wie die Objekte in Metaverse gefunden werden. Für jede Datenquelle wird ein separater Agent verwendet. Mit der Verwendung von Management Agents wird die Installation zusätzlicher Client-Software überflüssig.

Die von den Management Agents gesammelten Identitätsdaten werden in zwei logischen Namensräumen gespeichert. Hierbei handelt es sich um den *Connector Space* und *Metaverse*.

Connector Space

Der *Connector Space* (CS) ist ein Zwischenspeicher, der von den Management Agents beim Verschieben von Daten in oder aus der Datenquelle verwendet wird. Dabei wird die gerade aktuell verwendete Datenquelle mit allen ihren Objekten im CS gespiegelt. Dabei ist nicht das Objekt selbst im CS vorhanden, sondern eine Untergruppe der Objektattribute. Diese Untergruppe wird durch den jeweiligen Management Agent definiert. Jede Datenquelle verwendet einen unabhängigen logischen Bereich innerhalb des CS.

Gegenüber anderen Metadirectory-Produkten bietet der CS des MIIS 2003 einige wichtige Vorzüge. Im CS befinden sich sämtliche relevanten Attribute aus allen angeschlossenen Datenbanken und Verzeichnissen. Es ist keine Abfrage aller einzelnen Datenquellen mehr notwendig, um auf die Daten zugreifen zu können. Bei Änderungen an einem Objekt bzw. Attribut bleiben im CS die originalen sowie die geänderten Informationen enthalten. Angenommen, in der Personaldatenbank wird ein Mitarbeiter nach dem Ausscheiden aus der Mitarbeiterdatenbank gelöscht, so ist im CS die Information über diesen Löschvorgang enthalten. MIIS 2003 kann dann zum Mitarbeiter gehörende weitere Objekte wie z.B. sein Mailkonto oder Benutzerkonten automatisch ebenfalls entfernen. Diese Änderungen können an allen zum Benutzer gehörenden Objekten vorgenommen werden, die sich im CS befinden. Objektänderungen sowie Änderungen auf Attributebene werden im CS transparent vorgehalten, sodass für einen Administrator jederzeit die Möglichkeit besteht, diese Änderungen zu betrachten oder zu dokumentieren, bevor diese endgültig übernommen werden.

Metaverse

Der zweite Speicherbereich ist das *Metaverse* (MV). Das MV besteht aus einer Reihe von Tabellen, die die Identitätsinformationen aus allen verbundenen Datenquellen enthalten. Die Informationen über jede einzelne Person werden im MV aus allen Tabellen ausgelesen, und pro Person wird ein Eintrag generiert, der die Daten sämtlicher Tabellen enthält.

Innerhalb des CS befinden sich Connector-Objekte und Disconnecter-Objekte. Ein Connector-Objekt ist dabei mit einem Objekt im MV verbunden, ein Disconnecter-Objekt ist mit keinem Objekt des MV verbunden. Sobald ein neues Objekt aus einer Datenquelle in den CS geschrieben wird, wird automatisch ein Disconnecter-Objekt erstellt. Erst über Regeln innerhalb des Management Agents wird festgelegt, ob das Objekt im MV erstellt werden kann und damit zum Connector-Objekt wird. Bei sicherheitsrelevanten Objekten wie z.B. dem Administratorkonto ist es nicht sinnvoll, dass dieses innerhalb des MV existiert. Sofern ein Objekt nicht im MV vorhanden ist, kann diese nicht mit anderen verbundenen Datenbanken oder Quellen synchronisiert werden. Im Gegensatz zu anderen Metadirectory-Produkten erfolgt die Einstellung für Connector- und Disconnecter-Objekte über die GUI der MIIS 2003 und muss nicht über eine Kommandozeile vorgenommen werden.

Ein weiteres Feature des MV ist das sog. Attribute Flow&Precedence. Hierbei handelt es sich um definierbare Regeln für den Import und Export von Attributen vom CS in den MV und umgekehrt sowie die Priorität von gleichen Attributen, die aus verschiedenen Datenquellen in ein MV-Attribut zusammengeführt werden. Angenommen, in mehreren Datenquellen befindet sich das Attribut für die E-Mail-Adresse eines Benutzers, so werden alle diese Attribute im MV in ein einzelnes Attribut E-Mail-Adresse aufgenommen. Hierbei sollten sie jedoch aus Gründen der Datenintegrität eine Priorität der verschiedenen Attributquellen festlegen. Die mit der höchsten Priorität versehene Datenquelle gibt immer den Wert des Attributs an. Ist diese nicht verfügbar, wird die Datenquelle mit der nächsthöheren Priorität herangezogen usw. Auch beim Überschreiben von Einträgen ist die Priorisierung wichtig.

Benutzerdefinierte Erweiterungen – Custom Extensions

MIIS 2003 kann durch benutzerdefinierte Erweiterungen (*Custom Extensions*) den Erfordernissen eines Unternehmens weiter angepasst werden. Die Custom Extensions nehmen Einfluss auf die Funktion der Management Agents und des Metaverse. Diese Extensions werden über eine Programmiersprache wie MS Visual Basic.NET, C# oder C++ erstellt. Deren Implementierung kann entweder über eine Microsoft .NET Framework-Klassenbibliothek oder über eine dll erfolgen.

Custom Extensions weisen ein breites Spektrum von Einsatzmöglichkeiten auf. Die folgenden Einsatzmöglichkeiten sind nur einige Beispiele. Beim Hinzufügen neuer Objekte in das Metaverse können über Custom Extensions automatisch die neuen Einträge im Connector Space erstellt werden. Werden Änderungen an einem Objekt im Metaverse vorgenommen und wird dadurch ein neuer Distinguished Name in einer Datenquelle erforderlich, so kann dieser automatisch über eine Custom Extension erstellt werden. Beim Synchronisierungsprozess können bestimmte Ausnahmen dazu führen, dass die Synchronisation abgebrochen wird. Mithilfe von Custom Extensions kann bestimmt werden, bei welchen Ausnahmen ein Abbruch erfolgen und bei welchen Ausnahmen die

Synchronisation fortgesetzt werden soll. Sobald sich der Status einer Person ändert, z.B. wenn die Person das Unternehmen verlässt, kann über Custom Extensions sichergestellt werden, dass das zum Benutzer gehörige Benutzerkonto im Active Directory automatisch deaktiviert wird. Auch beim Hinzufügen neuer Benutzer zum Metaverse kann für diese Benutzer automatisch ein anfängliches Passwort gesetzt werden.

Data Lineage

Je umfangreicher die Datenquellen sind und je mehr verschiedene es gibt, desto schwieriger wird der Überblick, welches Objekt in welcher Datenquelle erstellt wurde oder in welcher Quelle Änderungen an dem Objekt oder einem seiner Attribute vorgenommen wurden. *Data Lineage* erlaubt eine übersichtliche Darstellung eines Objekts mit all seinen Attributen. Für jedes Attribut wird sein Wert, die Datenquelle und das Datum der letzten Änderung ausgegeben. Auch die History aller Änderungen kann nachverfolgt werden. Dieses Feature bietet als einziges Metadirectory-Product MIIS 2003.

Die MIIS2003-Datenbank

Im Gegensatz zu anderen Metadirectory Service-Produkten verwendet MIIS als Speicherort kein Verzeichnis, sondern eine SQL-Datenbank. Eine SQL-Datenbank bietet gegenüber einem Verzeichnis den Vorteil, dass die Datenbank gleichermaßen für Schreib- und Lesezugriffe optimiert ist, während ein Verzeichnis lediglich für lesenden Zugriff optimale Leistung bringen kann. Zudem bietet der SQL-Server weitere Features wie XML-Unterstützung, Webzugriff auf Datenbankinformationen sowie umfangreiche Analysewerkzeuge.

30.2.2 Die Installation des MIIS 2003

Für die Installation des MIIS 2003 müssen auf dem Server die folgenden Komponenten installiert sein:

- Windows Server 2003 Enterprise Version
- Microsoft SQL Server 2000 Enterprise Version SP3 (Der SQL-Server kann auch auf einem anderen Server installiert sein. MIIS 2003 kann auch Remote-Zugriffe auf die SQL-Datenbank durchführen. Während der Installation ist die entsprechende Instanz anzugeben.)
- Visual Studio .NET



Bei der Installation des SQL Servers 2000 unter Windows Server 2003 erhalten Sie eine Warnmeldung, dass SQL Server 2000 mit Servicepack 2 oder weniger nicht mit Windows Server 2003 kompatibel ist. Ignorieren Sie die Meldung an dieser Stelle, führen die Installation durch und installieren sofort nach Abschluss der Installation das Servicepack 3. Sofern Sie den SQL Server 2000 bereits auf einem Windows Server 2000 installiert haben, installieren Sie unter Windows 2000 das SP3 für SQL Server 2000 und aktualisieren danach den Windows Server 2000 auf 2003.

Windows Server 2003 muss lediglich auf dem Server ausgeführt werden, auf dem MIIS 2003 installiert wird. Alle übrigen Server können auch unter Windows 2000 betrieben werden. Dies beeinträchtigt nicht die Funktionalität des MIIS 2003.

Nach Abschluss der Installation müssen Sie sich vom System abmelden und wieder neu anmelden, damit Mitgliedschaft in der Sicherheitsgruppe übernommen werden kann.

Der MIIS 2003 läuft nach der Installation als Windows-Dienst (MICROSOFT IDENTITY INTEGRATION SERVER).

30.3 Der Identity Manager

Zur Steuerung der MIIS 2003 wird der *Identity Manager* verwendet. Über dieses GUI-basierte Verwaltungsprogramm können Sie alle Verwaltungsaufgaben durchführen. Dazu zählen z.B. das Anlegen und Konfigurieren von Management Agents, Metaverse-Design oder die Verwaltung der Joiner. Folgend werden anhand der verschiedenen Registerkarten die Konfigurationsmöglichkeiten beschrieben.

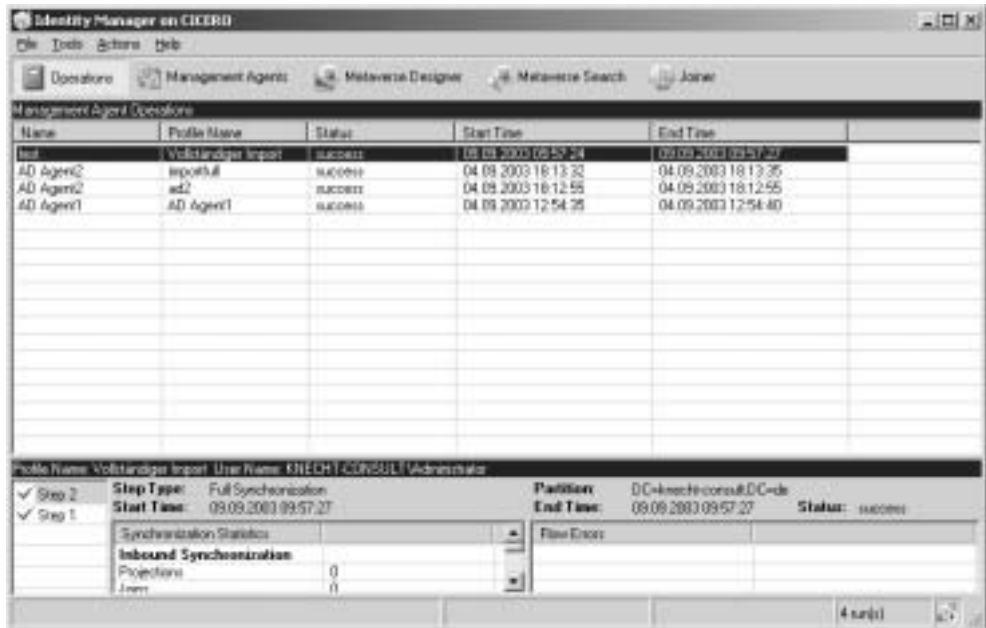


Abbildung 30.1: Der Identity Manager des MIIS 2003

Auf der Registerkarte OPERATIONS (siehe Abbildung 30.1) befindet sich eine Übersicht über alle durchgeführten Aktionen. Im oberen Fensterabschnitt werden für die Aktionen der Management Agents Statusangaben sowie die Start- und Endzeit angegeben. Im unteren Bereich werden Statistiken für Synchronisierungen sowie deren Fehler angezeigt.

30.3.1 Management Agents (MA)

Die Management Agents (MA) stellen die mit dem Metadirectory Service verbundenen Datenquellen dar. Die Konfiguration der Management Agents erfolgt über die gleichnamige Registerkarte des Identity Managers. Um einen neuen Management Agent zu erstellen, führen Sie die folgenden Schritte durch:

1. Wählen Sie aus der Sektion ACTIONS den Link CREATE oder das Menü ACTIONS / CREATE.



Während Sie einen neuen MA erstellen, sollten keine WMI-Skripte ausgeführt werden. Dies könnte zu unvorhergesehenen Fehlern führen.

2. Zunächst müssen Sie einen MA-Typ auswählen (siehe Abbildung 30.2). Welche Optionen Ihnen dabei zur Verfügung stehen, ist abhängig davon, ob Sie die Standard- oder Enterprise-Version verwenden. In der Standardversion sind Management Agents für Active Directory und Exchange 2000 vorhanden. Die Enterprise-Version bietet MAs für die folgenden Datenquellen:

- ▶ Active Directory
- ▶ AD Application Mode (ADAM)
- ▶ AD Global Address List (GAL)
- ▶ Directory Services Markup Language (DSML) 2.0
- ▶ Exchange Server 5.5 sowie 5.5 Bridgehead-Server
- ▶ Exchange Server 2000
- ▶ LDAP Data Interchange Format (LDIF)
- ▶ Lotus Notes Release 4.6 und 5.0
- ▶ Netscape Directory Server 4.1 und 6.01
- ▶ Novell eDirectory 8.6.2 und 8.7
- ▶ Oracle8i- und 9i-Datenbank
- ▶ SQL Server 7.0 und 2000
- ▶ Sun One Directory Server 4.12, 4.13, 5.0 und 5.1 (ehemals iPlanet Directory Server)
- ▶ Windows NT 4.0
- ▶ Textdateien (paarweise Attributwerte oder wertesepariert)

File-based und call-based Management Agents

Die verschiedenen Management Agents werden dabei in zwei Typen unterschieden. Es gibt die sog. file-based und call-based MAs. Zu den file-based Management Agents zählen diejenigen, deren Datenquelle auf einer Datei basiert (sämtliche Textdateien, LDIF sowie DSML). Alle anderen MAs gehören zu der Gruppe call-based.

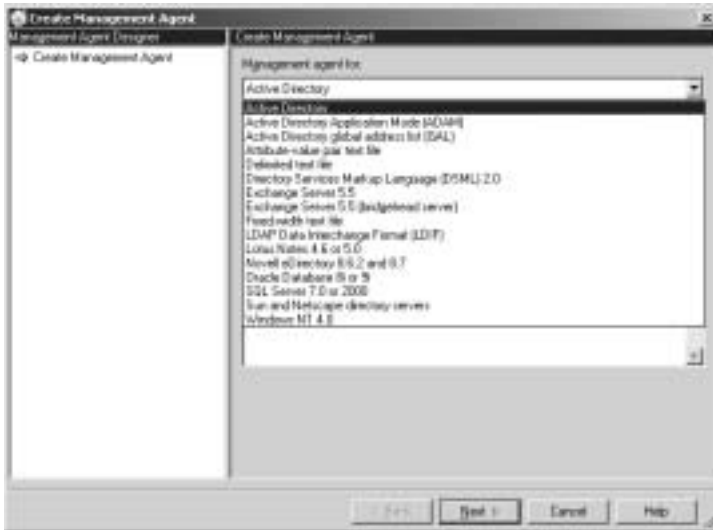


Abbildung 30.2: Den Typ des Management Agents bestimmen

3. Als Nächstes geben Sie einen Namen und optional eine Beschreibung an. Ab diesem Punkt sind die Konfigurationsoptionen für die einzelnen MAs unterschiedlich. In unserem Beispiel wird ein Management Agent für das Active Directory erstellt. Klicken Sie dann auf NEXT.
4. Danach geben Sie den Namen der Gesamtstruktur, Benutzernamen, Passwort und die Domäne an (siehe Abbildung 30.3). Das angegebene Benutzerkonto muss dabei über die Berechtigungen verfügen, das Schema sowie die Verzeichnispartitionen der Gesamtstruktur lesen zu dürfen. Klicken Sie dann auf NEXT.

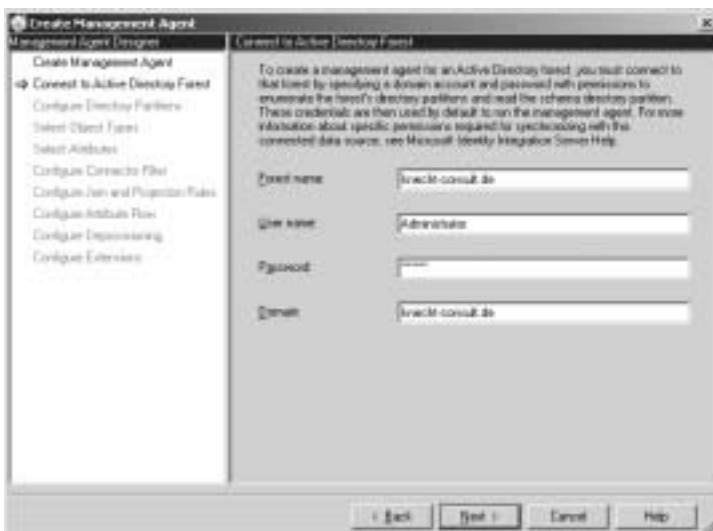


Abbildung 30.3: Festlegen des Benutzerkontos für MIIS 2003

- Im Fenster **CONFIGURE DIRECTORY PARTITIONS** (siehe Abbildung 30.4) wählen Sie die Verzeichnispartitionen aus, die der MA verwenden soll. Über die Checkbox **SHOW ALL** können Sie sämtliche Partitionen der Gesamtstruktur anzeigen. Standardmäßig werden keine DNS-Zonen- oder Konfigurationsdaten-Partitionen angezeigt. In der Sektion **DOMAIN CONTROLLER CONNECTION SETTINGS** können Sie optional Domänencontroller auswählen, von denen bevorzugt Informationen bezogen werden sollen. Dabei sollte es sich um Domänencontroller handeln, die über eine schnelle Netzwerkanbindung verfügen. Unter **CREDENTIALS** können für eine bestimmte Verzeichnispartition alternative Anmeldeinformationen bestimmt werden, als in Schritt 3 festgelegt wurden. Über die Schaltfläche **CONTAINERS** können Sie die Container auswählen, die in den MA mit einbezogen werden sollen. Standardmäßig werden alle Container ausgewählt. Klicken Sie dann auf **NEXT**.

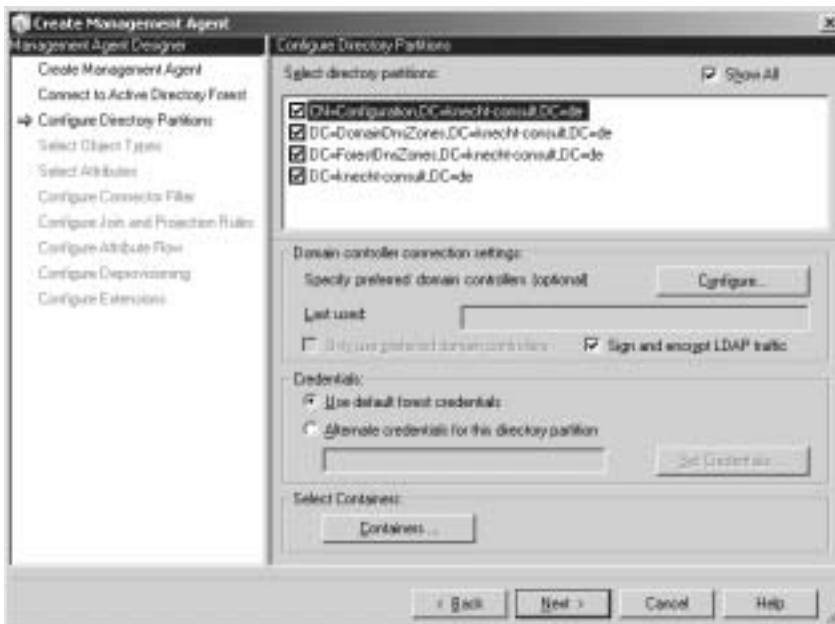


Abbildung 30.4: Auswahl der Verzeichnispartitionen

- Im Fenster **SELECT OBJECT TYPES** (siehe Abbildung 30.5) wählen Sie die gewünschten Objekttypen aus. Auch hier können Sie wieder über die Checkbox **SHOW ALL** sämtliche verfügbaren Objekttypen anzeigen lassen. Klicken Sie dann auf **NEXT**.

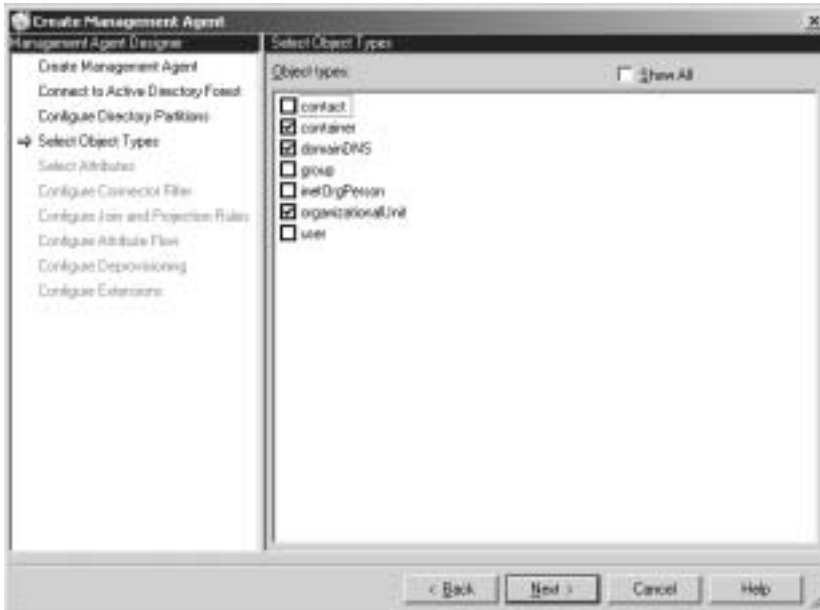


Abbildung 30.5: Auswahl der Objekttypen

7. Unter SELECT ATTRIBUTES (siehe Abbildung 30.6) werden die gewünschten Attribute gewählt. Auch hier können Sie wieder über die Checkbox SHOW ALL sämtliche verfügbaren Attributtypen anzeigen lassen. Klicken Sie dann auf NEXT.

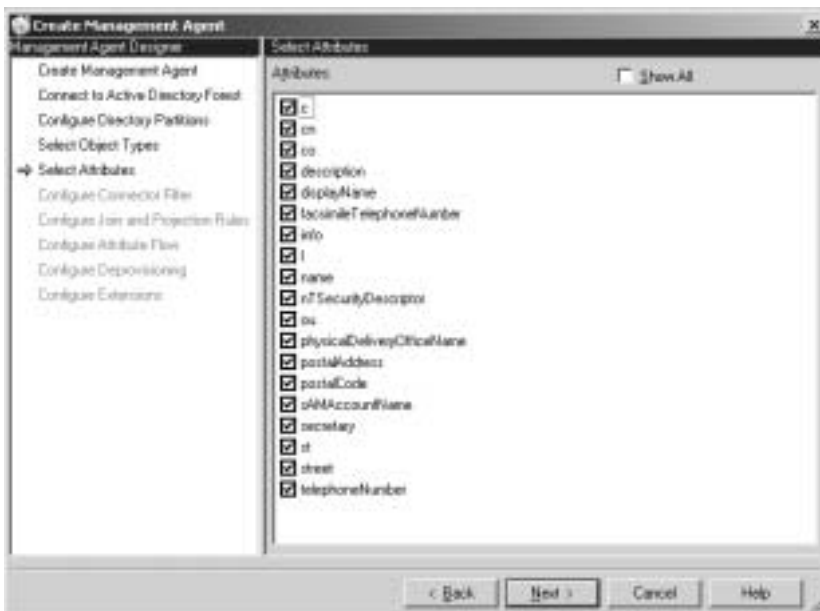


Abbildung 30.6: Auswahl der Attribute

8. Im Fenster CONFIGURE CONNECTOR FILTER (siehe Abbildung 30.7) können für jeden Objekttyp der Datenquellen Filter festgelegt werden.

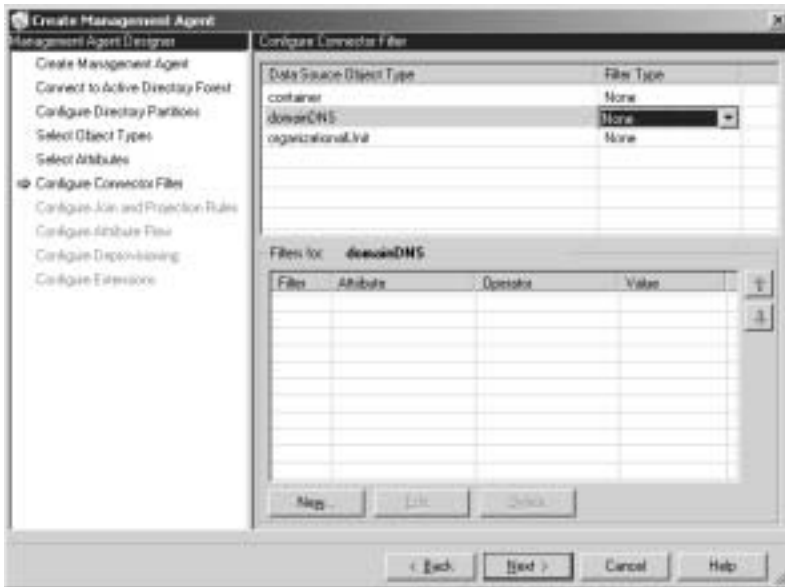


Abbildung 30.7: Konfiguration des Connector Filters

9. Sie können entweder den Filtertyp None, Declared oder Rule Extension aus der Drop-down-Liste wählen oder aber über die Schaltfläche NEW einen neuen Filter erstellen (siehe Abbildung 30.8). Hierbei wählen Sie das Attribut (z.B. name), den Operator (z.B. Starts with) und einen Wert (z.B. S). Diese sind wichtig, wenn der MA im Importmodus ausgeführt wird. Klicken Sie dann auf NEXT.

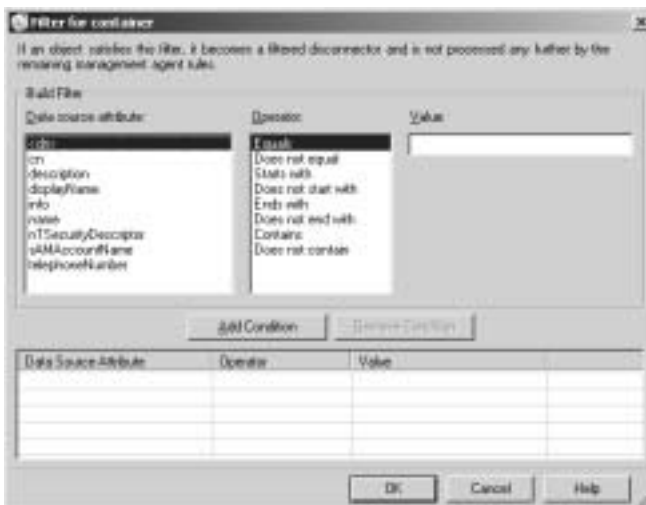


Abbildung 30.8: Erstellen eines neuen Container-Filters

10. Als Nächstes werden die Join und Projection Rules definiert (siehe Abbildung 30.9). Diese Regeln bestimmen, wie die Objekte im Connector Space und Metaverse miteinander verglichen werden. In der Sektion DATA SOURCE OBJECT TYPE sehen Sie, ob für die in Schritt 6 gewählten Objekte Join und Projection Rules angewendet werden. Sofern Regeln definiert sind, können Sie diese hier auswählen. Um eine neue Regel zu erstellen, klicken Sie auf die Schaltfläche NEW JOIN RULE oder NEW PROJECTION RULE. Klicken Sie dann auf NEXT.

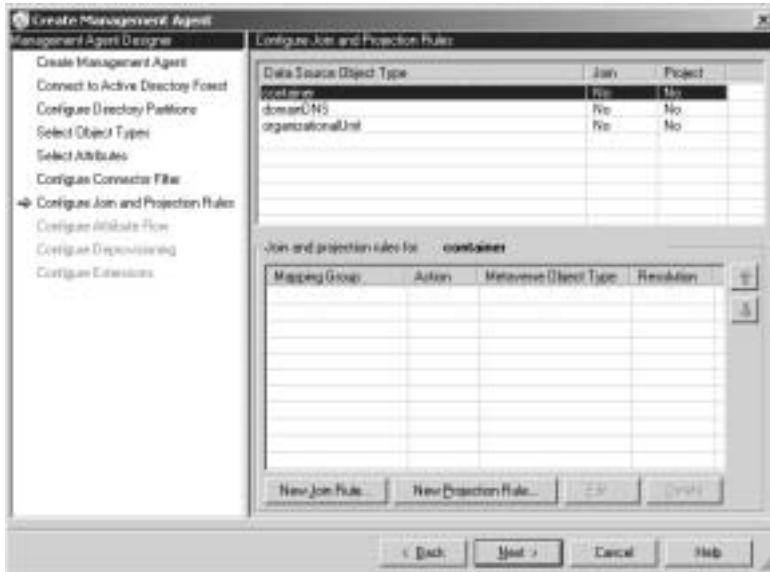


Abbildung 30.9: Konfiguration der Join und Projection Rules

Join Rules und Projection Rules

Join Rules bestimmen die Verbindung zwischen einem CS-Objekt und einem MV-Objekt. Über definierbare Suchkriterien werden die Attribute der Objekte im CS mit denen der Objekte im MV verglichen. Wird der MA gestartet, wird eine auf den Join Rules basierende Join Suche an jedem CS-Objekt gestartet, wobei das korrespondierende Objekt im MV gefunden werden soll. Werden dabei keine Objekte im MV gefunden, werden die Projection Rules angewendet. Wird genau ein übereinstimmendes MV-Objekt gefunden, so wird das CS-Objekt mit dem MV-Objekt verbunden. Werden im MV mehrere Objekte gefunden, wird das CS-Objekt nicht mit dem MV-Objekt gejoinet. In diesem Fall greifen entweder die Rules Extensions (siehe Kapitel 30.3.3), oder Sie wählen manuell auf der Registerkarte Joiner ein MV-Objekt aus, das mit dem CS-Objekt verbunden werden soll.

Die Projection Rules legen fest, ob im Metaverse ein neues Objekt angelegt ist oder nicht, das mit dem CS-Objekt verlinkt werden kann. Diese Regeln werden nur dann angewendet, wenn die Join Rules entweder nicht konfiguriert sind oder bei der Suche nach einem korrespondierenden Objekt im MV kein passender Eintrag gefunden wird. Für jeden Objekttyp im CS kann jeweils nur eine Projection Rule festgelegt werden. Dabei kann es sich entweder um eine Declarative Rule oder um Rules Extension handeln.

11. Im Fenster CONFIGURE ATTRIBUTE FLOW (siehe Abbildung 30.10) werden die Attribute Flow-Regeln konfiguriert. Unter Attribute Flow versteht man den Vorgang, wie Attribute der Objekte im Connector Space sowie im Metaverse beim Import oder Export verbunden und abgebildet werden sollen. Wählen Sie in der Sektion BUILD ATTRIBUTE FLOW aus der Drop-down-Liste DATA SOURCE OBJECT TYPE zunächst den gewünschten Objekttyp. Aus der Liste DATA SOURCE ATTRIBUTE wählen Sie ein Attribut des Objekts, das Sie projizieren möchten. Unter MAPPING TYPE wählen Sie die Option DIRECT, wenn das Attribut des CS direkt mit einem Attribut des Metaverse verbunden werden soll. In diesem Fall müssen beide Attribute denselben Typ haben. Dies ist die Standardeinstellung. Wählen Sie ADVANCED, wenn Sie Rules Extensions beim Attribut-Mapping verwenden möchten. Unter METAVERSE OBJECT TYPE wählen Sie den MV-Objekttyp und unter METAVERSE ATTRIBUTE das entsprechende MV-Attribut, das verbunden werden soll. Unter Flow Direction wählen Sie IMPORT, wenn die Werte des Quellattributs in das Zielattribut des MV übergehen soll bzw. EXPORT für die umgekehrte Richtung. Sollen während eines Exports keine Werte vom MV-Attribut zum verbundenen Zielobjekt fließen, wählen Sie ALLOW NULLS. In diesem Fall wird der Wert des verbundenen Attributs gelöscht, wenn sämtliche MV-Attribute, die für den Export Attribute Flow zu diesem Attribut bestimmt sind, keine Werte enthalten. Um alle Einstellungen zu speichern, klicken Sie auf NEW. Im oberen Bereich werden dann für jedes Objekt alle Attribute Flows der gewählten Attribute aufgelistet. Um später einen Eintrag zu ändern, markieren Sie das gewünschte Attribut und klicken auf EDIT, zum Löschen auf DELETE. Klicken Sie dann auf NEXT.

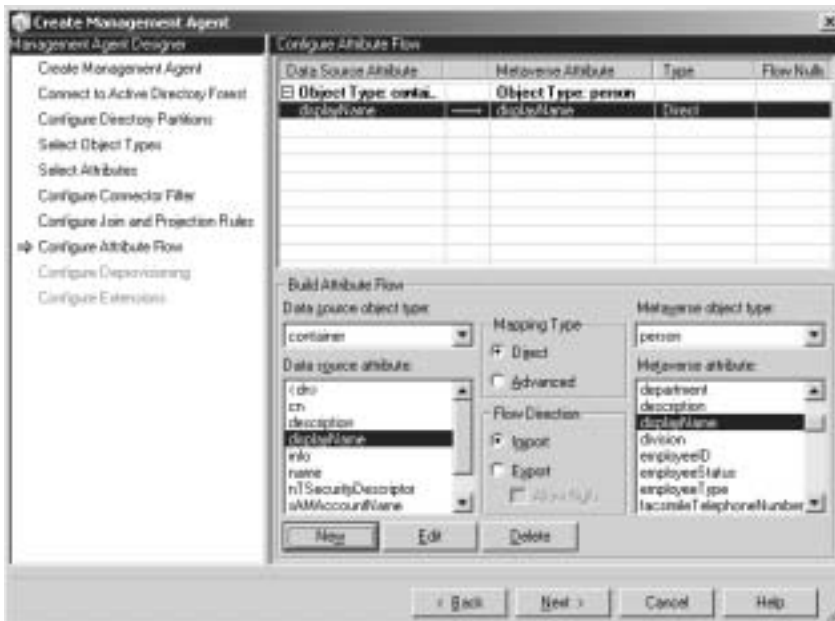


Abbildung 30.10: Konfiguration des Attribute Flow

12. Im Fenster CONFIGURE DEPROVISIONING (siehe Abbildung 30.11) wird das Verhalten der CS-Objekte festgelegt, wenn diese vom entsprechenden MV entkoppelt werden.

Diese Entkoppelung kann entweder eintreten, wenn das verbundene MV-Objekt gelöscht wird oder Rules Extensions angewendet werden. Es stehen vier Optionen zur Verfügung:

- ▶ **MAKE THEM DISCONNECTORS** bewirkt, dass die entkoppelten Objekte im CS verbleiben. Bei folgenden Synchronisationsläufen wird versucht, das Objekt über Join und Projection Rules ins Metaverse zu bringen.
- ▶ Auch bei der Option **MAKE THEM EXPLICIT DISCONNECTORS** bleiben die entkoppelten Objekte im CS erhalten. Allerdings wird bei folgenden Synchronisationsläufen nicht mehr versucht, das Objekt über Join und Projection Rules ins Metaverse zu bringen.
- ▶ Die Option **STAGE A DELETE ON THE OBJECT FOR THE NEXT EXPORT RUN** bewirkt, dass die entkoppelten Objekte im CS sowie in der verbundenen Datenquelle gelöscht werden. Bei den folgenden Synchronisationsläufen wird geprüft, ob das Objekt in der Datenquelle gelöscht wurde. Danach wird das Objekt im CS gelöscht. Hierzu müssen Sie nach dem Erstellen des Management Agent unter **CONFIGURE RUN PROFILES** einen Export einrichten.
- ▶ Sollen Rules Extensions angewendet werden, so wählen Sie **DETERMINE WITH A RULES EXTENSION**.

Sollen Metaverse-Attribute beibehalten werden, die nach der Entkoppelung des Objekts durch diesen Management Agent beigesteuert werden, so markieren Sie die Checkbox **DO NOT RECALL ATTRIBUTES CONTRIBUTED BY OBJECTS FROM THIS MANAGEMENT AGENT WHEN DISCONNECTED**. Standardmäßig werden nach der Entkoppelung eines CS-Objekts vom MV-Objekt die Attribute, die vom CS-Objekt beigesteuert wurden, aus dem MV gelöscht. Klicken Sie dann auf **NEXT**.

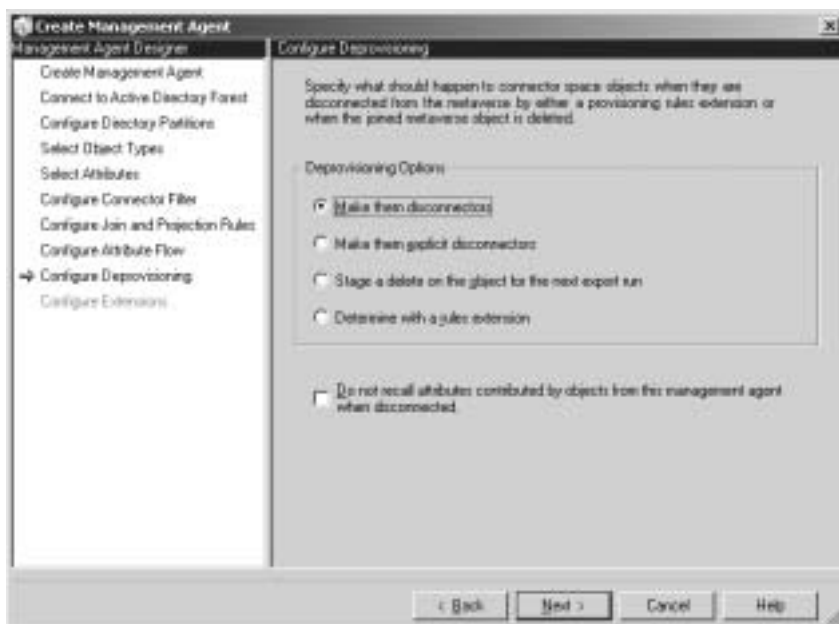


Abbildung 30.11: Konfiguration von Disconnectoren

13. Im Fenster **CONFIGURE EXTENSIONS** (siehe Abbildung 30.12) können für den MA Rules Extensions konfiguriert werden. Zusätzlich können Sie über die Checkbox **ENABLE PASSWORD MANAGEMENT FOR THIS MANAGEMENT AGENT** das Passwortmanagement aktivieren.

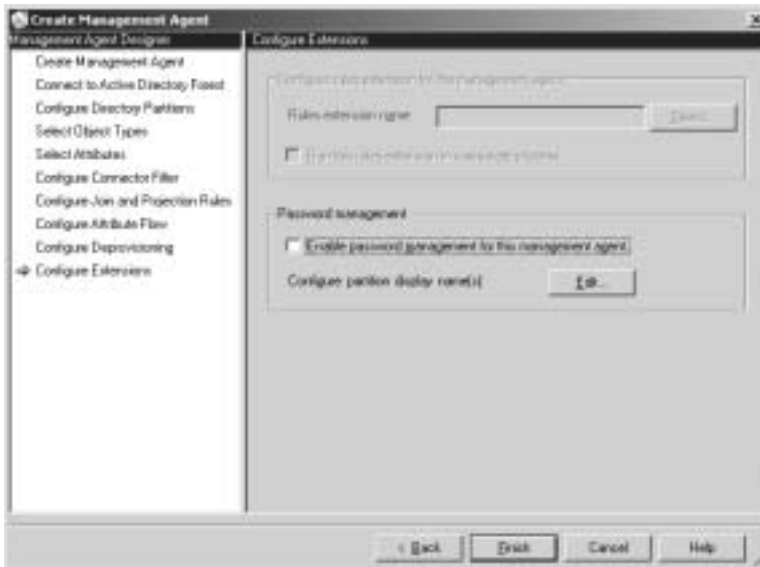


Abbildung 30.12: Aktivieren des Passwortmanagements

Passwortmanagement des MIIS 2003

Der Aufwand für die Verwaltung von Benutzerkennwörtern hinsichtlich Zeit und Kosten sollte von keinem Unternehmen unterschätzt werden. Die Kosten für den Helpdesk bezüglich der Passwortverwaltung können bis zu der Hälfte der gesamten Helpdesk-Kosten betragen. Dieses Feature ist lediglich in der Enterprise-Version des MIIS 2003 vorhanden. Das Passwortmanagement ist für die Management Agents Active Directory, ADAM, Lotus Notes, Novell eDirectory, Windows NT sowie Sun und Netscape Directory Server anwendbar. Für diese Verzeichnisse und Datenbanken kann pro Benutzer ein einziges Passwort verwendet werden. MIIS 2003 bietet eine eigene API sowie Webapplikationen, die der Helpdesk zum Zurücksetzen von Passwörtern oder der Benutzer selbst zum Ändern seines Passworts benutzen kann. Somit ist es möglich, in den eben genannten Datenquellen die Anzahl verschiedener Benutzerpasswörter zu reduzieren. Passwörter können zudem in Echtzeit verwaltet werden, unabhängig von den MIIS 2003-Operationen. Weitere Hinweise zur Implementierung finden Sie in der MIIS 2003 Developer Reference, die Bestandteil der MIIS 2003-Dokumentation ist.

14. Um den Assistenten zur Erstellung des MA abzuschließen, klicken Sie auf **FINISH**.

Sämtliche Einstellungen, die Sie beim Anlegen eines Management Agents getroffen haben, können Sie später über **PROPERTIES** in der Sektion **ACTIONS** oder über das Menü **ACTIONS/PROPERTIES** separat ändern.

Export von Management Agents

Management Agents können auch exportiert werden. Dies geschieht über den Link UPDATE MANAGEMENT AGENT in der Sektion ACTIONS. Beim Export wird der MA in eine xml-Datei gespeichert. Diese xml-Datei kann später zum Import oder Update benutzt werden. Sie sollten die Exportfunktion auch wählen, um einen MA zu sichern und bei Bedarf zurückzuspielen.

Für den Export kann auch das Kommandozeilenprogramm Maexport benutzt werden. Dieses befindet sich im Ordner \BIN des MIIS-Installationsverzeichnis. Hierzu verwenden Sie die folgende Syntax:

```
Maexport Name des MA [Name der Exportdatei]
```

Wird kein Name für die Exportdatei angegeben, wird automatisch der Name des MA mit der Dateiendung xml benutzt.

Beim Export des MA werden nicht die mit dem MA verbundenen Objekte des Connector Space sowie der CS selbst gespeichert. Auch Rules Extensions, Skripte sowie die Custom Data-Einstellungen des Run Profiles werden nicht gespeichert.

