

Inhaltsverzeichnis

1	Das Active Directory-Domänenkonzept von Windows Server 2008 R2.....	13
1.1	Bestandteile der Active Directory Domain Services	13
1.2	Forest – Tree – Domain.....	14
1.3	Entstehung des Active Directory-Konzepts	16
1.4	Active Directory-Namenskonventionen	17
2	Gesamtstruktur- und Domänenfunktionsebenen.....	19
2.1	Domänenfunktionsebenen von Windows Server 2008 R2-Domänen.....	19
2.2	Gesamtstrukturfunktionsebenen von Windows Server 2008 R2-Gesamtstrukturen.....	23
3	Aufbau einer Gesamtstruktur	25
3.1	Erster DC in der Gesamtstruktur	25
3.2	Installation eines weiteren DCs in derselben Domäne von einem Medium	30
3.3	Installation einer untergeordneten Domäne	45
3.4	Installation eines neuen Trees (Domäne mit neuem Namespace)	53
3.5	RODC (Read-Only Domain Controllers)	55
3.6	ADDS auf Server Core	78
3.7	Herunterstufen eines Domänencontrollers zu einem Mitgliedsserver.....	78
3.8	Herunterstufen eines Server-Core-DCs	86
4	Interner Aufbau der ADDS-Datenbank	87
4.1	ADDS-Partitionen (ADDS-Namenskontexte)	87
4.2	ADDS-Replikation innerhalb eines Standorts.....	88
4.3	Replikationskontrolle	90
4.4	Replikation von Löschvorgängen	94
4.5	Replikationskonflikte.....	95
4.6	Lingering Objects (Veraltete Objekte, „Zombies“).....	96
5	Globaler Katalog-Server (GC).....	99
5.1	Konfiguration.....	100
5.2	Zwischengespeicherte Anmeldeinformationen.....	102
5.3	Gründe für das Anpassen eines globalen Katalogservers	103
5.4	Richtlinien für die Platzierung globaler Katalogserver.....	103
6	Betriebsmasterrollen in AD-Gesamtstrukturen.....	105
6.1	Schema-Master	107
6.2	Domänennamen-Betriebsmaster.....	110
6.3	RID-Master	111
6.4	PDC-Emulator.....	114
6.5	Zeitserver (SNTP-Server).....	115
6.6	Infrastrukturmaster	118
7	Migration bzw. Update bestehender Gesamtstrukturen.....	121
8	Tools zur Verwaltung von Active Directory	125
8.1	MMC-Snap-Ins.....	125
8.2	Active Directory-Supporttools	127
8.3	ADSIEdit.msc.....	130
8.4	Active Directory Module for Windows PowerShell	133
8.5	Active Directory-Verwaltungszentrum	134
8.6	Active Directory Migration Tool (ADMT).....	134
8.7	Windows Server 2003 Resource Kit.....	134
8.8	Weitere Active Directory-Tools	137
9	LAN-Authentifizierungsprotokolle in Windows-Betriebssystemen	141
9.1	Funktionsweise der LM-Authentifizierung	141
9.2	Funktionsweise der NTLM-Authentifizierung.....	142
9.3	Gruppenrichtlinien zu Authentifizierungsprotokollen	142
9.4	Gruppenrichtlinien für den anonymen Zugriff	144

