
Inhaltsverzeichnis

Einführung	xv
Inhalt	xv
Teil I: Festlegen der Grundlagen	xv
Teil II: Migrations- und Integrationsszenarios	xvi
Teil III: Verwaltung und Sicherheit	xvii
Symbole im Text	xviii
Inhalt der Begleit-CD-ROM	xviii
Verwenden der Begleit-CD-ROM	xx
Systemanforderungen	xx
Danksagung	xxi
Ein Hinweis zum Schluss	xxi
 Teil I Festlegen der Grundlagen	 1
Kapitel 1 Das Design von Windows 2000 Active Directory	3
Der gesamte Entwurfsprozess der Woodgrove Bank	4
Phasen und Teillieferungen	4
Team	5
Entwurfsziele auf hoher Ebene	6
Bewertung der aktuellen Windows NT 4.0-Umgebung	7
Aktuelle Netzwerkarchitektur	7
Aktuelle inländische Windows NT 4.0-Domänenarchitektur	8
Aktuelle internationale Windows NT 4.0-Domänenarchitektur	9
Das Windows 2000-Design	12
Unternehmensanforderungen für Active Directory	12
Das Active Directory-Design der Woodgrove Bank	12
Einzelne inländische und separate internationale Domänen	13
Der internationale Entwurf der nächsten Generation	52
Zusammenfassung	54

Kapitel 2 Das Design der Standorttopologie von Compaq für Windows 2000	57
Grundlagen der Active Directory-Replikation	58
Domänencontroller	58
Auslösen der Replikation	60
Aktualisierungstypen	60
Namenskontext	61
Standorte	62
Bridgeheadserver	63
Replikationstransport	64
Konsistenzprüfung (KCC)	65
Verbindungsobjekte	66
Replikation des globalen Katalogs	67
Der Unternehmensnamespace von Compaq	69
Netzwerkinfrastruktur	70
GlobalNet	70
Überlegungen zur Adressierung	72
Legacynetze	73
Der Entwurf für die Standorttopologie	74
Standortinterne und standortübergreifende Replikation	75
Erstellen von Replikationstopologien	77
Standorttopologie	77
Serverstandort	83
Zusammenfassung	89
Kapitel 3 Anpassen der Datenbankgröße unter Active Directory	91
Architektur und Komponenten der Active Directory-Datenbank	92
Prinzipielle Struktur	92
Datenbankstruktur	93
Änderungen an der Datenbank	94
Speicherbereinigung	96
Tests zur Berechnung der Active Directory-Datenbankgröße –	
Einzelne Objekte	98
Berechnen des Wachstums und der Größe von Objekten	99
Lasten einzelner Objekttypen	99
Benutzerobjekte	99
Hinzufügen von Attributen	100
Organisationseinheiten	102
Gruppen	103
Kontakte	108
Speichern von Zertifikaten für öffentliche Schlüssel in	
Active Directory	109
Drucker und Datenträger	110

Speichern von Abschnitten in Active Directory	112
Tests zur Berechnung der Active Directory-Datenbankgröße – Beispielunternehmen	112
Beispielunternehmen mit Grundeigenschaften	113
Beispielunternehmen mit benutzerdefinierten Attributen	114
ACE-Einträge	115
Schaffen von Speicherplatz in der Datenbank	116
Zusammenfassung der Tests zur Berechnung der Datenbankgröße	119
Tests zur Berechnung der Active Directory-Datenbankgröße – Globale Katalogserver	120
Globaler Katalogserver mit Beispielunternehmen	120
Globale Katalogserver und Beispielunternehmen mit universellen Gruppen	121
Berechnung der Größe des globalen Katalogs mit individuellen Objekten	123
Zusammenfassung für globalen Katalog	125
Hinzufügen von Microsoft Exchange 2000	126
Erweitern des Schemas mit Exchange 2000	127
Hinzufügen von Mailboxen zu Benutzern	128
E-Mail für Gruppen aktivieren	130
E-Mail für Kontakte aktivieren	132
Beispielunternehmen mit Exchange 2000	134
Active Directory – Zusammenfassung der Objekte mit und ohne Exchange 2000	136
Zusammenfassung	137
Kapitel 4 Analyse der Replikationsaktivitäten unter Active Directory	139
Sinn und Zweck der Messung von Replikationsaktivitäten	140
Arten von Replikationsaktivitäten	142
Replikationsszenarios	143
Messung der Replikationsaktivitäten	144
Replikation innerhalb eines Standortes	145
RepAdmin	146
MMC erzwungene Replikation	148
Zusammenfassung der Replikationsoptionen	149
Erfassen der Replikationsaktivitäten	151
Globaler Katalog und Vergleich der Replikation innerhalb einer Domäne mit der Replikation zwischen mehreren Domänen	152
Änderungen einzelner Attribute	153
Domänenobjektreplication innerhalb eines Standortes	158
Replikation des globalen Katalogs innerhalb eines Standortes	163