Import von Management Agents

Um einen Management Agent zu importieren, wählen Sie das Menü ACTIONS/IMPORT MANAGEMENT AGENT. Dort wählen Sie die zu importierende xml-Datei aus. Beim Import wird ein neuer MA erstellt, d.h., der zu importierende MA darf noch nicht vorhanden sein. Nach dem Import wird ein neuer Connector Space angelegt, sobald der MA das erste Mal gestartet wird. Der importierte MA erhält auch eine neue GUID, sodass die Exportdatei auf mehreren Servern zum Import verwendet werden kann. Soll hingegen der ursprüngliche GUID beibehalten werden, so verwenden Sie die Update-Funktion.

Bei allen call-basierten Management Agents wird das Schema der verbundenen Datenquelle geprüft, und die vorhandenen Partitionen werden aufgelistet. Stimmen dabei die vorhandenen Partitionen mit denen in der xml-Datei aufgeführten in Hinblick auf Name und GUID überein, wird der Importvorgang automatisch fortgesetzt. Werden Abweichungen ermittelt, muss im Fenster PARTITION MATCHING festgelegt werden, wie mit den abweichenden Partitionen verfahren werden soll. Dort werden alle Partitionen aufgelistet, die übereinstimmen. Für diese sind keine weiteren Aktionen erforderlich. Auch die Partitionen, deren Name bei abweichendem GUID übereinstimmt, werden als übereinstimmend vorgeschlagen. Auch hier ist keine weitere Aktion notwendig. Werden für Partitionen keine korrespondierenden Namen und GUIDs gefunden, so muss die Partition manuell ausgewählt werden. Weiterhin ist es auch möglich, bestehende bzw. vorgeschlagene Übereinstimmungen zu löschen sowie Partitionen aus der Auswahl zu entfernen.

Update von Management Agents

Um einen Management Agent upzudaten, wählen Sie das Menü ACTIONS/UPDATE MANAGEMENT AGENT. Dort wählen Sie die xml-Datei aus, mit der Sie das Update durchführen möchten. Updates sind sinnvoll, wenn z.B. ein MA auf einem produktiven System mit den auf einem Textsystem geprüften Änderungen aktualisiert werden soll.

Auch beim Update wird wie beim Import die Korrespondenz der Partitionen geprüft. Dies geschieht nach demselben Mechanismus wie beim Import.

30.3.2 Run Profiles für Management Agents

Jedem Management Agent muss nach der Erstellung mindestens ein Run Profile zugewiesen werden. Run Profiles geben die Reihe der Schritte an, die der MA durchführen soll, z.B. ob es sich um einen Import, Export oder eine Synchronisierung handeln soll. Dieses Run Profile (oder auch mehrere zugewiesene) werden zusammen mit dem MA gespeichert. Um ein Run Profile zu erstellen, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der Registerkarte MANAGEMENT AGENT unter ACTIONS auf den Link CONFIGURE RUN PROFILES, oder wählen Sie das Menü ACTIONS / CONFIGURE RUN PROFILES.
2. Im Fenster CONFIGURE RUN PROFILES (siehe Abbildung 30.13) klicken Sie auf die Schaltfläche NEW PROFILE.

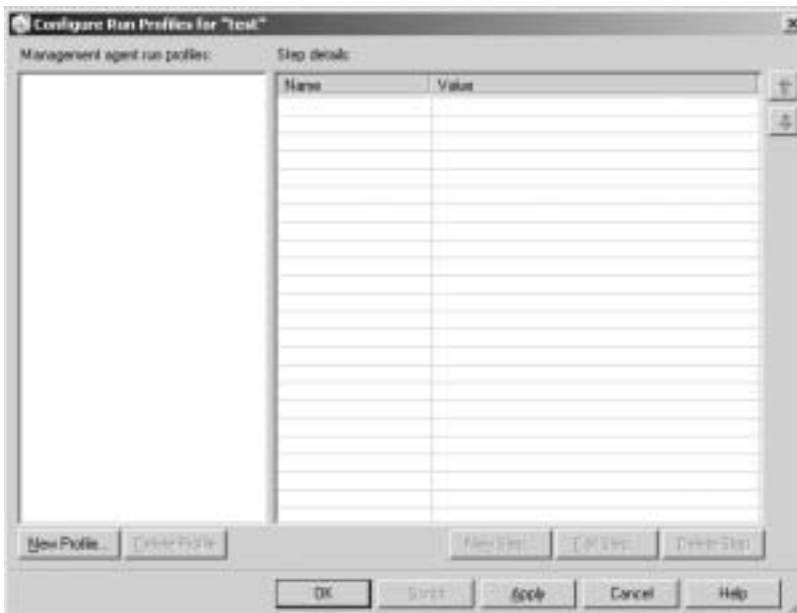


Abbildung 30.13: Erstellen eines neuen Run Profiles

3. Im Fenster CONFIGURE RUN PROFILE (siehe Abbildung 30.14) geben Sie zunächst einen Namen für das Run Profile ein. Klicken Sie dann auf NEXT.

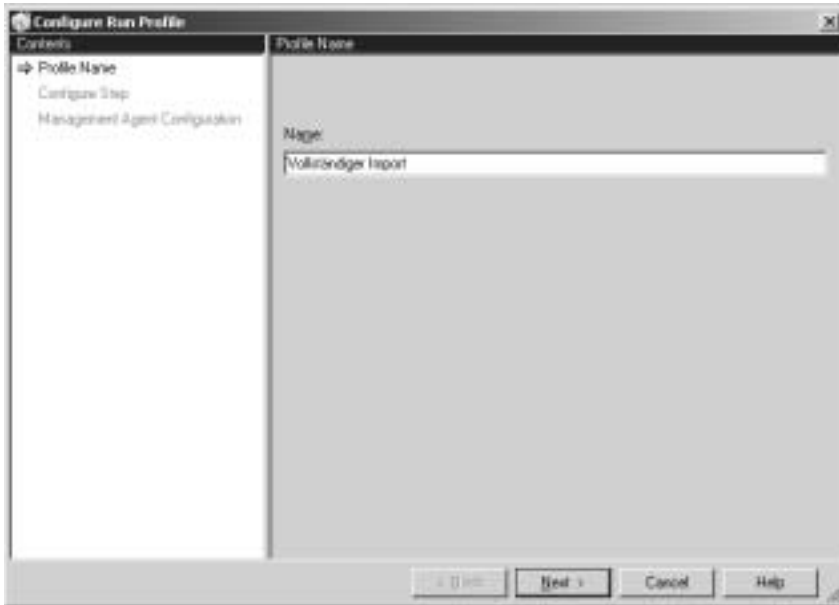


Abbildung 30.14: Name des Run Profiles

4. Als Nächstes müssen Sie die durchzuführende Aktion auswählen (siehe Abbildung 30.15). Hierfür stehen in der Drop-down-Liste SPECIFY STEP TYPE acht Optionen zur Verfügung:
 - ▶ DELTA IMPORT (STAGE ONLY) wird gewählt, um einen Import der Objekte durchzuführen, die in der Datenquelle geändert worden sind. Diese Daten werden lediglich in den Connector Space importiert.
 - ▶ FULL IMPORT (STAGE ONLY) führt einen vollständigen Import aller Objekte und Attribute der Datenquelle durch. Diese Daten werden lediglich in den Connector Space importiert.
 - ▶ DELTA IMPORT AND DELTA SYNCHRONIZATION wird gewählt, um einen Import der Objekte durchzuführen, die in der Datenquelle geändert worden sind. Zusätzlich werden diese Objekte mit den im CS geänderten verglichen und gemäß den Synchronisierungsregeln modifiziert. Die in der Datenquelle geänderten Dateien werden mit denen des MV synchronisiert oder diskonnektiert.
 - ▶ FULL IMPORT AND DELTA SYNCHRONIZATION wird gewählt, um einen Import der Objekte durchzuführen, die in der Datenquelle geändert worden sind. Zusätzlich werden diese Objekte mit den im CS geänderten verglichen und gemäß den Synchronisierungsregeln modifiziert. Die in der Datenquelle geänderten Dateien werden mit denen des MV synchronisiert oder diskonnektiert. Objekte des Connector Space, die nicht mehr in der Datenquelle vorhanden sind, werden markiert. Auf diese werden die Disconnecter Rules angewendet.

- ▶ **FULL IMPORT AND FULL SYNCHRONIZATION** wird gewählt, um einen Import der Objekte durchzuführen, die in der Datenquelle geändert worden sind. Zusätzlich werden diese Objekte mit den im CS geänderten verglichen und gemäß den Synchronisierungsregeln modifiziert. Dabei wird der Schwebezustand / Status außer Acht gelassen. Die in der Datenquelle geänderten Dateien werden mit denen des MV synchronisiert oder diskonnektiert. Objekte des Connector Space, die nicht mehr in der Datenquelle vorhanden sind, werden markiert. Auf diese werden die Disconnecter Rules angewendet. Objekte, die gerade vom Export betroffen sind, werden aus dem CS gelöscht, neu analysiert und abhängig von den Exportregeln neu in den CS geschrieben.
- ▶ **DELTA SYNCHRONIZATION** wird gewählt, um die Synchronisationsregeln an den Objekten und Attributen zu prüfen und anzuwenden, die nach einer Änderung im CS zwischengespeichert werden. Die Objekte und Attribute werden entweder mit dem MV synchronisiert oder diskonnektiert.
- ▶ **FULL SYNCHRONIZATION** wird gewählt, um die Synchronisationsregeln an sämtlichen Objekten und Attributen im CS zu prüfen und anzuwenden. Die Objekte und Attribute werden entweder mit dem MV synchronisiert oder diskonnektiert.
- ▶ **EXPORT** wird benutzt, um die Objekte und Attribute aus dem CS in eine Datenquelle oder eine Exportdatei zu exportieren. Es werden grundsätzlich nur die Objekte und Attribute aus dem CS exportiert, die Änderungen gegenüber den Objekten und Attributen in der Datenquelle aufweisen (Delta-Export).

Im Bereich **THRESHOLD** können Sie die Anzahl der Objekte festlegen, die bei einem Lauf des MA abgearbeitet werden sollen. Ist kein Wert festgelegt, werden alle Objekte abgearbeitet. Klicken Sie dann auf **NEXT**.

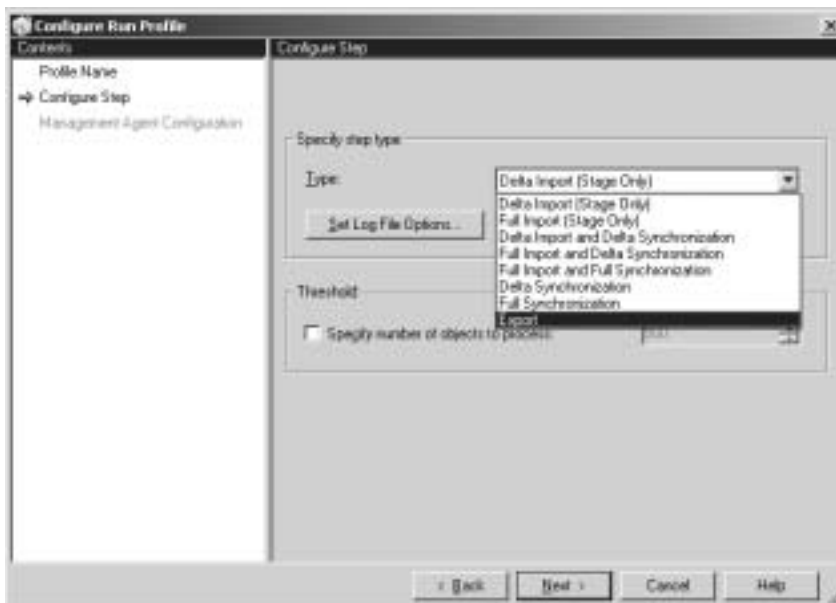


Abbildung 30.15: Auswahl der durchzuführenden MA-Aktion

5. Im Fenster **MANAGEMENT AGENT CONFIGURATION** (siehe Abbildung 30.16) wählen Sie unter **PARTITION** eine Partition aus. Unter **Custom Data** können Sie die Standardwerte für **Batch Size**, **Page Size** sowie den **Timeout** ändern. Sofern während eines MA-Durchlaufs die Verbindung mit der Datenquelle unterbrochen wird, so setzt der MA für den unter **Timeout** angegebenen Zeitraum die Kommunikation fort. Erst nach Ablauf dieses Intervalls reagiert der MA auf den Stopp-Befehl, um den Durchlauf abubrechen. Zum Abschluss klicken Sie auf **FINISH**.

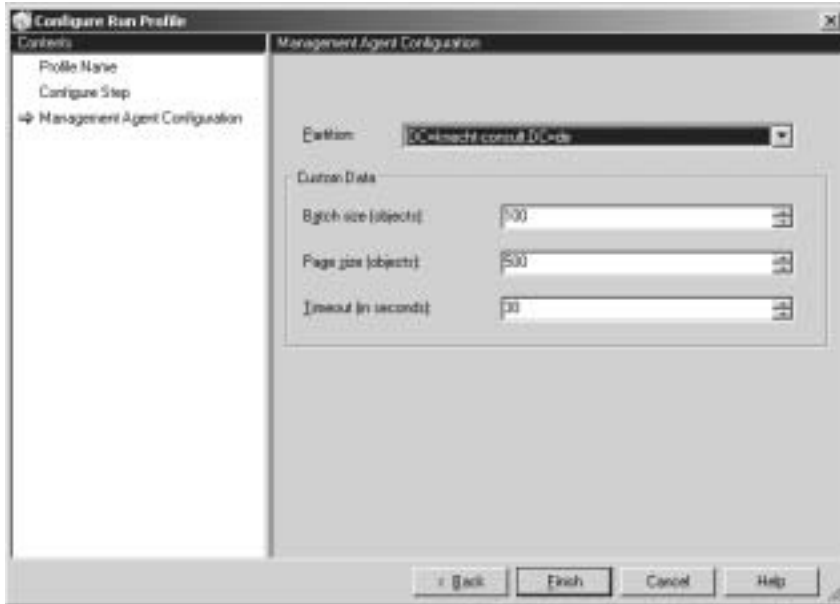


Abbildung 30.16: Abschluss der Run Profile-Konfiguration

Nachdem Sie ein Run Profile konfiguriert haben, können Sie dieses weiter bearbeiten. Klicken Sie dazu auf der Registerkarte **MANAGEMENT AGENTS** auf das Menü **ACTIONS / CONFIGURE RUN PROFILES**. Im Konfigurationsfenster (siehe Abbildung 30.17) sehen Sie links eine Liste der angelegten Run Profiles. Sobald Sie dort ein Run Profile markieren, sehen Sie rechts die einzelnen dem Profile zugewiesenen Schritte. Über die Schaltfläche **NEW STEP** können neue Schritte hinzugefügt werden. Auch das Bearbeiten und Löschen einzelner Schritte ist möglich. Zusätzlich können Sie über **SCRIPT** ein Skript generieren lassen, das sämtliche Schritte des Run Profiles enthält. Das Skript kann entweder als vbs-Datei oder cs-Datei gespeichert werden.

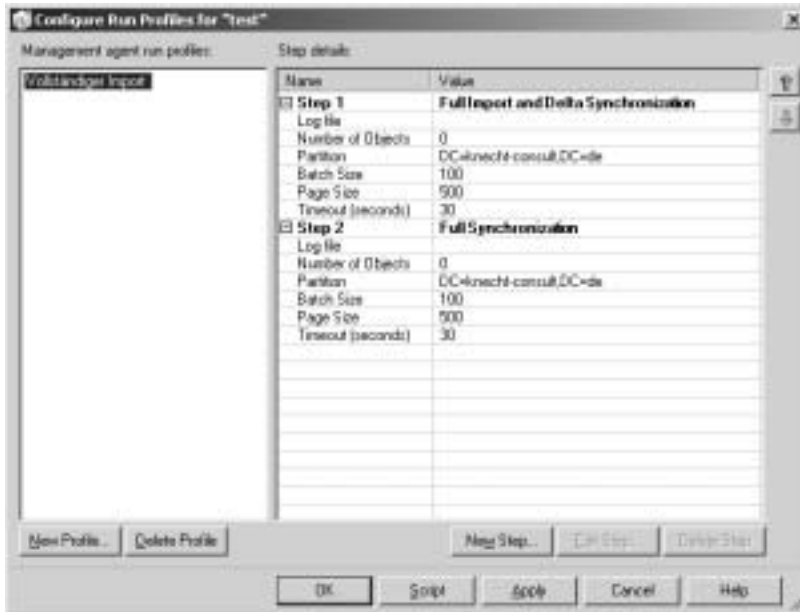


Abbildung 30.17: Bearbeiten eines Run Profiles

30.3.3 Rules Extensions

Rules Extensions (RE) sind programmierbare Erweiterungen, die die Funktion der Management Agents sowie des Metaverse beeinflussen können. Sie können optional erstellt werden, ihr Einsatz ist jedoch nicht zwingend. Diese Erweiterungen werden in einer Programmiersprache wie z.B. Visual Basic .NET oder C# geschrieben. Implementiert sind die Extension Rules in einer Klassenbibliothek des Microsoft .NET Framework oder als DLL. Sämtliche Extension Rules befinden sich im Ordner \EXTENSIONS im Installationsverzeichnis des MIIS 2003.

Rules Extensions werden in zwei Typen unterteilt. Zum einen gibt es REs des Typs Management Agent, zum anderen des Typs Metaverse. Jeder Management Agent und jedes Metaverse darf lediglich über eine Rules Extension verfügen. Rules Extensions vom Type Management Agent werden auf die Daten angewendet, die vom Connector Space ins Metaverse einfließen. Es gibt die folgenden MA Rules Extensions: Attribute Flow Rules, Connector Filter Rules, Deprovisioning Rules, Join Rules und Projection Rules. Metaverse Rules Extension werden auf die Daten angewendet, die vom Metaverse in den Connector Space fließen. Es gibt Object Deletion Rules sowie Provisioning Rules.

Um Rules Extensions zu erstellen, wählen Sie auf der Registerkarte Management Agents das Menü ACTIONS / CREATE RULES EXTENSIONS PROJECT.

30.3.4 Metaverse Designer

Auf der Registerkarte METAVERSE DESIGNER des Identity Managers können Sie neue Objekttypen erstellen oder die Attribute beliebiger Objekttypen, die sich im Metaverse befinden, hinzufügen, löschen und editieren. Die Änderungen, die Sie hier an den Objekten und Attributen vornehmen, werden im Schema des MIIS 2003 gespeichert. Dieses Schema definiert genau wie das Active Directory-Schema Sätze von Objekttypen und Attributen. Ebenso ist in dem Schema des MIIS 2003 festgelegt, welche Datentypen die einzelnen Attribute beschreiben und welche Attribute für ein Objekt erforderlich sind und welche nicht.

Auf der Registerkarte METAVERSE DESIGNER sehen Sie im Bereich OBJECT TYPES eine Auflistung aller Objekttypen wie Personen, Gruppen, Drucker, Domänen usw. (siehe Abbildung 30.18). Wenn Sie dort ein Objekt markieren, werden im Bereich ATTRIBUTES sämtliche Attribute angezeigt, die das Objekt enthalten kann. Über die jeweiligen Links in den Bereichen ACTIONS können Sie die Objekte und Attribute bearbeiten.

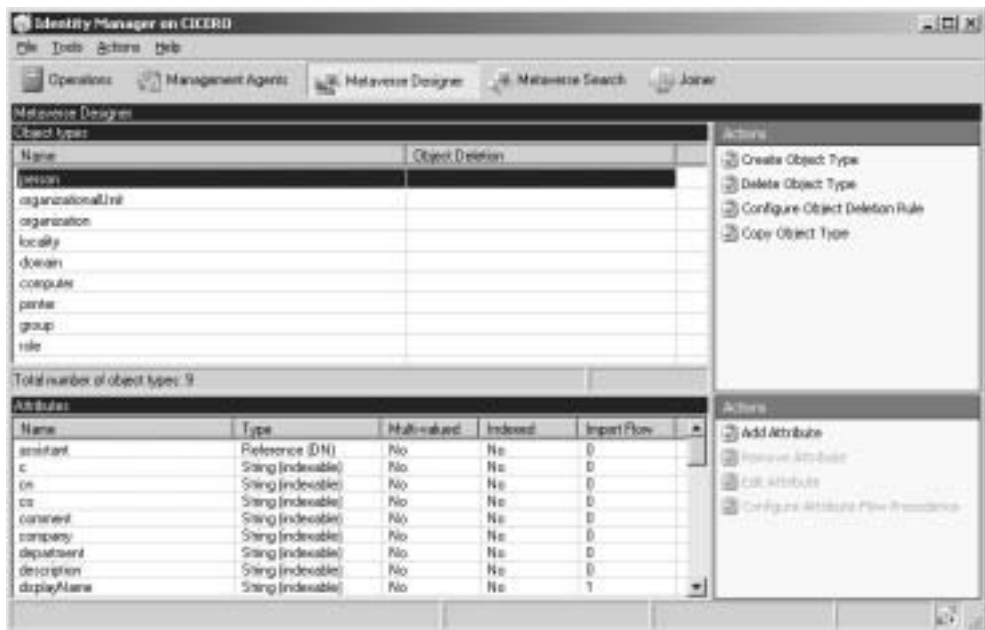


Abbildung 30.18: Der Metaverse Designer

Weiterhin können Sie im Metaverse Designer auch die *Object Deletion Rules* konfigurieren (Menü ACTIONS/CONFIGURE OBJECT DELETION RULES). Diese Regel kann für jedes Objekt im Metaverse festgelegt werden. Sie bestimmt, wann ein Objekt aus dem Metaverse gelöscht wird (siehe Abbildung 30.19). Ein Objekt kann gelöscht werden, wenn das letzte Objekt im Connector Space, das auf dieses Objekt im MV zeigt, entkoppelt ist. Dies ist die Standardeinstellung. Markieren Sie dazu die erste Checkbox. Soll ein Objekt gelöscht werden, sobald das letzte CS-Objekt von einem bestimmten Management Agent entkoppelt wird, so markieren Sie die zweite Checkbox und wählen aus der Drop-down-

Liste den entsprechenden Management Agent aus. Soll der Löschvorgang über Rules Extension geregelt werden, so markieren Sie die dritte Checkbox.

Haben Sie eine der Deletion Rules ausgewählt, so erscheint diese im Metaverse Designer in der Spalte OBJECT DELETION neben dem jeweiligen Objekt.

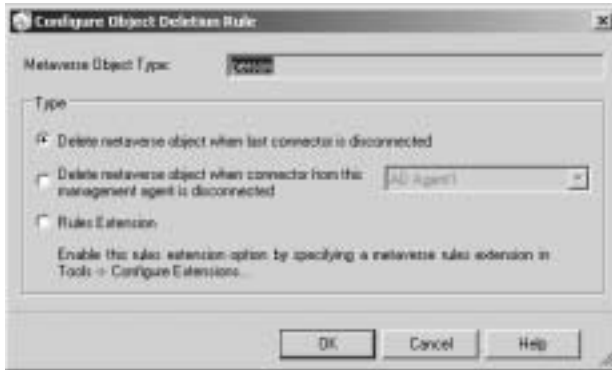


Abbildung 30.19: Konfiguration der Object Deletion Rules

Im Metaverse Designer können Sie für Attribute auch die *Attribute Flow Precedence* konfigurieren. Dies geschieht über den gleichnamigen Eintrag im Menü ACTIONS. Sobald zwei oder mehr Datenquellen ihre Daten in einem Objekt des Metaverse synchronisieren, kann eine der Datenquellen als autorisierend markiert werden. Werte, die aus einer autorisierenden Datenquelle stammen, haben grundsätzlich Vorrang und werden nicht durch einen Wert überschrieben, der aus einer Quelle mit niedrigerer Priorität stammt. Um einer Datenquelle die höchste Priorität zu geben, wählen Sie im Fenster CONFIGURE ATTRIBUTE FLOW PRECEDENCE den Management Agent aus. Markieren Sie diesen, und setzen Sie ihn über die Pfeil-Schaltfläche an die oberste Position. Das Menü kann nur aufgerufen werden, wenn das Attribut in mindestens einem Attribute Flow konfiguriert ist.

Import und Export des MIIS 2003-Schemas

Nachdem an einem MIIS 2003-Server Änderungen am Schema vorgenommen worden sind, kann dieses aktualisierte Schema exportiert und auf jedem anderen MIIS 2003-Server wieder importiert werden. Diese Funktion ist sinnvoll, wenn Sie in einer Testumgebung diverse Änderungen vorgenommen haben und diese Konfiguration nun in der produktiven Umgebung einsetzen möchten. Beim Export werden sämtliche Schemadaten in eine XML-Datei geschrieben.

Um den Export bzw. Import zu starten, wählen Sie das Menü FILE/EXPORT SERVER CONFIGURATION oder FILE/IMPORT SERVER CONFIGURATION. Sie erhalten den Hinweis, dass während des Import- und Exportvorgangs kein Management Agent laufen darf. Bestätigen Sie diesen Hinweis mit OK. Als Zielverzeichnis für den Export muss ein leerer Ordner angegeben werden. Ansonsten kann der Export nicht durchgeführt werden. Während des Exports erhalten Sie ein Fenster mit Statusmeldungen. Wird ein Import durchgeführt, wählen Sie das Quellverzeichnis, in dem sich die XML-Dateien befinden. Sie erhalten ebenfalls Statusmeldungen (siehe Abbildung 30.20).

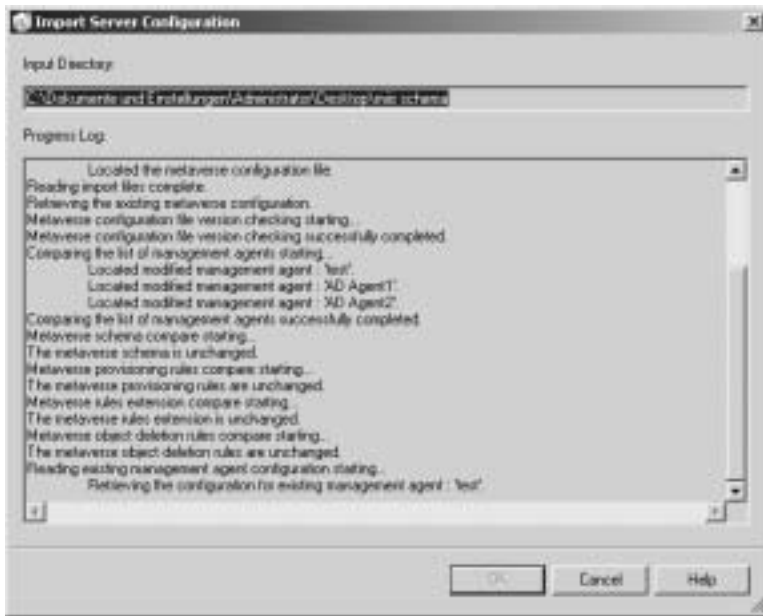


Abbildung 30.20: Die Statusmeldungen während des Imports des MIIS-Schemas

Im Zielverzeichnis sind nach dem Export mehrere XML-Dateien zu finden. Die Datei *mv.xml* enthält die Einstellungen des Metaverse. Zudem wird für jeden Management Agent eine separate XML-Datei erstellt.

Beim Import des Schemas können Sie keine Objekttypen aus dem Metaverse entfernen.

30.3.5 Metaverse Search

Auf der Registerkarte METAVERSE SEARCH (siehe Abbildung 30.21) können Sie nach Objekten im Metaverse suchen. Hierzu müssen Sie eigene Abfragen erstellen. Für ein Objekt können Sie beliebig viele Abfragen erstellen. In der Abfrage müssen ein Attribut, der Operator sowie der Wert angegeben werden.

Um eine neue Abfrage zu erstellen, wählen Sie ACTIONS/ADD CLAUSE. Als Nächstes wählen Sie aus der Listbox SCOPE BY OBJECT TYPE das gewünschte Objekt aus. So werden unter ATTRIBUTES nur die Attribute angezeigt, über die das Objekt verfügen kann. Aus der Listbox COLLATION wählen Sie eine Sprache aus, nach der die Reihenfolge der Suchergebnisse sortiert werden soll. Wählen Sie danach aus der Listbox ATTRIBUTE das gewünschte Attribut aus. Aus der Listbox OPERATOR fügen Sie einen Operator hinzu. Die zur Verfügung stehenden Operatoren sind abhängig von der Wahl des Attributs. Schließlich legen Sie unter VALUE den Wert fest, der dem Operator zugewiesen wird.

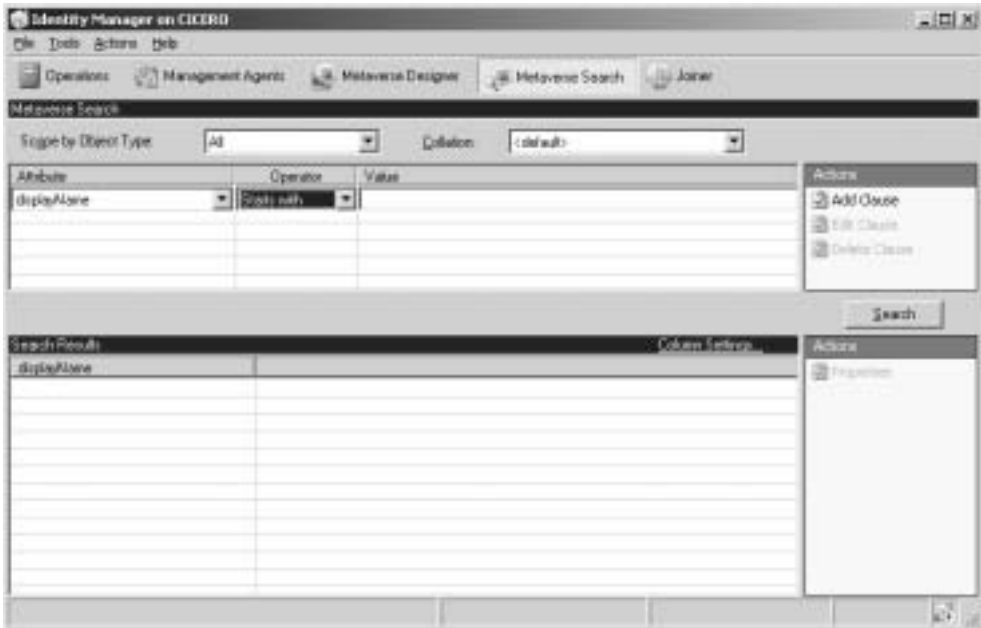


Abbildung 30.21: Die Registerkarte Metaverse Search

Sobald Sie eine Abfrage erstellt haben, klicken Sie auf die Schaltfläche **SEARCH**, um die Suche zu starten. Die Suchergebnisse werden im Bereich **SEARCH RESULTS** angezeigt.

Wollen Sie später eine Abfrage modifizieren oder löschen, so markieren Sie die Abfrage im Bereich **METVERSE SEARCH** und wählen **ACTIONS/EDIT CLAUSE** bzw. **ACTIONS/DELETE CLAUSE**.

30.3.6 Joiner

Auf der Registerkarte **JOINER** können Sie Disconnecter-Objekte für bestimmte Management Agents suchen und anzeigen lassen (siehe Abbildung 30.22). Joiner werden benutzt, um die Disconnecter-Objekte zu modifizieren. Um eine Suche zu starten, wählen Sie im Bereich **JOINER** den Management Agent und aus der Listbox **DISCONNECTOR TYPE** den Typ des Disconnectors. Sie können entweder nach sämtlichen Disconnecter-Typen suchen oder lediglich nach bestimmten Typen. Klicken Sie dann auf die Schaltfläche **SEARCH**. Das Suchergebnis wird im Bereich **DISCONNECTORS** angezeigt.

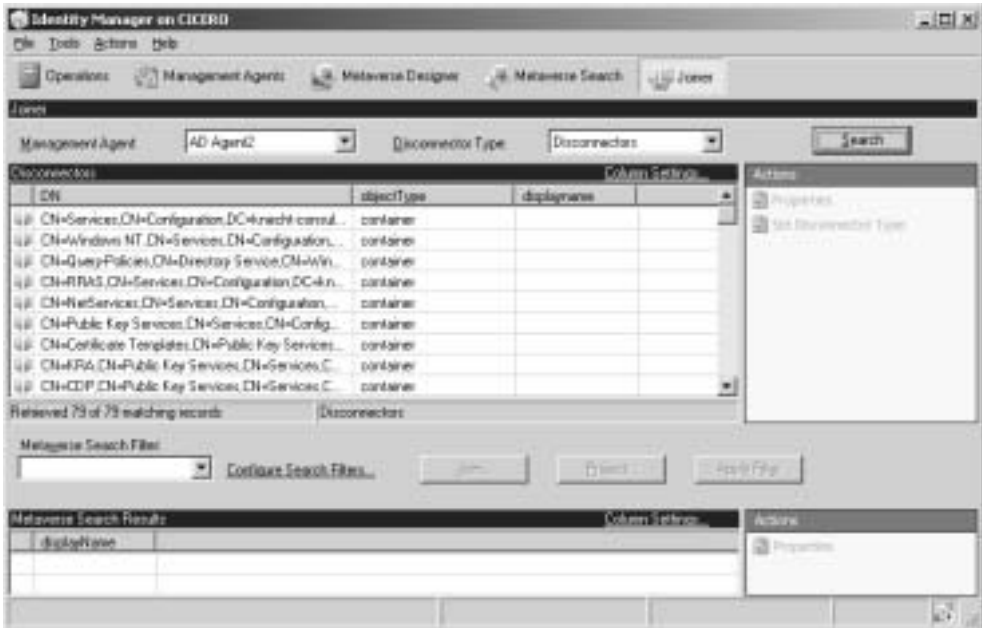


Abbildung 30.22: Die Registerkarte Joiner

Hier haben Sie die Möglichkeit, den Typ des Disconnecter-Objekts zu ändern. Hierzu wählen Sie ACTIONS/SET DISCONNECTOR TYPE. Wird ein Disconnecter-Typ als explizit festgelegt, werden keine Regeln der Management Agents mehr auf das Objekt angewendet. Es bleibt ein expliziter Disconnecter (siehe Abbildung 30.23).



Abbildung 30.23: Den Status eines Disconnectors ändern

Alle aufgelisteten Objekte können über die Schaltflächen JOIN und PROJECT auch manuell verbunden werden. Angenommen, während eines Imports wurde versucht, ein Objekt zu verbinden, aber im Metaverse wurde mehr als ein Objekt gefunden, das die Join-Kriterien erfüllt. Sie können nun nach den Disconnectoren suchen und in der Ergebnisliste das Disconnecter-Objekt auswählen. Konfigurieren Sie dann über den Link CONFIGURE SEARCH FILTERS einen Metaverse-Suchfilter, um die passenden Objekte aus dem Metaverse zu finden. Das Disconnecter-Objekt kann dann mit dem ausgewählten Metaverse-Objekt verbunden werden.

31 Active Directory und Firewalls

Dieses Kapitel beschäftigt sich mit der Konfiguration von Firewalls in einer verteilten Active Directory-Umgebung. In Unternehmen mit mehreren Standorten ist es wahrscheinlich, dass einzelne oder alle Standorte hinter einer Firewall liegen. Dennoch darf durch die Firewall die ordnungsgemäße Funktion des Active Directory nicht behindert werden, wobei gleichzeitig darauf zu achten ist, dass keine Sicherheitslücken entstehen. Als Grundlage erhalten Sie zunächst eine Übersicht über sämtliche Ports, die von Domänencontrollern im Active Directory benutzt werden. Anschließend erhalten Sie Hinweise zur Firewall-Konfiguration für die RPCs (Remote Procedure Calls), die für den Replikationsverkehr sowie beim Hinzufügen neuer Domänencontroller zu einer Domäne benutzt werden.

31.1 Portbelegung eines Domänencontrollers im Active Directory

In diesem Kapitel erfolgt eine Auflistung sämtlicher Ports, die von bestimmten Protokollen und Diensten auf einem Domänencontroller im Active Directory benutzt werden. Hierbei handelt es sich um eine bloße Auflistung, die Hinweise zur Konfiguration einer Firewall finden Sie in den folgenden Kapiteln.

Port	Protokoll	Dienst	Beschreibung
21	TCP	FTP	Das FTP (File Transfer Protocol) wird zum Datenaustausch sowie zur Remote-Speicherung von Daten benutzt. Der FTP-Server ist Bestandteil von IIS (Internet Information Services).
25	TCP	SMTP	Der SMTP-(Simple Mail Transfer Protocol-)Dienst ist für das Versenden von E-Mails zuständig.
53	TCP	DNS	Der DNS-(Domain Name Service-)Dienst ist für die Namensauflösung im Active Directory zuständig.
80	TCP	HTTP	HTTP (Hypertext Transfer Protocol) definiert die Regeln für den Datenaustausch im Internet.
88	UDP	Kerberos	Kerberos ist eine Authentifizierungsmethode, siehe Kapitel 2.2.3. Der KDC (Key Distribution Center) benutzt den Port für Ticketanfragen.
119	TCP	NNTP	Das NNTP (Network News Transfer Protocol) wird für den Nachrichtenaustausch in den Usenet Newsgroups verwendet.

Port	Protokoll	Dienst	Beschreibung
123	UDP	NTP	Das Network Time Protocol wird vom Windows-Zeitdienst verwendet.
135	TCP	RPC Port Mapper	Per RPC (Remote Procedure Call) kann der Client in einem beliebigen TCP/IP-Netzwerk auf einem Server bestimmte Dienste aufrufen.
137	UDP	NetBIOS Name Server	Das NetBIOS Name Server-(NBNS-)Protokoll ist Bestandteil der NetBIOS über TCP/IP-(NetBT-)Protokolle. Es ist im NetBIOS-Netzwerk für die Zuordnung von Hostnamen und Adressen zuständig.
138	UDP	NetBIOS Datagramm	Wird im NetBIOS-Netzwerk für Netzwerk browsing und Netzwerkanmeldung benutzt.
139	UDP	NetBIOS Session Services	Wird im NetBIOS-Netzwerk für SMB-(Server Message Block-)Dienste, Drucken und Dateifreigaben benutzt.
389	UDP	LDAP	Standardport für das Lightweight Directory Access Protocol (LDAP), das Active Directory-Zugriffsprotokoll.
443	TCP	HTTPS	Das Secure HTTP-Protokoll wird für SSL-gesicherte HTTP-Transaktionen benutzt.
445	TCP	SMB	Das SMB-(Server Message Block-)Protokoll wird für Dateifreigaben benutzt.
464	TCP	Kerberos V5	Das Kerberos Change Password Protocol wird benutzt, um einem Administrator das Setzen von Passwörtern für neue Benutzer zu untersagen, damit nur die Benutzer selbst das Passwort ändern können.
500	TCP	ISAKMP	Das Internet Security Association and Key Management Protocol ist für den Austausch von Schlüsseln und die Herstellung der IPSec-Verbindung im VPN zuständig.
563	TCP	SNEWS	Hierbei handelt es sich um die gesicherte Variante von NNTP.
593	TCP	RPC over HTTP	Ermöglicht Remote Procedure Calls via HTTP für COM + Internet-Dienste. Dazu muss der IIS installiert sein.
636	TCP	LDAP over SSL	Die LDAP-Daten werden verschlüsselt übertragen, wenn SSL (Secure Socket Layer) aktiviert ist.
1067	TCP	IBS	Wird vom Installation Bootstrap Protocol-Server verwendet.
1068	TCP	IBS	Wird vom Installation Bootstrap Protocol-Client verwendet.
1645	UDP	IAS	Wird vom IAS (Internet Authentication Service) benutzt, um RADIUS-Authentifizierungen älterer RADIUS-Server verarbeiten zu können.
1646	UDP	IAS	Wird vom IAS benutzt, um RADIUS Account-Messages älterer RADIUS-Server verarbeiten zu können.

Port	Protokoll	Dienst	Beschreibung
1701	UDP	L2TP	L2TP (Layer 2 Tunneling Protocol) kapselt das PPP (Point-to-Point Protocol).
1723	UDP	PPTP	Das Point-to-Point Tunneling Protocol wird von zahlreichen VPN-Produkten benutzt.
1812	UDP	IAS	Dient zur Verarbeitung von RADIUS-Authentifizierungsmeldungen.
1813	UDP	IAS	Dient zur Verarbeitung von RADIUS-Authentifizierungsmeldungen.
3268	TCP	GC	Dieser Port wird von den globalen Katalog-Servern des Active Directory benutzt.
3269	TCP	GC mit LDAP/SSL	SSL-Verbindungen zum globalen Katalog benutzen diesen Port.
3389	TCP	RDP	Das Remote Desktop Protocol wird von einem Thin-Client für die Kommunikation mit einem Terminal-Server verwendet.

Tabelle 31.1: Die Portbelegung eines Domänencontrollers im Active Directory

Ist der Domänencontroller zusätzlich für WINS konfiguriert, so werden auch die Ports 42 TCP / UDP für die WINS-Replikation und Port 1512 TCP / UDP für die WINS-Auflösung benutzt.

31.1.1 Tools zur Portüberwachung

Um herauszufinden, welche Ports aktuell von einem Domänencontroller benutzt werden, gibt es eine Reihe von Tools, z.T. auch als Freeware, die Ihnen diese Informationen liefern. Weitere Tools finden sie über Free- und Shareware-Sammlungen oder über Internet-Suchmaschinen.

Sehr gut geeignet ist das Kommandozeilenprogramm Fport der Firma Foundstone. Dieses Programm listet alle benutzten Ports auf und sortiert das Ergebnis wahlweise nach benutzten Ports, der PID, der Applikation, die diesen Port benutzt, und dem Pfad zu dieser Applikation. Dieses Tool kann kostenlos von der Website http://www.foundstone.com/knowledge/intrusion_detection.html heruntergeladen werden.

Ein weiteres gutes Programm ist das Freeware-Tool ActivePorts der Firma Smartline. Dieses Programm bietet Ihnen eine Liste aller aktuell benutzten Ports. Die Anzeige wird dabei nahezu in Echtzeit aktualisiert. Sie finden Informationen zum lokalen Port und Remote-Port, zur lokalen IP-Adresse und Remote IP-Adresse, PID, Prozess, der den Port benutzt, sowie den Pfad zur Executable dieses Prozesses, das verwendete Protokoll (TCP und UDP) und den Status. Das Programm kann unter folgender Adresse heruntergeladen werden: <http://www.protect-me.com/freeware.html>.

31.2 Die Konfiguration von Firewalls für RPC-Aufrufe

Dieses Kapitel beschäftigt sich mit RPCs und deren sicherer Konfiguration im Zusammenhang mit Firewalls. RPCs werden im Active Directory aufseiten der Domänencontroller bei der Replikation benutzt sowie beim Hinzufügen neuer Domänencontroller zu einer bestehenden Domäne.