10 Kerberos-Anmeldung und Ressourcenzugriff	145
10.1 Authentifizierung.....	145
10.2 Autorisierung.....	146
11 Active Directory-integriertes DNS	149
11.1 Active Directory-integrierte DNS-Zonen	149
11.2 Was sind SRV-Ressourceneinträge?.....	151
11.3 Wie Clientcomputer DNS zur Lokalisierung von Domänencontrollern und Diensten verwenden.....	153
11.4 Reverse Lookup-Zonen	154
11.5 Probleme mit der Namensauflösung durch EDNS0.....	157
12 Vertrauensstellungen	159
12.1 Erstellen einer Gesamtstruktur-Vertrauensstellung	159
12.2 Namenssuffixrouting.....	167
12.3 SID-Filter.....	169
12.4 Erstellen einer externen Vertrauensstellung	171
12.5 Erstellen einer Verknüpfungs-Vertrauensstellung.....	177
12.6 Verbindung mit anderer Gesamtstruktur herstellen.....	182
13 Organisationseinheiten (Organizational Units, OUs)	183
13.1 Verwalten von Organisationseinheiten mit ds-Befehlszeilenprogrammen.....	183
13.2 OU hinzufügen mit Ldifde	184
13.3 OU hinzufügen mit Windows Scripting Host.....	184
13.4 Delegieren der OU-Verwaltung an andere Benutzer.....	184
13.5 Active Directory-Kontingente	188
14 Benutzerkonten	189
14.1 Alternative UPN-Suffixe.....	189
14.2 Erstellen und Verwalten von Benutzerkonten mit LDIFDE.....	191
14.3 Erstellen und Verwalten von Benutzerkonten mit CSVDE	192
14.4 Erstellen und Verwalten von Konten mithilfe von Windows Script Host.....	193
14.5 PowerShell-Extensions für Active Directory	194
14.6 Erstellen und Verwalten von Benutzerkonten mit PowerShell	195
14.7 Erstellen von LDAP-Abfragen.....	197
15 Migration von AD-Objekten (zB Benutzerkonten) in andere Domänen	201
15.1 Verwendung von ADMT 3.2	201
15.2 Deaktivierung des SID-Filters von Gesamtstruktur-Vertrauensstellungen.....	215
15.3 Verwendung von LDP.....	218
16 NTFS-Berechtigungen in Multi-Domänen-Forests	221
16.1 Gruppentypen und Gruppenbereiche	221
16.2 Strategie	223
16.3 Globale Gruppen	225
16.4 Universelle Gruppen.....	225
16.5 Domänenlokale und lokale Gruppen	225
16.6 Globale Gruppe in einer OU erzeugen mit Visual Basic Script.....	227
17 Gruppenrichtlinien	229
17.1 Konzept, Einrichten von Gruppenrichtlinien	229
17.2 Komponenten von Gruppenrichtlinienobjekten	231
17.3 Gruppenrichtlinienverarbeitung durch CSE (Client Side Extensions)	235
17.4 Erstellen eines „Central Store“ für *.admx und *.adml-Dateien.....	238
17.5 ADMX-Migrator.....	239
17.6 Group Policy Management Console (GPMC)	242
17.7 Beispiele aus der Praxis	244
17.8 Gruppenrichtlinien-Vorgaben.....	252
17.9 Zusammenwirkung mehrerer GPOs.....	252
17.10 Filtern von GPOs	253

