

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 Verzeichnispartitionen 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-Ordnern	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