Zunächst erhalten Sie jedoch einen kurzen Überblick über die standardmäßige Arbeitsweise der RPCs für die Active Directory-Replikation, bei der die Ports dynamisch zugewiesen werden, damit Sie erkennen, warum die Konfiguration kompliziert werden kann. Dasselbe gilt auch für Exchange. Der RPC-Dienst konfiguriert sich im Wesentlichen selbst über die Registry. Hierzu verwendet der Dienst UUIDs (Universally Unique Identifiers), die mit den GUIDs vergleichbar sind. Wird ein RPC-Aufruf gestartet, so erhält er einen zufällig zugewiesenen freien Port aus dem Bereich 1024 bis 65536 zugewiesen, den er mit seiner UUID registriert. Einige Dienste versuchen auch immer, denselben Port zu benutzen, sofern dieser nicht belegt ist. Damit nun der Client weiß, welcher Port einem bestimmten Dienst zugewiesen wurde, stellt er eine Anfrage an den Server auf Port 135. Dieser teilt dem Client den Port sowie die registrierte UUID mit und schließt die Verbindung wieder. Nachdem der Client diese Informationen erhalten hat, stellt er eine neue Verbindung zum Server her, wobei er den Port benutzt, der ihm eben vom Server mitgeteilt wurde. Da im Vorfeld nicht absehbar ist, welcher Port benutzt wird, müsste eine Firewall alle Ports zwischen 1024 und 65535 offen lassen. Da dies aber nicht im Sinne des Erfinders sein kann, müssen Sie die benutzbaren Ports einschränken. Hierzu stehen Ihnen zwei Möglichkeiten zur Verfügung. Die erste Möglichkeit besteht darin, den Gebrauch von Ports für die RPCs zu beschränken und lediglich diese freizuschalten. Eine andere Alternative ist es, für den gesamten Replikationsverkehr zwischen den Domänencontrollern IPSec zu verwenden und die Firewall lediglich dafür zu öffnen. Diese beiden Konfigurationsmethoden werden in den folgenden Kapiteln vorgestellt. Der Vollständigkeit halber – oder auch als abschreckendes Beispiel – wird Ihnen zum Schluss gezeigt, wie die Firewall aussehen würde, wenn Sie die dynamische Portzuweisung zulassen.

31.2.1 Einschränken der dynamisch zugewiesenen RPC-Ports

Eine Möglichkeit, um zu verhindern, dass die RPC-Ports dynamisch zugewiesen werden, besteht darin, die RPC-Aufrufe auf einen bestimmten Port zu beschränken. Hierzu müssen jedoch an sämtlichen Domänencontrollern im Active Directory Änderungen an der Registry durchgeführt werden.

1. Zunächst einmal müssen Sie entscheiden, welchen Port Sie für die RPC-Aufrufe spezifizieren möchten. Am besten benutzen Sie einen Port aus dem Bereich zwischen 49152 und 65535. Dieser Bereich wurde von der IANA (Internet Assigned Numbers Authority) für spezielle Zuweisungen reserviert. Nachdem Sie sich für einen Port entschieden haben, müssen Sie diesen Port in die Registry sämtlicher Domänencontroller eintragen.
2. Öffnen Sie hierzu in der Registry den Schlüssel `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\`. Dort fügen Sie einen neuen DWORD-Wert mit dem Namen `TCP/IP Port` ein. Tragen Sie hier die gewünschte Port-

nummer ein. In diesem Fall wird auch zunächst wieder eine Anfrage an den Server über den Port 135 gestellt. Da nun aber lediglich ein Port für die RPCs zugewiesen wurde, wird grundsätzlich dieser Port als Antwort geliefert.

Die Firewall muss in diesem Fall so konfiguriert werden, dass die folgenden Ports freigeschaltet sind: (Die Zuordnung der einzelnen Ports entnehmen Sie Tabelle 31.1.)

- ▶ 53 TCP/UDP
- ▶ 88 TCP/UDP
- ▶ 123 UDP
- ▶ 135 TCP/UDP
- ▶ 137 TCP/UDP
- ▶ 138 UDP
- ▶ 139 TCP
- ▶ 389 TCP
- ▶ 445 TCP/UDP
- ▶ 636 TCP
- ▶ 3268 TCP
- ▶ 3269 TCP
- ▶ der für den RPC-Verkehr festgelegte Port

Ist zusätzlich noch eine WINS-Auflösung erforderlich, so muss Port 1512 TCP/UDP freigeschaltet werden, für die WINS-Replikation Port 42 TCP/UDP.

Um generell nur einen bestimmten Bereich für dynamisch zugewiesene Ports in der Firewall für RPC-Aufrufe zu reservieren, muss ebenfalls die Registry angepasst werden. Damit werden auch andere Dienste, die dynamisch die RPC-Ports zuweisen, wie DHCP oder WINS auf einen Bereich von erlaubten Ports reduziert.

Die Änderungen werden alle in dem Schlüssel `HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc\` vorgenommen. Fügen Sie dort als Erstes den Schlüssel `Internet` hinzu. Dort fügen Sie die folgenden Werte ein (siehe Tabelle 31.2):

Name	Typ	Beschreibung
Ports	REG_MULTI_SZ	Gibt den Bereich der Ports an, der entweder vom Internet aus zugänglich sein soll oder nicht. Sie sollten nicht mehr als 20 Ports wählen, diese sollten in einem Bereich über 5000 liegen.
PortsInternet- Available	REG_SZ	Wird hier der Wert Y gesetzt, sind die unter <code>Ports</code> aufgeführten Ports vom Internet aus erreichbar, ist der Wert auf N gesetzt, sind sie nicht erreichbar.
UseInternet- Ports	REG_SZ	Mit Y werden den Diensten nur die vom Internet aus erreichbaren Ports zugewiesen, mit N nur die für das Intranet zugänglichen.

Tabelle 31.2: Registry-Änderungen für RPC-Ports

3. Starten Sie den Server danach neu, damit die Änderungen wirksam werden.

31.2.2 RPC-Aufrufe über IPSec

Die zweite Methode zur Absicherung der RPC-Aufrufe besteht darin, den RPC-Verkehr über IPSec einzukapseln und lediglich diesen über die Firewall laufen zu lassen. Auch für dieses Verfahren müssen Sie auf jedem Domänencontroller Anpassungen vornehmen, die weit umfangreicher sind als die eben beschriebene Anpassung der Registry. Allerdings wird auf der anderen Seite auch die Sicherheit zwischen den Domänencontrollern erhöht, wenn Sie IPSec in Verbindung mit Zertifikaten oder Kerberos verwenden, da somit die Identifizierung der Kommunikationspartner vor dem eigentlichen Datenaustausch stattfindet.

Bevor Sie mit der Implementierung von IPSec beginnen, entscheiden Sie, ob Sie für die Authentifizierung Kerberos oder Zertifikate benutzen möchten. Kerberos können Sie nur verwenden, wenn sich die Domänencontroller entweder in derselben Domäne oder in zwei Domänen befinden, die über Vertrauensstellungen miteinander verbunden sind. Sie sehen also, dass Sie die Kerberos-Authentifizierung nicht verwenden können, wenn Sie einen Domänencontroller zu einer Domäne hinzufügen möchten. Um diesen Vorgang abzusichern, können Sie PPTP (Point-to-Point Tunneling Protocol) benutzen. Entscheiden Sie sich für den Einsatz von Zertifikaten, so müssen Sie die Domäne entsprechend vorbereiten. Die Beschreibung dieser Prozeduren würde jedoch den Rahmen dieses Buches sprengen. Hinweise zum Erstellen von Zertifikaten finden Sie in der Windows Server-Hilfe.

Hier wird zunächst allgemein die IPSec-Konfiguration für die Kommunikation der Domänencontroller untereinander für Replikationszwecke vorgestellt. Danach erfahren Sie, wie Sie eine PPTP-Verbindung herstellen, um einen neuen Domänencontroller zu einer Domäne hinzuzufügen.

Konfiguration von IPSec für die Domänencontroller-Replikation

Im Folgenden wird die IPSec-Konfiguration beschrieben, die für die Domänencontroller-Kommunikation bei der Replikation angewendet werden soll. Mit dieser Methode werden lediglich IPSec-Verbindungen über die Firewall geschickt und keine RPCs. Hierzu muss auf jedem Domänencontroller eine IPSec-Sicherheitsrichtlinie für die Replikation erstellt werden mit zugehöriger IP-Filter-Liste und Filtern.

1. Um die Sicherheitsrichtlinie zu erstellen, wählen Sie STARTMENÜ/PROGRAMME/VERWALTUNG/LOKALE SICHERHEITSRICHTLINIE. Dort sehen Sie in der mmc den Knoten IP-SICHERHEITSRICHTLINIEN FÜR LOKALEN COMPUTER. Bevor Sie mit dem Erstellen der Sicherheitsrichtlinie beginnen, müssen Sie zunächst die IP-Filter-Liste erstellen und die Filter konfigurieren. Hier wird festgelegt, von welchen IP-Adressen, Ports und Protokollen aus IPSec verwendet werden soll. Für jeden Domänencontroller wird ein eigener Filter erstellt. Alle diese Filter befinden sich gemeinsam in der Filterliste. Zum Erstellen einer Liste klicken Sie in den Detailbereich der mmc und wählen aus dem Kontextmenü IP-FILTERLISTEN UND FILTERAKTION VERWALTEN (siehe Abbildung 31.1).



Abbildung 31.1: IP-Filterlisten

2. Über HINZUFÜGEN wird eine neue Filterliste erstellt. Nennen Sie diese z.B. Replikation. Sobald Sie erneut auf HINZUFÜGEN geklickt haben, erscheint ein Wizard, der Sie beim Erstellen eines Filters begleitet. Hier geben Sie der Reihe nach die folgenden Informationen an: den Namen des Filters, die IP-Adresse, die die Quelle des IP-Verkehrs darstellt (Auswahl EIGENE ADRESSE), die Ziel-IP-Adresse des anderen Domänencontrollers und den Protokolltyp (BELIEBIG). Klicken Sie dann auf FERTIG STELLEN. Dieser Filter sorgt nun dafür, dass der gesamte Verkehr zwischen den beiden Computern über IPsec gesichert wird.
3. Erstellen Sie jetzt weitere Filter für die übrigen Domänencontroller, mit denen der Quellserver kommunizieren soll. Danach müssen die Filteraktionen konfiguriert werden. Wählen Sie dazu die Registerkarte FILTERAKTIONEN VERWALTEN aus. Über HINZUFÜGEN werden neue Aktionen erstellt. Dieser Prozess läuft auch wizard-gesteuert ab. Geben Sie dazu nacheinander die folgenden Informationen an: Name der Filteraktion, z.B. DC-Replikation, Verhalten der Filteraktion (Sicherheit aushandeln), Keine Kommunikation mit Computern zulassen, die IPsec nicht unterstützen und Sicherheitslevel des IP-Verkehrs (Verschlüsselung und Integrität). Bevor Sie auf FERTIG STELLEN klicken, markieren Sie noch die Checkbox EIGENSCHAFTEN BEARBEITEN. Sie können dann die Eigenschaften der Filteraktion bearbeiten (siehe Abbildung 31.2).
4. Entfernen Sie dort das Häkchen aus der Checkbox UNSICHERE KOMMUNIKATION MIT COMPUTERN ZULASSEN, DIE IPSEC NICHT UNTERSTÜTZEN. Damit verhindern Sie, dass der Domänencontroller auf ungesicherte Verbindungen antwortet. Schließen Sie danach alle geöffneten Dialogfelder. Nun wird die neue IP-Sicherheitsrichtlinie erstellt.



Abbildung 31.2: Eigenschaften der Filter-Aktion

5. Klicken Sie in den Detailbereich der mmc und wählen aus dem Kontextmenü IP-SICHERHEITSRICHTLINIE ERSTELLEN. Auch bei diesem Vorgang werden Sie wieder von einem Wizard begleitet. Geben Sie hier nacheinander die folgenden Informationen an: Den Namen der Sicherheitsrichtlinie (DC-Replikation), deaktivieren Sie die Checkbox DIE STANDARDANTWORTREGEL AKTIVIEREN und aktivieren dann die Checkbox EIGENSCHAFTEN BEARBEITEN. Klicken Sie dann auf FERTIG STELLEN. In dem dann folgenden Fenster (siehe Abbildung 31.3) müssen für die Richtlinie IP-Sicherheitsregeln erstellt werden.



Abbildung 31.3: Hinzufügen von Regeln zur Sicherheitsrichtlinie

6. Klicken Sie auf HINZUFÜGEN und geben in dem Wizard nacheinander die folgenden Informationen ein: Markieren Sie die Checkbox DIESE REGEL SPEZIFIZIERT KEINEN TUNNEL, Netzwerktyp LAN, aus den Filterlisten wählen Sie die eben erstellte Liste, bei den Filteraktionen die eben erstellte Aktion aus, als Authentifizierungsmethode wählen Sie WINDOWS 2000 STANDARD (KERBEROS) oder ZERTIFIKATE und deaktivieren die Checkbox EIGENSCHAFTEN BEARBEITEN. Klicken Sie auf FERTIG STELLEN und schließen alle Fenster.
7. Sie sehen die neu erstellte Richtlinie nun im Detailbereich der mmc. Damit diese Richtlinie wirksam wird, wählen Sie aus ihrem Kontextmenü ZUWEISEN. Die Zuweisung erfolgt sofort ohne Neustart des Domänencontrollers.
8. Auf dieselbe Art und Weise erstellen Sie nun für sämtliche Domänencontroller die IP-Sicherheitsrichtlinie, sodass die komplette Kommunikation über IPSec laufen kann. Dabei ist es gleichgültig, ob sich die Domänencontroller im internen oder externen Netzwerk oder in der DMZ befinden.

Alternativ zu der eben beschriebenen Konfiguration über die GUI können Sie auch das Kommandozeilenprogramm *IPSecPol.exe* aus dem Resource Kit benutzen. Hinweise zur Benutzung dieses Programms finden Sie in der Online-Hilfe des Resource Kits sowie über den Programmaufruf mit dem Parameter `/?`.

Bei der Verwendung von IPSec für den Replikationsverkehr sollten in einer Firewall die folgenden Ports freigeschaltet sein:

1. 50, IP: ESP= IPSec encapsulated security payload
2. 51, IP: AH= IPSec authenticated header
3. 53 TCP/UDP: DNS
4. 88 TCP/UDP: Kerberos
5. 500 UDP: IKE= Internet Key Exchange

Diese Ports sollten auch für den gesicherten DCPROMO-Prozess freigeschaltet sein. Verwenden Sie die PPTP-Verbindung für DCPROMO, so müssen zusätzlich noch die beiden folgenden Ports freigeschaltet werden:

1. 47 IP: GRE (Generic Routing Encapsulation), wenn PPTP verwendet wird
2. 1723 TCP: Herstellung einer PPTP-Verbindung



IPSec arbeitet nicht mit NAT (Network Address Translation) zusammen, da IPSec zur Erstellung der Paketchecksummen die IP-Adressen benutzt. Wurde nun eine Quelladresse durch NAT geändert, werden die Pakete vom Zielcomputer als ungültig betrachtet, und die Kommunikation schlägt fehl.

Neben der Absicherung des Replikationsverkehrs zwischen den Domänencontrollern sollte auch der Promote-Prozess eines Domänencontrollers gesichert werden. Hierzu können Sie entweder PPTP-Tunnel oder IPSec und Zertifikate verwenden. Die Benutzung von Kerberos scheidet aus, da sich zum Zeitpunkt des Promotes der neue Domänencontroller noch nicht in derselben Domäne befindet wie die übrigen DCs.

DCPROMO über PPTP

Zur Herstellung einer PPTP-Verbindung für den Promote-Prozess müssen Sie die Routing- und RAS-Komponenten (RRAS) konfigurieren. Idealerweise befindet sich der RRAS-Server in demselben Subnetz wie der Domänencontroller, ansonsten müssen statische Routen konfiguriert werden.

1. Zur Konfiguration öffnen Sie VERWALTUNG / ROUTING UND RAS. Wählen Sie aus dem Kontextmenü des Servers RRAS KONFIGURIEREN UND AKTIVIEREN. Es wird ein Wizard gestartet. Wählen Sie hier die Option BENUTZERDEFINIERTER KONFIGURATION und treffen die gewünschte Entscheidung bei der Wahl der Verbindung. Beenden Sie den Wizard und starten den Dienst.
2. Wählen Sie nun aus dem Kontextmenü des Servers EIGENSCHAFTEN und wählen die Registerkarte IP. Markieren Sie dort die Checkbox STATISCHER ADRESSPOOL. Über HINZUFÜGEN geben Sie nun einen Adressbereich von ca. zehn Adressen im selben Subnetz wie der Domänencontroller an, z.B. 172.20.20.170 bis 172.20.20.179. Übernehmen Sie diese Einstellungen und schließen das Fenster.
3. Wählen Sie nun links aus dem Knoten PORTS die Eigenschaften. Klicken Sie auf KONFIGURIEREN, um allen Geräten bis auf WAN-Miniport (PPTP) Routing und RAS-Verbindungen zu untersagen. Die Konfiguration sollte folgendermaßen aussehen (siehe Abbildung 31.4):



Abbildung 31.4: Die Konfiguration des RRAS-Ports

Damit ist die Konfiguration abgeschlossen. Um nun einen Server, der sich im externen Netzwerk oder in der DMZ befindet, zum Domänencontroller zu promoten, stellen Sie einen PPTP-Tunnel zum RRAS-Server des internen Netzwerks her. Gehen Sie dazu folgendermaßen vor:

1. Rufen Sie den Assistenten für eine neue Netzwerkverbindung auf. In dem Wizard wählen Sie VERBINDUNG MIT EINEM PRIVATEN NETZWERK ÜBER DAS INTERNET HERSTELLEN.
2. Aktivieren Sie die Checkbox KEINE ANFANGSVERBINDUNG AUTOMATISCH WÄHLEN. Geben Sie dann die IP-Adresse des internen RRAS-Servers an. Diese Verbindung soll allen Benutzern zur Verfügung stehen. Zum Schluss geben Sie der Verbindung noch einen Namen.
3. Dann erscheint das Fenster VERBINDUNG HERSTELLEN. Klicken Sie hier auf EIGENSCHAFTEN und markieren auf der Registerkarte OPTIONEN die Checkbox WINDOWS-ANMELDEDOMÄNE EINBEZIEHEN. Geben Sie nun das Benutzerkonto des Domänenadministrators an. Nachdem die Verbindung hergestellt ist, können Sie mit DCPROMO beginnen. Die PPTP-Verbindung wird automatisch beim Neustart des Domänencontrollers getrennt. Ab diesem Zeitpunkt ist sie auch nicht länger notwendig.

Sie müssen nun die oben beschriebene IPSec-Konfiguration auf den Domänencontrollern einrichten, damit diese gesicherte Verbindungen für den Replikationsverkehr benutzen.

DCPROMO über IPSec und Zertifikate

Um diese Methode zu verwenden, stellen Sie sicher, dass die Domäne für den Einsatz von Zertifikaten vorbereitet ist. Dazu müssen auf sämtlichen Domänencontrollern Zertifikate installiert sein, die alle Signaturen von derselben autorisierenden Zertifikatsstelle (CA) erfordern. Über die Gruppenrichtlinien können Sie festlegen, dass alle Computer der Domäne automatisch Zertifikate erhalten. Hierzu ist jedoch eine Windows 2000-CA erforderlich, während IPSec mit beliebigen CAs zusammenarbeitet. Weitere Hinweise zur Konfiguration der Zertifikatsoptionen entnehmen Sie den Checklisten in der Windows-Hilfe.

Um den Promote-Prozess über IPSec und Zertifikate sicherzustellen, sind die folgenden Schritte erforderlich:

1. Es muss eine autorisierende Zertifikatsstelle (CA) eingerichtet sein.
2. Stellen Sie sicher, dass auf allen Domänencontrollern sowie den Servern, die zu Domänencontrollern promoted werden sollen, Maschinenzertifikate vorhanden sind.
3. Führen Sie auf allen Domänencontrollern die im Kapitel „Konfiguration von IPSec für die Domänencontroller-Kommunikation“ beschriebenen Schritte zur IPSec-Konfiguration aus.
4. Starten Sie DCPROMO auf den gewünschten Servern.

Nach Abschluss des Promotes sind die Server bereits für IPSec-gesicherte Verbindungen zur Replikation eingerichtet. Sie müssen keine weiteren Konfigurationen vornehmen.

31.2.3 Zulassen dynamischer RPC-Aufrufe

Wie bereits gesagt, ist diese Methode keineswegs zur Nachahmung empfohlen, da sie so gut wie keine Sicherheit bietet. Prinzipiell können Sie sich bei dieser Konfiguration auch gleich die gesamte Firewall sparen. Der einzige Vorteil besteht darin, dass Sie keine der oben beschriebenen Einstellungen an den Domänencontrollern vornehmen müssen, aber diese Bequemlichkeit darf nicht zu Lasten der Sicherheit gehen.

Um eine Firewall für dynamische RPC-Aufrufe zu konfigurieren, müssten Sie die folgenden Ports freischalten:

- ▶ 53 TCP / UDP
- ▶ 88 TCP / UDP
- ▶ 123 UDP
- ▶ 135 TCP / UDP
- ▶ 137 TCP / UDP
- ▶ 138 UDP
- ▶ 139 TCP
- ▶ 389 TCP
- ▶ 445 TCP / UDP
- ▶ 636 TCP
- ▶ 1024 bis 65535 TCP
- ▶ 3268 TCP
- ▶ 3269 TCP

Ist zusätzlich noch WINS-Auflösung erforderlich, so muss Port 1512 TCP / UDP freigeschaltet werden, für WINS-Replikation Port 42 TCP / UDP. Sie sehen, dass bei dieser Konfiguration eine Firewall kaum noch diesen Namen verdient.

31.3 Die Konfiguration von Firewalls für Domänen und Vertrauensstellungen

Dieses Kapitel gibt Ihnen eine Übersicht über die Ports, die auf einer Firewall zur Aufrechterhaltung der Vertrauensstellungen freigeschaltet sein müssen.

Für Windows 2000 / 2003-Domänen, die im gemischten Modus betrieben werden und in denen noch NT-Domänencontroller vorhanden sind, sowie für Vertrauensstellungen zwischen zwei Windows 2000 / 2003-Domänencontrollern in verschiedenen Gesamtstrukturen müssen folgende Ports freigeschaltet sein (siehe Tabelle 31.3):

Server-Port	Client-Port	Dienst
53 TCP/UDP	53, fest zugewiesene Ports oder 1024 bis 65535 TCP/UDP	DNS
88 TCP/UDP	Fest zugewiesene Ports oder 1024 bis 65535 TCP / UDP	Kerberos
135 TCP	Für RPC zugewiesene Ports oder 1024 bis 65535 TCP	RPC
389 TCP/UDP	Fest zugewiesene Ports oder 1024 bis 65535 TCP / UDP	LDAP

Server-Port	Client-Port	Dienst
445 TCP	Fest zugewiesene Ports oder 1024 bis 65535 TCP	SMB
636 TCP	Fest zugewiesene Ports oder 1024 bis 65535 TCP	LDAP SSL
3268 TCP	Fest zugewiesene Ports oder 1024 bis 65535 TCP	LDAP globaler Katalog
3269 TCP	Fest zugewiesene Ports oder 1024 bis 65535 TCP	LDAP globaler Katalog SSL

Tabelle 31.3: Freizuschaltende Ports für Windows 2000/2003

Zusätzlich sind die folgenden für Windows NT 4.0 erforderlichen Ports zu öffnen (siehe Tabelle 31.4):

Server-Port	Client-Port	Dienst
42 TCP	Fest zugewiesene Ports oder 1024 bis 65535 TCP	WINS-Replikation
135 TCP	Für RPC zugewiesene Ports oder 1024 bis 65535 TCP	RPC
137 UDP	137 UDP	NetBIOS Name Server
138 UDP	138 UDP	NetBIOS Netlogon
139 TCP	Fest zugewiesene Ports oder 1024 bis 65535 TCP	NetBIOS Session

Tabelle 31.4: Freizuschaltende Ports für Windows NT

Verwenden Sie eine PPTP-Verbindung, so muss der folgende Port freigeschaltet werden (siehe Tabelle 31.5):

Server-Port	Client-Port	Dienst
1723 TCP	Fest zugewiesene Ports oder 1024 bis 65535 TCP	PPTP

Tabelle 31.5: Ports für eine PPTP-Verbindung

Zusätzlich muss der IP-Port 47 für General Routing Encapsulation (GRE) freigeschaltet werden.

31.4 Active Directory- und Firewall-Szenarien

In diesem Kapitel werden Ihnen verschiedene Szenarien vorgestellt, in denen die Domänencontroller und Active Directory-Clients durch Firewalls voneinander getrennt sind. Für jedes dieser Szenarien werden Konfigurationen der Firewalls und Domänencontroller sowie Sicherheitsaspekte aufgezeigt.

31.4.1 Zwei durch eine Firewall getrennte Gesamtstrukturen

In diesem Szenario (siehe Abbildung 31.5) werden zwei Gesamtstrukturen eingerichtet, die durch eine Firewall getrennt sind. Eine Gesamtstruktur befindet sich somit im internen Netzwerk, die andere Gesamtstruktur in der DMZ. Diese Konzeption bietet höhere Sicherheit als eine Gesamtstruktur, die auf das interne Netzwerk und die DMZ verteilt ist. Dieses Verfahren ist sinnvoll, wenn für verschiedene Netzwerke unterschiedliche Sicherheitslevel erforderlich sind. Für den gegenseitigen Ressourcenzugriff der Benutzer müssen explizite Vertrauensstellungen zwischen den beiden Gesamtstrukturen eingerichtet werden.

Zusätzlich konfigurieren Sie Point-to-Point-Verbindungen für die Domänencontroller und erlauben in diesen ausschließlich den Domänencontrollern beider Gesamtstrukturen eine Kommunikation über die Firewall hinweg.

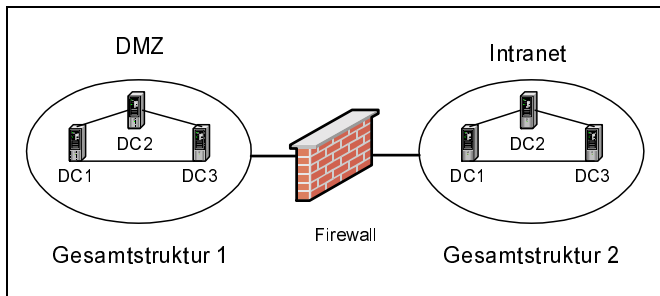


Abbildung 31.5: Zwei durch eine Firewall getrennte Gesamtstrukturen

In diesem Szenario müssen in der Firewall die folgenden Ports geöffnet werden:

- ▶ Für die Kerberos-Authentifizierung sind die Kerberos-Ports 88/TCP und 88/UDP zu öffnen.
- ▶ Zusätzlich sind die DNS-Ports 53/TCP und 53/UDP, die LDAP-Ports 389/TCP und 389/UDP bzw. 636 für SSL-verschlüsselten LDAP-Verkehr sowie die Ports 445/TCP und 445/UDP für das SMB-Protokoll freizuschalten.
- ▶ Weitere applikationsspezifische Ports entnehmen Sie der Dokumentation der jeweiligen Applikation.

Sofern es nicht möglich ist, eine separate Gesamtstruktur in der DMZ zu erstellen, sondern lediglich, die Domänencontroller einer Gesamtstruktur in der DMZ und dem internen Netzwerk zu verteilen, muss die Firewall für den Replikationsverkehr zwischen den Domänencontrollern konfiguriert werden.

31.4.2 Mehrere durch Firewalls getrennte Domänen

In diesem Szenario (siehe Abbildung 31.6) sind mehrere Domänen durch mehrere Firewalls getrennt. Diese Domänen können einer oder verschiedenen Gesamtstrukturen angehören. Das Szenario kann sowohl über das Intranet als auch über das Internet oder auch über eine Kombination aus beiden vorhanden sein.

In diesem Beispiel sind drei Domänen (Domäne A, B und C) durch mehrere Firewalls voneinander getrennt. Dabei ist der Client 1 von seinem Domänencontroller DC A durch eine Firewall getrennt (Firewall 1 und 2). Diese beiden Computer sind Mitglieder der Domäne A. Der Benutzer 1 ist Mitglied in den Domänen A und B. Von DC A für die Domäne A ist er durch die Firewalls 1 und 2 getrennt, von DC B für die Domäne B durch die Firewalls 2 und 3. Zusätzlich soll dieser Benutzer auf Ressourcen des Clients 2 zugreifen. Dieser Client ist Mitglied der Domäne C. Somit ist der Benutzer durch 3 Firewalls von den Ressourcen getrennt: Er selbst befindet sich hinter Firewall 2, der DC C für seine Authentifizierung an der Domäne C befindet sich hinter der Firewall 4 und Client 2 mit den Ressourcen hinter der Firewall 5. Dieses Szenario ist in der folgenden Abbildung dargestellt.

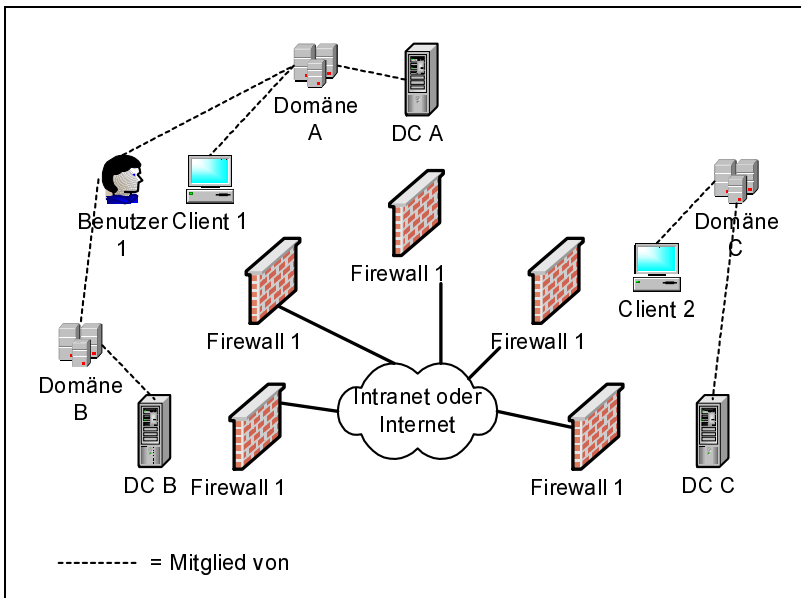


Abbildung 31.6: Durch Firewalls getrennte Domänen

In diesem Szenario sind die folgenden Ports freizuschalten:

- ▶ Für die Kerberos-Authentifizierung sind die Kerberos-Ports 88/TCP und 88/UDP zu öffnen.
- ▶ Zusätzlich sind die DNS-Ports 53/TCP und 53/UDP, die LDAP-Ports 389/TCP und 389/UDP bzw. 636 für SSL-verschlüsselten LDAP-Verkehr sowie die Ports 445/TCP und 445/UDP für das SMB-Protokoll freizuschalten.
- ▶ Weitere applikationsspezifische Ports entnehmen Sie der Dokumentation der jeweiligen Applikation.

31.4.3 Durch eine Firewall abgetrennte Mitgliedsserver

In diesem Szenario (siehe Abbildung 31.7) sind der oder die Mitgliedsserver von den Domänencontrollern durch eine Firewall getrennt. Diese Konstellation bietet sich für Mitgliedsserver an, auf denen Microsoft Exchange ausgeführt wird. Die Exchange-Server befinden sich in der DMZ. Sie können auf interne Ressourcen wie Dateifreigaben zugreifen und Authentifizierungen an den Domänencontrollern im Intranet vornehmen. Damit die Mitgliedsserver in der DMZ auf die internen Ressourcen zugreifen können, konfigurieren Sie IPSec-Verbindungen und beschränken in diesen die Computer, mit denen eine Kommunikation über die Firewall hinweg gestattet ist.

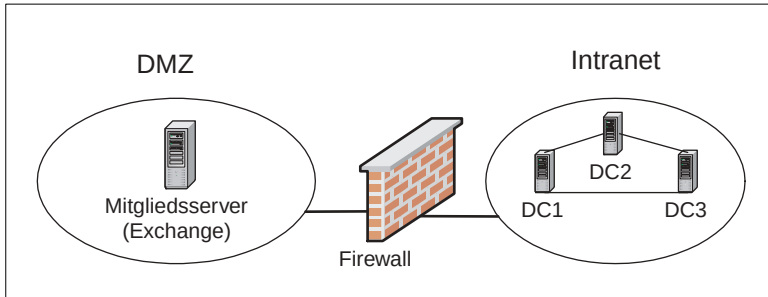


Abbildung 31.7: Durch eine Firewall getrennter Mitgliedsserver und Domänencontroller

In diesem Szenario müssen in der Firewall die folgenden Ports geöffnet werden:

- ▶ Für den Zugriff von Exchange-Servern auf die erforderlichen Daten des globalen Katalogservers muss Port 3268 geöffnet werden.
- ▶ Für die Kerberos-Authentifizierung zwischen dem Mitgliedsserver und den Domänencontrollern sind die Kerberos-Ports 88/TCP und 88/UDP zu öffnen.
- ▶ Zusätzlich sind die DNS-Ports 53/TCP und 53/UDP, die LDAP-Ports 389/TCP und 389/UDP bzw. 636 für SSL-verschlüsselten LDAP-Verkehr sowie die Ports 445/TCP und 445/UDP für das SMB-Protokoll freizuschalten.
- ▶ Weitere applikationsspezifische Ports entnehmen Sie der Dokumentation der jeweiligen Applikation.

32 ADSI-Skripte

Dieses Kapitel beschäftigt sich mit der ADSI-(Active Directory Services Interface-)Technologie sowie dem weiten Feld der ADSI-Skripte. Zunächst erhalten Sie eine allgemeine Einführung in die Grundlagen und Schlagwörter von ADSI. Daran schließt sich eine Reihe von Kapiteln an, in denen die häufigsten Einsatzbereiche von ADSI-Skripten an Beispielen beschrieben werden. Dazu zählen z.B. das Anlegen von neuen Benutzern, das Bearbeiten von Berechtigungen, das Ändern von Objekten oder auch das Anpassen des Active Directory-Schemas und Erweitern der Windows-GUI. Dieses Kapitel erfordert prinzipiell keine Kenntnisse des Lesers im Bereich Skripte und Skriptsprachen. Eine gute und ausführliche Einleitung in die Thematik Skripte, Windows Scripting Host und ADSI finden Sie unter den folgenden Links:

<http://msdn.microsoft.com/scripting>

<http://msdn.microsoft.com/scripting/default.htm?/scripting/windowshost/docs/reference/default.htm>

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/adsi/active_directory_service_interfaces_adsi.asp

32.1 Einführung in ADSI und ADSI-Skripte

In diesem Kapitel wird Ihnen zunächst eine kurze Einführung in die Vorteile von Skripten gegenüber der Verwaltung über die Windows-GUI sowie das Zusammenspiel von Skripten unter Windows und dem Windows Scripting Host (WSH) gegeben. Darauf aufbauend wird Ihnen das Grundkonzept von ADSI-Skripten sowie eine Reihe von Schlagwörtern wie ProgIDs oder Ads-Pfaden vorgestellt.

32.1.1 ADSI-Skripte unter Windows

Mit Hilfe von Skripten können Sie eine Reihe von Verwaltungsaufgaben im Active Directory durchführen, die auch über die GUI der mmc ausgeführt werden kann. Allerdings bietet der Einsatz von Skripten auch bestimmte Vorteile. Immer wiederkehrende Aufgaben können per Skript automatisiert werden. Anstatt sich z.B. bei jedem Anlegen eines neuen Benutzers durch die GUI klicken zu müssen, können Sie über ein Skript die gewünschten Variablen eingeben und somit direkt auf die Active Directory-Datenbank zugreifen. Je größer beispielsweise die Anzahl der neu einzurichtenden Benutzer, desto schneller und effektiver kann die Aufgabe mit einem Skript erledigt werden. So ist es bei zehn neuen Benutzern noch möglich, diese über die mmc einzupflegen, aber es wird wohl kaum ein Administrator auf die Idee kommen, mehrere hundert Benutzer manuell ins Active Directory einzupflegen. Beim Öffnen eines Objekts in der mmc und bei dem Betrachten von dessen Eigenschaften greift das Active Directory im Hintergrund auf sein Schema zurück. Es werden der Name des Objekts sowie dessen Eigenschaften ausgele-

sen und dem Benutzer auf einer oder mehreren Registerkarten angezeigt. Hier besteht für ihn die Möglichkeit, die Werte der Eigenschaften zu ändern. Diese Vorgänge laufen bei der Verwendung der GUI als Hintergrundprozess ab. Mit Hilfe von Skripten können Sie direkt auf diese Windows-Funktionen zugreifen.

Skripte sind standardisierbar, und somit ist stets nachvollziehbar, welche Aktionen durchgeführt wurden. Zusätzlich können die Skripte noch protokolliert werden. Auf diese Weise sind Sie bei der Fehlersuche immer im Vorteil gegenüber den Arbeitsschritten, die an der GUI ausgeführt worden sind. Ein falscher Mausklick an der falschen Stelle ist nicht mehr nachvollziehbar und kann schnell zu großen Problemen führen. Weiterhin können die Skripte auch in Webseiten eingebunden werden, sodass für Administratoren auch die Möglichkeit besteht, ihre Verwaltungsaufgaben über ein Web-Interface auszuführen.

Selbstverständlich soll dies keine Aufforderung sein, sämtliche administrativen Aufgaben nur noch über Skripte auszuführen. Für einmalige Eingriffe oder auch Überprüfungen ist die Arbeit an der GUI mit Sicherheit weniger aufwändig als ein neues Skript zu generieren und anzuwenden. Außerdem wird die Einsatzhäufigkeit der Skripte auch von den individuellen Vorlieben eines Administrators abhängig sein.

Nach diesem kurzen Vorgeschmack auf die Fähigkeiten und Möglichkeiten des Skripteneinsatzes sollen nun kurz die technischen Grundlagen für den Einsatz von Skripten vorgestellt werden. Skriptdateien können unter Windows über den WSH direkt ausgeführt werden. Der WSH ist fester Bestandteil von Windows 98, 2000, XP sowie 2003. Für Windows NT ist der WSH über die Servicepacks oder das Option Pack verfügbar. Über den WSH können automatisch alle in Microsoft VBScript oder JScript verfassten Skripte auf dem Client ausgeführt werden. Über WSH haben Sie die Möglichkeit, auf alle COM-(Component Object Model-)Komponenten des Clients zuzugreifen. Soll beispielsweise eine Datei geändert werden, so erfolgt der Zugriff eigentlich auf ein COM-Dateiobjekt. Über entsprechende Schnittstellen können die zu bearbeitenden Elemente als Objekte modifiziert werden. Die Schnittstelle – üblicherweise eine dll – bestimmt, welche Aktionen an einem Objekt und seinen Eigenschaften durchgeführt werden können, z.B. Löschen oder Ändern. Sie können auch Skripte in HTML-Code einbauen. In diesem Fall spricht man von Active Server Pages (ASPs). Diese HTML-Seiten bieten einen dynamischen Inhalt, und zwar abhängig davon, welches Skript in die ASP eingebunden ist und vom Webserver ausgeführt wird.

Bereits 1997 wurde von Microsoft eine Sammlung von Schnittstellen veröffentlicht, die den programmiersprachenübergreifenden Zugriff auf verschiedene Verzeichnisdienste via LDAP ermöglicht. Hierbei handelt es sich um das ADSI-SDK (Software Development Kit). ADSI abstrahiert die Leistungsfähigkeit verschiedener Verzeichnisdienste und präsentiert dabei einen einzigen Satz von Verzeichnisdienst-Schnittstellen. Entwicklern ist somit die Möglichkeit gegeben, über ihren Code auf Objekte in unterschiedlichen Verzeichnisdiensten wie z.B. Active Directory oder NDS zugreifen zu können – und dies unabhängig vom Anbieter oder Hersteller des Verzeichnisdienstes. Administratoren können über ADSI ihre Verwaltungsaufgaben durchführen – ebenfalls unabhängig vom verwendeten Netzwerkumfeld. Unter Windows 2000 wird ADSI in der Version 2.5 eingesetzt. Die wichtigste Neuerung in dieser Version ist die Active Directory Client-Extension.

Neben ADSI ist auch die Funktionsweise der ActiveX Data Objects (ADO) wichtig. Hiermit wird gewährleistet, dass über Skripte oder andere Applikationen auf die Daten eines Datenbankservers zugegriffen werden kann. Voraussetzung dafür ist jedoch, dass der

Datenbankserver über eine OLE-Datenbank-Provider-Schnittstelle verfügt. Von Microsoft wurde ein derartiger Provider für ADSI entwickelt. So besteht die Möglichkeit, dass Entwickler direkt auf die Daten des Active Directory oder eines anderen Verzeichnisdienstes über einen ADSI-OLE-DB-Connector zugreifen können.

32.1.2 Methoden und Eigenschaftsmethoden

Die Grundlagen der Funktion von ADSI und COM erleichtern das Verständnis für die ADSI-Skripte. ADSI ist als Standard definiert und gibt Spezifikationen für verschiedene Schnittstellen vor, damit der Zugriff auf mehrere Verzeichnisse von unterschiedlichen Herstellern gewährleistet ist. COM bildet unter Windows die Schnittstelle, um auf ein Objekt, z.B. eine Datei, zuzugreifen. ADSI definiert für jede Schnittstelle zwei verschiedene Informationen: die Methoden und Eigenschaften bzw. Eigenschaftsmethoden. Eine Methode gibt an, welche Aktionen an einem bestimmten Objekt durchgeführt werden können. Diese Aktionen sind spezifisch für jedes Objekt. Während es z.B. für das Objekt Benutzergruppe die Methode zum Hinzufügen und Löschen von Mitgliedern gibt, ist diese Methode logischerweise für ein Benutzerobjekt nicht vorhanden. Auf die spezifischen Eigenschaften einer Schnittstelle wird mit den Methoden zugegriffen.

Sämtliche ADSI-Objekte unterstützen eine IADs-Schnittstelle. Jede dieser Schnittstellen beinhaltet neben Methoden und spezifischen Eigenschaften auch sechs verschiedene Kerneigenschaften für das zugehörige Objekt. Dabei handelt es sich um folgende Attribute:

- ▶ **AdsPath:** Der Ads-Pfad des Objekts in seinem Namensraum
- ▶ **Class:** Die Schemaklasse des Objekts
- ▶ **GUID:** Die GUID des Objekts
- ▶ **Name:** Der Name des Objekts
- ▶ **Parent:** Der Ads-Pfad zum übergeordneten Objekt
- ▶ **Schema:** Der Ads-Pfad zur Schemaklasse des Objekts

Selbstverständlich können Objekte noch weitere spezifische Attribute besitzen, aber die eben genannten sechs Eigenschaften besitzt jedes Objekt. Diese sechs Eigenschaften verfügen jeweils über eine eigene Eigenschaftsmethode, die denselben Namen wie die Eigenschaft besitzt. Mithilfe der Eigenschaftsmethode können Sie auf den Wert der Eigenschaft zugreifen und diesen bearbeiten. Um die Fähigkeiten der Eigenschaftsmethoden darzustellen, soll folgendes kleines Skript dienen, mit dem die sechs Eigenschaften des Benutzerobjekts Administrator über die Methoden ausgelesen und angezeigt werden.

```
dim adsUser
dim str
set adsUser=GetObject_
    ("LDAP://cn=Administrator,cn=Users,dc=firma,dc=de")
str = "Name: " & adsUser.Name & vbCrLf
str = str & "GUID: " & adsUser.GUID & vbCrLf
str = str & "Class: " & adsUser.Class & vbCrLf
str = str & "AdsPath: " & adsUser.AdsPath & vbCrLf
str = str & "Parent: " & adsUser.Parent & vbCrLf
str = str & "Schema: " & adsUser.Schema & vbCrLf
wscript.Echo str
Set adsUser = Nothing
```

Listing 32.1: Auslesen von Objekteigenschaften

Das Skript beginnt mit der Deklaration zweier Variablen. Über die VBScript-Methode *GetObject* wird das Benutzerobjekt Administrator referenziert und mit *adsObject* auf diese Referenz gezeigt. Über die Eigenschaftsmethode *IADs::Name* wird der Name des Benutzerobjekts ausgelesen und der Variablen *str* hinzugefügt. Bei *vbCrLf* handelt es sich um eine Konstante für den Zeilenumbruch und Wagenrücklauf (Carriage Return and Line Feed) unter VBScript. Sie sorgt lediglich dafür, dass im Ausgabefenster jeder Wert in einer neuen Zeile steht.