17.11	WMI-Filter	254
17.12	Starter-Gruppenrichtlinienobjekte.....	259
17.13	Backup und Restore von Gruppenrichtlinienobjekten	261
17.14	Import von Einstellungen	264
17.15	Domänenübergreifendes Kopieren von GPOs.....	269
17.16	Gruppenrichtlinien zur Steuerung von Gruppenrichtlinien	274
17.17	Überprüfung und Problembehandlung von Gruppenrichtlinien	279
17.18	Gruppenrichtlinienprotokollierung.....	292
17.19	Delegieren von Gruppenrichtlinienobjekten	293
17.20	Sicherheitsrichtlinien.....	295
17.21	Das lokale GPO	302
18	Gruppenrichtlinien für Softwareverteilung.....	309
18.1	Varianten	309
18.2	Technologien	310
18.3	Vorgangsweise.....	310
18.4	Standardoptionen für die Softwareinstallation.....	314
18.5	Neue Softwareversion über GPO verteilen	315
18.6	Durch *.MSP-Datei gepatchte MSI-Datei erneut bereitstellen	317
18.7	Entfernen von Software über GPO.....	317
18.8	Verteilen von Office 2007	318
19	Erstellen von ZAP-Dateien.....	321
20	Erstellen von MSI-Paketen.....	323
20.2	Erstellen von MST-Dateien.....	330
20.3	Konfigurieren einer MST-Datei für eine Office 2003-Installation.....	330
20.4	Office 2007 über Gruppenrichtlinien verteilen	345
21	Richtlinien für Softwareeinschränkung in Windows Server 2008.....	349
21.1	Zusammenfassung	350
21.2	Festlegen von Richtlinien für Softwareeinschränkung	350
21.3	Verhindern der Anwendung von Richtlinien für Softwareeinschränkung auf lokale Administratoren.....	352
21.4	Erstellen einer Pfadregel	354
21.5	Erstellen einer Zertifikatregel.....	356
21.6	Erstellen einer Hashregel	358
21.7	Erstellen einer Internetzonenregel	360
21.8	Erstellen einer Registrierungspfadregel	361
21.9	Hinzufügen oder Löschen eines designierten Dateityps	362
21.10	Ändern der Standardsicherheitsstufe von Richtlinien für Softwareeinschränkung	362
21.11	Einstellen von Optionen für vertrauenswürdige Herausgeber.....	363
21.12	Vorrang der Richtlinien für Softwareeinschränkung	364
21.13	Reihenfolge der Anwendungen	365
21.14	Prüfliste: Schritte zum Schutz des Computers vor E-Mail-Viren	366
22	Fein abgestimmte Kennwortrichtlinien	367
23	Active Directory-Replikation und Standort-Design.....	377
23.1	Replikation zwischen Standorten	377
23.2	Standort-Konfiguration:.....	377
23.3	Bevorzugte Bridgeheadserver:	384
23.4	Wie Clients über DNS ihre Standort-Zugehörigkeit erfahren	387
23.5	Einrichten von Universal Group Membership Caching	388
23.6	TCP-Ports für Active Directory-Replikation	390
23.7	Design von Standortverknüpfungen (Beispiel)	392
23.8	Standortverknüpfungsbrücken zur Kontrolle des Active Directory-Replikationsflusses.....	395
24	Wartung der ADDS-Dienste	399
24.1	Datenänderungsprozess	399
24.2	Verschieben der ADDS-Datenbank in einen anderen Ordner	400
24.3	Offline-Defragmentierung	401
24.4	Integritätsprüfung.....	401

25	Sichern und Wiederherstellen von Active Directory	403
25.1	Sichern und Nicht-autorisierendes Wiederherstellen von Active Directory	403
25.2	Autorisierende Wiederherstellung einer OU	403
25.3	Reanimierung eines Benutzerobjekts	404
25.4	AD-Snapshots	407
25.5	Entfernen von Daten aus Active Directory nach fehlgeschlagener Domänencontroller-Herabstufung	409
26	Entfernen von verwaisten Domänen	415
26.1	Erzwingenes Entfernen von AD mit dcpromo /forceremoval	417
27	Überwachung von Active Directory	423
27.1	Ereignisanzeige	423
27.2	Zuverlässigkeits- und Leistungsüberwachung	434
27.3	Überwachungsrichtlinien	440
28	Active Directory Lightweight Directory Services (AD LDS)	445
28.1	Installation	445
28.2	Zugriff auf die AD LDS-Instanz mit ntdsutil	452
28.3	Verzeichnispartitionen einer AD LDS-Instanz	452
28.4	Abfragen von AD LDS-Instanzen mit dem ADSI-Editor	452
28.5	Erstellen von AD LDS-Anwendungspartitionen	453
28.6	Synchronisieren zwischen AD LDS und ADDS mit adamsync	454
29	Active Directory-Verbunddienste (ADFS, Active Directory Federation Services)	457
29.1	Vorbereitende Tätigkeiten	458
29.2	Einrichten eines einzelnen ADFS-Servers	458
29.3	Konfiguration eines Kontenverbundservers (vertrauende Seite)	463
29.4	Verbundserverfarm	463
29.5	Verbundserverproxy	464
30	Active Directory-Rechteverwaltungsdienste (ADRMS, Active Directory Rights Management Services)	467