In den folgenden fünf Zeilen wird jeweils eine der Eigenschaftsmethoden aufgerufen und der ermittelte Wert an die Variable *str* übergeben. Mit dem Befehl *str = str &* wird der Wert den bisherigen Variablenwerten angefügt. Der Befehl *wscript.Echo* gibt sämtliche Werte der Variablen *str* in einem Fenster aus. Die letzte Zeile sorgt dafür, dass nach dem Durchlauf des Skripts die Variablenwerte von *adsUser* wieder gelöscht werden. Dies ist wichtig, wenn dieses Skript mehrfach für verschiedene Objekte ablaufen soll. Sie erhalten mit diesem Skript für das Benutzerobjekt Administrator die folgenden Werte (siehe Abbildung 32.1):



Abbildung 32.1: Ausgabe der Objekteigenschaften über Eigenschaftsmethoden

Jede Methode einer Schnittstelle wird in der Schreibweise *Schnittstelle::Methodenname* dargestellt. Zwei wichtige Methoden der IADs-Schnittstelle sind *IADs::Get* und *IADs::Put*. So können beispielsweise mit *IADs::Put* Eigenschaften eines Objekts geschrieben und mit *IADs::Get* ausgelesen werden. Allerdings arbeitet ein Skript unter der Benutzung von Methoden langsamer als bei der Benutzung von Eigenschaftsmethoden, die dasselbe Ergebnis erzielen. Die beiden Arten von Methoden unterscheiden sich nicht in ihrer Funktionsweise, wohl aber in der Benutzung der Syntax. Angenommen, Sie wollen die Methode *IADs::Get* benutzen, um damit eine Eigenschaft, nämlich die GUID des Objekts *adsUser*, herauszufinden und an die String-Variablen *GUID* zu übergeben, so müssten Sie folgende Syntax verwenden:

```
StrGUID = adsUser.Get("GUID")
```

Die Verwendung der Methode *IADs::Get* wird durch den dem Methodennamen vorangestellten Punkt gekennzeichnet. Der für die Methode notwendige Parameter *GUID* wird der Methode angefügt.

Für häufig benutzte Methoden wie auch *IADs::Get* sind die jeweiligen Eigenschaften in spezielle Eigenschaftsmethoden integriert. Die Eigenschaftsmethoden bieten den Vorteil, dass sie denselben Namen besitzen wie die Eigenschaft. Im eben erwähnten Beispiel lautete die Eigenschaft *GUID*. Diese Eigenschaft verfügt über eine Eigenschaftsmethode des gleichen Namens, nämlich *IADs::GUID*. Also kann die Syntax folgendermaßen vereinfacht werden auf *StrGUID = adsUser.GUID*.

Diese Schreibweise wurde auch im obigen Beispiel zur Ausgabe der Objekteigenschaften des Benutzerobjekts Administrator verwendet.

32.1.3 IADs-Schnittstellen

Insgesamt gibt es über 40 IADs-Schnittstellen und für jede davon schnittstellenspezifische Methoden. Diese Schnittstellen beziehen sich z.B. auf Verzeichnisobjekte wie Benutzer (*IADsUser*) oder auch Sicherheitseinstellungen (*IADsAccessControlList*).

Tabelle 32.1 gibt Ihnen eine Übersicht über die wichtigsten verfügbaren IADs-Schnittstellen. Eine komplette Auflistung aller verfügbaren IADs-Schnittstellen sowie der zugehörigen Methoden und Eigenschaften finden Sie unter

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/adsi/adsi_interfaces.asp

IADs-Schnittstelle	Beschreibung
IADsAccessControlEntry	Ermöglicht den Verzeichnisdienst-Clients den Zugriff sowie Änderungen an den ACEs der Eigentumsobjekte.
IADsAccessControlList	Verwaltet die Sicherheitseinstellungen über die ACEs der Objekte.
IADsAcl	Bietet Methoden zum Bearbeiten von ACL-Werten unter Novell Directory Services (NDS). Weitere NDS-spezifische Schnittstellen sind z.B. IADsBackLink, IADsCaseIgnoreList, IADsEmail, IADsFaxNumber oder IADsHold.
IADsADSystemInfo	Bezieht Informationen über Computer in einer Windows 2000-Domäne wie Standort, definierter Name u.Ä.
IADsClass	Managt die Klassenobjekte des Active Directory-Schemas.
IADsComputer	Bearbeitet und gibt Daten über Computerobjekte an, z.B. Betriebssystem, Prozessor oder Netzwerkadresse.
IADsComputerOperations	Bietet Methoden für die Statusabfrage eines Computers im Netzwerk oder zum Remote-Shutdown.
IADsContainer	Ermöglicht, die in einem ADSI-Container enthaltenen Objekte zu bearbeiten.
IADsDeleteOps	Ermöglicht einem Objekt, sich in einem untergeordneten Verzeichnis zu löschen sowie untergeordnete Objekte zu löschen.
IADsDNWithBinary	Ermöglicht die Verbindung zwischen einem definierten Namen und der GUID eines Objekts.
IADsDomain	Bietet Methoden zur Benutzerkontenverwaltung in einer Domäne, z.B. die Anzahl ungültiger Anmeldungen.
IADsFileService	Zeigt die vom Verzeichnisdienst unterstützten File Services an. Einstellungen wie z.B. Anzahl des gleichzeitigen Clientzugriffs sind einstellbar.
IADsFileServiceOperations	Bietet Methoden zum Managen der Files Services im Netzwerk wie z.B. offene Sitzungen.
IADsFileShare	Zeigt die Dateifreigaben im Netzwerk an.
IADsGroup	Bearbeitet die Daten zur Gruppenmitgliedschaft.

IADs-Schnittstelle	Beschreibung
IADsLocality	Gibt die geografischen Angaben (Land, Region) zu Verzeichniseinträgen an.
IADsMembers	Managt eine Sammlung von ADSI-Objekten, die Mitglied einer Gruppe sind.
IADsNamespaces	Zum Verwalten von Namespace-Objekten (Top-Level-Container mit dem Namen des Verzeichnisstammes).
IADsObjectOptions	Bietet provider-spezifische Optionen zum Bearbeiten von ADSI-Objekten.
IADsOpenDSObject	Wird im Sicherheitskontext zur Authentifizierung bei der Verbindung zu einem Objekt benutzt.
IADsPrintJob	Erlaubt den Zugriff auf Informationen eines Druckjobs, z.B. Seitenzahl, Datum des Druckjobs etc.
IADsPrintJobOperations	Kontrolliert einen Druckjob im Netzwerk.
IADsPrintQueue	Repräsentiert Informationen über einen Drucker wie Standort, Netzwerkadresse usw.
IADsPrintQueueOperations	Kontrolliert einen Drucker im Netzwerk.
IADsProperty	Zum Verwalten von einzelnen Attributdefinitionen für ein Klassenobjekt im Schema, z.B. Minimal- und Maximalwerte usw.
IADsPropertyEntry	Verwaltet einen oder mehrere Eigenschaftswerte eines Attributs, wie es im Schema definiert ist.
IADsPropertyList	Zum Bearbeiten und Lesen der Eigenschaften im Eigenschaftscache eines Objekts.
IADsSecurityDescriptor	Ermöglicht den Zugriff auf die Eigenschaften der Sicherheitsbeschreiber von ADSI-Objekten.
IADsService	Liefert Informationen über laufende Systemdienste sowie Informationen dazu auf einem Computer.
IADsServiceOperations	Verwaltet die auf einem Computer installierten Systemdienste (starten, beenden usw.).
IADsSession	Zeigt Informationen über aktive Sitzungen im Netzwerk an.
IADsUser	Bietet Methoden zur Verwaltung von Benutzerkonten.
IADsWinNTSystemInfo	Zeigt die Windows NT 4.0-Systeminformationen auf einem Windows 2000-Computer an.

Tabelle 32.1: Die IADs-Schnittstellen

Nach diesen theoretischen Grundlagen geht es nun an allgemein gültige Bereiche von Skripten, die Sie in jedem Skript verwenden müssen. Dabei handelt es sich um Bereiche wie Herstellen einer Verbindung mit dem Verzeichnis, Referenzierung des zu bearbeitenden Objekts sowie Authentifizierung am Verzeichnisserver.

32.1.4 Namensräume und ProgIDs

Um mit den Schnittstellen und deren Methoden arbeiten zu können, müssen Sie zunächst die Verbindung zu einem Verzeichnis herstellen, in dem sich das zu bearbeitende Objekt befindet. Über ADSI können Sie auf Verzeichnisse verschiedener Server zugreifen, z.B. Windows 2000 oder NetWare. Damit eine ADSI-Methode auf einem bestimmten Server ausgeführt werden kann, muss dieser als Namensraum (Namespace) referenziert werden. ADSI verwendet dabei für jeden Server eine eindeutige ProgID, die im Skript anzugeben ist. Wird bei der Ausführung des Skripts eine ProgID gefunden, lädt ADSI die dll des entsprechenden ADSI-Anbieters, und die Verbindung zum Server wird hergestellt. Tabelle 32.2 gibt Ihnen eine Übersicht der fest definierten ProgIDs für bestimmte Server. Bei allen ProgIDs ist unbedingt die angegebene Groß- und Kleinschreibung zu beachten.

ProgID	Server
WinNT://	Windows NT 3.51, 4.0, 2000 und Windows 2003
NDS://	NetWare 4.x und 5.x
NWCOMPAT://	NetWare 3.11, 3.12, 3.2 und 4.x (Bindery)
IIS://	Metabase-Pfade auf Servern mit mindestens IIS 3.0
LDAP://	LDAP-konforme Verzeichnisse wie Active Directory oder NetWare 5.x

Tabelle 32.2: Übersicht über die ADSIProgIDs

Zur Verbindung mit einem LDAP-konformen Verzeichnisdienst wie Active Directory sollten Sie immer den Namensraum `LDAP://` benutzen. Sie können zwar auch über `WinNT://` auf eine Windows 2000-Domäne zugreifen, aber der volle Funktionsumfang der ADSI-Methoden und Eigenschaften steht Ihnen nur in einem LDAP-Namensraum zur Verfügung. Der WinNT-Namensraum ist lediglich in der Lage, auf einzelne Objekte auf einem einzelnen Computer zuzugreifen. Ein LDAP-Zugriff auf einzelne Computer ist nicht möglich. Sie können über `WinNT://` den Zugriff auf lokale Objekte in einer Arbeitsgruppe steuern, da Objekte in Arbeitsgruppen nicht Bestandteil des Active Directory sind. Alle Active Directory-Objekte müssen über `LDAP://` referenziert werden.

32.1.5 Zugriff auf Objekte

Nach der Verbindung mit dem gewünschten Namensraum müssen Sie auch das Objekt angeben, mit dem eine bestimmte Aktion durchgeführt werden soll. Der komplette Pfad zu einem Objekt besteht aus der Referenzierung des Namensraumes und des Objekts. Der vollständige Pfad wird als ADs-Pfad bezeichnet. Im Folgenden sehen Sie einige Beispiele für einen vollständigen ADs-Pfad.

1. `WinNT://Arbeitsgruppe/pmustermann`
2. `WinNT://Arbeitsgruppe/pmustermann, User`
3. `WinNT://Arbeitsgruppe/Computernamen/pmustermann`

Beispiel 1 und 2 referenzieren beide einen bestimmten Benutzer in einer Arbeitsgruppe. Im zweiten Beispiel ist zusätzlich der Typ des Namens, nämlich User, angegeben. Diesen

Zusatz sollten Sie in jedem Fall hinzufügen, wenn verschiedene Objekttypen denselben Namen besitzen, z.B. eine Benutzergruppe und ein einzelner Benutzer oder Computer.

Im LDAP-Namensraum haben Sie verschiedene Möglichkeiten, ein Objekt zu referenzieren. Sie können den Verzeichnisbaum (DIT) von oben nach unten und umgekehrt angeben (Beispiel 1 und 2). Zusätzlich können Sie den Server und die DNS-Zone angeben, der das Objekt enthält (Beispiele 3 bis 5).

1. LDAP://DC=de,DC=firma,CN=Benutzer,CN=pmustermann
2. LDAP://cn=pmustermann,cn=Benutzer,dc=firma,dc=de
3. LDAP://archimedes.firma.de/cn=pmustermann,cn=Benutzer,dc=firma,dc=de
4. LDAP://archimedes.firma.de/DC=de,DC=firma,CN=Benutzer,CN=pmustermann
5. LDAP://archimedes/cn=pmustermann,cn=Benutzer,dc=firma,dc=de

Enthält irgendein Namensteil Sonderzeichen wie etwa „/“ oder „“, so muss dieser Teil in Anführungszeichen gesetzt oder durch \ gekennzeichnet werden. Haben Sie Benutzer nach dem Schema „Mustermann,Peter“ vergeben, so müssen Sie eine der beiden folgenden Schreibweisen wählen:

1. LDAP://"cn=Mustermann,Peter",cn=Benutzer,dc=firma,dc=de
2. LDAP://cn=Mustermann\,Peter,cn=Benutzer,dc=firma,dc=de

32.1.6 Authentifizierung bei der Verbindung zum Verzeichnisserver

Bei der Verbindung mit einem Server über einen ADs-Pfad muss auch die Authentifizierung gegenüber dem Verzeichnisserver bedacht werden. Sie haben dabei die Möglichkeit, für rein lesenden Zugriff eine anonyme Verbindung zu verwenden. Als anonyme Verbindung gilt dabei die Anmeldung über das gerade aktuell verwendete Benutzerkonto, sofern Sie nicht bereits am Verzeichnis angemeldet sind. Um jedoch Daten modifizieren oder auf Objekte zugreifen zu können, die nur über eingeschränkte Zugriffsberechtigungen verfügen, müssen Sie eine authentifizierte Verbindung aufbauen. Die authentifizierte Verbindung kann dabei das aktuelle Benutzerkonto, mit dem Sie am Verzeichnis angemeldet sind, benutzen oder ein beliebiges anderes Konto mit ausreichenden Berechtigungen.

Anonyme Verbindung

Beginnen wir mit dem einfachen Fall, dass Sie eine anonyme Verbindung im Sicherheitskontext des aktuellen Benutzerkontos durchführen möchten und noch nicht am Verzeichnis angemeldet sind.

Zunächst müssen Sie im Skript zwei Variablen deklarieren, und zwar eine String-Variable für den ADs-Pfad und eine ADSI-Objekt-Variable. Eine Übersicht über die Präfixe verschiedener Variablentypen finden Sie in Tabelle 32.3. Diese Deklaration sieht folgendermaßen aus:

```
Dim strPath 'Pfad zum Verzeichnisserver
Dim adsObjekt 'Stammobjekt des Verzeichnisses
```

Die Kommentare, die dem ' nachgestellt sind, sind selbstverständlich optional und dienen nur der besseren Lesbarkeit des Skripts. Sie weisen dann der Variablen *strPath* als Wert den LDAP-Pfad zu dem Server zu, mit dem Sie sich verbinden möchten. Dieses ist der Anmeldepunkt für die Verbindung. Der Wert für den Pfad wird in Anführungszeichen gesetzt, da es sich um eine Zeichenkette handelt. Diese Zuweisung sieht folgendermaßen aus:

```
strPath = "LDAP://DC=De,DC=Firma"
```

Letztlich wird über den *set*-Befehl die Methode *getObject* verwendet. Damit wird die Verbindung zwischen der deklarierten Variablen *adsObjekt* und dem Objekt selbst hergestellt, auf das in *strPath* verwiesen wird, sodass das Objekt bearbeitet werden kann.

Authentifizierte Verbindung

Müssen Sie sich für die Verbindung authentifizieren, so wird hierzu die Schnittstelle *IAdsOpenDSObject* verwendet. Die von der Schnittstelle benutzte Methode *OpenDSObject* benötigt die folgenden vier Argumente: ADs-Pfad, Benutzername, Passwort sowie eine Sicherheitseinstellung.

In einem Skript müssen Sie hierzu zunächst einige String- und Objekt-Variablen deklarieren. Als String-Variablen müssen der ADs-Pfad als Einstiegspunkt der Anmeldung, der Benutzername als definierter Name und das Passwort deklariert werden. Zusätzlich ist die Deklaration der Objekt-Variablen *adsNamespaceLDAP* und *adsObjekt* notwendig. Die Deklaration könnte folgendermaßen aussehen:

```
Dim strPath 'Pfad zum Anmeldepunkt im Verzeichnis
Dim strUsername 'definierter Name des Benutzers
Dim strPassword 'Passwort im Klartext
Dim adsNamespaceLDAP 'ADSI Namespace-Objekt
Dim adsObjekt 'Stammobjekt des Verzeichnisses
```

Die hinter den Variablen angegebenen Kommentare sind optional. Kommentare sind durch ein vorangestelltes ' abzutrennen. Als Nächstes werden im Skript den drei String-Variablen Werte zugewiesen. Dies könnte folgendermaßen aussehen:

```
strPath = "LDAP://DC=de,DC=Firma"
strUsername = "cn=Administrator,cn=Benutzer,dc=firma,dc=de"
strPassword = "Passwort"
```

Die Variable *strPath* gibt den Anmeldepunkt im Verzeichnis an. Der Wert für den Pfad wird in Anführungszeichen gesetzt, da es sich um eine Zeichenkette handelt. Liegen für den Benutzer keine genügenden Berechtigungen im Stamm des Verzeichnisses vor, so kann er hier einen hierarchisch tieferen Punkt zur Anmeldung angeben. Mit *strUsername* geben Sie den Benutzernamen als definierten Namen an. Als Nächstes muss die Variable *adsNamespaceLDAP* referenziert werden. Hierzu wird ein *set*-Befehl mit der Anweisung *GetObject* benutzt. Die Eigenschaft für *GetObject* lautet *LDAP*. An dieser Stelle muss zwangsweise mit *LDAP* gearbeitet werden und nicht, wie eher zu erwarten wäre, mit *strPath*, weil nur für den LDAP-Namensraum die Methode *OpenDSObject* zur Authentifizierung aufgerufen werden kann. Die beiden letzten Zeilen des Skriptes würden somit folgendermaßen aussehen:

```
Set adsNamespaceLDAP = GetObject("LDAP:")
Set adsObjekt = adsNamespaceLDAP.OpenDSObject(strPath,strUsername,
strPassword,0)
```

Der Methode *OpenDSObject* werden als Parameter der Pfad, Benutzername und das Kennwort sowie als Letztes eine Sicherheitseinstellung übergeben. Der Wert 0 bedeutet dabei, dass weder eine Echtheitsbestätigung noch eine Verschlüsselung vom Skript durchgeführt werden. Dieses könnte jedoch ein hohes Sicherheitsrisiko darstellen, da im Netzwerk unbefugte Personen über einen Netzwerksniffer den Namen und das Passwort im Klartext lesen könnten. Sie können für eine Erhöhung der Sicherheit auch folgende Werte angeben:

ADS_USE_ENCRYPTION, *ADS_SECURE_AUTHENTICATION* sowie *ADS_READONLY_SERVER*. Sollen mehrere dieser Parameter verwendet werden, so werden die durch das Zeichen + miteinander verbunden, also etwa *ADS_USE_ENCRYPTION + ADS_SECURE_AUTHENTICATION*.

Eine weitere Möglichkeit zur Absicherung besteht darin, das Passwort nicht als Klartext zu senden, sondern für den Benutzer eine Eingabemaske anzuzeigen, in die er das Passwort eingeben muss. Um diese Eingabemaske einzubauen, muss das oben beschriebene Skript lediglich in der Zeile *strPassword* abgeändert werden. Die Zeile würde durch folgende ersetzt werden:

```
strPassword = InputBox("Geben Sie das Passwort ein")
```

Da in der Eingabemaske das Kennwort im Klartext erscheint, ist aber auch dies nicht die sicherste Methode. Visual Basic-Skripte unterstützen es nicht, das Passwort im Eingabefeld durch Sternchen zu ersetzen. Diese Funktionalität bietet stattdessen beispielsweise ein Perl-Skript.

Wollen Sie sich mit denselben Benutzerinformationen, mit denen Sie momentan am Verzeichnis angemeldet sind, auch über das Skript anmelden, so können Sie für die Variablen des Benutzernamens und des Passworts die VBScript-Konstante *vbNullString* benutzen. Diese beiden Variablen werden somit nicht im Bereich der Deklaration aufgeführt, und die letzte Zeile des Skripts ist entsprechend abzuändern:

```
set adsObjekt = adsNamespaceLDAP.OpenDSObject (strPath, vbNullString,
vbNullstring, 0)
```

32.1.7 Konventionen für Variablenpräfixe

In den eben gezeigten Beispielen haben Sie bereits einige Präfixe von Variablen wie *str* für Stringvariablen und *ads* für ADSI-Objekt-Variablen kennen gelernt. Für bestimmte Typen von Daten sind feste Präfixe festgelegt. Die Definitionen sind in dieser Form zwar nicht zwingend vorgeschrieben, aber beim Schreiben von Skripten sollten Sie sich auch an diese Konvention halten. Der eigentliche Name der Variablen folgt ohne Leerzeichen direkt auf das Präfix und beginnt mit einem Großbuchstaben, z.B. *strPath* oder *adsNamespaceLDAP*. Innerhalb des Namens selbst ist die Groß- und Kleinschreibung irrelevant. Tabelle 32.3 zeigt eine Übersicht über die wichtigsten Präfixe.

Präfix	Bedeutung
ado	ADO-Objekt
ads	ADSI-Objekt
app	Application-Objekt (Anwendungsobjekt)
arr	Array (Datenfeld)
bol	Boolescher Wert
fil	File-Object (Dateiobjekt)
fol	Folder-Object (Ordnerobjekt)
fso	Folder-System-Objekt (Ordnersystemobjekt)
int	Integer (ganze Zahl)
lgn	Long Integer (große ganze Zahl)
obj	Objekt
str	String (Zeichenkette)
wsh	Windows Scripting Host-Objekt

Tabelle 32.3: Die wichtigsten Variablenpräfixe

32.2 ADSI-Skripte zur Benutzerverwaltung

In diesem Kapitel und den nächsten steht nun die praktische Anwendung von ADSI-Skripten für verschiedene Einsatzbereiche im Mittelpunkt. Sämtliche Skriptbeispiele sind in VBScript verfasst. Es werden zwar nicht unbedingt Vorkenntnisse in dieser Skriptsprache vorausgesetzt, aber dennoch sind sie nicht zwingend erforderlich. Es sollte eigentlich eine nicht mehr zu erwähnende notwendige Selbstverständlichkeit sein, aber dennoch sei darauf hingewiesen, dass Sie alle Skripte vor dem Einsatz in der produktiven Umgebung vorher hinreichend in einem Testumfeld auf fehlerfreie Funktionalität hin überprüfen. Die hier gezeigten Skriptbeispiele können selbstverständlich keinen Anspruch darauf erheben, dass nur die gezeigten Funktionalitäten umsetzbar sind. Viele Skriptbeispiele für hier nicht gezeigte Zwecke können Sie, z.T. sogar kostenlos, aus dem Internet beziehen.

In diesem Kapitel erhalten Sie einige Beispiele für das Anlegen von Benutzerkonten in einer Windows 2000-Domäne. Diese reichen vom einfachen Anlegen eines Benutzers bis zu komplexen Einstellungen der Eigenschaften für Kennwörter, verbundene Netzlaufwerke, Profildfad usw.

An dieser Stelle ist noch folgende Information wichtig: Um die Attribute der einzelnen Objekte korrekt zu setzen, muss auf deren korrekte Schreibweise geachtet werden. Sollten Sie bei der Fülle der Attribute einmal nicht wissen, wie das gewünschte Attribut heißt, so starten Sie das Support-Tool *ADSIEDIT*. Hier können Sie sämtliche Attribute (obligatorische und optionale) sowie deren tatsächlichen Namen auflühren.

32.2.1 Anlegen und Löschen eines Benutzerkontos

Beginnen wir mit dem Erstellen eines simplen Benutzerkontos für den Benutzer pmustermann in der Windows 2000-Domäne *firma.de*. Hierfür könnte ein ADSI-Skript folgendermaßen aussehen:

```
Dim adsDomain, adsUser
Set adsDomain = GetObj("LDAP://cn=Users,dc=firma,dc=de")
set adsUser = adsDomain.create("User","cn=pmustermann")
adsUser.Put "SamAccountName", "pmustermann"
adsUser.Put "userPrincipalName", "pmustermann@firma.de"
adsUser.SetInfo
```

Listing 32.2: Anlegen eines einfachen Domänenbenutzerkontos

Über die beiden *set*-Befehle stellen Sie zunächst eine Verbindung zum Container Users im LDAP-Namensraum her, dann wird an dieser Stelle der Benutzer mit dem Common Name (CN) pmustermann angelegt. Mit der *Put*-Methode werden dem Objekt nun zwei Attributwerte zugewiesen. Für ein Benutzerobjekt in einer Domäne müssen zwar nicht alle Attribute zwangsläufig ausgefüllt werden. Obligatorisch ist jedoch das Attribut *sAMAccountName*. Dies ist der Name des Benutzerkontos. Das zweite Attribut *userPrincipalName* ist zwar nicht zwingend erforderlich, jedoch kann der Benutzer die Anmeldung so über seine vollständige E-Mail-Adresse vornehmen. Diese beiden Werte werden abschließend über die *SetInfo*-Methode in das Objekt geschrieben. Selbstverständlich können Sie über ein solches Skript auch Benutzer in Windows NT-Domänen sowie lokale Benutzer unter Windows 2000/2003 anlegen, aber diese Möglichkeiten sind nicht Thema dieses Buches.

32.2.2 Die Schnittstelle IADsUser

Dieses Beispiel diene nur der kurzen Einführung. In der Praxis wird wohl kaum ein Administrator Benutzerkonten erstellen, die lediglich den Namen als Information enthalten. Mit ADSI können Sie Benutzerobjekte über die IADs-Schnittstelle *IADsUser* bearbeiten. Diese Schnittstelle bietet Ihnen eine Reihe von Methoden und Eigenschaftsmethoden. Für jede Eigenschaft des Benutzerobjekts ist eine eigene Eigenschaftsmethode vorhanden. Zusätzlich gibt es die drei Methoden *IADsUser::ChangePassword*, *IADsUser::SetPassword* sowie *IADsUser::Gruppen*. Mit den beiden ersten Methoden können Sie das Kennwort ändern bzw. neu festlegen. Dabei muss das alte Passwort nicht bekannt sein. Bei der Verwendung der Methode *IADsUser::SetPassword* kann es zu einer Fehlermeldung (Fehler *0x8007202f* bzw. *Logon failure: unknown user name or bad password*) kommen. Dieser Fehler tritt lediglich in der ADSI-Version 2.5 auf, wenn Sie ADSI über eine 128-Bit-SSL-Verbindung verwenden. In diesem Fall müssen Sie das Kennwort in Anführungszeichen setzen. Spätere ADSI-Versionen führen diesen Schritt automatisch durch. Weitere Hinweise dazu finden Sie unter

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q290278>.

Über die Methode *IADsUser::Gruppen* erhalten Sie eine Liste von Gruppen, in denen der Benutzer Mitglied ist. Die Eigenschaftsmethoden von *IADsUser* für die verschiedenen Attribute sind die folgenden (das vorangestellte *IADsUser::* lasse ich an dieser Stelle weg)

und zum größten Teil selbsterklärend, auf welches Attribut sie sich beziehen: *AccountDisabled*, *AccountExpirationDate*, *Department*, *Description*, *Division*, *EmailAddress*, *EmployeeID*, *FaxNumber*, *FirstName*, *FullName*, *GraceLoginsAllowed*, *GraceLoginsRemaining*, *HomeDirDrive*, *HomeDirectory*, *HomePage*, *IsAccountLocked*, *Languages*, *LastName*, *LoginHours*, *LoginScript*, *LoginWorkstations*, *Manager*, *MaxLogins*, *MaxStorage*, *NamePrefix*, *NameSuffix*, *OfficeLocations*, *OtherName*, *PasswordExpirationDate*, *PasswordMinimumLength*, *PasswordRequired*, *Picture*, *PostalAddresses*, *PostalCodes*, *Profile*, *RequireUniquePassword*, *SeeAlso*, *TelephoneHome*, *TelephoneMobile*, *TelephoneNumber*, *TelephonePager*, *Title*.

Allen diesen Eigenschaften können Sie über die Methoden Werte zuweisen. Zusätzlich gibt es noch sechs weitere Eigenschaftsmethoden, deren Werte Sie nicht editieren, sondern lediglich auslesen können. Dabei handelt es sich um die Methoden *BadLoginsAddress*, *BadLoginsCount*, *LastFailedLogin*, *LastLogin*, *LastLogoff* und *PasswordLastChanged*.

32.2.3 Komplexe Benutzerkonten anlegen

Das folgende Beispiel erstellt einen Benutzer in der Windows 2000-Domäne *firma.de*. Dem Benutzer werden verschiedene Attribute zugewiesen. Per Skript wird ihm z.B. ein Benutzerverzeichnis zugewiesen und angelegt, falls dieses noch nicht vorhanden ist. Für dieses Verzeichnis werden ihm zusätzlich Rechte zugewiesen.

```
Const vbMinimizedNoFocus = 6
Dim adsDomain, adsUser, fso
Dim fldUserHomedir, wshShell
'Verbindung zum Namensraum, Anlegen des Users
Set adsDomain = GetObject("LDAP://cn=Users,dc=firma,dc=de")
Set adsUser = adsDomain.Create("user", "cn=pmustermann")
adsUser.put "sAMAccountName", "pmustermann"
adsUser.put "userPrincipalName", "pmustermann@firma.de"
'Auslesen des eben geschriebenen Objekts aus dem
'Zwischenspeicher und Auslesen aller Eigenschaften des Objekts
adsUser.SetInfo
adsUser.GetInfo
'Setzen von optionalen Attributen für das Objekt
adsUser.AccountDisabled = False
adsUser.Description = "Mitarbeiter der Werbeabteilung"
adsUser.IsAccountLocked = False
adsUser.LoginScript = "\\Firma\Skripte>Login\pmustermann.vbs
adsUser.Profile = "\\Firma\Benutzer\pmustermann\Profile"
adsUser.PasswordRequired = True
adsUser.NamePrefix = "Herr"
adsUser.FirstName = "Peter"
adsUser.LastName = "Mustermann"
adsUser.DisplayName = "Peter Mustermann"
'Laufwerksbuchstabe für Benutzerverzeichnis
adsUser.HomeDirectory = "\\Firma\Benutzer\pmustermann"
adsUser.Put "HomeDrive", "Z:"
'Setzen der festgelegten Eigenschaften sowie der Standardwerte
adsUser.SetInfo
adsUser.GetInfo
'Erstellen des Benutzerverzeichnisses
Set fso = CreateObject("Scripting.FileSystemObject")
```

```

if not fso.FolderExists("\\Firma\Benutzer\pmustermann") then
set fldUserHomedir = _
fso.CreateFolder("\\Firma\Benutzer\pmustermann")
end if
'Setzen von voller Berechtigung für das Benutzerverzeichnis
set wshShell = WScript.CreateObject("WScript.Shell")
wshShell.run cacls \\Firma\Benutzer\pmustermann /e /g pmustermann:F",_
vbMinimizedNoFocus, True
'Setzen des Passworts
adsUser.SetPassword "Borussia"

```

Listing 32.3: Anlegen eines Benutzerkontos

Dieses Skript ist bis auf zwei Sektionen im Wesentlichen selbsterklärend. Um für den Benutzer ein eigenes Benutzerverzeichnis anzulegen, ist eine Referenz auf FileSystem-Object notwendig. Über die Methode *FileSystemObject::CreateFolder* wird dort ein neuer Ordner angelegt, wenn die Prüfung mit *fso.FolderExists* ergab, dass noch kein Ordner vorhanden ist. Um für den angelegten Ordner Berechtigungen zu vergeben, wird das Programm CACLS.EXE über den Windows Scripting Host mit der Methode *wshShell::run* aufgerufen. Diese Methode erfordert drei Parameter. Als Erstes wird ihr der komplette Befehl mitgegeben, hier also CACLS mit allen erforderlichen Parametern. Der zweite Wert gibt an, wie der Befehl ausgeführt wird (sichtbar/im Hintergrund/Fokussierung). Dazu können Sie folgende Werte angeben:

```

Const vbHide = 0, Const vbNormalFocus = 1, Const vbMinimizedFocus = 2,
Const vbMaximizedFocus = 3, Const vbNormalNoFocus = 4 oder
Const vbMinimizedNoFocus = 6.

```

Als Letztes geben Sie den Wert *true* oder *false* mit. Ist der Wert auf *true* gesetzt, wird das Skript erst in der nächsten Zeile fortgesetzt, wenn CACLS abgeschlossen ist. Dann erst wird in unserem Beispiel das Passwort gesetzt.

32.2.4 Ändern von Benutzerattributen

Im Folgenden wird Ihnen gezeigt, wie Sie Benutzerattribute über ADSI ändern können. Sie haben in Kapitel 17.3.4 bereits gesehen, wie Sie beispielsweise Telefon- und Faxnummern mithilfe einer LDIF-Datei bearbeiten können. Das folgende Skript zeigt, wie Sie für die Benutzer einer bestimmten OU die Faxnummer bearbeiten können.

```

set oContainer=GetObject(LDAP://OU=Finanzen,DC=Firma,DC=De")
modifyUsers oContainer
Set oContainer = Nothing
Wscript.Echo "Der Vorgang wurde abgeschlossen"
Sub ModifyUsers(oObject)
    Dim oUser
    oObject.Filter = Array("user")
    for each oUser in oObject
        oUser.Put "FaxNumber","112233"
        oUser.SetInfo
    Next
End Sub

```

Listing 32.4: Bearbeiten von Benutzereigenschaften

Zunächst wird eine Verbindung zum gewünschten OU-Container hergestellt. Der eigentliche Änderungsprozess wird in der Subroutine ausgeführt. Das ausgelesene OU-Objekt wird in der Variablen *oObject* gespeichert. Über den Filter wird sichergestellt, dass nur Benutzerobjekte innerhalb der OU verwendet werden. Anschließend wird für jeden Benutzer der OU über die *Put*-Methode der neue Wert der Faxnummer eingefügt. Über *SetInfo* wird der neue Wert in das Active Directory zurückgeschrieben. Wurden bei allen Benutzern der OU die Faxnummern geändert, erhalten Sie eine entsprechende Statusmeldung.

32.2.5 Weitere Beispiele

Eine Reihe von Beispielskripten finden Sie auch auf den Support-Seiten von Microsoft. Dort finden Sie auch eine große Auswahl von Skripten z.B. für Benutzerverwaltung und Exchange-Server. Folgend nun einige ausgewählte Links auf Skriptbeispiele zur Benutzer- und Computerverwaltung.

Automatisiertes Anlegen von Computerkonten

Hier wird Ihnen das automatisierte Erstellen von Computerkonten via Skript vorgestellt. Dieses Vorgehen bietet eine Alternative zum Erstellen der Konten über *Netdom.exe*.

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q222525>

Codebeispiel in Visual C++:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q255042>

Anlegen von Home-Shares für jeden Benutzer einer Domäne

Mit diesem Skript wird für jeden Benutzer ein Home-Share in einer Freigabe erstellt. Den Benutzerverzeichnissen können Sie feste Laufwerksbuchstaben zuweisen oder auch Attribute wie sichtbar oder unsichtbar per Skript mitgeben.

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q234746>

Ändern des Anzeigenamen-Formats

Der Anzeigename jedes Benutzers wird standardmäßig in dem Format *FirstName LastName* ausgegeben. Aus Gründen der Übersichtlichkeit wäre jedoch oftmals die Ausgabe im Format *LastName FirstName* wünschenswerter. Dieser Artikel zeigt, wie Sie die Änderung an bestehenden Benutzerkonten vornehmen können.

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q277717>

Soll der Anzeigename bereits bei der Erstellung der Benutzer in diesem Format ausgegeben werden, so sollten Sie folgenden Artikel zu Rate ziehen:

<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q250455>

Ändern von Passwörtern für Benutzerkonten

Ein C++-Codebeispiel zum planmäßigen Ändern von Passwörtern für Benutzerkonten unter Windows XP, 2000, 2003 und NT.

<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q151546>

32.3 ADSI-Skripte für Zugriff, Überwachung und Sicherheit

In diesem Kapitel werden Ihnen Möglichkeiten vorgestellt, wie Sie skriptgesteuert die Berechtigungen für Objekte bearbeiten können. Hierzu wird auf die ACEs (Access Control Entries) in den ACLs (Access Control Lists) zugegriffen. So kann der Zugriff für Benutzer und Gruppen auf Objekte oder spezielle Eigenschaften gesteuert werden. Unter ADSI stehen Ihnen drei Schnittstellen zur Verfügung, die Sie für zugriffs- und sicherheitsbezogene Aufgaben benutzen können. Dabei handelt es sich um *IADsAccessControlEntry*, *IADsAccessControlList* sowie *IADsSecurityDescriptor*. Diese Schnittstellen haben im Wesentlichen die folgenden Funktionen (siehe Tabelle 32.4):

Schnittstelle	Beschreibung
<i>IADsAccessControlEntry</i>	Zum Bearbeiten von ACEs, die für die Zugriffsberechtigungen und Überwachung an Objekten und Eigenschaften von Benutzern und Gruppen zuständig sind.
<i>IADsAccessControlList</i>	Zur Verwaltung einer Reihe von ACEs in einer ACL.
<i>IADsSecurityDescriptor</i>	Zuständig für die objektspezifischen ACL-Sätze.

Tabelle 32.4: Die sicherheitsbezogenen ADSI-Schnittstellen

32.3.1 Erstellen eines ACEs

Bevor Sie mit dem Erstellen oder Bearbeiten von ACEs beginnen, muss der ACE an sich näher betrachtet werden. ACEs werden sowohl für Berechtigungs- als auch für Überwachungseinträge benutzt. Jeder ACE verfügt dafür über insgesamt fünf Eigenschaften. Diese zeigt Tabelle 32.5.

ACE-Eigenschaft	Beschreibung
<i>AccessMask</i>	Gibt die festzulegenden Berechtigungen oder die zu überwachenden Ereignisse an.
<i>AceFlags</i>	Gibt die gewünschten Vererbungsoptionen an. Bei einem Überwachungseintrag wird zusätzlich angegeben, ob erfolgreiche oder fehlgeschlagene Versuche überwacht werden sollen.
<i>AceType</i>	Hier wird entschieden, ob für ein Objekt oder eine Eigenschaft Berechtigungen oder Überwachungen festgelegt werden sollen.
Flags: <i>ObjectType</i> , <i>InheritedObjectType</i>	Gibt an, ob sich der ACE auf das gesamte Objekt oder nur auf den im Flag gesetzten Bereich bezieht.
<i>Trustee</i>	Das Ziel, auf das sich die Berechtigungen/Überwachungen beziehen.

Tabelle 32.5: Die Eigenschaften der ACEs

Die Werte für die ACE-Eigenschaften werden in verschiedenen Formen angegeben. Bis auf *Trustee* werden alle Werte im hexadezimalen Format gesetzt. Im Folgenden werden für alle ACE-Eigenschaften die möglichen Werte vorgeführt. Danach sehen Sie ein praktisches Beispiel, wie ein ACE per Skript erstellt werden kann.



Die in den folgenden Tabellen angegebenen Konstantennamen sind in dieser Form von Microsoft festgelegt worden. Diese Konstanten funktionieren nur in Programmier- und Skriptsprachen, die die ADSI-Bibliotheken benutzen (z.B. Visual Basic oder Visual C++). VBScript unterstützt diese Funktionalität nicht. Sie müssen im VB-Skript also erst die Konstanten definieren.

32.3.2 AccessMask

Über die AccessMask werden sowohl die zu überwachenden Ereignisse als auch die zu vergebenden Berechtigungen festgelegt, abhängig davon, welche Aufgabe Sie durchführen möchten. Die Vererbung der in AccessMask gesetzten Berechtigungen sowie die Auswahl, ob erfolgreiche und/oder fehlgeschlagene Ereignisse aufgezeichnet werden, wird über AceFlags bestimmt. Von allen ACE-Eigenschaften besitzt AccessMask die größte Anzahl möglicher Werte. Tabelle 32.6 gibt Ihnen eine Übersicht über die verfügbaren Namen der Werte sowie die hexadezimalen und dezimalen Werte.

ADSI-Name (Konstantenname)	Hexadezimaler/ dezimaler Wert	Beschreibung
ADS_RIGHT_ACCESS_SYSTEM_SECURITY	0x1000000/ 16777216	Lesen und Setzen der SACLs eines Objekts im Security Descriptor.
ADS_RIGHT_ACTRL_DS_LIST	0x4/ 4	Auflisten von untergeordneten Objekten eines Objekts.
ADS_RIGHT_DELETE	0x10000/ 65536	Das Objekt darf gelöscht werden.
ADS_RIGHT_GENERIC_ALL	0x10000000/ 268435456	Kombination von ADS_RIGHT_GENERIC_EXECUTE, READ und WRITE.
ADS_RIGHT_GENERIC_EXECUTE	0x20000000/ 536870912	Auflisten der untergeordneten Objektelemente.
ADS_RIGHT_GENERIC_READ	0x80000000/ 2147483648	Lesen der Objekteigenschaften und Sicherheitsbeschreibungen, Durchsuchen des Objekts und dessen untergeordneten Objekten.
ADS_RIGHT_GENERIC_WRITE	0x40000000/ 1073741824	Schreiben aller Eigenschaften und der DACL; Hinzufügen und Löschen des Objekts in/aus der Struktur.
ADS_RIGHT_DS_CONTROL_ACCESS	0x100/ 256	Ausführen von Operationen, die über erweiterte Zugriffsrechte kontrolliert werden. Diese erweiterte Berechtigung kann über die GUID eines ObjectType des ACE identifiziert werden. Ist keine GUID gesetzt, kontrolliert der ACE alle Zugriffe erweiterter Berechtigungen am Objekt.

ADSI-Name (Konstantenname)	Hexadezimaler/ dezimaler Wert	Beschreibung
ADS_RIGHT_DS_CREATE_CHILD	0x1/ 1	Anlegen von untergeordneten Objekten. Der Typ des anzulegenden Child-Objekts kann über die GUID eines ObjectType des ACE identifiziert werden. Ist keine GUID gesetzt, kontrolliert der ACE das Erstellen aller Child-Objekttypen.
ADS_RIGHT_DS_DELETE_CHILD	0x2/ 2	Löschen von untergeordneten Objekten. Der Typ des zu löschenden Child-Objekts kann über die GUID eines ObjectType des ACE identifiziert werden. Ist keine GUID gesetzt, kontrolliert der ACE das Löschen aller Child-Objekttypen.
ADS_RIGHT_DS_DELETE_TREE	0x40/ 64	Löschen aller untergeordneten Objekte, ohne dass die Berechtigungen dieser Objekte berücksichtigt werden.
ADS_RIGHT_DS_LIST_OBJECT	0x80/ 128	Auflisten eines Objekts. Fehlt dem Benutzer die Berechtigung und ist ADS_RIGHT_ACTRL_DS_LIST nicht auf das übergeordnete Objekt gesetzt, so bleibt ihm das Objekt verborgen.
ADS_RIGHT_DS_READ_PROP	0x10/ 16	Lesen von Objekteigenschaften. Die Eigenschaften des Objekts können über die GUID eines ObjectType des ACE identifiziert werden. Ist keine GUID gesetzt, kontrolliert der ACE das Lesen aller Objekteigenschaften.
ADS_RIGHT_DS_SELF	0x8/ 8	Ausführen von Operationen, die von validierten Schreibzugriffsrechten kontrolliert werden. Das validierte Schreibrecht kann über die GUID eines ObjectType des ACE identifiziert werden. Ist keine GUID gesetzt, kontrolliert der ACE alle validierten Schreibzugriffe am Objekt.

ADSI-Name (Konstantenname)	Hexadezimaler/ dezimaler Wert	Beschreibung
ADS_RIGHT_DS_WRITE_PROP	0x20/ 32	Schreiben von Eigenschaften eines Objekts. Die Eigenschaften können über die GUID eines ObjectType des ACE identifiziert werden. Ist keine GUID gesetzt, kontrolliert der ACE das Schreiben aller Objekteigenschaften.
ADS_RIGHT_READ_CONTROL	0x20000/ 131073	Der Security Descriptor darf gelesen werden, nicht aber die Daten in der SACL.
ADS_RIGHT_SYNCHRONIZE	0x100000/ 1048576	Synchronisationsverwendung des Objekts. Weiteres siehe http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/ads/ads_interfaces.asp
ADS_RIGHT_WRITE_DAC	0x40000/ 262144	Die DACLs im Security Descriptor dürfen geändert werden.
ADS_RIGHT_WRITE_OWNER	0x80000/ 524288	Der Benutzer kann den Objektbesitz übernehmen, diesen aber nicht weitergeben. Der Benutzer muss Trustee des Objekts sein.
Ohne Namen	FFFFFFFFFFFFFF/ -1	Vollzugriff

Tabelle 32.6: Die AccessMask-Werte

Es können einem ACE auch mehrere AccessMask-Attribute zugewiesen werden. In diesem Fall addieren Sie die entsprechenden Werte aller gewünschten Attribute. Das Resultat ist die kumulative Summe der einzelnen Berechtigungen.

32.3.3 AceFlags

Der Bereich AceFlags beinhaltet zwei verschiedene Angaben, je nachdem, ob der ACE für Berechtigungen oder Überwachungen konfiguriert wird. Für die Überwachung wird festgelegt, ob erfolgreiche und/oder fehlgeschlagene Ereignisse protokolliert werden sollen. Die zu überwachenden Ereignisse an sich werden unter AccessMask angegeben. Werden hingegen Berechtigungen konfiguriert, können Sie den Wirkungs- und Vererbungsbereich des ACE bestimmen. Die Berechtigungen an sich sind unter AccessMask festgelegt (siehe Tabelle 32.7).

ADSI-Name (Konstantenname)	Hexadezimaler/dezimaler Wert	Beschreibung
Überwachungsbezogen		
ADS_ACEFLAG_FAILED_ACCESS	0x80/ 128	Fehlgeschlagene Zugriffe werden protokolliert.
ADS_ACEFLAG_SUCCESSFUL_ACCESS	0x40/ 64	Erfolgreiche Zugriffe werden protokolliert.
Berechtigungsbezogen		
ADS_ACEFLAG_INHERIT_ACE	0x2/ 2	Die untergeordneten Objekte erben den ACE. Allerdings darf dazu nicht das Flag ADS_ACEFLAG_NO_PROPAGATE_INHERIT_ACE gesetzt sein.
ADS_ACEFLAG_INHERIT_ONLY_ACE	0x8/ 8	Es handelt sich um einen nur vererbaren ACE. Das Objekt selbst, in dessen Sicherheitsbeschreibung der ACE steht, ist von den Einstellungen nicht betroffen. Dieser ACE dient nur als Überbringer der Eigenschaften.
ADS_ACEFLAG_INHERITED_ACE	0x10/ 16	Legt fest, ob der ACE geerbt wurde oder nicht. Dieses Bit wird vom System geschrieben.
ADS_ACEFLAG_NO_PROPAGATE_INHERIT_ACE	0x4/ 4	Der ACE wird nicht an untergeordnete Objekte weitervererbt. Dabei wird vom System das Flag ADS_ACEFLAG_INHERIT_ACE bei den geerbten ACEs der Child-Objekte gelöscht.
ADS_ACEFLAG_VALID_INHERIT_FLAGS	0x1F/ 31	Kennzeichnet die vererbungsbezogenen Flags als gültig. Das Bit wird vom System gesetzt.

Tabelle 32.7: Die AceFlag-Werte

32.3.4 AceType

Über den ACETYPE wird geregelt, ob die Berechtigungen vom ACE gestattet oder verweigert werden oder ob die Anwendung von Berechtigungen vom ACE überwacht wird. Dabei legt AceFlag fest, ob die erfolgreichen oder fehlgeschlagenen Zugriffsversuche überwacht werden sollen. Im Gegensatz zu AccessMask und AceFlags können die einzelnen Werte für AceType nicht addiert werden. Es kann immer nur einer der Werte angegeben werden.

Die Benutzung der AceType-Werte hängt davon ab, ob der ACE eine GUID unter *ObjectType* oder *InheritedObjectType* (siehe Sektion Flags) besitzt. Verfügt der ACE über keine GUID, d.h., steht in den Feldern *ObjectType* und *InheritedObjectType* der Wert Null, werden die übrigen AceType-Werte verwendet. Diese verwenden die standardmäßige Windows-Sicherheitsbeschreibung. Besitzt der ACE eine GUID, werden jeweils die _OBJECT-Werte benutzt. Über die GUID werden eine Eigenschaft oder ein Satz von Eigenschaften, erweiterte Berechtigungen oder ein untergeordnetes Objekt identifiziert, für das die Berechtigungen gelten sollen (siehe Tabelle 32.8).

ADSI-Name (Konstantenname)	Hexadezimaler/dezimaler Wert	Beschreibung
ADS_ACETYPE_ACCESS_ALLOWED	0x0/ 0	Standardtyp des ACE für Zugriff erlaubt.
ADS_ACETYPE_ACCESS_ALLOWED_OBJECT	0x5/ 5	Erlaubt den Zugriff auf den in der GUID angegebenen Wirkungsbereich.
ADS_ACETYPE_ACCESS_DENIED	0x1/ 1	Standardtyp des ACE für Zugriff verweigert.
ADS_ACETYPE_ACCESS_DENIED_OBJECT	0x6/ 6	Verweigert den Zugriff auf den in der GUID angegebenen Wirkungsbereich.
ADS_ACETYPE_SYSTEM_AUDIT	0x2/ 2	Standardtyp des ACE zur Systemüberwachung.
ADS_ACETYPE_SYSTEM_AUDIT_OBJECT	0x7/ 7	Systemüberwachung des in der GUID gesetzten Wirkungsbereichs.

Tabelle 32.8: Die AceType-Werte

Für späteren Gebrauch ist zusätzlich ADS_ACETYPE_SYSTEM_ALARM_OBJECT definiert (Hex-Wert 0x8, Dezimalwert 8). Zu diesem Zeitpunkt ist es aber noch mit keiner Funktion versehen.

32.3.5 Flags: ObjectType, InheritedObjectType

Jeder ACE verfügt über die Eigenschaft Flags. Über die Flags erkennt der ACE, ob in ihm das Feld *ObjectType* oder *InheritedObjectType* enthalten ist. Das Feld *ObjectType* gibt an, auf welchen Objekttyp, welche Eigenschaft oder welchen Satz von Eigenschaften sich der ACE bezieht. Die GUID des Objekttyps oder der Eigenschaft bildet den Wert für *ObjectType*. Dieser Wert ist physisch nicht im ACE vorhanden, sofern nicht das Flag ADS_FLAGS_OBJECT_TYPE_PRESENT gesetzt ist. Ist dieses Flag nicht gesetzt, ist *InheritedObjectType* im ACE nicht vorhanden. Das Feld *InheritedObjectType* im ACE gibt die GUID des Objekts an, das den ACE erben soll. Diese GUID ist ebenfalls physisch nicht im ACE vorhanden, sofern hierfür nicht das ADS_FLAG_INHERITED_OBJECT_TYPE_PRESENT-Flag gesetzt ist. Wollen Sie mit ADSI einen ACE für Berechtigungen festlegen, so müssen Sie über die Flags die GUID des Objekts oder der Eigenschaft angeben (siehe Tabelle 32.9).

ADSI-Name (Konstantenname)	Hexadezimaler/ dezimaler Wert	Beschreibung
ADS_FLAG_INHERITED_OBJECT_TYPE_PRESENT	0x2/ 2	Siehe oberer Absatz.
ADS_FLAG_OBJECT_TYPE_PRESENT	0x1/ 1	Im ACE ist das Feld <i>ObjectType</i> vorhanden, nicht aber das Feld <i>InheritedObjectType</i> .

Tabelle 32.9: Die Flag-Werte

In den Feldern *ObjectType* und *InheritedObjectType* ist entweder eine GUID als Wert oder der Wert `Null` zu setzen. Diese Werte legen fest, worauf sich der ACE bezieht. Soll der ACE für das gesamte Objekt gelten, werden keine Flags gesetzt. In beiden *ObjectType*-Feldern ist somit der Wert "null" gesetzt. Die *AceFlags* müssen so gesetzt sein, dass der ACE nur für das Objekt gilt und nicht an untergeordnete Objekte weitervererbt wird.

Sofern der ACE für alle untergeordneten Objekte gültig sein soll, wird in beiden *ObjectType*-Feldern der Wert `Null` gesetzt, obwohl das Flag *ObjectType* gesetzt ist. Allerdings klingt dies auf den ersten Blick für das Feld *ObjectType* merkwürdig, man würde eher erwarten, eine GUID anzugeben. Es wird aber automatisch erkannt, dass mit dem Wert `Null` die Berechtigungen für sämtliche untergeordneten Objekte gelten sollen. Die *AceFlags* müssen so konfiguriert werden, dass die Einstellungen nicht für das Objekt selbst, wohl aber für alle untergeordneten Objekte gelten sollen.

Soll der ACE für spezielle Attribute des Objekts gelten, so wird nur das Flag *ObjectType* gesetzt. Dies muss als Wert die *schemaIDGUID* des Attributschema-Objekts besitzen. Das Feld *InheritedObjectType* wird auf "null" gesetzt. Die *AceFlags* müssen so gesetzt sein, dass der ACE nur für das Objekt gilt und nicht an untergeordnete Objekte weitervererbt wird.

Sollen sich die ACE-Berechtigungen auf alle untergeordneten Objekte einer bestimmten Klasse beziehen, so wird nur das Flag *ObjectType* gesetzt. Dieses erhält als Wert die *schemaIDGUID* des übergeordneten Objekts.

32.3.6 Trustee

Nach den eben gezeigten umfangreichen Auflistungen der Werte für die ACE-Eigenschaften sind die Werte für den Trustee sehr simpel. Der Trustee bestimmt den Benutzer oder die Benutzergruppe, dem eine Berechtigung zugewiesen oder für die die Überwachung konfiguriert werden soll. Das Benutzerkonto kann dabei in vier verschiedenen Formen angegeben werden. Die einfachste Lösung besteht darin, das Konto im Format *Domäne\Benutzer* anzugeben. Als Benutzername muss der Wert der Eigenschaft *sAMAccountName* angegeben sein. Weiterhin können Sie auch den kompletten definierten Namen in der Form *cn=,cn=,dc=,dc=* angeben. Sie können auch eine Benutzergruppe aus den vordefinierten Gruppen wählen. Hierfür lautet das Format *BUILTIN\Gruppenname*. Als Letztes haben Sie noch die Möglichkeit, die SID des Benutzers oder der Gruppe anzugeben.

32.3.7 Beispiel

Doch nun genug der Theorie. Um eine bessere Vorstellung zu bekommen, sollten Sie sich mithilfe des Tools LDP einmal den ACE einiger Benutzerobjekte betrachten. Wählen Sie hierzu aus dem LDP-Menü BROWSE den Eintrag SECURITY/SECURITY DESCRIPTOR und geben den Namen in der Form CN=,CN=,DC=,DC= an.

Das folgende Skript zeigt, wie ein ACE für die Benutzergruppe "Buchhaltung" erstellt wird, sodass diese Gruppe Vollzugriff auf die OU "Finanzen" sowie deren untergeordnete Objekte erhält. Zunächst deklarieren Sie die nötigen Konstanten für AccessMask, AceType und Flag.

```
Const FULL_CONTROL = -1
Const ADS_ACETYPE_ACCESS_ALLOWED = 0
Const ADS_FLAG_INHERITED_OBJECT_TYPE_PRESENT = 2
```

Danach werden die Variablen für das Objekt, den Sicherheitsbeschreiber sowie ACL und ACE deklariert.

```
dim adsObject
dim adsSecDesc
dim adsDACL
dim adsNewACE
```

Im nächsten Teil des Skripts wird der neue ACE erzeugt und mit den gewünschten Werten versehen.

```
set adsNewACE = CreateObject("AccessControlEntry")
adsNewACE.Trustee = "Windows\E:\\Buch\\aktuelles Projekt\\
Gesamtdokument\\Buchhaltung"
adsNewACE.AccessMask = FULL_CONTROL
adsNewACE.AceType = ADS_ACETYPE_ACCESS_ALLOWED
adsNewACE.AceFlags = ADS_FLAG_INHERITED_OBJECT_TYPE_PRESENT
```

Dieser neu erstellte ACE wird dem OU-Objekt hinzugefügt.

```
set adsObject = GetObject("LDAP://ou=finanzen,dc=firma,dc=de")
```

Es wird eine Verbindung zum Verzeichnis hergestellt, und über zwei IADS-Methoden werden der Sicherheitsbeschreiber sowie die vorhandene DACL ausgelesen.

```
set adsSecDesc = adsObject.Get("ntSecurityDescriptor")
set adsDACL = adsSecDesc.DiscretionaryAcl
```

Der neu erstellte ACE wird nun zur bestehenden DACL hinzugefügt:

```
adsDACL.AddAce adsNewACE
```

Abschließend müssen die geänderte DACL sowie der Sicherheitsbeschreiber des Objekts ersetzt werden.

```
adsSecDesc.DiscretionaryAcl = adsDACL
adsObject.Put "ntSecurityDescriptor", Array(adsSecDesc)
```

Im letzten Schritt wird der Inhalt des Eigenschaftszwischenspeichers über eine IADS-Methode in das Active Directory zurückgeschrieben.

```
adsObject.SetInfo
```

Selbstverständlich kann in einem Skript auch ein ganzer Satz von ACEs mit verschiedenen Berechtigungen für unterschiedliche Benutzer und Gruppen erstellt werden. In diesem Fall werden zunächst alle benötigten Konstanten von `AccessMask`, `AceFlag`, `AceType` und `Flags` deklariert. Anschließend fügen Sie die ACEs mit verschiedenen Berechtigungen dem Objekt hinzu.

32.4 ADSI-Skripte zum Ändern des Schemas

Dieses Kapitel zeigt Ihnen, wie Sie per Skript das Active Directory um Klassen und Attribute erweitern können. Anschließend lernen Sie verschiedene Methoden kennen, wie Sie die Windows-GUI so anpassen können, dass auch die erweiterten Schemaattribute eingesehen werden können. Zunächst werden jedoch die Zugriffsarten auf das Active Directory-Schema beschrieben.

32.4.1 Herstellen einer Verbindung zum Schema

Wie zu allen Objekten im Active Directory können Sie auch eine Verbindung zum Schema herstellen. Dabei wird unterschieden in die Verbindungsherstellung zum abstrakten Schema und zum Schema Container selbst bzw. einem Klassen- oder Attribut-Container im Schema. Letztere enthalten die komplette formale Definition aller Klassen bzw. Attribute der Gesamtstruktur. Das abstrakte Schema enthält nur einen begrenzten Satz an Informationen zu den Klassen und Attributen. Dafür ist das abstrakte Schema für den lesenden Zugriff optimiert.

Ob Sie die Verbindung zum abstrakten Schema oder zu einem `classSchema`- bzw. `attributeSchema`-Objekt herstellen, hängt davon ab, welche Aufgabe Sie durchführen möchten. Wollen Sie das Schema bearbeiten oder erweitern, müssen Sie sich direkt mit dem Schema-Container verbinden. Das abstrakte Schema ist schreibgeschützt. Eine Verbindung dazu ist sinnvoll, wenn lediglich Informationen gelesen werden sollen.

Zum Auslesen der Informationen des abstrakten Schemas werden beispielsweise die ADSI-Schnittstellen `IADsClass` oder `IADsProperty` benutzt. Diese verwenden den `LDAP_DisplayName` zur Ausgabe der Klassen- und Attributnamen, auch wenn diese Informationen im Verzeichnis in Form der OIDs gespeichert sind. Weiterhin besitzt jeder Eintrag einer Objektklasse im abstrakten Schema gesammelt diverse Informationen, die von verschiedenen `classSchema`-Objekten stammen. Dazu zählen die möglichen Parents sowie die obligatorischen und optionalen Attribute aller übergeordneten und Hilfsklassen der aktuellen Klasse. Beim direkten Zugriff auf den Container der Klasse muss aus jeder übergeordneten und Hilfsklasse einzeln die Information bezogen werden.

Da das abstrakte Schema nur einen begrenzten Satz an Informationen besitzt, müssen Sie auf die Container selbst zugreifen, wenn Sie Informationen wie `attributeSyntax`, `oMSyntax` oder `defaultSecurityDescriptor` erhalten möchten.

Um die Verbindung zum abstrakten Schema herzustellen, benutzen Sie den Befehl `LDAP://Schema`. Dies sieht in Visual Basic folgendermaßen aus:

```
dim adschema As IADsContainer
set adschema = GetObject("LDAP://Schema")
```

Sie können auch eine Verbindung zu einer bestimmten Klasse oder einem Attribut im abstrakten Schema herstellen. Für die Benutzerklasse verwenden Sie folgenden Befehl:

```
dim userclass As IADsClass
set userclass = GetObject("LDAP://Schema/User")
```

Für den Zugriff auf eine Klasse benutzen Sie die Schnittstelle *IADsClass*, für den Zugriff auf ein Attribut die Schnittstelle *IADsProperty*. Für das gewünschte Objekt ist in beiden Fällen der *IDAPDisplayName* anzugeben.

32.4.2 Neue Schemaattribute und -klassen erstellen

Dieses Kapitel zeigt Ihnen, wie Sie mit einem ADSI-Skript ein neues Benutzerattribut und eine neue Klasse anlegen können. Es wird ein neues Attribut namens "Qualifikation" erstellt, das die Qualifikationen und Zertifizierungen der Mitarbeiter enthalten soll. Dieses Attribut können Sie wie jedes andere Attribut auch in den globalen Katalog aufnehmen oder für die schnellere Suche indizieren. Das Attribut wird einer neuen Klasse hinzugefügt. Danach werden Instanzen dieser Klasse gebildet.

Erstellen eines neuen Attributs

Zunächst wird das neue Attribut erstellt. Bedenken Sie, dass Sie auch bei der Schemaänderung per ADSI-Skript die Voraussetzungen (siehe Kapitel 24.3) erfüllen müssen, damit die Änderung wirksam wird.

```
dim adsAttribute
dim adsSchemaContainer
set adsSchemaContainer =
GetObject("LDAP://cn=Schema,cn=Configuration,dc=firma,dc=de")
Set adsAttribute =
adsSchemaContainer.Create("attributeSchema","cn=Qualifikation")
```

In diesen Zeilen wird eine Verbindung zum Schema-Container des Active Directory hergestellt. In diesem Container wird das neue Objekt "Qualifikation" angelegt. Als Nächstes werden diesem Attribut obligatorische Werte zugewiesen. Hierzu wird eine *Put*-Methode verwendet.

```
adsAttribute.Put "cn", "Qualifikation"
adsAttribute.Put "LDAPDisplayName", "Qualifikation"
adsAttribute.Put "attributeID", "1.2.840.113556.1.4.7000.144"
adsAttribute.Put "oMSyntax", "27"
adsAttribute.Put "attributeSyntax", "2.5.5.3"
adsAttribute.Put "isSingleValued", False
```

Das Attribut erhält den gemeinsamen Namen "Qualifikation". Dies ist gleichzeitig auch der LDAP-Anzeigename. Unter Attribute-ID wird die eindeutige OID angegeben. Das Attribut *oMSyntax* bestimmt zusammen mit der Attribute-Syntax die zulässige Syntax des Attributs. Die Attribut-Syntax 2.5.5.3 besagt, dass es sich um eine Zeichenkette handelt, bei der zwischen Groß- und Kleinschreibung unterschieden wird. Eine Übersicht aller gültigen Attribut-Syntax-Werte sowie *oMSyntax*-Werte finden Sie unter

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/ad/syntaxes_for_active_directory_attributes.asp

Außerdem handelt es sich um ein Attribut, das mehrere Werte besitzen kann. Nachdem die obligatorischen Werte angegeben worden sind, müssen die neuen Inhalte ins Active Directory geschrieben werden. Hierzu wird die *SetInfo*-Methode benutzt.

```
adsAttribute.SetInfo
```

Nach dem Speichern der obligatorischen Attribute können Sie noch einige optionale Attribute festlegen. Hierzu werden über *GetInfo* zunächst die bestehenden Informationen ausgelesen. Danach werden optionale Attribute hinzugefügt.

```
adsAttribute.GetInfo
adsAttribute.Description = "Zeigt die Qualifikationen an"
adsAttribute.Put "rangeLower", 1
adsAttribute.Put "rangeUpper", 100
adsAttribute.Put "searchFlags", True
adsAttribute.Put "isMemberOfPartialAttributeSet", True
adsAttribute.SetInfo
```

Dem Attribut wird nun eine Beschreibung hinzugefügt. Außerdem wird angegeben, dass die erlaubte Länge dieses Attributs zwischen 1 und 100 Zeichen liegen muss. Der Eintrag *searchFlags* legt fest, dass das Attribut für die schnelle Suche indiziert werden soll. Danach wird zusätzlich festgelegt, dass das Attribut in den globalen Katalog aufgenommen werden soll. Zum Schluss werden diese optionalen Informationen über *SetInfo* ebenfalls in das Active Directory aufgenommen.

Erstellen einer neuen Klasse

Nachdem das neue Attribut erstellt worden ist, soll dieses einer neuen strukturellen Klasse namens *Consulting* hinzugefügt und zusätzlich an alle Benutzerklassen vererbt werden. Zunächst wird wieder die Verbindung zum Schema-Container hergestellt und die neue Klasse angelegt.

```
dim adsClass
dim adsSchemaContainer
set adsSchemaContainer = GetObject("LDAP://cn=Schema,
cn=Configuration,dc=firma,dc=de")
Set adsClass = adsSchemaContainer.Create("classSchema", "cn=Consulting")
```

Dann werden die obligatorischen Attribute dieser Klasse festgelegt.

```
adsClass.Put "cn", "Consulting"
adsClass.Put "LDAPDisplayName", "Consulting"
adsClass.Put "governsID", "1.2.840.113556.1.4.7000.21"
adsClass.Put "objectClassCategory", 1
adsClass.Put "subClassOf", "user"
adsClass.SetInfo
```

Der gemeinsame und LDAP-Anzeigename lauten *Consulting*. Die OID wird gemäß der firmeninternen OID-Struktur vergeben. Der Wert 1 der *objectClassCategory* zeigt an, dass es sich um eine strukturelle Klasse handelt (siehe Tabelle 24.1). Schließlich wird festgelegt, dass die neue Klasse eine untergeordnete Klasse von Usern sein soll. Danach werden die Informationen ins Verzeichnis geschrieben. Anschließend werden die optionalen Attribute festgelegt.

```
adsClass.GetInfo  
adsClass.Description = "Benutzer des Bereichs Consulting"  
adsClass.Put "mustContain", "1.2.840.113556.1.4.7000.144"  
adsClass.SetInfo
```

Hier wird der Klasse eine Beschreibung zugewiesen sowie festgelegt, dass in dieser Klasse das Attribut *Qualifikation* enthalten sein muss. Hierfür wird die OID dieses Attributs unter *mustContain* angegeben. Auch diese Informationen werden im Verzeichnis gespeichert.

Nachdem Sie das neue Attribut und die neue Klasse angelegt haben, können Sie diese in der mmc ACTIVE DIRECTORY-SCHEMA analysieren, ob alle Einstellungen wie gewünscht übernommen worden sind.

Erstellen von Klasseninstanzen

Sie können nun den Benutzern die notwendigen Informationen hinzufügen, indem Sie Instanzen der neuen Klasse anlegen. Dazu muss zunächst eine Verbindung zu dem Container hergestellt werden, in dem die Instanz erstellt werden soll.

```
dim adsContainer  
dim adsConsulting  
set adsContainer = GetObject("LDAP://ou=test,dc=firma,dc=de")  
In dem OU-Container wird nun ein neuer Benutzer angelegt.  
set adsConsulting = adsContainer.Create("Consulting",  
"cn=PeterMustermann")
```

Diesem Benutzerobjekt werden die obligatorischen Attribute zugewiesen. Neben dem Attribut *Qualifikation* der neuen Klasse *Consulting* müssen auch die Attribute der Klasse *User* angegeben werden, da die Klasse *Consulting* eine untergeordnete Klasse von *User* ist und deshalb auch deren Attribute besitzt.

```
adsConsulting.Put "sAMAccountName", "PeterMustermann"  
adsConsulting.Put "userPrincipalName", "pmustermann@firma.de"  
adsConsulting.Put "Qualifikation", Array("MCP 70-215", "MCP 70-217",  
"MCP 70-086")  
adsConsulting.SetInfo
```

Diese Informationen werden zum Schluss in das Active Directory geschrieben.

32.4.3 Die Windows-GUI modifizieren und erweitern

Nachdem Sie verschiedene Werte für die Qualifikationen der Benutzer per Skript eingepflegt haben, werden Sie feststellen, dass das neue Attribut und seine Informationen nicht in den Eigenschaften der Benutzer in der mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER vorhanden sind. Dies liegt darin begründet, dass nur die Eigenschaften angezeigt werden, die Windows standardmäßig bekannt sind. Es gibt jedoch verschiedene Möglichkeiten, die GUI wunschgemäß anzupassen. So können Sie selbst definierte Registerkarten einfügen, Kontextmenüs erweitern oder sogar eigene Assistenten erstellen. Es ist auch möglich, die GUI durch Skripte zu erweitern.

32.4.4 Display Specifier für Klassen und Attribute

Ein simples Verfahren zum Anpassen der GUI ist das Bearbeiten der Display Specifier (Anzeigebezeichner). Um diese Display Specifier zu betrachten, verwenden Sie das Tool *ADSIEDIT* und öffnen den Knoten *CONFIGURATION CONTAINER/CN=CONFIGURATION, DC=FILIALE,DC=DE/CN=DISPLAYSPECIFIERS*. Dort finden Sie eine lange Liste von durchnummerierten Containern. Jeder Container steht dabei für die Display Specifier einer bestimmten Sprachversion. Container 407 beinhaltet die Einträge für das Gebietsschema Deutschland. In der Detailansicht der mmc sehen Sie sämtliche Objekte der Klasse *DISPLAYSPECIFIER*. Jede Schemaklasse besitzt ihren eigenen Display Specifier, so verwendet z.B. die Klasse *Computer* den *Computer-Display-Specifier* usw.

Soll beispielsweise in der mmc *ACTIVE DIRECTORY-BENUTZER UND -COMPUTER* der Kontextmenüeintrag zum Erstellen neuer Computer geändert werden, so führen Sie folgende Schritte aus:

1. Wählen Sie in der ADSI-mmc die Eigenschaften des Klassenobjekts *CN=COMPUTER-DISPLAY*.
2. Wählen Sie aus der Listbox *SELECT A PROPERTY TO VIEW* den Eintrag *CLASSDISPLAY-NAME*. Im Feld *VALUE* steht der aktuelle Wert *COMPUTER*. Entfernen Sie diesen und geben im Feld *EDIT ATTRIBUTE* einen neuen Wert ein. Fügen Sie diesen über *ADD* hinzu.

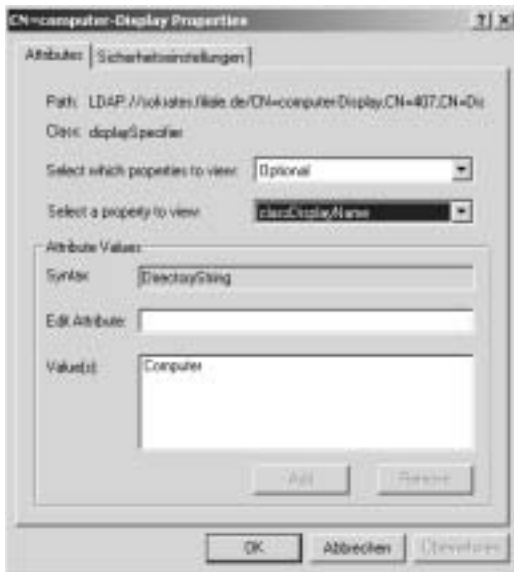


Abbildung 32.2: Der Computer-Display-Specifier

Dieser neue Wert erscheint nun im Kontextmenü *NEU* der mmc *ACTIVE DIRECTORY-BENUTZER UND -COMPUTER*. Diese Einstellungen können Sie für jedes Gebietsschema separat vornehmen.

Selbstverständlich können Sie auch den Anzeigenamen für Attribute ändern. In diesem Fall wählen Sie aus der Listbox SELECT PROPERTY TO VIEW den Eintrag ATTRIBUTEDISPLAY-NAMES. Sie sehen in der Klasse *Computer* eine Reihe von Werten, die in der folgenden Form angegeben sind:

```
...
operatingSystemVersion,Betriebssystemversion
operatingSystem,Betriebssystem
managedBy,verwaltet von
...
```

Der erste Eintrag ist der *IDAPDisplayName*, der zweite Wert repräsentiert den Namen, wie er in der Windows-GUI erscheint. Achten Sie beim Ändern der Werte darauf, dass sich kein Leerzeichen hinter dem Komma befindet. Ansonsten beginnt der Name in der GUI mit einem Leerzeichen. In diesen beiden Beispielen wurde lediglich ein GUI-Eintrag modifiziert, aber es wurden noch nicht neue Elemente hinzugefügt.

32.4.5 Erweitern der Kontextmenüs

Die Einträge in den Kontextmenüs können nicht nur geändert, sondern auch durch zusätzliche Einträge erweitert werden. Über die neuen Erweiterungen kann ein COM-Objekt aufgerufen werden oder aber auch ein Skript oder eine beliebige andere ausführbare Datei.

Um das Kontextmenü zu erweitern, wählen Sie unter *ADSIEDIT* den gewünschten Display Specifier und in dessen Eigenschaften aus der Listbox SELECT A PROPERTY TO VIEW den Eintrag ADMINCONTEXTMENU. Soll die Benutzeroberfläche angepasst werden, so wählen Sie stattdessen SHELLCONTEXTMENU. Um ein zusätzliches COM-Objekt einzubinden, geben Sie dessen UUID (Universally Unique Identifier) in der folgenden Form an:

```
1,{5a96f2d8-736e-11d1-bd0d-00c004fd8d5b6}
```

Achten Sie beim Erstellen des COM-Objekts darauf, dass dieses die Schnittstellen *IShellExtInit* sowie *IContextMenu* unterstützt. Andernfalls wird das Einbinden fehlschlagen. Die Zahl gibt die Position des Objekts an, und in den geschweiften Klammern steht die UUID. Nach dem Komma darf kein Leerzeichen folgen.

Wollen Sie ein Skript oder eine andere ausführbare Datei aufrufen, so geben Sie die Werte in der folgenden Form an:

```
1,zusätzliches &Skript, d:\Skript.vbs
2,zusätzliches &Programm, d:\Programm.exe
```

Auch hier gibt die Zahl die Position an. Der zweite Wert entspricht der Zeichenkette, die neu in das Kontextmenü oder in die Benutzeroberfläche aufgenommen wird. Das "&"-Zeichen aktiviert den folgenden Buchstaben für die Windows-Schnellansicht. Das Einbinden eines Skriptes ist sinnvoll, wenn Sie die Angaben der selbst definierten Schemaattribute für den Administrator und andere Benutzer sichtbar machen möchten. Wollen Sie aus dem Kontextmenü jedes Benutzers eine Übersicht über seine Qualifikationen erhalten, so fügen Sie unter CONTEXTMENU folgenden Wert ein:

```
1,&Qualifikation, d:\Qualifikation.vbs
```

Das Skript *Qualifikation.vbs* stellt eine Verbindung zum neu erstellten Attribut *Qualifikation* her, liest die Werte aus und zeigt in einer eigenen Messagebox die hinterlegten Qualifikationen des Benutzers an.

```
set wshArgs = Wscript.Arguments
set adsUser = GetObject(wshArgs(0))
MsgBox adsUser.Qualifikation,,"Qualifikation"
```

32.4.6 Definieren eigener Registerkarten

Sie haben auch die Möglichkeit, die standardmäßig vorhandenen Registerkarten, z.B. die Eigenschaften von Objekten, durch selbst definierte Registerkarten zu ersetzen. Die neuen Registerkarten müssen Sie zunächst in einer beliebigen Programmiersprache anlegen. Dabei ist wichtig, die neue Registerkarte als COM-Objekt anzulegen, sodass sie die beiden Schnittstellen *IShellExitInit* sowie *IShellPropSheetExt* unterstützt. Diesem COM-Objekt müssen Sie eine eindeutige UUID zuweisen.

Um die neue Registerkarte beispielsweise den Computerobjekten zuzuweisen, wählen Sie unter *ADSIEDIT* den Display Specifier der Computer-Klasse. Je nachdem, ob Sie die Administratoroberfläche und/oder die Shell anpassen möchten, wählen Sie den Eintrag *ADMINPROPERTYPAGES* oder *SHELLPROPERTYPAGES* aus der Listbox *SELECT A PROPERTY TO VIEW*. Beide Attribute speichern die Werte in der folgenden Form:

```
2,{6dfe6488-a212-11d0-bcd5-00c004fd8d5b6}
1,{5a96f2d8-736e-11d1-bd0d-00c004fd8d5b6}
```

Dabei gibt die Zahl die Position der Registerkarte an. Die Registerkarte wird durch die UUID angegeben. Um die Reihenfolge bestehender Registerkarten zu ändern, müssen Sie lediglich die neuen Positionsangaben setzen. Wollen Sie auch Ihre eigenen Registerkarten hinzufügen, so müssen Sie lediglich in einer neuen Zeile die Position sowie die UUID der Karte angeben. Damit wurde die Registerkarte dem Objekt hinzugefügt.

32.4.7 Anlegen selbst definierter Assistenten

Sie haben nicht nur die Möglichkeit, zusätzliche Registerkarten zu Objekten hinzuzufügen, Sie können sogar die Assistenten individuell anpassen, mit denen Benutzer oder Benutzergruppen in der mmc *ACTIVE DIRECTORY-BENUTZER UND -COMPUTER* erstellt werden. Diesen Assistenten können Sie wahlweise durch zusätzliche Fenster erweitern oder komplett durch eigene Fenster ersetzen. Die neuen Seiten des Assistenten werden wie die neuen Registerkarten als COM-Objekte angelegt. Diese müssen die Schnittstelle *IDsAdminWizExt* unterstützen. Die Anpassung des Assistenten kann notwendig werden, wenn Sie beispielsweise den Benutzerobjekten das selbst definierte verbindliche Attribut *Qualifikation* hinzugefügt haben. Beim Anlegen der Benutzer wird diese zusätzliche Angabe abgefragt, die der Standard-Assistent nicht kennt.

Sie müssen sich entscheiden, ob Sie den kompletten Assistenten durch einen neuen ersetzen oder ob Sie lediglich die betreffende Seite hinzufügen möchten, auf der das zusätzliche Attribut seinen Wert erhalten soll.

Wollen Sie für die Benutzererstellung einen komplett neuen Assistenten erstellen, so wählen Sie den User-Display Specifier und dort aus der Listbox SELECT A PROPERTY TO VIEW den Eintrag CREATEDIALOG. Geben Sie dort die UUID des COM-Objekts an. Bei einem neuen Assistenten spricht man auch von einer primären Erweiterung. Wollen Sie hingegen nur eine zusätzliche Seite zu einem bestehenden Assistenten hinzufügen, so wählen Sie den Eintrag CREATEWIZARDEXT. Die Werte sind hier in derselben Form wie bei den Registerkarten angegeben. Passen Sie also die Reihenfolge der einzelnen Fenster an und fügen die UUID der neuen Seite(n) hinzu.

32.4.8 Container und Endknotenobjekte

Schließlich können Sie auch wählen, ob ein Objekt als Container oder Endknotenobjekt (Leaf) dargestellt werden soll. Standardmäßig werden einige Objekte als Endknotenobjekt dargestellt, obwohl Sie untergeordnete Objekte besitzen. Ein klassisches Beispiel dafür sind Computerobjekte in der mmc ACTIVE DIRECTORY-BENUTZER UND -COMPUTER, an die im Active Directory veröffentlichte Drucker angeschlossen sind. Diese werden dennoch als Endknoten dargestellt.

Wollen Sie diese Darstellungsweise ändern, so wählen Sie im Display Specifier der gewünschten Klasse aus der Listbox SELECT A PROPERTY TO VIEW den Eintrag TREAT ASLEAF und setzen diesen auf TRUE oder FALSE. Bei True wird das Objekt als Endknotenobjekt angezeigt, bei False als Container.

33 Auflistung der erwähnten RFCs

Hier finden Sie zunächst eine Auflistung aller RFCs (Request for Comments), die die Standards für Windows 2000 Server und Active Directory beschreiben. Danach erfolgt eine Aufzählung der RFCs, auf die in diesem Buch verwiesen wurde, mit ihrer jeweiligen Nummer und dem Titel. Alle hier genannten RFCs befinden sich auf der mitgelieferten CD.

Insgesamt gibt es über 3200 RFCs. Eine Übersicht über alle RFCs finden Sie unter der Adresse www.ietf.org.

33.1 Standards für Windows 2000/2003 sowie Active Directory

Active Directory unterstützt die in den folgenden RFCs definierten Standards:

RFC	Titel	Standard
2251	Lightweight Directory Access Protocol (v3)	LDAP Version 3
1777	Lightweight Directory Access Protocol	LDAP, C', Verzeichnis-API
2247	Using Domains in LDAP/X.500 Distinguished Names	LDAP und Schema
2252	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions	
2256	A Summary of the X.500(96) User Schema for use with LDAPv3	
2052	A DNS RR for specifying the location of services (DNS SRV)	Dynamisches DNS
2136	Dynamic Updates in the Domain Name System (DNS UPDATE)	
2131	Dynamic Host Configuration Protocol	DHCP
791	Internet Protocol	TCP/IP
793	Transmission Control Protocol	
1769	Simple Network Time Protocol (SNTP)	Simple Network Time Protocol
ISO-Norm		X.509 v3 Public Key
1510	The Kerberos Network Authentication Service (V5)	MIT v5 Kerberos-Authentifizierung
Entwurf		LDIF zur Verzeichnis-synchronisierung

Tabelle 33.1: Die RFC-Standards des Active Directory

33.2 In diesem Buch referenzierte RFCs

Teil A

Kapitel 1.2.1

- ▶ RFC 1487: X.500 Lightweight Directory Access Protocol
- ▶ RFC 1777: Lightweight Directory Access Protocol
- ▶ RFC 2251: Lightweight Directory Access Protocol (v3)
- ▶ RFC 2252: Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions
- ▶ RFC 2253: Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names
- ▶ RFC 2254: The String Representation of LDAP Search Filters
- ▶ RFC 2255: The LDAP URL Format
- ▶ RFC 2256: A Summary of the X.500(96) User Schema for use with LDAPv3

Kapitel 3.8.1

- ▶ RFC 1823: The LDAP Application Program Interface

Teil B

Kapitel 5.4.3

- ▶ RFC 1542: Clarifications and Extensions for the Bootstrap Protocol

Kapitel 6.1.2

- ▶ RFC 1779: A String Representation of Distinguished Names
- ▶ RFC 2044: UTF-8, a transformation format of Unicode and ISO 10646

Teil C

Kapitel 16.1

- ▶ RFC 1034: Domain names – concepts and facilities
- ▶ RFC 1035: Domain names – implementation and specification

Kapitel 16.4

- ▶ RFC 2052: A DNS RR for specifying the location of services (DNS SRV)
- ▶ RFC 2136: Dynamic Updates in the Domain Name System (DNS Update)

Kapitel 16.4.1

- ▶ RFC 2136: Dynamic Updates in the Domain Name System (DNS Update)
- ▶ RFC 2137: Secure Domain Name System (Dynamic Update)

Kapitel 16.6.4

- ▶ RFC 2136: Dynamic Updates in the Domain Name System (DNS Update)
- ▶ RFC 2052: A DNS RR for specifying the location of services (DNS SRV)

Kapitel 25.1

- ▶ RFC 2045: Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies

Kapitel 27.3.3

- ▶ RFC 2052: A DNS RR for specifying the location of services (DNS SRV)
- ▶ RFC 2136: Dynamic Updates in the Domain Name System (DNS Update)

Kapitel 29.8

- ▶ RFC 2052: A DNS RR for specifying the location of services (DNS SRV)
- ▶ RFC 2136: Dynamic Updates in the Domain Name System (DNS Update)

Kapitel 29.8.2

- ▶ RFC 1995: Incremental Zone Transfer in DNS

34 Verweise auf weitere Programme

In diesem Kapitel finden Sie eine Auflistung sämtlicher Produkte und Programme sowie deren Hersteller, auf die in diesem Buch verwiesen wurde. Diese Produkte erweitern teils den Funktionsumfang von Active Directory, teils stellen sie verbesserte Administrationswerkzeuge bereit. Um schneller die gewünschten Informationen zu finden, ist jeweils ein Link zu der betreffenden Internet-Seite hinzugefügt.

Teil A

Kapitel 3.8.5

Microsoft Directory Synchronization Services (MSDSS)

<http://www.microsoft.com/windows2000/techinfo/interop/msdssimp.asp>

Teil B

Kapitel 4.2

NetVision Synchronicity 3.5

<http://netvision.com/products/sywhatsnew.html>

Microsoft Metadirectory Services (MMS) 2.2

<http://www.microsoft.com/windows2000/technologies/directory/mms/default.asp>

Kapitel 5.3

Microsoft Solution Framework (MSF)

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/tandp/innsol/msfrl/default.asp>

Kapitel 6.1.7

Verisign

<http://www.verisign.com>

Kapitel 6.2.1

Novell Z.E.N. Works

<http://www.novell.com/products/zenworks/>

Novell DirXML

<http://www.novell.com/products/edirectory/dirxml/>

Teil C

Kapitel 18.3.5

Aelita Software Domain Migration Wizard

<http://www.aelita.com/products/DMW.htm>

Kapitel 20.2.6

Aelita Software Enterprise Directory Manager (EDM)

<http://www.aelita.com/products/EDM4.htm>

Kapitel 20.5.1

Wise Package Studio Version 3

<http://www.wise.com/wps.asp>

Installshield AdminStudio

<http://www.installshield.com/isas/>

Kapitel 21.6.2

Aelita Software ERDisk for Active Directory

<http://www.aelita.com/products/erdisk.htm>

Veritas Backup Exec

<http://www.veritas.com/products/category/ProductDetail.jhtml?productId=bews>

Computer Associates BrightStor ARCserve Backup

<http://www3.ca.com/Solutions/ProductFamily.asp?ID=115>

Kapitel 21.6.3

NetIQ: Directory and Resource Manager

<http://www.netiq.com/products/dra/default.asp>

Aelitas Software ERDisk for Active Directory

<http://www.aelita.com/products/erdisk.htm>

Veritas Backup Exec

<http://www.veritas.com/products/category/ProductDetail.jhtml?productId=bews>

Kapitel 21.10.3

Microsoft Operation Manager (MOM)

www.microsoft.com/MOM/default.asp

Kapitel 24.3.5

Aelitas Software ERDisk for Active Directory

<http://www.aelita.com/products/erdisk.htm>

Kapitel 26

Microsoft Visio und Visio Enterprise Tools (VENT)

<http://www.microsoft.com/office/visio/default.asp>

Kapitel 27.2.4

Microsoft SysPrep

<http://www.microsoft.com/windows2000/downloads/tools/sysprep/default.asp>

PowerQuest SIDchanger

<http://www.powerquest.com/deploycenter/>

Kapitel 27.5.4

Aelita Software, Domain Migration Wizard

<http://www.aelita.com/products/DMW.htm>

NetIQ, Domain Migration Administrator

<http://www.netiq.com/products/dma/default.asp>

BindView, bv-Admin for Windows 2000 Migration

<http://www.bindview.com/products/admin/winmig.cfm>

Quest Software, FastLane Migrator

www.quest.com/fastlane/migrator/

Kapitel 27.6

Aelita Software, Domain Migration Wizard

<http://www.aelita.com/products/DMW.htm>

Kapitel 27.8.1

Aelita Software, Domain Migration Wizard

<http://www.aelita.com/products/DMW.htm>

Kapitel 29.2

Microsoft Services for Unix 3.0

<http://www.microsoft.com/windows/sfu/default.asp>

Kapitel 29.3

CSS-Solutions, AD4Unix

<http://www.css-solutions.ca/ad4unix/>

Kapitel 29.10

HiResolution Software, MacAdmin

http://www.hi-resolution.com/products_admin_overview.html

Kapitel 30.2

Microsoft Identity Integration Server 2003

<http://www.microsoft.com/windows2000/server/evaluation/features/miisoview2003.asp>

Kapitel 31.1.1

Foundstone, Fport

<http://www.foundstone.com/knowledge/proddesc/fport.html>

Active Ports, Freeware

35 Glossar

A

Abstraktes Schema: Das abstrakte Schema beinhaltet eine Untermenge der Schemaklassen und -attribute, die für den schnellen Abfragezugriff optimiert sind. Das abstrakte Schema kann nicht geändert werden. Es wird auch als das Objekt „Aggregate“ bezeichnet.

Access Control Entry: siehe ACE.

Access Control List: siehe ACL.

ACE: Access Control Entry. Ein ACE muss in der ACL für eine Ressource vorhanden sein, damit einem Benutzer Zugriff auf diese Ressource gewährt werden kann. Der ACE beinhaltet die Berechtigungen sowie die SID für den Benutzer.

ACL: Access Control List/Zugriffssteuerungsliste. Für jedes Objekt wird eine ACL erstellt, die aus verschiedenen ACE-Einträgen besteht. Es gibt DACLs, die die Zugriffsberechtigungen für ein Objekt enthalten, sowie SACLs, die das Auditing für den Objektzugriff überwachen.

Active Directory: Der auf LDAP basierende Verzeichnisdienst unter Windows 2000/2003 Server. Active Directory ermöglicht über eine Anmeldung den Zugriff auf sämtliche Ressourcen des Verzeichnisses. Zudem vereinfacht Active Directory die Administration der Netzwerkobjekte.

Active Directory-Anwendungsmodus: siehe ADAM.

Active Directory-Installations-Assistent: Nach Abschluss der Installation von Windows 2000/2003 Server wird mit diesem Assistenten das Active Directory installiert und dadurch der Server zum Domänencontroller. Der Assistent wird auch zur Deinstallation verwendet.

Active Directory Service Interfaces: siehe ADSI.

Active Directory-Benutzer und -Computer: Eine Konsole zur Administration der Benutzer, Gruppen, Computer, OUs, Kontakte, Drucker sowie Freigaben. Diese mmc kann über den Befehl `dsa.msc` aufgerufen werden.

Active Directory-Domänen und Vertrauensstellungen: Eine Konsole zur Administration der Vertrauensstellungen zwischen verschiedenen Domänen (Windows NT/2000/2003-Domänen sowie Kerberos V5-Bereiche).

Active Directory Migration Tool: siehe ADMT.

Active Directory-Schema: Das Schema beschreibt alle Klassen und Attribute, die im Active Directory vorhanden sind. Das Schema ist durch eigene Klassen und Attribute erweiterbar. Der Zugriff auf Schemaobjekte wird auch über ACLs gesteuert.

Active Directory-Support-Tools: Ein Konglomerat von Programmen zur Vereinfachung und Erweiterung der Verwaltung des Betriebssystems. Ein Teil dieser Programme ist für die AD-Verwaltung nutzbar. Diese sind im Lieferumfang von Windows 2000/2003 Server enthalten.

Active Directory-Standorte und -Dienste: Über diese Konsole werden die Standorte konfiguriert und Replikationseinstellungen vorgenommen.

Active Directory-Verwaltung: Diese neue mmc des Windows Server 2003 bietet eine zentrale Verwaltungsmöglichkeit. In dieser mmc sind die mmcs Active Directory-Benutzer und -Computer, -Standorte und -Dienste, -Domänen und -Vertrauensstellungen sowie die DNS-mmc enthalten.

AD: Allgemeine Abkürzung für Active Directory.

ADAM: Active Directory-Anwendungsmodus/AD Application Mode. ADAM ist ein eigenständiger Verzeichnisdienst für die Zusammenarbeit mit verzeichnisdienstfähigen Applikationen. Es werden dort lediglich die applikationsbezogenen Informationen gespeichert, nicht jedoch die des Active Directory selbst. Der Zugriff geschieht über LDAP oder SSL.

ADAM-Instanz: In einer ADAM-Instanz befinden sich die lokale Kopie des ADAM-Verzeichnisdienstes sowie der damit verknüpfte Speicher, die Zugriffsports für LDAP und SSL und die Logdatei. Auf einem Server können gleichzeitig mehrere Instanzen ausgeführt werden.

ADMT: Active Directory Migration Tool. Mit diesem Programm können Sie die Migration von Objekten einer NT-Domäne in eine Active Directory-Domäne planen und durchführen. Die aktuelle Version ist ADMT 2.0.

ADSI: Active Directory Service Interfaces. ADSI ist ein Satz von COM-Objekten und Schnittstellen, womit Applikationen für das Active Directory entwickelt werden können. Über ADSI können beliebige Windows-Clients auf Verzeichnisdienste, z.B. das Active Directory, zugreifen. Über ADSI-Objekte können auch administrative Aufgaben durchgeführt werden.

ADSI-Clients: ADSI-Clients stehen für Windows NT und Windows 9.x zur Verfügung. Hiermit stehen diesen Clients Grundfunktionalitäten der Active Directory-Features zur Verfügung.

ADSI-Skripte: Diese Skripte werden zur Administration des Active Directory verwendet. Dafür steht eine große Anzahl an ADSI-Schnittstellen zur Verfügung.

Aggregate: Objektname für das abstrakte Schema.

Aktualisierungsintervall: Dieses Intervall bestimmt, wie oft die sekundären Master einer Zone ihre Zonendaten mit der Zonenquelle auf Aktualität hin abgleichen. Das Intervall wird im SOA-Ressourceneintrag jeder Zone festgelegt.

Anwendungsverzeichnispartition: siehe Applikationspartition.

Applikationspartition: Unter Windows Server 2003 wird dieser neue Typ einer Verzeichnispaltung bereitgestellt. Applikationspartitionen speichern anwendungsspezifische Daten, die auch dynamisch sein können. Es können dort alle Typen von Daten bis auf Sicherheitsprincipals gespeichert werden. Die Inhalte der Applikationspartitionen werden nicht in den globalen Katalog repliziert. Unter Windows Server 2000 gibt es noch keine Applikationspartitionen.

Arbeitsgruppe: Zusammenschluss von Computern zur gemeinsamen Nutzung von Ressourcen. Dabei erfolgt jedoch keine zentrale Authentifizierung wie in einer Domäne.

Architekturplan: In der Designphase des Projekts wird die Architektur aller AD-bezogenen Komponenten wie Domänenstruktur, DNS, Standorte oder Hardware-Anforderungen festgelegt.

Attribut: Attribute sind Eigenschaften der Verzeichnisobjekte. Die Objekte werden durch die Attributwerte beschrieben. Attribute können einen oder mehrere Werte beinhalten. Anstatt des Begriffs Attribut wird oft auch Eigenschaft verwendet.

Ausführen als: Ein Dienst, über den es ermöglicht wird, ein bestimmtes Programm mit Administratorrechten von einem beliebigen Konto aus auszuführen, sofern das Admin-Passwort bekannt ist. Dafür ist keine Neuanmeldung unter Windows erforderlich.

Ausgebende Aktualisierung: Hiermit werden alle Änderungen an den USNs von Objekten bezeichnet, die der Domänencontroller selbst oder eine mit ihm verbundene Applikation durchführt. Dieser Vorgang wird auch als Originating Update bezeichnet.

Authentifizierung: Bei der Anmeldung werden der Benutzername und das Kennwort mit den Einträgen in einer autorisierten Liste verglichen. Sind die Daten gültig, kann sich der Benutzer anmelden und erhält die festgelegten Berechtigungen. Im Active Directory erfolgt die Authentifizierung an einem beliebigen Domänencontroller.

Autorenmodus: Im Autorenmodus erstellte mmcs gestatten den Vollzugriff auf die Konsole. Es können Snap-Ins hinzugefügt und entfernt oder neue Fenster erstellt werden. Im Benutzermodus erstellte Konsolen sind eingeschränkt.

Autorisierende Wiederherstellung: Mit NTDSUTIL kann das gesamte Active Directory oder Teile daraus von einem Backup wiederhergestellt werden. Dabei werden Objekte als autorisierend markiert, indem ihre USN heraufgesetzt wird. Diese wiederhergestellten Objekte ersetzen vorhandene Objekte. Dieses Verfahren wird angewendet, wenn vorhandene Objekte fehlerhaft sind.

Autoritätsursprung: siehe SOA-Ressourceneintrag.

AXFR: vollständige Zonenübertragung. Diese wird durchgeführt, wenn ein neuer sekundärer DNS-Server hinzugefügt wird. Dabei bezieht dieser die komplette Kopie der Ressourceneinträge des primären DNS-Servers. Die vollständige Zonenübertragung wird im Gegensatz zur inkrementellen Zonenübertragung von sämtlichen DNS-Servern unterstützt.

B

BackOffice-Server: siehe Microsoft BackOffice-Server.

Backup Domain Controller: siehe BDC.

Basisverzeichnis: Ein Ordner mit Dateien und Programmen, der für einen oder mehrere Benutzer freigegeben ist. Das Basisverzeichnis kann als Standardordner für Öffnen/Speichern festgelegt werden.

BDC: Backup Domain Controller / Sicherungsdomänencontroller. In einer Windows NT-Domäne gibt es einen PDC und beliebig viele BDCs mit einer Datenbankkopie des PDC. BDCs können auch Benutzer authentifizieren. Unter Windows 2000/2003 gibt es nur gleichberechtigte Domänencontroller. BDCs können in einer 2000/2003-Domäne betrieben werden, solange diese im gemischten Modus ausgeführt wird.

Benachrichtigungsliste: Liste auf dem primären DNS-Server mit den Einträgen der IP-Adressen sekundärer Server, die bei Änderungen an der Zone benachrichtigt werden sollen.

Benutzerdefinierte Konsolen: Es können neben den vordefinierten Konsolen auch eigene Konsolen erstellt werden, die beliebige Snap-Ins beinhalten.

Benutzergruppe: siehe Gruppe.

Benutzerkonto: In einem Benutzerkonto werden benutzerspezifische Angaben wie Anmeldename, Kennwort, Anmeldezeiten, Gruppenmitgliedschaft, Berechtigungen usw. zusammengefasst.

Benutzermodus: Im Benutzermodus erstellte Konsolen können im Gegensatz zu Konsolen im Autorenmodus eingeschränkt werden, sodass keine Snap-Ins hinzugefügt oder entfernt werden können. Diese Konsolen eignen sich, um sie für bestimmte Aufgaben an Benutzer zu verteilen.

Benutzername: Der Benutzername kennzeichnet eindeutig einen Benutzer innerhalb einer Domäne oder Arbeitsgruppe.

Benutzerprofil: Fest vorgegebenes Profil, das bei der Benutzeranmeldung Einstellungen wie Bildschirmeinstellungen, Ansichtsoptionen oder Druckereinstellungen lädt. Benutzerprofile können lokal oder servergespeichert vorliegen.

Benutzerrechte: Diese Rechte können einzelnen Benutzern oder Gruppen zugewiesen werden. Sie sind in den Gruppenrichtlinien festgelegt und umfassen Einstellungen wie Herunterfahren des Systems usw.

Berechtigung: Für jedes Objekt kann festgelegt werden, welche Benutzer und Gruppen welche Zugriffsberechtigungen besitzen. Die Berechtigungen sind in der ACL jedes Objekts hinterlegt.

Berechtigungsvererbung: Dabei werden sämtliche Berechtigungen eines Containers an alle untergeordneten Container weitergegeben. Die Vererbung kann an beliebiger Hierarchieebene auch wieder unterbrochen werden.

Bereichsabschnitt: der linke Abschnitt jeder mmc. Dort werden der Name des Snap-Ins sowie alle untergeordneten Snap-Ins in einer Baumstruktur angezeigt.

Besitzer: Der Besitzer eines Objekts kann die Berechtigungen für dieses Objekt bearbeiten und weiteren Benutzern Zugriff erteilen.

Betriebsführungshandbuch: Dieses Handbuch sollte in der Designphase erstellt werden. Es enthält alle Anweisungen und Details, die für den späteren täglichen Betrieb des Active Directory notwendig sind.

Betriebsführungskonzept: In diesem Konzept werden Zieldefinition des Active Directory-Projekts, benötigte Ressourcen und Zuständigkeiten definiert.

Betriebsmaster: Es gibt insgesamt fünf Betriebsmasterrollen. Die beiden Betriebsmaster der Gesamtstruktur sind der Schemamaster und der Domännennamen-Master, die drei der Domänenstruktur der PDC-Emulator, der RID-Master sowie der Infrastrukturmaster. Die Betriebsmaster werden auch als FSMOs bezeichnet.

Betriebsmodus: Windows 2000-Domänen können im einheitlichen und gemischten Betriebsmodus betrieben werden, Windows 2003-Domänen zusätzlich im .NET-Betriebsmodus.

Bidirektionale Vertrauensstellung: Innerhalb einer Windows 2000/2003-Gesamtstruktur sind alle impliziten transitiven Vertrauensstellungen bidirektional. Sie vertrauen sich gegenseitig und können Authentifizierungsanfragen in beide Richtungen austauschen. Auch verknüpfte Vertrauensstellungen sind bidirektional.

Bridgehead-Server: Dies ist der Domänencontroller an einem Standort, der bevorzugt alle Replikationsinformationen bezieht, sofern mehrere Domänencontroller am Standort vorhanden sind.

C

Cache: a) DNS-Cache: Im DNS-Cache werden lokal alle kürzlich aufgelösten Namen von Hosts gespeichert. Durch das lokale Vorhalten dieser Informationen wird die Anfragezeit optimiert.

b) Login-Cache: Steht für die Anmeldung kein Domänencontroller zur Verfügung, so kann über den Login-Cache dennoch eine Anmeldung an der Domäne erfolgen. In diesem Cache sind die letzten zehn erfolgreichen Anmeldungen enthalten.

CACLS: Befehlszeilendienstprogramm zum Bearbeiten der DACLs für Dateien und Ordner.

Client: Clients sind sämtliche Computer, die eine Verbindung zu einem anderen Computer (Server) herstellen und von diesem Dienste anfordern. Im Active Directory können Clients unter Windows 2000 oder XP betrieben werden, mithilfe des ADSI-Clients auch unter Windows NT und 9x.

CN: Common Name. Alle Objekte des Active Directory besitzen ein Namensattribut, den Common Name, aus dem der relativ definierte Name (RDN) des Objekts gebildet wird. Ein Benutzer mit dem CN=Peter Mustermann könnte den definierten Namen CN=Peter Mustermann,DC=Firma,DC=DE besitzen.

Computerkonto: In einer Domäne trägt jedes Computerkonto einen eindeutigen Namen, über den der Computer eindeutig bestimmt wird.

Containerobjekt: Objekt im Active Directory, das weitere untergeordnete Objekte beherbergt, z.B. eine OU mit Benutzern und Computern. Gegenteil zu Endknotenobjekt / Leaf.

D

DACL: Discretionary Access Control List. Die DACL ist ein Bestandteil der ACL. In der DACL werden die Zugriffsberechtigungen für ein Objekt beschrieben.

Dateireplikationsdienst: Wird auch als FRS (File Replication Service) bezeichnet. Über den Dateireplikationsdienst wird die Replikation zwischen Domänencontrollern und globalen Katalogservern durchgeführt.

Datenbankdatei: Der physische Speicherort des Active Directory ist die Datenbankdatei NTDS.DIT. Diese befindet sich standardmäßig im Verzeichnis %Systemroot%\NTDS.

Datenbankschicht: Im Architekturmodell des Active Directory ist die Datenbankschicht von den oberen Schichten getrennt, damit kein direkter Zugriff auf die Extensible Storage Engine (ESE) erfolgen kann.

Datenträgerkontingent: Über Datenträgerkontingente können Sie festlegen, wie viel Speicherplatz einem Benutzer maximal zur Verfügung steht. Datenträgerkontingente können nur unter NTFS eingerichtet werden. Sie müssen bereits vorhanden sein, bevor die Benutzer auf dem Datenträger Daten speichern.

DCPROMO: Rufen Sie DCPROMO an der Eingabeaufforderung oder unter „Ausführen“ auf, um den Installations- oder Deinstallationsassistenten für das Active Directory zu starten.

DDNS: Dynamisches DNS. Im DDNS können sich Clients, die eine dynamische IP-Adresse besitzen, direkt am DNS-Server registrieren und die DNS-Tabelle aktualisieren. In einer reinen DDNS-Umgebung (ab Windows 2000 einsetzbar) sind WINS-Server überflüssig.

Definierter Name: Der definierte Name (oft auch als DN oder distinguished Name bezeichnet) wird für jedes Objekt in dem Format CN=Objektname,DC=Domäne, DC=Domäne angegeben. Ein vollständiger DN eines Computerkontos wäre z.B. hippokrates.firma.de. Der DN ist grundsätzlich eindeutig. Zusätzlich gibt er die Position des Objekts innerhalb des Active Directory an.

Delegierung: Bei der Übertragung der Verwaltung für einen Teil des Namensraums, z.B. bestimmte Container oder einen Subtree an eine andere Person, Gruppe oder Organisation, spricht man von Delegierung.

Desaster Recovery-Plan: Dieser Plan beinhaltet einerseits Grundlagen zur Erhöhung der Ausfallsicherheit, wie z.B. physische Trennung von DCs oder redundante Netzwerkverbindungen, andererseits auch Pläne und Anleitungen, wie möglichst schnell wieder ein bestimmter Stand hergestellt werden kann.

Designphase: Nach der Planungsphase steht die Designphase. In ihr werden u.a. der Architekturplan des Active Directory entworfen und eine Migrationsstrategie entwickelt.

DFS: Distributed File System / Verteiltes Dateisystem. Ein DFS besteht aus mehreren Freigaben, die sich an physikalisch unterschiedlichen Speicherorten befinden, dem Benutzer aber als eine einzige Freigabe dargestellt werden.

DFS-Stamm: In diesem Container sind die Dateien und DFS-Verknüpfungen enthalten.

DFS-Verknüpfung: Ein DFS-Stamm kann mit freigegebenen Dateien, einem weiteren DFS-Stamm oder einem domänenbasierten Datenträger verknüpft sein. Jede Verknüpfung zeigt auf eine Freigabe.

DHCP: Dynamic Host Configuration Protocol. Über DHCP können Clients IP-Adressen sowie weitere Konfigurationen wie z.B. Routeradressen vom DHCP-Server leasen. Bei der dynamischen Zuweisung von Adressen kann es zu keinen Adresskonflikten kommen.

DHCP-Bereich: Ein Bereich von IP-Adressen, von denen ein DHCP-Client eine Adresse beziehen kann.

DHCP-Client: Der Client least beim Start seines Netzwerks eine IP-Adresse vom DHCP-Server.

DHCP-Server: Der Server stellt IP-Adressbereiche bereit sowie mit den IP-Adressen verknüpfte Konfigurationen und überwacht die Verteilung an die Clients.

Dienstressourceneintrag: siehe SRV-Ressourceneintrag.

Directory System Agent: siehe DSA.

Discretionary Access Control List: siehe DACL.

Distinguished Name: siehe definierter Name.

DN: siehe definierter Name.

DNS: Domain Name Service. Ein hierarchischer Namensdienst, durch den IP-Adressen der Hosts in die benutzerfreundlichen Namen der Hosts konvertiert werden. Das Active Directory-Konzept benutzt DNS.

DNS-Server: Der DNS-Server enthält Teile oder die komplette DNS-Datenbank, auf die die Clients zugreifen, um die Hostnamen für bestimmte IP-Adressen zu erfragen.

Domain Name Service: siehe DNS.

Domäne: Eine Domäne ist ein Verbund von Computern, die über mindestens einen Domänencontroller zur Authentifizierung verfügen. Jede Domäne verfügt über eigene Sicherheitseinstellungen und Vertrauensstellungen zu anderen Domänen. Im Windows NT/2000/2003-Netzwerk bildet die Domäne eine Sicherheits-Grenzlinie. Mehrere Domänenstrukturen können zu einer Gesamtstruktur zusammengefügt werden. Das Active Directory kann beliebig viele Domänen an physikalisch unterschiedlichen Standorten umfassen.

Domäne erster Ebene: Diese Domäne wird auch als Top Level Domain (TLD) bezeichnet. Sie ist die erste Domäne unterhalb des Domänenstamms (.). Domänen erster Ebene sind z.B. .de, .com oder .net.

Domänen zweiter Ebene: Diese Domänen befinden sich hierarchisch unter der TLD. Sie klassifizieren im Internet den Namen von Firmen, z.B. microsoft.com, und können registriert werden. Im Active Directory kann derselbe oder ein anderer Domänenname wie der im Internet registrierte verwendet werden. Domänen zweiter Ebene können theoretisch beliebig viele untergeordnete Domänen dritter, vierter usw. Ebene besitzen.

Domänenbenutzerkonto: Mit diesem Konto kann sich ein Benutzer an der Domäne authentifizieren und auf alle Ressourcen in der Domäne zugreifen, für die er die entsprechenden Berechtigungen besitzt.

Domänencontroller: Im Active Directory wird auf einem Domänencontroller (DC) Windows 2000 oder 2003 Server ausgeführt. Jeder DC verfügt über ein Replikat der Verzeichnisdatenbank. Er besitzt ein Replikat der Domänenpartition seiner Domäne sowie Replikate der Konfigurations- und Schemapartition der Gesamtstruktur. Optional kann er auch den globalen Katalog enthalten. Über den DC erfolgt die Anmeldung und Authentifizierung am Active Directory. Es wird nicht mehr wie im NT-Domänenmodell zwischen PDC und BDC unterschieden, da alle DCs gleichberechtigt sind.

Domänenfunktionsmodus: Unter Windows Server 2003 können Sie für die Domänenstruktur den Betriebsmodus Windows Server 2003 wählen. Standardmäßig befindet sich der Domänenfunktionsmodus im gemischten Modus. Sobald Sie den Windows Server 2003-Modus wählen, werden die zusätzlichen Features innerhalb der Domäne wirksam. Zu dieser Domäne können keine NT/2000-DCs mehr hinzugefügt werden.

Domänenmodell: Das Modell von einer oder mehreren Domänen, die untereinander zur Benutzer- und Ressourcenverwaltung verbunden sind.

Domänennamen-Master: Der Betriebsmaster der Gesamtstruktur, der das Hinzufügen und Entfernen von Domänen in der Gesamtstruktur überwacht. Dieser wird auch als DNS-Master bezeichnet. Es darf in der Gesamtstruktur nur einen Domänennamen-Master geben.

Domänennamespace: Dies ist die vom DNS benutzte Struktur der DNS-Datenbank.

Domänenpartition: In dieser Verzeichnispartition sind die Objekte wie Benutzer, Computer usw. der lokalen Domäne enthalten. Jeder Domänencontroller enthält ein vollständiges Replikat der Domänenpartition seiner Domäne. Er besitzt jedoch keine Replikate der Domänenpartitionen anderer Domänen.

Domänenstruktur: In einer Domänenstruktur (Tree) befinden sich Domänen, die einer Domäne zweiter Ebene hierarchisch untergeordnet sind. Die Domänen verfügen alle über einen fortlaufenden hierarchischen Namensraum. Eine solche Struktur kann etwa die Domäne firma.de sowie untergeordnete Domänen vertrieb.firma.de, marketing.firma.de usw. enthalten. Mehrere Domänenstrukturen können zu einer Gesamtstruktur verbunden werden. Innerhalb einer Domänenstruktur bestehen automatisch Vertrauensstellungen.

Domänenübergreifende lokale Gruppe: Diese Gruppe kann als Mitglieder Benutzer und globale Gruppen aus allen Domänen der Gesamtstruktur sowie universelle und andere lokale Domänengruppen der lokalen Domäne besitzen. Der Zugriff ist nur auf Ressourcen der eigenen Domäne möglich. Diese Gruppen sind nicht im globalen Katalog enthalten. Sie wird auch als lokale Domänengruppe bezeichnet.

DSA: Directory Service Agent. Der DSA ist ein Prozess, der Zugriff auf den physikalischen Speicher für das Active Directory bietet.

Dynamic Host Configuration Protocol: siehe DHCP.

Dynamisches DNS: siehe DDNS.

E

Eigenschaft: Jedes Active Directory-Objekt verfügt über Eigenschaften. Eine Eigenschaft ist ein Wert, der gelesen und geschrieben werden kann.

Eigenschaftsmethode: Diese sind ein Bestandteil der IADs-Schnittstellen. Über die Eigenschaftsmethoden wird auf die Eigenschaft eines Objekts zugegriffen.

Einheitlicher Betriebsmodus: Dieser Modus wird auch als native mode bezeichnet. In diesem Modus können keine NT-BDCs mehr zur Domäne hinzugefügt werden. Der einheitliche Modus ermöglicht zusätzliche Features wie das Einrichten universeller Gruppen oder das Abschalten des NetBIOS-Protokolls.

Einseitige Vertrauensstellung: Bei einseitigen (unidirektionalen) Vertrauensstellungen vertraut Domäne 1 der Domäne 2, aber umgekehrt Domäne 2 nicht Domäne 1. Diese Art der Vertrauensstellung muss immer manuell konfiguriert werden.

Endknotenobjekt: siehe Leaf.

Ereignis: Ein bestimmtes Geschehnis, das vom Betriebssystem oder einer Applikation hervorgerufen wird. Es erfolgt ein Eintrag in das Ereignisprotokoll oder die Benachrichtigung einer administrativen Person.

Erster Master: siehe primärer Master.

Erweiterungs-Snap-Ins: Diese Snap-Ins werden auch als Erweiterungen bezeichnet. Mit Erweiterungen wird der Funktionsumfang eines Snap-Ins vergrößert.

Explizite Vertrauensstellung: Diese wird manuell konfiguriert. Es gibt zwei Arten expliziter Vertrauensstellungen: Externe Vertrauensstellungen sowie verknüpfte Vertrauensstellungen.

Externe Vertrauensstellung: Diese sind eine Form expliziter Vertrauensstellungen. Sie dient zur Authentifizierung von Benutzern einer Domäne außerhalb der Gesamtstruktur. Diese Vertrauensstellungen sind immer unidirektional und transitiv.

F

Firewall: Über eine Firewall wird die direkte Kommunikation zwischen einem internen und externen Netzwerk verhindert, sodass von außen kein unerlaubter Zugriff erfolgen kann. Bei einer Active Directory-Architektur, die durch Firewalls getrennt ist, müssen bestimmte Ports für die Kommunikation zur Replikation und für Vertrauensstellungen freigeschaltet werden.

Flexible Single Master Operations: siehe FSMO.

Forest: siehe Gesamtstruktur.

Forward-Lookup: Eine DNS-Abfrage, bei der die zum Hostnamen des Computers zugehörige IP-Adresse gesucht wird, um auf diesen Host zugreifen zu können.

FQDN: Fully Qualified Domain Name/Vollqualifizierter Domänenname. Er setzt sich aus dem Namen des Objekts sowie den Domännennamen zusammen. Der FQDN gibt immer den hierarchischen Speicherort im Active Directory an. Für ein Computerkonto wird der FQDN z.B. in dem Format hippokrates.firma.de angegeben.

FSMO: Flexible Single Master Operations. Unter diesem Begriff werden die fünf Betriebsmasterrollen der Domänen- bzw. Gesamtstruktur zusammengefasst.

FSMORoleOwner-Attribut: Dieses Attribut speichert den definierten Namen des Servers sowie den Pfad zu diesem Server innerhalb des Active Directory.

G

Garbage Collection: Dieser Vorgang wird alle zwölf Stunden durchgeführt. Es werden alle Objekte endgültig aus der Active Directory-Datenbank gelöscht, deren Tombstone-Eintrag älter als 60 Tage ist.

Gastkonto: Dies ist ein standardmäßig deaktiviertes Benutzerkonto. Dieses Konto sollte über möglichst wenige Berechtigungen verfügen und von Benutzern verwendet werden, die nur zeitweise Zugriff auf das Verzeichnis haben müssen und deshalb kein eigenes Konto in der Domäne besitzen.

Gemischter Betriebsmodus: Dieser Modus wird auch als mixed mode bezeichnet. Nach der Installation des Active Directory befinden sich die Domänen in diesem Modus. Lediglich in diesem Modus können NT-BDCs in der Domäne betrieben werden. Features des einheitlichen Modus sind noch nicht verfügbar.

Gesamtbetriebskosten: siehe TCO.

Gesamtstruktur: Eine Gesamtstruktur wird auch als Forest bezeichnet. Die Gesamtstruktur umfasst sämtliche Domänenstrukturen, die durch transitive Vertrauensstellungen miteinander verbunden sind. Alle Domänenstrukturen innerhalb der Gesamtstruktur verwenden dasselbe Active Directory-Schema und denselben globalen Katalog.

Gesamtstrukturfunktionsmodus: Unter Windows Server 2003 können Sie neben einzelnen Domänen auch die Gesamtstruktur auf den Betriebsmodus Windows Server 2003 heraufstufen. Damit sind die zusätzlichen Features in allen Domänen der Gesamtstruktur verfügbar. Voraussetzung ist, dass sich der Domänenfunktionsmodus aller Domänen mindestens im einheitlichen Modus befindet. Im Windows Server 2003-Modus können lediglich Windows 2003-Domänencontroller betrieben werden.

Global Unique Identifier: siehe GUID.

Globale Gruppe: Globale Gruppen können als Mitglieder Benutzer sowie globale Gruppen der eigenen Domäne haben. Mitglieder globaler Gruppen können auf Ressourcen der kompletten Gesamtstruktur und nicht nur der eigenen Domäne zugreifen. Globale Gruppen erscheinen im globalen Katalog, jedoch nicht ihre Mitglieder.

Globaler Katalog: Der globale Katalog befindet sich auf globalen Katalogservern. In ihm befindet sich eine Replik von jedem Objekt der Gesamtstruktur. Allerdings sind hier zu jedem Objekt nur die wichtigsten Attribute gespeichert, die am häufigsten abgefragt werden. Die Anfrage an den globalen Katalog bringt den definierten Namen als Ergebnis, wenn das gesuchte Attribut nicht enthalten ist. Sobald der definierte Name bekannt ist, verbindet sich der Client oder die Applikation mit einem Domänencontroller, der über ein vollständiges Replikat des Objekts verfügt.

Globaler Katalogserver: Der Katalogserver ist ein Domänencontroller, auf dem sich eine Kopie des globalen Katalogs für die Gesamtstruktur befindet.

GPC: Group Policy Container/Gruppenrichtliniencontainer. Im GPC befinden sich Informationen über ein GPO wie sein Status oder seine Version. Das GPC enthält die Untercontainer für die Richtlinien des GPO. Der GPC bildet die Beschreibung des GPO. Dort sind die Informationen enthalten, die keinen häufigen Änderungen unterworfen sind.

GPMC: Group Policy Management Console. Die GPMC ist eine neue Komponente für Windows Server 2003. Über diese mmc erfolgt eine zentrale Verwaltung aller Aufgaben, die die Gruppenrichtlinien betreffen. Neben der Erstellung und Konfiguration können Einstellungen getestet werden, die Delegation verschiedener Aufgaben ist möglich, und es können WMI-Filter auf die verschiedenen Richtlinien angewendet werden.

GPO: Group Policy Object/Gruppenrichtlinienobjekt. Ein GPO ist eine Zusammenstellung von Richtlinieneinstellungen. GPOs können auf OUs, Domänen und Standorte angewendet werden. Zusätzlich kann auf jedem Computer ein lokales GPO erstellt werden.

GPT: Group Policy Template/Gruppenrichtlinienvorlage. Hier werden die Einstellungen der Richtlinien des GPO gespeichert.

Group Policy Management Console: siehe GPMC.

Gruppe: Es gibt drei Bereiche von Benutzergruppen: globale, domänenübergreifende lokale sowie universelle Gruppen. Zudem werden Gruppen in Sicherheitsgruppen und Verteilergruppen unterteilt. Für Sicherheitsgruppen wird der Ressourcenzugriff konfiguriert, Verteilergruppen werden in E-Mail-Verteilern verwendet. Eine Gruppe kann Benutzer, Computer, weitere Gruppen und Kontakte enthalten.

Gruppenbereich: Es gibt drei verschiedene Gruppenbereiche: globale, domänenübergreifende lokale sowie universelle Gruppen. Für diese Gruppen sind jeweils Mitglieder aus unterschiedlichen Domänen sowie Zugriffsberechtigungen für verschiedene Ressourcen konfigurierbar.

Gruppenkonto: Sämtliche Benutzerkonten, die zu einer Gruppe hinzugefügt sind, verfügen über die Berechtigungen, die für dieses Gruppenkonto definiert sind.

Gruppenmitgliedschaft: Ein Benutzer kann einer oder mehreren Benutzergruppen angehören. Die Summe aller Berechtigungen in den Gruppen, in denen er Mitglied ist, ergibt die effektiven Berechtigungen des Benutzers.

Gruppenrichtlinie: Gruppenrichtlinien können auf Computer und/oder Benutzer angewendet werden. Sie beinhalten mannigfaltige Konfigurationsmöglichkeiten, z.B. Softwareverteilung, Logon-/Logoff-Skripte, IPsec oder Internet Explorer-Einstellungen. Ein Satz von definierten Gruppenrichtlinien wird in einem GPO zusammengefasst.

Gruppenrichtliniencontainer: siehe GPC.

Gruppenrichtlinienobjekt: siehe GPO.

Gruppenrichtlinienvorlage: siehe GPT.

GUID: Global Unique Identifier. Jedes Active Directory-Objekt verfügt über eine eindeutige GUID von 128 Bit. Die GUID ändert sich nicht, wenn ein Objekt umbenannt oder verschoben wird.

H

Herabstufen: Ein Domänencontroller kann über den Active Directory-Installationsassistenten wieder zum Mitgliedsserver herabgestuft werden. Dabei wird auf dem Server die gesamte Active Directory-Datenbank gelöscht.

Heraufstufen: Jeder Mitgliedsserver unter Windows 2000/2003 kann über den Active Directory-Installations-Assistenten zum Domänencontroller heraufgestuft werden. Dabei wird die Datenbank eingerichtet, und der neue DC wird in die bestehende Replikationstopologie eingebunden.

Hierarchischer Namespace: Ein Beispiel dafür ist der DNS-Namensraum. Dieser besitzt eine hierarchische Struktur, die beim Einbinden von Domänen und Objekten eingehalten werden muss.

High Watermark-Vektor: Dieser Vektor gehört zu den Metadaten der Replikation. Beim Erstellen jedes Objekts wird eine USN angelegt (uSN-Created). Über die USN wird gezählt, wie viele Änderungen des Objekts auf dem Domänencontroller durchgeführt wurden. Der USN-Zählerwert der Aktualisierungen wird als High Watermark-Vektor bezeichnet. In diesem Vektor ist jeweils die höchste USN angegeben, die im Active Directory für ein bestimmtes Objekt vorhanden ist.

High Watermark Vektor-Tabelle: Jeder Domänencontroller enthält eine Tabelle mit den High Watermark-Vektoren seiner Replikationspartner. Dies ist die High Watermark Vektor-Tabelle. Dort werden lokale Änderungen der USN sofort eingetragen, sodass diese bei der nächsten Replikation weitergegeben werden kann.

Hostname: Der Hostname ist der Name eines Computers, der vom DNS-Server benutzt wird oder in der Hosts-Datei enthalten ist, damit der Computer gefunden werden kann. Dieser Name kann, aber muss nicht mit dem Computernamen übereinstimmen.

I

IADs-Schnittstelle: Sämtliche ADSI-Objekte unterstützen eine solche Schnittstelle. Diese Schnittstelle garantiert den Zugriff auf verschiedene Verzeichnisse. Jede Schnittstelle verfügt über Methoden und Eigenschaftsmethoden. Es gibt über 40 IADs-Schnittstellen.

Identity Manager: Über die GUI des Identity Managers wird der MIIS 2003 gesteuert und konfiguriert.

Implizite Vertrauensstellung: Hierbei handelt es sich um automatisch eingerichtete transitive, bidirektionale Vertrauensstellungen, sobald eine Domäne zu einer Domänenstruktur oder eine Domänenstruktur in einer Gesamtstruktur erstellt wird.

In-addr.arpa: Dies ist eine spezielle DNS-Domäne auf der obersten Ebene. Sie wird beim reverse Lookup für die Zuordnung von Hostnamen zu IP-Adressen benutzt.

Infrastrukturmaster: Einer der Betriebsmaster der Domänenstruktur. Er aktualisiert Verweise zwischen Benutzern und Gruppen, wenn Mitglieder einer Gruppe umbenannt oder verschoben worden sind. Diese Änderungen repliziert er an die übrigen Domänencontroller der Domäne.

Inkrementelle Zonenübertragung: siehe IXFR.

Integrierte Gruppen: Hierbei handelt es sich um standardmäßig vorhandene Gruppen wie Administrator, Gäste oder Benutzer. Diese Gruppen gehören zum Gruppenbereich domänenübergreifend lokal.

Interdomänen-Schlüssel: Dieser Schlüssel ermöglicht die Kerberos-Authentifizierung von Client und Server über Domänengrenzen innerhalb einer Gesamtstruktur hinweg.

Internetprotokoll: siehe IP.

Intransitive Vertrauensstellung: Diese Vertrauensstellungen müssen manuell eingerichtet werden. Sie beziehen sich lediglich auf zwei Domänen und werden nicht an untergeordnete Domänen weitervererbt. Intransitive Vertrauensstellungen können zwischen Domänen in verschiedenen Gesamtstrukturen eingerichtet werden oder zwischen einer NT und einer Windows 2000/2003-Domäne.

IP: Internetprotokoll. Dieses Protokoll wird unter TCP/IP zum Versenden und Adressieren der IP-Pakete benutzt. Dieses Protokoll garantiert nicht, dass sämtliche Pakete ihr Ziel erreichen bzw. die Pakete in der Reihenfolge des Sendens eintreffen.

IP-Adresse: Eine IP-Adresse besteht aus der Netzwerk-ID und der Host-ID und muss für jeden Knoten im Netzwerk eindeutig sein. Die Adresse ist 32 Bit lang und hat das Format 172.20.20.106.

IP-Replikation: Die IP-Replikation wird bei standortinterner und standortübergreifender Replikation verwendet. Dazu werden RPCs eingesetzt. Die standortübergreifende IP-Replikation benutzt definierbare Zeitpläne.

IPSec: IP-Security. IPSec basiert auf einer Reihe von Internetstandards und gewährleistet verschlüsselten Datenverkehr, der ohne Verschlüsselungsschlüssel nicht gelesen werden kann. Über diesen Schlüssel werden die Nachrichten signiert, sodass erkennbar ist, wenn die Nachricht modifiziert wurde. Zusätzlich ist eine kryptografische Checksumme im Verschlüsselungsschlüssel enthalten.

IXFR: inkrementelle Zonenübertragung. Dieses neue Feature ist ab Windows 2000 verfügbar. Bei Änderungen an der DNS-Datenbank des primären Masters werden lediglich die Änderungen zur Synchronisation an die übrigen DNS-Server übertragen. Dies bedeutet einen Performance-Gewinn gegenüber der vollständigen Zonenübertragung.

J

Jeder: Vordefinierte Windows-Benutzergruppe. Zu dieser Gruppe gehören sämtliche lokalen und Netzwerkbenutzer, die eine Verbindung mit dem Computer hergestellt haben. Dazu zählen auch die Gäste. Aus Sicherheitsaspekten sollte diese Gruppe aus den ACLs schützenswerter Dateien und Ordner entfernt werden.

K

Kanonischer Name: Der kanonische Name eines Objekts entspricht dem definierten Namen, allerdings wird er in einem benutzerfreundlicheren Format angegeben. Der definierte Name CN=Hippokrates,DC=Firma,DC=De wird als kanonischer Name in der Form Firma.de/Hippokrates angegeben.

KCC: Knowledge Consistency Checker / Konsistenzprüfung. Dieser Dienst wird auf sämtlichen Domänencontrollern ausgeführt. Der KCC berechnet automatisch die Replikationstopologie der Domänencontroller innerhalb eines Standorts und fügt neue Domänencontroller in diese Topologie ein. Diese automatisch hergestellten Verbindungen zwischen den Replikationspartnern werden auch als Verbindungsobjekte bezeichnet.

Kerberos V5-Authentifizierungsprotokoll: Standardsicherheitsprotokoll für die Benutzerauthentifizierung. Dabei werden Kennwörter verschlüsselt und nicht im Klartext gesendet.

Klasse: Eine Klasse ist eine formale Beschreibung sämtlicher Objekttypen, die in einem Verzeichnis gespeichert werden können wie z.B. Benutzer oder Gruppen. Die Klasse selbst wird im Active Directory-Schema definiert. Dort dient die Klasse als Vorlage für die Instanzen dieser Klasse. Klassen werden auch als Objektklassen bezeichnet.

Klasseninstanz: Eine Klasseninstanz ist ein spezielles Auftreten einer Klasse. So ist ein Benutzerobjekt mit einem Attribut „P. Mustermann“ eine spezielle Klasseninstanz der Klasse Benutzer. Klasseninstanzen werden auch als Objektklasseninstanzen oder vereinfacht Objekt bezeichnet.

Konfigurationspartition: Jeder Domänencontroller in der Gesamtstruktur verfügt über ein Replikat der Konfigurationspartition. Diese Partition enthält Konfigurationsinformationen wie die Replikationstopologie. Diese Informationen werden innerhalb der Gesamtstruktur repliziert. Somit ist diese Partition für alle Domänencontroller identisch.

Konsistenzprüfung: siehe KCC.

Konsole: In einer Konsole sind Snap-Ins zur Windows-Verwaltung enthalten. Es gibt Konsolen im Autorenmodus und Benutzermodus.

Konsolenmodi: Der Konsolenmodus bestimmt die Zugriffsmöglichkeiten für eine Konsole. Im Autorenmodus erstellte Konsolen besitzen höhere Anpassungs- und Zugriffsmöglichkeiten als im Benutzermodus erstellte Konsolen.

Kontensperrung: Ein Benutzerkonto wird automatisch gesperrt, wenn eine bestimmte Anzahl ungültiger Anmeldungen vorgenommen wurde. Dann ist keine Anmeldung mit diesem Konto mehr möglich. Diese Einstellungen werden über die Sicherheitsrichtlinien festgelegt.

L

L2TP: Layer 2 Tunneling Protocol. Für eine Client-Server-Verbindung wird eine paket-orientierte Point-to-Point-Verbindung durch einen Tunnel benötigt. Es muss sich dabei im Gegensatz zu PPTP nicht um eine IP-Verbindung handeln. Es kann auch ATM, X.25 oder Frame Relay verwendet werden.

Layer 2 Tunneling Protocol: siehe L2TP.

LDAP: Lightweight Directory Access Protocol. Dies ist das Standardzugriffsprotokoll des Active Directory. Active Directory unterstützt die LDAP-Versionen 2 und 3.

LDIF: LDAP Data Interchange Format. Dies ist das Standardformat für Daten in LDAP-konformen Verzeichnissen. LDIF-Dateien ermöglichen eine simple Modifizierung von Verzeichnisdaten und vereinfachen den Im- und Export von Daten zwischen verschiedenen Verzeichnisservern. Eine LDIF-Datei kann ASCII- und Binärdaten enthalten.

LDIFDE: LDIF Data Exchange. Ein Kommandozeilenprogramm, mit dem Objekte zum Bearbeiten aus dem Active Directory exportiert und später wieder importiert werden können. Auch für die Suche von Verzeichnisobjekten kann LDIFDE verwendet werden.

Leaf: Ein Leaf ist ein Endknotenobjekt. Im Gegensatz zu einem Container befinden sich unterhalb eines Endknotens keine weiteren untergeordneten Objekte. Ein Beispiel sind Benutzerobjekte.

Lightweight Directory Access Protocol: siehe LDAP.

Lokale Domänengruppe: siehe domänenübergreifende lokale Gruppe.

Lokale Gruppe: Lokale Gruppen, die unter Windows NT erstellt worden sind, werden nicht im Active Directory angezeigt. Windows 2000 verwendet stattdessen die domänenübergreifenden lokalen Gruppen, die auch im Verzeichnis vorhanden sind.

Lokale Sicherheitsdatenbank: In dieser Datenbank sind die Benutzerkonten sowie die Sicherheitsinformationen zu den Ressourcen des lokalen Computers enthalten.

Lokales Benutzerprofil: Dieses Profil wird automatisch bei der ersten Anmeldung eines Benutzers an einem Windows 2000 / XP-Computer eingerichtet.

Lokales Gruppenrichtlinienobjekt: Jeder Windows 2000 / XP-Computer besitzt ein lokales GPO. Sobald dieser Computer Mitglied einer Active Directory-Domäne wird, kann das lokale GPO durch die Einstellungen der domänenbasierten GPOs außer Kraft gesetzt werden, wenn sich die Einstellungen widersprechen.

M

MAPI: Messaging API. Die MAPI wird vom Active Directory für die Abwärtskompatibilität mit Exchange-Anwendungen benutzt. Neuere Anwendungen sollten ADSI für den Verzeichniszugriff benutzen.

Masterdomäne: Im Windows NT-Domänenmodell beinhaltet die Masterdomäne den PDC sowie die BDCs, die die Anmeldeinformationen verarbeiten. Die Größe der Benutzerdatenbank darf dabei 40 MB nicht überschreiten.

Masterserver: Ein Masterserver ist der DNS-Server für eine bestimmte DNS-Zone. Dabei kann es sich um einen primären oder sekundären Masterserver handeln. Primäre Master besitzen die Zonendaten und können diese ändern. Sekundäre Master besitzen lediglich eine Kopie und empfangen die Änderungen bei einer Zonenübertragung vom primären Master.

Messaging API: siehe MAPI.

Metadaten: Bei der Replikation werden die Namenskontexte (NC) ausgetauscht. Jeder NC besitzt Metadaten, damit die Replikation der erforderlichen Daten durchgeführt werden kann. Zu den Metadaten gehören der High Watermark-Vektor und der Up-to-Dateness-Vektor sowie die jeweils zugehörigen Tabellen.

Metadirectory-Services: Über diese Dienste wird eine Synchronisation aller Informationen vorgenommen, die in verschiedenen Verzeichnisdiensten gespeichert sind. Beispiele für Metadirectory-Services sind MMS und MIIS 2003.

Methode: Methoden sind ein Bestandteil der IADs-Schnittstellen. Sie bestimmen, welche Aktionen an einem bestimmten Objekt durchgeführt werden können. Die möglichen Aktionen sind abhängig vom Objekt.

Microsoft BackOffice-Server: Eine breite Palette von Microsoft-Servern. Dazu zählen z.B. der Exchange, Systems Management, ISA oder Small Business Server.

Microsoft Identity Integration Server 2003: siehe MIIS 2003.

Microsoft Management Console: siehe mmc.

Microsoft Metadirectory Services: siehe MMS.

Migration: Bei der Migration von Windows NT auf Windows 2000/2003 werden im Gegensatz zum Update die Domänen sowie sämtliche darin enthaltenen Objekte neu erstellt. Dabei ist eine Umstrukturierung der Domänen möglich.

MIIS 2003: Microsoft Identity Integration Server 2003. Dies ist die aktuelle Version der Microsoft Metadirectory-Services. Mit MIIS 2003 können Daten aus verschiedenen Verzeichnissen wie z.B. Active Directory, Exchange 2000, Novell eDirectory oder Lotus Notes synchronisiert werden.

Mitgliedsserver: Hierbei handelt es sich um Server, die nicht als Domänencontroller konfiguriert sind. Ein Mitgliedsserver kann wie ein herkömmlicher Client Mitglied in einer Domäne sein. Über DCPROMO können Sie Mitgliedsserver unter Windows 2000/2003 zum Domänencontroller heraufstufen.

Mixed mode: siehe gemischter Betriebsmodus.

mmc: Microsoft Management Console. Windows 2000/XP stellt für diverse Verwaltungsaufgaben verschiedene mmcs mit unterschiedlichen Snap-Ins bereit, die zudem individuell anpassbar und verteilbar sind. Die aktuelle Version der mmc ist Version 1.2.

MMS: Microsoft Metadirectory Services. Die Version 2.2 ist die Vorgängerversion des aktuellen MIIS 2003.

MOVETREE: Kommandozeilenprogramm zum Verschieben von Benutzern, Gruppen (jedoch keine globalen Gruppen) oder OUs zwischen verschiedenen Domänen der Gesamtstruktur.

Multimaster-Replikation: In diesem Modell kann jeder Domänencontroller Änderungen an der Verzeichnisdatenbank vornehmen und diese Änderungen an die übrigen Domänencontroller replizieren. Unter Windows NT besaß lediglich der PDC die Berechtigung zum Durchführen von Änderungen. Die BDCs besaßen nur eine Sicherungskopie.

N

Namensauflösung: Bei diesem Vorgang wird der Name selbst in die zugehörige Information übersetzt, die der Name bezeichnet.

Namenskontext: Der Namenskontext (NC) wird auch als Verzeichnispartment bezeichnet. Der NC ist ein aneinander grenzender Subtree des Active Directory, der an alle Domänencontroller der Gesamtstruktur repliziert wird.

Namensserverressourceneintrag (NS): Über diesen Eintrag im DNS werden die DNS-Namen für die autorisierenden DNS-Server der Domäne festgelegt und gefunden.

Namensraum: Als Namensraum wird ein Verzeichnisdienst wie LDAP, WinNT oder NDS bezeichnet, der eine bestimmte Syntax für seine Namenskonvention verwendet.

Namespace: siehe Namensraum.

Native mode: siehe einheitlicher Betriebsmodus.

NDS: Novell Directory Service. Ein ebenfalls LDAP-konformer Verzeichnisdienst des Herstellers Novell.

.NET-Betriebsmodi: siehe Windows Server 2003-Modus.

NETDOM: Kommandozeilenprogramm zum Verschieben von Computern und Mitgliedsservern zwischen zwei Domänen.

Nicht autorisierende Wiederherstellung: Dabei wird ein Backup der Verzeichnisdatenbank auf dem Domänencontroller eingespielt. Diese Objekte werden nicht als autorisierend markiert, sodass die Objekte bei der nächsten Replikation geändert werden können.

Nicht transitive Vertrauensstellung: siehe intransitive Vertrauensstellung.

Nicht-Containerobjekt: Dieses Objekt kann keine weiteren untergeordneten Objekte enthalten. Diese Objekte werden auch als Endknotenobjekte oder Leafs bezeichnet.

Novell Directory Services: siehe NDS.

NTDS.DIT: Diese Datei ist der physische Speicherort der Active Directory-Datenbank. Dieser Ordner ist im Gegensatz zu SYSVOL nicht freigegeben und bildet einen geschützten Speicherort. Die Dateierweiterung .DIT steht für Directory Information Tree.

NTDSUTIL: Umfangreiches Kommandozeilenprogramm, das u.a. für die Übernahme von Betriebsmasterrollen, die autorisierende Wiederherstellung oder das SID-Management verwendet wird.

NTFS: New Technology File System. Das Standarddateisystem in der Version 5 für Windows 2000 und höher. Im Gegensatz zum FAT/FAT32-Dateisystem bietet NTFS höhere Sicherheitsoptionen.

NTLM-Authentifizierung: Standardauthentifizierungsmethode zwischen Client und Server unter Windows NT. Sobald eine Domäne im einheitlichen Modus ausgeführt wird, kann die NTLM-Authentifizierung deaktiviert und durch die Kerberos-Authentifizierung ersetzt werden.

O

Object Identifier: siehe OID.

Objekt: Das Objekt ist die Basis-Namenseinheit im Active Directory. Objekte sind die Instanzen der Objektklassen, die durch das Active Directory-Schema definiert werden. Unter ADSI bezieht sich der Begriff Objekt auf ein COM-Objekt, das eine oder mehrere Schnittstellen implementiert.

Objektkennung: siehe OID.

Objektklasse: siehe Klasse.

Objektklasseninstanz: siehe Klasseninstanz.

OID: Object Identifier / Objektkennung. Über die OID werden Klassen und Attribute eindeutig identifiziert. Eine OID ist eine durch Punkte getrennte Dezimalzahl, z.B. 1.2.840.113556. Unternehmen und Einzelpersonen können Root-OIDs von einer übergeordneten Instanz beziehen und diese OIDs für selbst definierte Klassen und Attribute verwenden. Die o.g. OID wurde Microsoft zugewiesen.

Ordnerumleitung: Über diese Gruppenrichtlinie können Benutzerordner wie Eigene Dateien oder Desktop an einen Speicherort im Netzwerk weitergeleitet werden. Dies vereinfacht das Backup von Benutzerdaten.

Organisationseinheit: Organisationseinheiten (OUs) werden zur logischen Strukturierung innerhalb von Domänen verwendet. Die OU-Container können aus der übergeordneten Domäne Benutzer, Gruppen, Container und weitere OUs enthalten. Auf OU-Ebene können Gruppenrichtlinien angewendet werden.

Originating Update: siehe ausgehende Aktualisierung.

OU: siehe Organisationseinheit.

P

PDC: Primary Domain Controller / Primärer Domänencontroller. Der PDC ist ein Windows NT Server, der als einziger die Datenbank einer Windows NT-Domäne besitzt, an dieser Änderungen vornehmen kann und für die Authentifizierungen an dieser Domäne zuständig ist. Im Active Directory wird kein PDC benutzt, da alle Domänencontroller gleichberechtigt sind.

PDC-Emulationsmaster: Dieser Betriebsmaster der Domäne wird auch als PDC-Master bezeichnet. Solange sich in der Active Directory-Domäne noch NT-BDCs oder Windows NT/9x-Clients befinden, übernimmt er für diese die Rolle des NT-PDC. So führt er z.B. Kennwortänderungen der Nicht-Active Directory-Clients durch und repliziert diese Änderungen an die BDCs. Jede Domäne darf nur über einen DC-Emulator verfügen.

Pilot: Ein speziell ausgewählter Teil des Unternehmens, z.B. eine bestimmte OU, in der vor dem eigentlichen vollständigen Rollout oder anderen Prozessen dieser unter realistischeren Bedingungen als in der Testumgebung durchgeführt wird.

PKI: Public Key Infrastructure. Dies ist der Oberbegriff für das Sicherheitssystem, bei dem digitale Zertifikate, Zertifizierungsstellen und Zertifikatsserver benutzt werden. Für PKI gibt es zahlreiche Richtlinien und Standards.

Point-to-Point Tunneling-Protocol: siehe PPTP.

PPTP: Point-to-Point Tunneling Protocol. Über eine sichere VPN-Verbindung kann ein Benutzer über das Internet auf ein anderes Netzwerk, z.B. das Firmennetzwerk, zugreifen. Bei PPTP wird der gesamte IP/IPX/NetBEUI-Verkehr in IP-Pakete gekapselt, sodass Remote-Anwendungen ausgeführt werden können, die von einem bestimmten Netzwerkprotokoll abhängig sind.

Primäre Zonendatenbankdatei: Diese Datei befindet sich auf DNS-Servern, die als primärer Master eingerichtet sind. Verwenden Sie Active Directory-integrierte DNS-Zonen, werden die Daten im Active Directory und nicht in einer Zonendatenbankdatei gespeichert.

Primärer Domänencontroller: siehe PDC.

Primärer Master: Primäre Master sind autorisierende DNS-Server für eine Zone. Änderungen werden direkt auf diesen Mastern durchgeführt und bei der Zonenübertragung an die sekundären Master weitergegeben.

ProgID: Damit eine ADSI-Methode auf einen Server zugreifen kann, muss dessen Verzeichnisdienst durch eine eindeutige ProgID gekennzeichnet sein. Gültige ProgIDs sind z.B. LDAP:// oder NDS://.

Public Key Infrastructure: siehe PKI.

R

RDN: Relative distinguished Name/Relativ definierter Name. Der RDN ist der Teil des definierten Namens, der ein bestimmtes Attribut des Objekts bezeichnet. In den meisten Fällen wird der RDN für das Attribut „Allgemeiner Name“ angegeben. Für den definierten Namen CN=Peter Mustermann,CN=Users,DC=Firma,DC=DE lautet der RDN des Namens CN=Peter Mustermann oder für das übergeordnete Objekt CN=Users.

Relativ definierter Name: siehe RDN.

Relative ID: Jeder Domänencontroller verfügt über diverse relative IDs, die ihm vom relativen ID-Master zugewiesen werden. Sämtlichen Benutzer-, Computer- und Gruppenobjekten, die auf einem Domänencontroller erstellt werden, wird eine relative ID des DCs zugewiesen. Diese relative ID ergibt in Kombination mit der Sicherheits-ID der

Domäne die in der Gesamtstruktur eindeutige SID des Objekts. Jeder DC kann vom RID-Master zusätzliche relative IDs anfordern, wenn weitere benötigt werden.

Relativer ID-Master: siehe RID-Master.

Relativer Name: Dieser bildet jeweils einen Teil des DNS-Domänennamens in den Ressourceneinträgen und wird für die Suche in der jeweiligen DNS-Zone verwendet. Der relative Name befindet sich jeweils vor dem Namen der übergeordneten Domäne. Der vollqualifizierte Domänenname (FQDN) setzt sich aus den relativen Namen der jeweiligen DNS-Zone zusammen.

Remote Procedure Calls: siehe RPC.

Repackaging: siehe Repaketierung.

Repaketierung: Für die Softwareverteilung über die Gruppenrichtlinie müssen die Applikationen als Windows Installer-Paket vorliegen. Alle Applikationen, die ein altes Setup-Programm verwenden, müssen zunächst repaketiert werden, z.B. mit WinInstall LE, sodass sie als Windows Installer-Datei vorliegen.

Replicated Update: siehe replizierte Aktualisierung.

Replikation: Im Active Directory wird die Multimaster-Replikation verwendet. Dabei können Änderungen an jeder beliebigen Kopie der Verzeichnisdatenbank auf einem Domänencontroller vorgenommen werden. Diese Änderungen werden bei der Replikation an die Datenbankreplikate auf den übrigen Domänencontrollern weitergegeben und dort ebenfalls gespeichert. So befinden sich sämtliche Replikate immer auf demselben Stand.

Replikationspartner: Ein Domänencontroller, der Replikationsinformationen für einen oder mehrere andere Domänencontroller enthält. Diese führen untereinander die Replikation in der Reihenfolge durch, wie sie vom KCC für die Replikationstopologie berechnet wird.

Replikationstopologie: Diese beschreibt die Reihenfolge (Ringtopologie) der Replikation zwischen den Domänencontrollern an einem Standort. Sie wird vom KCC berechnet.

Replizierte Aktualisierung: Hiermit werden alle Änderungen an den USNs von Objekten bezeichnet, die der Domänencontroller während der Replikation von seinen Replikationspartnern empfängt. Dieser Vorgang wird auch als Replicated Update bezeichnet.

Ressourcendomäne: Im Windows NT-Domänenmodell vorhandene Domänen, die meistens nur eingerichtet wurden, da die Maximalgröße von 40 MB in der Masterdomäne überschritten wurde. Anstelle von Ressourcendomänen sollten im Active Directory OUs eingerichtet werden.

Ressourceneintrag: Diese Einträge befinden sich in der Zonendatenbank der DNS-Server. Sie sind Verknüpfungen zwischen den DNS-Domänennamen und Daten für Netzwerkressourcen. Wichtige Einträge sind Hosteinträge (Zuordnung zwischen Hostname und IP-Adresse), PTR- (Zuordnung zwischen IP-Adresse und Hostname) oder SOA-Einträge (autorisierender DNS-Server der Domäne). Insgesamt gibt es 19 verschiedene Ressourceneinträge.

Reverse-Lookup: Eine DNS-Abfrage, bei der der zur IP-Adresse des Computers zugehörige Hostname gesucht wird. Diese Anfrage durchläuft den umgekehrten Weg wie das Forward-Lookup.

Richtlinie: Richtlinien bestehen aus einer Reihe von Vorgaben, die die Konfiguration des Benutzer-Desktops betreffen. Es können eine oder mehrere Richtlinien eines bestimmten GPO der Gruppenrichtlinien zugewiesen werden.

RID-Master: Relativer ID-Master. Dieser Betriebsmaster der Domäne weist den Domänencontrollern relative IDs zu. Jedes Benutzer-, Computer- und Gruppenobjekt erhält die relative ID des Domänencontrollers, auf dem es erstellt wurde. Zusammen mit der Domänensicherheits-ID, die für alle in der Domäne erstellten Objekte identisch ist, ergibt die relative ID die SID des Objekts. Die SID ist in der Gesamtstruktur eindeutig. In jeder Domäne darf nur ein RID-Master vorhanden sein.

Rollout: Nachdem eine Implementierung vollständig geplant und in einer Testumgebung ausreichend getestet worden ist, erfolgt der Rollout in der produktiven Umgebung. Dabei kann zunächst ein bestimmter Bereich als Pilot für den Rollout definiert werden. Erst wenn dort alles reibungslos funktioniert, kann auch der Rollout in den übrigen Teilen des Unternehmens erfolgen.

RPC: Remote Procedure Call. Bei einem RPC erfolgt über das Netzwerk ein Aufruf an eine bestimmte Softwareprozedur auf einem entfernten Computer.

S

SACL: System Access Control List. Diese ist neben der DACL der zweite Bestandteil von ACLs. Die SACL kontrolliert das Generieren von Audit-Meldungen für die Zugriffsversuche auf das Objekt.

Schema: Das Active Directory-Schema liefert die Definition für jede Klasse und für jedes Attribut, die in der Gesamtstruktur erstellt werden können. Durch diese Definition ist vorgegeben, welche Objekte erstellt werden können. Das Schema kann zusätzlich durch selbst definierte Klassen und Attribute erweitert und somit speziellen Bedürfnissen angepasst werden. Standardmäßig ist das Schema schreibgeschützt.

Schemamaster: Ein Betriebsmaster der Gesamtstruktur. An diesem Master werden sämtliche Änderungen und Aktualisierungen am Schema der Gesamtstruktur vorgenommen. Es darf nur einen Schemamaster in der Gesamtstruktur geben.

Schemapartition: Diese Verzeichnispartition enthält sämtliche Klassen- und Attribut-Schemaobjekte. Die Schemapartition ist auf sämtlichen Domänencontrollern der Gesamtstruktur vorhanden und auf allen identisch.

SDP: Software Deployment Point, siehe Softwareverteilungspunkt.

Security Identifier: siehe SID.

Sekundärer Master: Ein DNS-Server, der lediglich eine schreibgeschützte Kopie der Zonendatenbank besitzt und Änderungen daran nur bei der Zonenübertragung vom primären Master empfängt.

Servergespeichertes Benutzerprofil: Dieses Benutzerprofil wird bei der Anmeldung eines Benutzers vom Server auf den Client geladen. Bei der Abmeldung werden die Änderungen sowohl lokal als auch auf dem Server gespeichert. Ist die lokale Kopie aktueller als die servergespeicherte, so wird die lokale Kopie verwendet.

Services for Macintosh: siehe SFM.

Services for Unix: siehe SFU.

SFM: Services for Macintosh. Diese befinden sich im Lieferumfang des Windows Server 2000/2003 und stellen verschiedene Dienste für die gemeinsame Nutzung von Dateien und Druckern zur Verfügung. Zusätzlich kann der Server als RAS-Server sowie Apple-Talk-Router fungieren.

SFU: Services for Unix. Die SFU erweitern das Active Directory-Schema, sodass eine Kommunikation zwischen Unix und Active Directory möglich wird. Verschiedene SFU-Komponenten ermöglichen Passwortsynchronisierung, Benutzerverwaltung oder gemeinsame Dateifreigaben zwischen beiden Systemen.

Sicherheitsgruppe: Sicherheitsgruppen und Verteilergruppen sind die beiden Gruppentypen im Active Directory. In Sicherheitsgruppen werden die Benutzer für Zugriffsberechtigungen auf Ressourcen zusammengefasst. Es gibt drei Gruppenbereiche für Sicherheitsgruppen: globale Gruppen, domänenübergreifende lokale sowie universelle Gruppen.

Sicherheitsprincipal: Ein Sicherheitsprincipal ist ein Benutzer, eine Gruppe oder ein Dienst auf einem Computer, dem für den Zugriff auf die Ressourcen automatisch eine SID zugewiesen wird.

Sicherheitsprotokoll: In diesem Protokoll werden alle Einträge der Sicherheitsereignisse eingetragen, die in der Überwachungsrichtlinie definiert sind.

Sicherungsdomänencontroller: siehe BDC.

SID: Security Identifier/Sicherheitskennung. Über die SID werden Benutzer, Gruppen und Computer eindeutig identifiziert. SIDs werden zur Zugriffssteuerung in die ACEs von Ressourcen eingetragen. Eine SID setzt sich aus der relativen ID des Domänencontrollers, auf dem das Objekt erstellt wurde, sowie der Sicherheits-ID der Domäne zusammen. Die daraus resultierende SID ist in der Gesamtstruktur eindeutig.

Simple Mail Transport Protocol: siehe SMTP.

Single Sign-on-Strategie: Im Active Directory ist eine Single Sign-on-Strategie möglich, bei der der Benutzer mit einer einzigen Anmeldung Zugriff auf sämtliche Ressourcen und Informationen der Domäne erhalten kann.

Site: siehe Standort.

SMTP-Replikation: Die SMTP-(Simple Mail Transport Protocol-)Replikation wird lediglich für standortübergreifende, nicht jedoch für standortinterne Replikation verwendet. SMTP arbeitet asynchron und ignoriert die definierten Replikationszeitpläne.

Snap-In: Snap-Ins können zu mmcs hinzugefügt werden. Snap-Ins sind für diverse Verwaltungsaufgaben verfügbar. Es gibt eigenständige Snap-Ins, die direkt hinzugefügt werden, und Erweiterungs-Snap-Ins, die die eigenständigen Snap-Ins in ihrer Funktion erweitern.

SOA-Ressourceneintrag: Source of Authority-Eintrag. Dieser Eintrag wird als Erstes beim Erstellen einer neuen DNS-Zone angelegt. Er bezeichnet den DNS-Server, der die autorisierende Quelle innerhalb der Domäne ist.

Softwareinstallation: Die Softwareinstallation ist ein Bestandteil der Gruppenrichtlinien. Über die Softwareinstallation wird richtlinienbasiert das Bereitstellen von Software, die Art der Installation, das Einspielen von Fixes und Updates sowie die Deinstallation geregelt.

Softwareverteilungspunkte: Über einen Softwareverteilungspunkt (SDP) – einen Speicherort im Netzwerk – kann der Benutzer die ihm bei der Softwareinstallation zugewiesenen Applikationen installieren.

Source of Authority: siehe SOA-Ressourceneintrag.

Spezielle Berechtigungen: Die Standardberechtigungen wie Lesen, Schreiben, Vollzugriff usw. setzen sich aus einer Reihe von einzelnen speziellen Berechtigungen zusammen. Um die Berechtigungen für eine Resource feiner abzustimmen, können Benutzern und Gruppen auch einzelne spezielle Berechtigungen zugewiesen werden.

SRV-Ressourceneintrag: Dienstressourceneintrag. Über diesen Eintrag in einer DNS-Zone werden TCP/IP-Dienste registriert und gesucht. Im Active Directory werden diese Einträge für das Auffinden von Domänencontrollern benutzt.

Stammdomäne: Die Stammdomäne befindet sich in der obersten Hierarchieebene und wird durch einen Punkt (.) repräsentiert.

Stand-alone-Server: siehe Mitgliedsserver.

Standardbenutzerprofil: Dieses Profil bildet die Grundlage für weitere Benutzerprofile. Sobald ein neuer Benutzer unter Windows 2000/XP angelegt wird, erhält er zunächst eine Kopie des Standardbenutzerprofils (Default User).

Standort: Ein Standort besteht aus einem oder mehreren gut miteinander verbundenen Subnetzen. Die Standortstruktur spiegelt die physische Struktur des Netzwerks wider. Innerhalb eines Standorts wird die Replikation vom KCC gesteuert. Bei der Anmeldung benutzt Active Directory nach Möglichkeit immer einen Domänencontroller, der sich an demselben Standort wie der Benutzer befindet, um die Authentifizierung zu beschleunigen. Standorte werden auch als Sites bezeichnet.

Standortinterne Replikation: Dies ist der Replikationsverkehr, der zwischen den Domänencontrollern eines Standorts stattfindet. Dabei wird ausschließlich die IP-Replikation verwendet. Die Replikationstopologie wird automatisch vom KCC berechnet.

Standortlizenzenserver: An jedem Standort sollte ein Server konfiguriert werden, der die Client- und Serverlizenzen der Betriebssysteme und Backoffice-Serverprodukte überwacht und verwaltet.

Standortübergreifende Replikation: Dies ist der Replikationsverkehr, der zwischen den Domänencontrollern bzw. den Bridgehead-Servern der Standorte stattfindet. Es kann IP- oder SMTP-Replikation benutzt werden. In der Regel werden Zeitpläne für die standortübergreifende Replikation benutzt.

Standortverknüpfung: In einer Standortverknüpfung zwischen zwei Standorten ist der Zeitplan (Replikationsintervalle und die Replikationsverfügbarkeit) enthalten, nach dem die standortübergreifende Replikation durchgeführt werden soll. Auch die Standortverknüpfungskosten sind in der Verknüpfung enthalten.

Standortverknüpfungsattribute: Jede Standortverknüpfung besitzt drei zu konfigurierende Attribute. Dabei handelt es sich um die Standortverknüpfungskosten, die Replikationsintervalle und die Replikationsverfügbarkeit.

Standortverknüpfungsbrücke: In einer Standortverknüpfungsbrücke werden mehr als zwei Standorte zusammengefasst, die dasselbe Replikationsprotokoll benutzen. Ist das Netzwerk vollständig geroutet, muss diese Brücke nicht manuell eingerichtet werden, da sämtliche Standorte automatisch überbrückt sind. Weitere Brücken können jedoch aus Redundanzgründen hinzugefügt werden.

Standortverknüpfungskosten: Hier wird für jede verfügbare Verbindung zwischen den Standorten ein Kostenfaktor definiert. Bei der Replikation wird die darin als günstigste Verbindung definierte Verbindung genutzt. Erst wenn diese nicht mehr verfügbar ist, wird eine alternative Verbindung benutzt.

Struktur: In einer Struktur verfügen die Domänen über einen fortlaufenden hierarchischen Namensraum. Sie verwenden alle dasselbe Schema, dieselbe Konfiguration und denselben globalen Katalog. Sämtliche Domänen sind über transitive, bidirektionale Vertrauensstellungen miteinander verbunden. Strukturen werden unterschieden in Domänenstrukturen und Gesamtstrukturen.

Support-Tools: Windows 2000/2003 Server stellt eine Reihe von nützlichen Hilfsprogrammen zur Verwaltung von Windows sowie des Active Directory bereit. Diese Programme werden über die Datei adminpak.msi auf der Server-CD installiert.

System Access Control List: siehe SACL.

SYSVOL: SYSVOL ist ein freigegebener Ordner auf jedem Domänencontroller. Darin befinden sich freigegebene Domänendateien wie Skripte und GPOs. Ist dieser Ordner nicht freigegeben, können keine Gruppenrichtlinien angewendet werden. Die Ordnerinhalte werden in demselben Intervall wie die übrige Replikation zwischen den Domänencontrollern repliziert.

T

TCO: Total Cost of Ownership / Gesamtbetriebskosten. Die Gesamtbetriebskosten sind die Summe für finanziellen und zeitlichen Aufwand für Anschaffung von Hard- und Software, Implementierung, Verwaltung, Support, Mitarbeiterschulung usw.

Teildomäne: Teildomänen werden auch als untergeordnete Domänen bezeichnet. Im DNS ist eine Teildomäne hierarchisch direkt unter einer übergeordneten Domäne angeordnet. Die Domäne vertrieb.firma.de ist eine Teildomäne der Domäne firma.de.

Teilstruktur: In einer Struktur kann jeder beliebige Knoten mit allen untergeordneten Knoten eine Teilstruktur darstellen.

Testcenter: Hier wird im Kleinen die produktive Umgebung des Unternehmens abgebildet. Vor dem Rollout muss hier die Implementierung von Active Directory getestet werden.

Testphase: In der Testphase wird ein Testcenter aufgebaut, in dem ein produktives Umfeld aufgebaut wird. Dort wird das Active Directory wie in einer realen Umgebung aufgesetzt und diversen Tests unterzogen. Sind in der Testphase alle aufgetretenen Fehler behoben worden, kann der Rollout beginnen.

TLD: Top Level Domain. Dies sind die Domänen erster Ordnung wie z.B. .de, .com, .net.

Tombstone: Mit dem Tombstone-Flag wird jedes gelöschte Objekt versehen. Es verbleibt aber noch standardmäßig 60 Tage in der Datenbank.

Top: Top ist eine Objektklasse im Active Directory-Schema, von der alle anderen Objektklassen unmittelbar hergeleitet werden.

Top Level Domain: siehe TLD.

Transitive Vertrauensstellung: Sämtliche Vertrauensstellungen innerhalb einer Gesamtstruktur sind transitiv. Transitive Vertrauensstellungen sind grundsätzlich bidirektional. Diese Vertrauensstellungen werden automatisch erstellt, wenn neue Domänen zu einer Domänen- oder Gesamtstruktur hinzugefügt werden. Transitive Vertrauensstellungen sind auf Windows 2000/2003-Domänen beschränkt.

Tree: siehe Domänenstruktur.

Trustee: Ein Trustee ist ein Benutzer- oder Gruppenkonto, für das ein bestimmter ACE gilt. Jeder ACE in einer ACL gilt für einen Trustee.

U

Übergeordnete Domäne: Eine im DNS einer untergeordneten Domäne direkt übergeordnete Domäne. Der Domäne vertrieb.firma.de ist die Domäne firma.de übergeordnet.

Überwachung: Im Sicherheitsprotokoll werden ausgewählte Ereignisse und Vorgänge aufgezeichnet.

Überwachungsrichtlinie: In dieser Richtlinie werden Ereignisse festgelegt, die aufgezeichnet werden und über die der Administrator informiert wird.

Unidirektionale Vertrauensstellung: siehe einseitige Vertrauensstellung.

Universelle Gruppe: Universelle Gruppen können als Mitglieder Benutzer, globale sowie universelle Gruppen aus sämtlichen Domänen der Gesamtstruktur enthalten. Sie selbst können aber nicht Mitglied globaler Gruppen sein. Universelle Gruppen erscheinen im globalen Katalog. Die Mitgliedschaft globaler Gruppen wechselt nicht häufig, nachdem die globalen Gruppen als Mitglieder eingerichtet worden sind.

Untergeordnete Domäne: Eine untergeordnete Domäne befindet sich im DNS direkt unter der übergeordneten Domäne. Die Domäne vertrieb.firma.de ist eine untergeordnete Domäne von firma.de.

Update: Bei einem Update von Windows NT Server auf Windows 2000/2003 Server bleibt die Domäne bestehen, und nur das Betriebssystem wird aktualisiert. Sämtliche Objekte der Domäne bleiben erhalten.

Update Sequence Number: siehe USN.

UPN: User Principal Name. Dieser Name wird zuweilen auch als „friendly name“ eines Benutzers oder einer Gruppe bezeichnet, da er kürzer ist als der definierte Name. Der UPN setzt sich aus dem DNS-Namen der Domänenstruktur zusammen, in der sich der Benutzer befindet, sowie dem Benutzernamen. Beide Komponenten werden durch das Zeichen „@“ getrennt. Ein Beispiel für einen UPN ist pmustermann@firma.de.

Up-to-Dateness-Vektor: Dieser Vektor gehört zu den Metadaten der Replikation. Dieser Vektor gibt den höchsten Wert der höchsten USN an, die durch ausgehende Aktualisierungen erhöht wurde. Zusätzlich wird die GUID des Domänencontrollers angegeben, der die Änderung durchgeführt hat.

Up-to-Dateness-Vektor-Tabelle: In dieser Tabelle sind die Up-to-Dateness-Vektoren aller Replikationspartner enthalten, die mindestens eine ausgehende Aktualisierung durchgeführt haben.

User Principal Name: siehe UPN.

USN: Update Sequence Number. Eine USN ist eine Zahl von 64 Bit Länge. Jedes Active Directory-Objekt erhält beim Erstellen eine USN (uSNCreated). Werden auf einem Domänencontroller Änderungen an einem Objekt vorgenommen, so erhöht sich die USN. Den erhöhten USN-Wert weist der Domänencontroller dem Attribut USNChanged des geänderten Objekts zu. Dieses Attribut wird nicht repliziert und kann auf jedem Domänencontroller unterschiedlich sein.

V

Verbindliches Benutzerprofil: Bei der Anmeldung des Benutzers wird das verbindliche Benutzerprofil geladen. Alle Änderungen, die er an den Desktop-Einstellungen vornimmt, werden nicht übernommen. Lediglich Administratoren können verbindliche Benutzerprofile bearbeiten.

Verbindungsobjekt: Der KCC stellt automatisch Verbindungen zwischen den Domänencontrollern eines Standorts zur Berechnung der Replikationstopologie her. Diese Verbindungen werden als Verbindungsobjekte bezeichnet.

Vererbung: Im Active Directory können Zugriffsberechtigungen vom übergeordneten an untergeordnete Objekte vererbt werden. Diese Vererbung von Berechtigungen kann an beliebiger Stelle der Hierarchie unterbrochen werden. Im Active Directory-Schema bedeutet Vererbung, dass neue Objektklassen von bestehenden Klassen hergeleitet werden können und deren Eigenschaften erben.

Verknüpfte Vertrauensstellung: Diese ist eine Form der expliziten Vertrauensstellungen. Innerhalb einer komplexen Gesamtstruktur kann ein direkter Vertrauenspfad zwischen zwei Domänen eingerichtet werden. Dies verkürzt die Berechnung des Vertrauenspfades über alle Hierarchieebenen der Quell- und Zieldomäne. Eine verknüpfte Vertrauensstellung ist immer bidirektional und transitiv.

Veröffentlichen von Software: Software, die über die Gruppenrichtlinie Softwareinstallation verteilt wird, kann für Benutzer, nicht aber für Computer veröffentlicht werden. Im Gegensatz zu zugewiesener Software werden die Informationen im Active Directory und nicht lokal gespeichert. Die Installation erfolgt, sobald eine Datei die entsprechende Applikation benötigt.

Verteilerguppe: Neben der Sicherheitsgruppe bildet die Verteilergruppe den zweiten Gruppentyp im Active Directory. Der häufigste Einsatz dieser Gruppe sind E-Mail-Verteiler. Verteilergruppen werden nicht wie Sicherheitsgruppen für den Ressourcenzugriff konfiguriert.

Verteiltes Dateisystem: siehe DFS.

Vertrauensstellung: Über Vertrauensstellungen werden Domänen logisch zusammengefasst. Die Domänencontroller können die Authentifizierungen für alle Domänen, zu denen eine Vertrauensstellung besteht, durchführen. Die vertrauende Domäne verfügt über Ressourcen, die vertraute Domäne ist die Anmeldedomäne des Benutzers, der Zugriff für die Ressource wünscht. Benutzer und Gruppen der vertrauten Domäne können in die ACLs sämtlicher Ressourcen der vertrauenden Domäne aufgenommen werden. Vertrauensstellungen werden unterschieden in bi- und unidirektional, implizit und explizit sowie transitiv und intransitiv.

Verzeichnis: In einem Verzeichnis werden Informationen zu Objekten gespeichert. Im Active Directory sind Informationen zu Verzeichnisobjekten wie Benutzern, Computern, Druckern usw. hinterlegt.

Verzeichnisdatenbank: Dies ist ein anderer Name für die Active Directory-Datenbankdatei NTDS.DIT, die den physischen Speicherort der Datenbank bildet.

Verzeichnisdienst: Ein Verzeichnisdienst ist die Quelle für die Verzeichnisinformation und stellt diese Informationen gleichzeitig auch Benutzern und Applikationen bereit. Ein Verzeichnis kann nach speziellen Attributen durchsucht werden, wenn der exakte Name eines Objekts nicht bekannt ist. Der Benutzer erhält eine Liste aller Objekte, die mit seiner Anfrage übereinstimmen. Das Verzeichnis ist optimiert für lesende Zugriffe, da häufiger Informationen angefordert als neue Informationen hinzugefügt werden.

Verzeichnisdienstwiederherstellung: Hierbei handelt es sich um einen besonderen abgesicherten Startmodus für Domänencontroller, in dem die Verzeichnisdatenbank sowie der Ordner SYSVOL wiederhergestellt werden können. Die Wiederherstellung muss lokal an dem gewünschten Domänencontroller durchgeführt werden.

Verzeichnisdienstbasierte Applikation: Eine Applikation, die in einem Verzeichnisdienst gespeicherte Informationen liest, schreibt oder modifiziert.

Verzeichnispartition: Verzeichnispartitionen werden auch als Namenskontext (NC) bezeichnet. Auf jedem Domänencontroller befinden sich mehrere Verzeichnispartitionen, die in der Gesamtstruktur repliziert werden. Unter Windows 2000 besitzt jeder DC eine Schemapartition, eine Konfigurationspartition sowie eine Domänendatenpartition. Der Windows Server 2003 verfügt zusätzlich über Applikationspartitionen.

Verzeichnissystem-Agent: siehe DSA.

Vollqualifizierter Domänenname: siehe FQDN.

Vollständige Zonenübertragung: siehe AXFR.

Vorkonfigurierte Konsolen: Windows 2000 verfügt über einen Satz an vorkonfigurierten Konsolen, die über die Verwaltung aufgerufen werden können. Zusätzlich können benutzerdefinierte Konsolen erstellt werden.

W

Windows Installer: Über den Windows Installer wird die Installation und Deinstallation sowie die Konfiguration (ausgewählte Features) und Reparatur der Applikation gesteuert. Für die Softwareverteilung über die Gruppenrichtlinie müssen die Applikationen als Windows Installer-Datei (msi-Datei) vorliegen.

Windows Internet Naming Service: siehe WINS.

Windows Server 2003-Modus: Der Windows Server 2003 stellt neben dem gemischten und einheitlichen Modus auch diesen Modus bereit. In diesem Modus ist es z.B. möglich, Domänen umzubenennen. Dieser Modus kann für die Domänenstruktur oder auch die Gesamtstruktur angewendet werden. Allerdings dürfen sich keine NT-BDCs und Windows 2000-Domänencontroller in der Domäne bzw. Gesamtstruktur befinden. In der Betaphase wurde dieser Modus noch als .NET-Betriebsmodus bezeichnet.

WINS: Windows Internet Naming Service. Dieser Dienst ist für die Zuordnung von Net-BIOS-Computernamen zu IP-Adressen zuständig. WINS-Server sind für Clients mit Windows NT oder 9x zuständig. Ab Windows 2000 wird standardmäßig DNS zur Namensauflösung benutzt.

X

X.500-Standard: Der X.500-Standard umfasst eine Reihe von Standards, die einen Verzeichnisdienst beschreiben. Diese Standards wurden von der International Organization for Standardization (ISO) entwickelt.

Z

Zeigerressourceneintrag: PTR-Eintrag. Dieser DNS-Ressourceneintrag wird ausschließlich in den Reverse-Lookup-Zonen verwendet. Dieser Eintrag ist das Gegenstück zum Host-Ressourceneintrag. Hier werden die Verknüpfungen zwischen IP-Adresse und Name gespeichert.

Zone: Eine Zone ist im DNS eine Teileinheit der kompletten DNS-Datenbank. Jede Zone enthält die Namensinformationen für eine oder mehrere DNS-Domänen. Die Zone bildet die autorisierende Quelle für alle in ihr enthaltenen DNS-Domännennamen. Jede Zone muss einen zusammenhängenden DNS-Namensraum besitzen. Auf jedem DNS-Server können eine oder mehrere Zonen vorhanden sein. Die Zonen werden unterteilt in Forward-Lookup- sowie Reverse-Lookup-Zonen.

Zonendatenbankdatei: In dieser Datei sind für jede Zone die Zuordnungen von DNS-Namen zu IP-Adressen gespeichert, sofern keine Active Directory-integrierten Zonen verwendet werden. Für jede Zone muss es mindestens einen DNS-Server geben. Dieser

ist der primäre Server dieser Zone und besitzt die primäre Datenbankdatei. Allein an dieser primären Datenbankdatei können Änderungen durchgeführt werden. Sekundäre Server erhalten lediglich eine schreibgeschützte Kopie der Datenbankdatei.

Zonendelegierung: Wenn in einer Domäne eine untergeordnete Domäne erstellt wird, kann die Unterdomäne entweder derselben DNS-Zone angehören wie die übergeordnete Domäne oder einer eigenen Zone. Die neue Domäne kann in die bereits vorhandenen Zoneneinträge integriert oder an eine neue Zone delegiert werden. Bei der Zonendelegierung müssen die SOA-Ressourceneinträge und der Verweis auf den autorisierenden DNS-Server der Zone erstellt werden.

Zonenübertragung: Bei der Zonenübertragung fragt ein sekundärer DNS-Server den primären Server nach Änderungen an der Zonendatenbankdatei ab und synchronisiert diese, sofern Änderungen vorliegen. Beim Hinzufügen eines neuen sekundären Masters findet die vollständige Zonenübertragung (AXFR) statt. Ab Windows 2000 wird für spätere Aktualisierungen die inkrementelle Zonenübertragung (IXFR) benutzt, bei der lediglich die Änderungen übertragen werden.

Zugriffssteuerungsliste: siehe ACL.

Zuweisen von Software: Bei der Softwareinstallation via Gruppenrichtlinie kann Software zugewiesen oder bereitgestellt werden. Zugewiesene Applikationen erscheinen im Startmenü und werden vollständig installiert, sobald die Software das erste Mal benötigt wird. Unter Windows Server 2003 kann auch die gesamte zugewiesene Software bei der ersten Anmeldung des Benutzers komplett installiert werden. Software kann Benutzern und Computern zugewiesen werden.

Zweiseitige Vertrauensstellung: siehe bidirektionale Vertrauensstellung.

Stichwortverzeichnis

A

- A siehe Ressourceneinträge
- Abmeldeskripte 368
- Abstraktes Schema 552
- Abwärtskompatibilität 131
- Access Control Entry 320
- Access Control List 319
- AccessMask 719
- ACE 320
 - Erstellen über ADSI 718
- AceFlags 721
- AceType 722
- ACL 319, 506
 - nach der Migration 611
- ACLDIAG 495
- ACL-Editor 320, 327
- Active Directory
 - Administrative Aufgaben 435
 - Anwendungsmodus 615
 - Architektur 43
 - Attribute 549
 - Backup 445
 - Bedeutung 23
 - Datenbank 149
 - Datenbankdefragmentierung 459
 - Deinstallation 157
 - Deinstallation erzwingen 161
 - Domänen 59
 - Features 45
 - Firewalls 687
 - Installation 145
 - Installation eines Replikats 163
 - Klassen 546
 - Kontingente 461
 - Migration 86, 589
 - netzwerkbasierte Installation 166
 - Objekte 70
 - Organisationseinheiten 68
 - Regelmäßige Aufgaben 464
 - Replikation 71
 - Schema 545
 - Standorte 66
 - Strukturdesign mit Visio 588
 - Strukturen 61
 - Suchfunktion 436
 - Support-Tools 493
 - Überwachung und Sicherheit 471
 - Verwaltungsdelegation 440
 - Visualisierung 581
 - Wiederherstellen 450
 - Zugriffsmechanismen 45
 - Zugriffsüberwachung 473
- Active Directory Connector 78, 93
- Active Directory Migration Tool siehe ADMT
- Active Directory Services Interface 81, 703
- Active Directory Sizer siehe ADSIZER
- Active Directory-integrierte DNS-Zone
 - Vorteile 231
- Active Directory-integrierte Zone 243
 - siehe DNS
- Active Directory-Replikant 163
- Active Directory-Schema 70
 - Attribut 70
 - Klasse 70
- Active Directory-Schichten 43
- Active Server Pages 704
- ActiveX Data Objects 704
- AD/AM 615
 - Einsatzmöglichkeiten 618
 - Funktionsweise 616
 - Installation 620
 - MIIS 674
 - Verwaltungswerkzeuge 626
- AD/AM-Dienst 628
- AD/AM-Instanz 621
 - Verwaltung 627
- AD/AM-Port 629
- AD/AM-Replikation 616
- AD4Unix 641, 647
- ADAM 615
- adamntds.dit 616
- ADAMSetup 626
- Adamuninstall 626
- ADC 93
 - siehe Active Directory Connector
- ADCheck 531
- Administrative Freigaben 331
- Administrative Vorlagen 342, 350
- Administratives Setup 416
- Administrator
 - Sicherheitsaspekte 317
- ADMT 593, 603
 - Features 604
 - Version 2.0 607
 - Voraussetzungen 606
- ADO 704
- ADPREP 166, 398
 - Zusammenspiel mit Windows-Diensten 167
- ADSI 81, 703
- ADSI-Clients 75
- ADSIEDIT 496
 - AD/AM 626
 - Tombstoning bearbeiten 440
- ADSI-OLE-DB-Connector 705

- ADSI-SDK 704
 - ADSI-Skripte 703
 - Benutzerverwaltung 713
 - für Überwachung, Zugriff und Sicherheit 718
 - unter Windows 703
 - Windows-GUI erweitern 729
 - zur Schemaänderung 726
 - ADSIZER 499
 - Aggregate 552
 - Alias siehe Ressourceneinträge
 - Anmeldeskripte 368
 - Anonyme Anmeldung 313
 - Anwendungsentwicklung 141
 - Anwendungsmodus 615
 - Anwendungspartition 56, 159
 - Apple-Authentifizierung 656
 - Arbeitsgruppe 59
 - Architektur
 - Active Directory 40
 - Windows 40
 - Architekturplan 110
 - ASP 704
 - Asset-Management 94
 - Assistenten
 - Über ADSI definieren 732
 - Attribut 70, 549
 - deaktivieren 564
 - Display Specifier 730
 - Erstellen über ADSI 727
 - Flow&Precedence 663
 - hinzufügen 559
 - im globalen Katalog 551
 - indizierte 551
 - Attributprüfung 564
 - Attributtyp 32
 - Ausführen als 317
 - Ausgebende Aktualisierung 255
 - Ausgebender Schreibvorgang 255
 - Authconfig 645
 - Authentifizierte Benutzer 313
 - Authentifizierung
 - ADSI 710
 - Apple-Authentifizierung 656
 - Microsoft UAM-Authentifizierung 657
 - Unix-Authentifizierung am
 - Active Directory 647
 - von MacOS-Clients 655
 - Authentifizierungsverfahren 38
 - Autorisierende Wiederherstellung 452, 522
 - Autoritätsursprung siehe Ressourceneinträge
 - AXFR siehe Zonenübertragungen
- B**
- BackOffice-Server 78, 93
 - Backup
 - des Active Directory 445
 - Domänencontroller-Wiederherstellung 457
 - Gruppenrichtlinien 449
 - Planung 446
 - Wiederherstellen eines Teil-Backups 448
 - Backup-Programme 448
 - Backup-Restore-Flags 203
 - Basisverzeichnisse 309
 - BDC 170, 590
 - Benutzer
 - Anlegen und Löschen über LDIF 578
 - Verschieben zwischen Domänen 609
 - Benutzeranmeldename 290
 - Benutzerattribute 299
 - Ändern 576
 - über ADSI-Skripte ändern 716
 - Benutzergruppe 310
 - ADMT 604
 - Anonyme Anmeldung 313
 - Authentifizierte Benutzer 313
 - domänenübergreifend lokal 311
 - Ersteller-Besitzer 313
 - globale 311
 - Interaktiv 313
 - Jeder 313, 321
 - Migration gleichnamiger
 - NT-Benutzergruppen 608
 - mit besonderer Identität 313
 - Netzwerk 313
 - Planung 314
 - Universelle 311
 - Verschieben zwischen Domänen 609
 - Wählverbindung 313
 - Benutzerkonto 287
 - ADMT 604
 - Anlegen über ADSI-Skripte 714
 - Domänenbenutzerkonten 287
 - Eigenschaften 292
 - Einrichten 289
 - integrierte 288
 - komplexe Konten über ADSI-Skripte
 - anlegen 715
 - lokale 287
 - tägliche Arbeit mit 297
 - Benutzermodus 41
 - Benutzerprofile 301
 - Checkliste zum Einrichten 303
 - lokale 301, 303
 - servergespeicherte 301, 303–304
 - verbindliche 303, 306
 - Benutzerverwaltung
 - über ADSI-Skripte 713
 - Berechtigungen 319
 - eines Objekts mit DSACLs bearbeiten 444
 - Fehlersuche 339
 - Freigabe 328
 - kombinieren 332
 - Prä-Windows 2000-kompatible
 - Berechtigungen 151
 - spezielle 323
 - standardmäßige 320

Berechtigungsvererbung 326
 Probleme bei der Verwaltungsdelegierung 442
 Berkeley Internet Name Domain 223
 Bestandsaufnahme 101
 Betriebsführungshandbuch 134
 Betriebsführungskonzept 134
 Betriebsmaster 175, 447
 Ändern der Rollen 179
 Ausfälle von Betriebsmastern 183
 der Domänenstruktur 176
 der Gesamtstruktur 175
 Standby-Betriebsmaster 178
 Übernahme der Rollen 183
 Verteilen der Rollen 178
 Wiederherstellung 458
 Betriebsmasterrollen 175, 509
 Betriebsmodus 169
 einheitlicher 169–170
 gemischter 169
 Wechsel unter Windows 2000 170
 Windows Server 2003 169
 Windows Server 2003-interims Modus 173
 Bidirektionale Vertrauensstellungen 187
 BIND 223
 Boolesche Operatoren 37
 Bridgehead-Server 119, 275–276
 BurFlags 203

C

CA 122
 CACLS 327
 CDFS 654
 Certificate Authority 122
 Citrix MetaFrame 132
 Citrix WinFrame 132
 Client for NFS 633
 CNAME siehe Ressourceneinträge
 COM 704
 Component Object Model 704
 Computer
 ADMT 605
 Verschieben zwischen Domänen 610
 Computerkonten
 Einrichten 298
 Tägliche Arbeit 298
 Connector Space 662
 Connector-Objekte 663
 Container 24
 über ADSI definieren 733
 Cross-Forest-Authentication 56
 CS 662
 CSVDE 572
 Custom Extensions 663
 Custom Installation Wizard 429

D

DACL 320, 327
 DAP 27
 Data Lineage 664
 Dateiberechtigungen 320
 Dateien
 Zugriffsüberwachung 474
 Datenbankdatei
 Größe 460
 Datenträgerkontingente 332
 dbsutil 629
 DCADMIN
 AD/AM 628
 DCDIAG 501
 Replikationsfehler 279
 DCPROMO 146, 153, 158
 in einer Gesamtstruktur erstellen 155
 über IPsec und Zertifikate 697
 über PPTP 696
 DCPROMO /ADV 165
 DCPROMO /FORCEREMOVAL 161
 DCPROMO.LOG 153
 DDNS 244
 Unix-basierte DNS-Server 651
 DDNS-fähige Clients 244
 Deaktiviert
 Reihenfolge der GPOs 351
 deep and small 136
 DEFAULTSITEIPLINK 208, 212
 Definierter Name 29, 115, 513
 Defragmentierung
 der Active Directory-Datenbank 459
 Offline-Defragmentierung 460
 Online-Defragmentierung 459
 Deinstallation
 des Active Directory 157
 erzwingen 161
 Delegieren der Active Directory-Verwaltung 440
 Disaster-Recovery-Plan 132, 455
 Designphase 86, 88, 109
 DFS 333
 Fehlersuche 339
 DFS-Client 334
 DFS-Ordner 338
 DFS-Replikation 338
 DFS-Stamm 333–334
 DFS-Topologie
 Domänenumbenennung 541
 DFS-Verknüpfung 333, 337
 Diagnostic-Event-Logging 492
 Dienstidentifizierung siehe Ressourceneinträge
 Dienstkonten
 ADMT 605
 Directory Access Protocol siehe DAP
 Directory Information Tree siehe DIT
 Directory Service Restore Mode siehe DSRM
 Directory System Agent siehe DSA
 DirXML 128

- Disconnector-Objekte 663
- Discretionary Access Control List 320
- Display Specifier 730
- Distinguished Name 115
 - siehe definierter Name
- Distributed File System siehe DFS
- DIT 29
 - Aufbau 32
- Dlint 652
- DN 513
 - siehe definierter Name
- DNS 223
 - Debugging 248
 - Fehlersuche 247
 - Fehlerszenarien 251
 - Funktionsweise 223
 - Iteration 228
 - Komponenten 224
 - lokale Abfragen 227
 - Namensgebung 112
 - Namenskonventionen 114
 - Rekursion 228
 - Stammserver 228
- DNS-Abfragen 223, 227
- DNS-Benachrichtigungsliste 243
- DNS-Client 224
- DNSCMD 250, 503
- DNS-Dienst 223
- DNS-Ereignisprotokoll 247
- DNSLint 282
- DNS-Logfile 247
- DNS-Master 178
 - Ändern der Rollen 179
 - siehe Betriebsmaster
- DNS-Modelle
 - planen 594
 - Unix-Server 595
- DNS-Name 148
- DNS-Namensraum 229
- DNS-Registrierungsdiagnose 150
- DNS-Ressourceneinträge 238
- DNS-Server 224, 227
 - Standorte 246
 - Unix-basierte 650
- DNS-Server-Abfragen 228
- DNS-Struktur
 - Vorbereiten der Migration 593
- DNS-Weiterleitungen 241
- DNS-Zonen 229
 - Delegierung 240
- DNS-Zonentypen 231
- DNS-Zonenübertragungen 241
 - Fehler 252
- Domain Name Service siehe DNS
- DOMAINRENAME siehe RENDOM
- Domäne 59
 - Anzahl der Domänen 110
 - durch Firewalls getrennt 701
 - erster Ebene 224
 - Firewallkonfiguration 698
 - Gliederung der Domänen 111
 - Löschen 611
 - Migration als Stammdomäne 601
 - Migrationsmodelle 596
 - übergeordnete 154
 - Umbenennen 467, 533
 - Umbenennen von Domänen 54
 - untergeordnete 153
 - vertrauende 185
 - vertrauenswürdige 185
 - zweiter Ebene 225
- Domänenbenutzerkonto 287
 - Einrichten 289
- Domänenbezeichner 224
- Domänencontroller 59
 - Clientanmeldung nach der Aktualisierung 612
 - Herabstufen 157
 - Installation zusätzlicher
 - Domänencontroller 156, 162
 - letzter Domänencontroller in der Domäne 159
 - Portbelegung 687
 - Synchronisieren der Systemzeit 266
 - Typ des Domänencontrollers 147
 - Überwachungsrichtlinien 472
 - Vorbereitung für Windows Server 2003 166
- Domänencontroller-Wiederherstellung 457
- Domänendaten 198, 221
 - siehe Verzeichnispartition
- Domänenfunktionsebene 173
- Domänenfunktionsmodus
 - Windows Server 2003 171
- Domänenmodell 47–50
- Domänen-Namensraum siehe DNS
- Domänenstamm 224
- Domänenstruktur 147, 602
 - in einer Gesamtstruktur erstellen 155
 - Verwaltungsvorgaben 602
 - Vorbereitung der Migration 591
 - siehe Tree
- Domänenübergreifende lokale Gruppe 311
- Domänenvorbereitung 166
- DOMMON 505
- DSA siehe Directory System Agent
- DSACLs 444, 506
- DSADD QUOTA 461
- DSASTAT 508
- DSMOD QUOTA 463
- DSRM-Passwort siehe
 - Verzeichnisdienstwiederherstellung
- Dumpel 491
- DUMPFMOS 509
- Dynamisches DNS 244
 - Einrichtung 245
 - Fehler 253
 - Unix-basierte DNS-Server 651

E

- Eigenschaftsmethoden 705
- Eigenschafts-USN 259
- Einheitlicher Betriebsmodus 169–170
 - Gruppenzuordnung 315
- Einheitlicher Modus 590
 - Domänenumbenennung 467
- Einseitige Vertrauensstellungen 187
- Einzelmaster 175
- Elogdmp 491
- Endknoten 24
- Endknotenobjekte
 - über ADSI definieren 733
- Ereignisanzeige 491
- Ersteller-Besitzer 313
- Erweiterte Vertrauensstellungen 192
- ESE siehe Extensible Storage Engine
- Exchange 2000 167
- Exchange 5.5 93
- Explizite Vertrauensstellungen 188, 190
- Extensible Storage Engine siehe ESE
- Externe Namensräume 113
- Externe Vertrauensstellungen 188

F

- FAZAM 2000 509
- File Replication Service 284, 450
- Firewalls 687
 - im Active Directory 700
 - Konfiguration für RPC-Aufrufe 690
- Flags
 - ADSI 723
- flat and wide 136
- Forest siehe Gesamtstruktur
- Forward Lookup Funktion siehe DNS
- Forward Lookup-Zone 230, 245
- FQDN 224
- Freigabeberechtigungen 332
- Freigaben 328
 - administrative 331
 - erstellen 330
 - für MacOS-Clients 654
- FRS 284, 450
- FRS-Datenbank 284
- Fully Qualified Domain Name 224

G

- Garbage Collection 440
- Gateway for NFS 633
- Gemischter Betriebsmodus 169
 - Gruppenzuordnung 314
- Gemischter Modus
 - Domänenumbenennung 468
- Generierer der standortübergreifenden Topologie 276
- Gesamtstruktur 147, 599, 602
 - durch Firewalls getrennt 700
 - Export von Objekten 576

- Gesamtstrukturfunktionsmodus
 - Windows Server 2003 172
- Gespeicherte Benutzernamen und Kennwörter 384
- GID 631
- Global Unique Identifier 116, 256
- Globale Gruppen 311
 - vordefinierte 312
- Globaler Katalog 64, 219
 - Attribute 551
 - Betriebsmasterrollen 178
 - Herabstufen 158
 - Inhalt 64
 - Standorte 65
 - Verbesserungen unter Windows Server 2003 220
 - Wiederherstellung 458
- Globaler Katalogserver
 - Occupancy Level 222
 - Replikation 221
- Globally Unique Identifier siehe GUID
- GPC 345
- GPMC 355, 371
 - Administration 373
 - Aufgabendelegierung 400
 - HTML-Berichte 391
 - WMI-Filter 403
- GPO 345
 - Anzahl 359
 - Anzahl der Richtlinien 360
 - Backup 377
 - Bearbeiten 362
 - Bearbeitung 347
 - bei Domänenumbenennung 541
 - Besondere Verarbeitungen 364
 - Domäne 348
 - Erstellen 361
 - Erstellen über die GPMC 374
 - Import und Export 384
 - Inhalte 348
 - Kopieren 383
 - lokales 347
 - Löschen 365
 - Organisationseinheit 348
 - Standort 348
 - Verwaltungsdelegierung 360, 363
 - Wiederherstellung 380
 - Wirksamkeit unter Windows XP 354
 - Zuweisen 366
- GPOTool 511
- GPRESULT 512
- GPT 345
- Group Policy Container siehe GPC
- Group Policy Management Console 355, 371
- Group Policy Object siehe GPO
- Group Policy siehe Gruppenrichtlinien
- Group Policy Template siehe GPC

- Gruppen
 - bearbeiten 316
 - mit besonderer Identität 313
 - Planung 119
 - siehe Benutzergruppen
 - verschachteln 315
- Gruppenbereiche 310–311
- Gruppenmitgliedschaft
 - Probleme nach autorisierender Wiederherstellung 454
- Gruppenrichtlinien 341
 - Abarbeitungsreihenfolge 351
 - Computerkonfiguration 353
 - deaktivieren 363
 - erstellen 358
 - FAZAM 2000 509
 - Fehlersuche 430
 - Grundlagen 341
 - Implementierungsstrategie 359
 - Inkonsistenz nach der Migration 432
 - Ordnerverwaltung 405
 - Planung 119
 - Planung für Organisationseinheiten 369
 - Resultant Set of Policy 355
 - Softwareverwaltung 413
 - Update 343
 - Verarbeitungsreihenfolge 346
- Gruppenrichtliniencontainer siehe GPC
- Gruppenrichtlinienergebnisse 391, 398
- Gruppenrichtlinienmodellierung 391
- Gruppenrichtlinienobjekt siehe GPO
- Gruppenrichtlinienvorlage siehe GPC
- Gruppentypen 310
- Gruppenzuordnung
 - im einheitlichen Betriebsmodus 315
 - im gemischten Betriebsmodus 314
- GUID 24, 116, 256, 513, 556, 690
- GUID2OBJ 513
- H**
 - Hardware 102
 - Hardware Compatibility List (HCL) 103
 - Hashregeln 477
 - HCL siehe Hardware Compatibility List
 - High-Watermark-Vektor 255–256, 261
 - High-Watermark-Vektor-Tabelle 256
 - HINFO siehe Ressourceneinträge
 - Holdback Time 268
 - Host siehe Ressourceneinträge
 - Hostinformationen siehe Ressourceneinträge
 - Hostkennung 226
 - Hostname 225
 - HOSTS-Datei 226
- I**
 - IADs-Schnittstelle 705, 707
 - IADsUser 714
 - Identity Manager 665
 - in-addr.arpa siehe DNS
 - Infrastruktur-Master 167, 178
 - Ändern der Rollen 182
 - siehe Betriebsmaster
 - Install from Media siehe Active Directory-Replikat
 - Installation
 - des Active Directory 145
 - netzwerkbasiert 166
 - Installationsassistent 145
 - INSTMSI.EXE 427
 - INSTMSIW.EXE 427
 - Integrierte Benutzerkonten 288
 - Integrierte Gruppen 312
 - Interaktiv 313
 - Interne Namensräume 113
 - Internetzonenregeln 478
 - Inter-Site Topology Generator 276
 - Intransitive Vertrauensstellung 187
 - IP Security 123
 - IPCONFIG 249
 - IPSec 123
 - ISTG 276
 - Iteration 228
 - IUSR_Computernamen siehe Integrierte Benutzerkonten
 - IWAM_Computernamen siehe Integrierte Benutzerkonten
 - IXFR siehe Zonenübertragungen
- J**
 - Jeder 313, 321
 - Join Rules 671
 - Joiner 684
 - Journal Wrap Condition 286
 - Junction Points 200, 202
- K**
 - Katalogserver 219
 - siehe globaler Katalog
 - KCC 221, 269, 278–279, 617
 - KDC 122
 - KDC-Dienst 57
 - Kein Vorrang 365
 - Reihenfolge der GPOs 351
 - Kennworteigenschaften 294
 - Kennwörter
 - Probleme nach autorisierender Wiederherstellung 455
 - Setzen über LDIF 578
 - Kennwortoptionen 292
 - Kerberos 38, 57, 121, 648
 - Kerberos-Domänen 123
 - Kerberos V5-Authentifizierung 58
 - für Vertrauensstellungen 186
 - Kerberos V5-Protokoll 598
 - Kerberos-Authentifizierung 612
 - Kerberos-Protokoll
 - Konfiguration 487

- Kerberos-Tickets 57
- Kernelmodus 42
- Key Distribution Center 122
- Klartext-Authentifizierung 38
- Klasse 70, 546
 - Attribute 547
 - deaktivieren 564
 - Display Specifier 730
 - Erstellen über ADSI 727
 - hinzufügen 559
- Klasseninstanzen
 - Erstellen über ADSI 729
- Klassenprüfung 564
- Klassentypen 546
- Knowledge Consistency Checker 269, 278–279, 617
- Konfigurationsdaten 198
- Konfigurationsinformationen siehe Verzeichnispartition
- Konsistenzprüfung 269
- Kontextmenü
 - über ADSI erweitern 731
- Kontingente
 - Active Directory-Kontingente 461

L

- LDAP 26
 - LDAP-Entwicklung 26
 - OpenLDAP-Client 643
 - Operationen 35
- LDAP Data Interchange Format siehe LDIF
- LDAP-API 27
- LDAP-Architektur 28
- LDAP-Modelle 30
 - Funktionsmodell 34
 - Informationsmodell 31
 - Namensmodell 32
 - Sicherheitsmodell 38
- LDAP-Standards 27
- LDIF 571
- LDIF-Datei 571
- LDIFDE 572
- LDP 514
 - AD/AM 626
 - Schemaänderungen verifizieren 565
- Leaf 24
 - über ADSI definieren 733
- Leistungsprotokolle 490
- Lightweight Directory Access Protocol siehe LDAP
- LINKD 200
- Linked-Value Replication 265
- Linux 77, 631
- LMHOSTS 590, 593
- Login-Caching 60
- Lokale Benutzerkonten 287
- Lokale Benutzerprofile
 - Probleme mit der SID-History 307
- Lokale DNS-Abfragen 227
- Lokale Gruppen 316

- Lokales Benutzerkonto 291
- Lokales GPO 347
- Loopback 365
 - Reihenfolge der GPOs 351
- LostAndFound 439

M

- MacAdministrator 658
- MacOS 631
- MacOS X-Clients 659
- MacOS-Clients 652
 - Authentifizierung 655
 - Freigaben 654
- Management Agents 662, 666, 680
 - Export 675
 - Import 675
 - Run Profiles 676
 - Update 675
- Masterdomäne siehe Domänenmodelle
- Metadaten der Replikation 255
 - Änderung 257
- Metadirectory 92, 661
 - Zweck 661
- Metadirectory-Services 661
- Metaverse 663, 680
- Metaverse Designer 681
- Metaverse Search 683
- Methoden 705
- Microsoft Directory Synchronization Services 80, 128
- Microsoft Identity Integration Server 661
 - siehe MIIS
- Microsoft Metadirectory Services 94
 - siehe MMS
- Microsoft UAM-Authentifizierung 657
- Microsoft User Authentication Module 653
- Migration 86, 589
 - gleichnamiger NT-Benutzergruppen 608
 - Inkonsistenz von Gruppenrichtlinien 432
 - manuelle Migration 608
 - Migration oder Update 590
 - nach der Migration 611
 - Planung 591
 - Probleme mit der SID-History 307
 - rückgängig machen 605
 - User State Migration Tool 529
 - Vorbereitung 596
 - Vorteile gegenüber einem Update 590
 - Zieldefinition 97
- Migrationsabschluss 141
- Migrationsmodelle für NT-Domänen 596
- Migrationsprozess
 - Migration 86
- Migrationsreihenfolge 129
- Migrationsstrategie 126
- Migrationstabellen 386
 - Aufbau 388
 - Erstellen 390

- Migrationstools 607
- MIIS 661
 - Architektur 662
 - Installation 664
 - Passwortmanagement 674
 - Schema 682
- MIIS 2003 94
- MIIS-Datenbank 664
- Mitgliedsserver
 - durch Firewalls getrennt 702
 - Verschieben zwischen Domänen 610
- mixed mode siehe Betriebsmodus
- mmc
 - Active Directory-Benutzer und Computer 153, 217, 289, 298
 - Active Directory-Domänen und Vertrauensstellungen 153
 - Active Directory-Schema 552
 - Active Directory-Standorte und Dienste 153, 207
 - Active Directory-Verwaltung 153
 - Sicherheitskonfiguration und -analyse 485
 - Verteilen über eine Gruppenrichtlinie 429
- MMS 94, 661
- MOVETREE 516
 - Verschieben von Objekten 438
- MSDSS 80, 128
- msi-Datei 427
- mst-Datei 429
- MS-UAM 653
- Multimaster 175
 - Replikation 71
- MV siehe Metaverse
- N**
- Name Service Provider Interface siehe NSPI
- Namensauflösung 226
- Namenskontext 72
- Namenskonventionen 114
- Namensraum 62, 223, 709
 - fortlaufender 62
 - zusammenhängender 62
- Namensserver siehe Ressourceneinträge
- native mode siehe Betriebsmodus
- NDS 79, 127–128, 704
- NetBEUI 592
- NetBIOS 131, 592
 - Netzwerk ohne NetBIOS 612
- NetBIOS-Name 148, 226
- NetBIOS-Protokoll 170
- NETDIAG 517
- NETDOM 518
 - Verschieben von Objekten 438
- NETLOGON 445
- NetWare 127–128
- Network Information System 637
- Netzwerkdienste
 - Veröffentlichen 435
- NFS 633
- NFS-Server 639
- Nicht autorisierende Wiederherstellung 451
- Nicht transitive Vertrauensstellungen 187
- Nicht-Container siehe Container
- NIS 637
- Novell 127–128, 615
 - MIIS 674
- Novell Directory Services 79
- NS siehe Ressourceneinträge
- NSLOOKUP 249
- NSPI 78
- NT LAN-Manager 75
- NTDS 149, 197
 - Datenobjekt 488
- NTDS.DIT 197, 445
 - Größe 460
 - Offline-Defragmentierung 460
 - Online-Defragmentierung 459
- NTDS-Settings 158
- NTDSUTIL 520
 - Authoritative Restore 522
 - Automatisierung 523
 - Files 522
 - IP Deny List 522
 - Metadata Cleanup 521
 - Roles 521
 - Übernahme der Betriebsmasterrollen 183
- NTFS 654
 - Berechtigungen 320
 - spezielle Berechtigungen 323
- NTFS Journal 286
- NTFS USN-Journal 286
- NTFS-Berechtigungen 332
- NT-LAN-Manager 170
- NTLM 75, 170
- NTLM-Authentifizierung 612
 - für Vertrauensstellungen 186
- NT-Systemrichtlinie 341
- O**
- Object Identifier 556
- Objekt 70
 - Aggregate 552
 - Bearbeiten über Visio 584
 - Connector 663
 - Disconnecter 663
 - Export aus Gesamtstruktur 576
 - Export über Visio 588
 - Import und Export 574
 - Import über Visio 582
 - löschen 439
 - Namensgebung 29
 - Namensregeln für Schema-Objekte 563
 - veröffentlichen 435
 - verschieben 438
 - Zugriff über ADSI 709
 - Zugriffsüberwachung 473

Occupancy-Level 222
Öffentlicher Schlüssel 122
Offline-Defragmentierung 460
Offline-Inhalte von Ordnern 409
OID 556
OLE-Datenbank-Interface 81
OLE-Datenbank-Provider-Schnittstelle 705
Online-Defragmentierung 459
OpenLDAP-Client 643
Ordner
 Offline-Inhalte 409
 Zugriffsüberwachung 474
Ordnerberechtigungen 320
Ordnerumleitung 405
 Probleme unter Windows XP 409
Organisationseinheiten 68, 217
 erstellen 217
 Planung 116
Originating Update 255
OU siehe Organisationseinheiten

P

pam_ldap-Authentifizierung 643, 646
PCNFS 635
PDC 170, 590
 Aktualisierungen während des Updates 598
PDC-Emulator 178
 Ändern der Rollen 182
PDC-Emulator siehe Betriebsmaster
PDC-Emulator-Betriebsmaster 169
Peer-Domänencontroller 147, 170
Perl 81
PERMS 524
Pfadregeln 479
Pilotphase 139
PKI 122
Planungsphase 86–87, 97
Portüberwachung 689
Primäre Standardzone
 Einstellungen siehe DNS
Primäre Zone
 Einstellungen siehe DNS
 siehe DNS
Privater Schlüssel 122
Produktive Umgebung 139
ProgIDs 709
Projection Rules 671
Projektteam 98
PTR siehe Ressourceneinträge
Public Key Infrastructure 122

R

RDN 115, 290
 siehe relativ definierter Name
RedirComp 543
RedirUsr 543
Referral 33

Registerkarten
 über ADSI definieren 732
Rekursion 228
Relativ definierter Name 29, 115, 290
Relative Distinguished Name siehe
 Relativ definierter Name
Relativer ID-Master 170
 siehe Betriebsmaster
RENDOM 467, 532
REPADMIN 525
 Replikationsfehler 279
Repaketierung 428
Replicated Update 256
Replikation 71, 255
 beschleunigen 267
 eines Objekts 260
 erzwingen 525
 Fehler 279
 Fehlerbehebung 283
 globaler Katalogserver 221
 IPSec-Konfiguration 692
 Linked-Value Replication 265
 Metadaten 525
 Multimaster-Replikation 71
 Planung 118
 standortübergreifende 269
 überprüfen 525
 zwischen Standorten konfigurieren 212
Replikationsintervall 271, 277
Replikationskonflikte 279
Replikationskosten 119
Replikationspfad 74
Replikationstopologie 73, 276
Replikationsverfügbarkeit 272
Replikationszeiten
 Bearbeiten 268
Replikationszeitplan 118, 278
Replizierte Aktualisierung 256
Replizierter Schreibvorgang 256
REPLMON 527
RepsFrom 278
RepsTo 278
Request for Comments siehe RFC
Ressourcendomäne siehe Domänenmodelle
Ressourceneinträge siehe DNS-Ressourceneinträge
Resultant Set of Policy 355
Reverse Lookup Funktion siehe DNS
Reverse Lookup-Zone 245
 siehe DNS
REXX 81
RFC 735
Richtlinien zur Softwareeinschränkung 477
 Priorität 481
RID-Master 178
 Ändern der Rollen 182
 siehe Betriebsmaster
Rollout 86, 89, 139–140
Root-DNS-Zone 241

- Root-DSE 34
- RPC-Aufrufe
 - dynamische 697
 - Firewallkonfiguration 690
 - über IPSec 692
- RPC-Ports 690
- RSOP 355, 397
- Rules Extensions 680
- Run Profiles 676
- RUNAS 318
- S**
- SACL 320
- Samba 648
- SASL 38
- Schema 70, 545
 - abstraktes Schema 552
 - Ändern über ADSI-Skripte 726
 - Änderungen 557
 - Änderungen dokumentieren 565
 - Änderungen durchführen 553
 - Bearbeiten über Visio 586
 - Einschränkungen bei der Erweiterung 555
 - Fehlerquellen bei der Änderung 569
 - MIIS 682
 - Objektkategorien 555
 - Verbindungsherstellung über ADSI 726
- Schemaattribute 549
 - deaktivieren 564
 - Erstellen über ADSI 727
 - hinzufügen 559
 - im globalen Katalog 551
 - indizierte 551
- Schemaattributprüfung 564
- Schema-Cache 555
- Schemadaten 198
- Schemadocfile.exe 566
- Schemainformationen siehe Verzeichnispartition
- Schemaklasse 546
 - Attribute 547
 - deaktivieren 564
 - Erstellen über ADSI 727
 - hinzufügen 559
 - Klassentypen 546
- Schemaklassenprüfung 564
- Schemamaster 167, 178
 - Ändern der Rollen 181
 - siehe Betriebsmaster
- Schema-Objekte
 - Namensregeln 563
- SDCHECK 528
- Secure Socket Layer siehe SSL
- Security Identifier 319
- Sekundäre Standardzone
 - Einstellungen siehe DNS
- Sekundäre Zone siehe DNS
- Server for NFS 633
- Server for NIS 637
- Server for PCNFS 635
- Server Message Block siehe SMB
- Serverkonfiguration 145
- Services for Macintosh 653
- Services for Unix 77, 168, 632
- SFM 653
- SFU 77, 632
- Sicherheit
 - Planung 120
- Sicherheitsanalyse 486
- Sicherheitsbereich 476
- Sicherheitsbeschreiber 319
- Sicherheitsgruppe 310
 - siehe Benutzergruppen
- Sicherheitskonfiguration 485
- Sicherheitsrichtlinien 475
- Sicherheitsvorlagen 482
 - Arbeiten mit 483
- Sicherung der Systemstatusdaten 164
- SID 176, 307, 319, 439, 513
 - Migration gleichnamiger NT-Benutzergruppen 608
 - Vorbereiten der Migration 593
- SID-History 307, 439, 593
 - nach der Migration 611
- Simple Authentication and Security Layer siehe SASL
- Single Point of Access 90
- Single Sign-on 90
- Site Link Bridges 273
- SMB 648
- SOA siehe Ressourceneinträge
- Softwareeinschränkung
 - Richtlinien 477
- Softwareeinstellungen 349
- Softwareverteilung 413
 - Aktualisierungen 423
 - Bearbeiten von Paketen 422
 - Bereitstellung von Software 422
 - Installationsoptionen 418
 - Repaketierung 428
 - Strategie 426
 - Zuweisung und Veröffentlichung von Paketen 419
- Softwareverteilungspunkte 416
- Softwareverwaltung 413
- Source of authority siehe Ressourceneinträge
- Spezielle Berechtigungen 323
- SQL Server 2000 664
- SRV siehe Ressourceneinträge
- SRV-Ressourceneinträge 223
- SSL 39
- SSL-Verbindung 39
- Stabilitätspflege 141
- Staging Area 200, 202, 205
 - Verschieben 205
- Stammdomäne 148, 224, 600–601
- Stammserver 228

- Stand-alone-Server 157
- Standardname des ersten Standorts siehe Standort
- Standby-Betriebsmaster siehe Betriebsmaster
- Standort 66, 101, 207
 - Erstellen eines Standorts 208
 - Konfiguration 207
 - Löschen von Serverobjekten 215
 - Netzwerkstruktur 102
 - Planung 117
 - Server als Mitglied mehrerer Standorte 216
 - Server am Standort 215
 - Serverobjekte 215
 - Struktur und Gliederung 102
 - Verschieben von Serverobjekten 216
- Standortlizenzen 213
- Standortübergreifende Replikation 269
- Standortübergreifende Replikationstopologie 276
- Standortverknüpfungen 212
- Standortverknüpfungsattribute 270
- Standortverknüpfungsbrücken 273
- Standortverknüpfungskosten 270
- stunnel-Authentifizierung 646
- Subdomäne 225
- Subnetz 209
 - Anzahl der Hosts 210
 - Erstellen eines neuen Subnetzes 211
- Suche
 - LDAP-Suche 35
- Suchfilter siehe LDAP-Suchfilter
- Suchfunktion im Active Directory 436
- Support-Tools 493
- Synchronisationsmodell 130
 - bidirektional 130
- Syntax
 - LDAP-Syntax 31
- SysPrep 593
- System Access Control List 320
- Systemdatenträger 150, 197–198
- Systemmonitor 488
- Systemrichtlinie 341
- Systemrichtlinien-Editor 343
- Systemstatus
 - Backup 446
- Systemstatusdaten 451
- SYSVOL 150, 197–198, 202, 445
 - manuelles Verschieben 200
 - nicht autorisierende Wiederherstellung 452
 - und Junction Points 200
 - verschieben 199
- sysvol.inf 204
- T**
- TCP/IP-Protokoll 592
- Testcenter 101, 135
- Testmatrix 137
- Testphase 86, 89, 135
- Testserver 135
- Testumgebung 139
- TLD 145
- TLS 39
- Tombstone 439
- Tombstoning 439, 447, 459
- Tombstoning-Intervall 164
- Top-Level-Domain 145
- Transaktions-USN 258
- Transform File siehe mst-Datei
- Transitive Vertrauensstellung 186, 599
- Transport Layer Security siehe TLS
- Tree siehe Domänenstruktur
- Trustee 724
- TsInternetUser siehe Integrierte Benutzerkonten
- U**
- UAM 657
- Übergeordnete Domäne 154
- Überwachung des Active Directory 471
- Überwachungsrichtlinien 471
 - Einrichten 471
 - für Domänencontroller 472
 - für Mitgliedsserver und Clients 473
- UID 631
- Umbenennen einer Windows 2000-Domäne
 - im einheitlichen Modus 467
 - im gemischten Modus 468
- Umbenennen einer Windows 2003-Domäne 467
- Umbenennen von Domänen 467
 - über RENDOM 533
- Unidirektionale Vertrauensstellungen 187
- Universal Group Membership Caching 220
- Universally Unique Identifier 690
- Universelle Gruppen 311
- Unix 77, 127, 631
 - Benutzerverwaltung 631
 - DNS-Server 650
- Unix Password Synchronisation 637
- Unix-Authentifizierung 647
- Untergeordnete Domäne 153
- Update
 - Aktualisierungen auf einem PDC 598
 - Migration oder Update 590
 - Vorbereitung 597
 - Vorteile gegenüber einer Migration 591
- Update Sequence Number 255
 - siehe USN
- UPN 115
- Up-to-Dateness-Vektor 256, 262
- Up-to-Dateness-Vektor-Tabelle 256, 261, 263, 265
- User Name Mapping 636
- User Principal Name 115
- User State Migration Tool 529
- USN 255
 - Eigenschafts-USN 259
 - Transaktions-USN 258
- uSN-Changed 255
- UUID 690
- uUSN-Created 255

V

Variablenpräfixe 712
VBScript 81
Verbundene Datenquelle 662
Verknüpfte Vertrauensstellungen 188
Verteilerguppe siehe Benutzergruppen
Vertrauende Domäne 185
Vertrauenspfad 185
Vertrauensstellung 185
 ADMT 605
 bidirektionale 187
 einseitige 187
 erweiterte unter Windows Server 2003 192
 explizite 188, 190
 externe 188
 Firewallkonfiguration 698
 intransitive 187
 nicht transitive 187
 Probleme nach autorisierender
 Wiederherstellung 455
 transitive 186
 Übersicht 188
 unidirektionale 187
 verknüpfte 188
 Verknüpfung von 192
 zwischen Gesamtstrukturen 54
Vertrauenswürdige Domäne 185
Verwaltungsdelegierung 440
 Assistent 440
 Probleme mit der Berechtigungsvererbung 442
Verzeichnis 24
Verzeichnisdatenbank 24, 197
Verzeichnisdienst 23
Verzeichnisdienstwiederherstellung 453
 Passwort 152
Verzeichnispartition 72
 einer AD/AM-Instanz 628
Verzeichnissystem-Agent siehe DSA
Visio 581
 Bearbeiten des Schemas 586
 Bearbeiten von Objekten 584
 Design einer Active Directory-Umgebung 588
 Export von Objekten 588
 Objektimport 582
Visio 2000 581
Visio 2002 581
Visualisierung der Active Directory-Umgebung 581
Vollqualifizierter Domänenname siehe FQDN
Vordefinierte lokale Gruppen 314

W

Wiederherstellung
 auf geänderter Hardware 458
 autorisierende 452
 autorisierende Wiederherstellung 522
 Betriebsmaster 458
 des Active Directory 450
 Globaler Katalog 458
 nicht autorisierende 451
Windows 2000
 Neuerungen gegenüber Windows NT 51
Windows 2003
 Neuerungen gegenüber Windows 2000 54
Windows Installer 426
Windows NT
 Domänenmodelle 47
 Migration 589
Windows Scripting Host siehe WSH
Windows Server 2003-Betriebsmodus 169
Windows Server 2003-interims-Modus 173
Windows-Einstellungen 349
WinInstall LE 428
WINS 590, 593
WMI-Filter 403
WSH 704

X

X.500 556, 615
X.500-Server 27
X.500-Standard 27

Z

Zeiger siehe Ressourceneinträge
Zeitstempel 259
Zertifikatsdienste 122
Zertifikatsregeln 480
Zertifizierungsstelle 122
Zone siehe DNS-Zone
Zonendatenbankdatei siehe DNS-Zone
Zonentypen 231
Zonenübertragung 241
 inkrementelle siehe DNS
 siehe DNS
 Unix-basierte DNS-Server 652
 vollständige siehe DNS
Zugriffssteuerungsliste 506
 siehe ACL
Zugriffstoken 307
Zugriffsüberwachung
 auf Active Directory-Ressourcen 473
 Drucker 474
Zwischenspeichern 331
 der universellen Gruppenmitgliedschaften 220



Copyright

Daten, Texte, Design und Grafiken dieses eBooks, sowie die eventuell angebotenen eBook-Zusatzdaten sind urheberrechtlich geschützt.

Dieses eBook stellen wir lediglich als **Einzelplatz-Lizenz** zur Verfügung!

Jede andere Verwendung dieses eBooks oder zugehöriger Materialien und Informationen, einschliesslich der Reproduktion, der Weitergabe, des Weitervertriebs, der Platzierung im Internet, in Intranets, in Extranets anderen Websites, der Veränderung, des Weiterverkaufs und der Veröffentlichung bedarf der schriftlichen Genehmigung des Verlags.

Bei Fragen zu diesem Thema wenden Sie sich bitte an:

<mailto:info@pearson.de>

Zusatzdaten

Möglicherweise liegt dem gedruckten Buch eine CD-ROM mit Zusatzdaten bei. Die Zurverfügungstellung dieser Daten auf der Website ist eine freiwillige Leistung des Verlags. Der Rechtsweg ist ausgeschlossen.

Hinweis

Dieses und andere eBooks können Sie rund um die Uhr und legal auf unserer Website



(<http://www.informit.de>)

herunterladen