Replikation zwischen mehreren Standorten	168
Domänenreplikation zwischen mehreren Standorten	169
Hinzufügen von Benutzerattributen	175
Replikation von Kennwortänderungen	177
Ändern der Gruppenmitgliedschaften	179
Administrative Operationen	180
Serverreplikation des globalen Katalogs	189
Hinzufügen von Benutzerobjekten	190
Replizieren von Gruppen	192
Drucker und Datenträger	195
Optimieren der SMTP-Replikation	196
Berechnungstabellen für die Aktivitäten zwischen mehreren Standorten	199
Replikation über langsame Verbindungen	199
Zusammenfassung	201
Kapitel 5 Clientnetzwerkverkehr in Active Directory	203
Windows NT 4-Clientanmeldeverkehr	204
Überblick	204
Bootprozess der Arbeitsstation	206
Benutzeranmeldung	210
Windows 2000 Professional-Anmeldeverkehr zu Active Directory	213
Aufbau der Testumgebung	216
Auswirkung der Gruppenmitgliedschaft auf den Anmeldeverkehr	216
Auswirkung der Gruppenrichtlinien auf den Anmeldeverkehr	219
IntelliMirror-Technologie	227
NetBIOS-Verkehr	233
Detaillierte Beschreibung des Anmeldeverkehrs einer Windows 2000 Professional-Arbeitsstation	233
LDAP-Konzepte, -Operationen, -Verkehr und -Kapazitätsplanung für Active Directory	234
Informationsmodell	235
Benennungsmodell	237
Funktionsmodell	237
Weitere Konzepte	239
LDAP-Verkehrsanalyse in Active Directory	254
Testumgebung	254
Analysieren der Abfrageoperationen	270
Analysieren der Aktualisierungoperationen	278
Nicht behandelte Themen	286
Zusammenfassung	287

Teil II Migrations- und Integrationsszenarios	289
Kapitel 6 Migration und Konsolidierung von Domänen	291
Die Umgebung	292
Das Windows NT 4.0-Domänenmodell	292
Vorgeschlagenes Active Directory-Modell	292
Festlegen des Migrationsszenarios	294
Erstellen der Active Directory-Infrastruktur	295
Domäne der Stammebene „NWT.INT“	295
Domäne der zweiten Ebene „NA.NWT.INT“	295
Migrieren der UK-Domäne (Aktualisierung an Ort und Stelle)	296
Warum an Ort und Stelle?	296
Reihenfolge der Aktualisierung	297
Der Prozess	297
Beibehalten der Interoperabilität	300
Konsolidieren der nordamerikanischen Domänen	301
Gründe für die Konsolidierung	301
Das Active Directory-Migrationsprogramm	301
Reihenfolge der Migrationen	302
Der Migrationsprozess	302
Entwickeln und Testen eines Plans für die vorzeitige Beendigung	302
Einrichten und Anwenden einer Richtlinie für doppelte Namen	303
Einrichten und Anwenden einer Richtlinie für Eindeutigkeit	303
Erkennen und Entfernen überflüssiger globaler und lokaler Gruppen	303
Einrichten der erforderlichen Vertrauensstellungen	304
Duplizieren globaler Gruppen in die Windows 2000-Domäne	305
Duplizieren freigegebener lokaler Gruppen in die Windows 2000-Domäne	307
Duplizieren von Benutzerkonten in die Windows 2000-Domäne	308
Verschieben von Computerkonten in die Windows 2000-Domäne	309
Migrieren einer Testgruppe in die Windows 2000-Domäne	310
Migrieren der restlichen Domänenmitglieder in die Windows 2000-Domäne	310
Interoperabilität während der Migration	311
Entfernen der Quelldomänen	312
Verwenden von ClonePrinciple, NetDom und MoveTree	313
Zukünftige Pläne	314
Ressourcendomäne NWTRDUK	314
Ressourcendomänen in Nordamerika	314
Zweigstellenniederlassungen	314
Zusammenfassung	314

Kapitel 7 Integrieren von Active Directory mit einer Unix-basierten DNS-Umgebung	315
Vorbemerkung	316
Infrastruktur und DNS-Strategie	316
Gründe für eine reine Unix-DNS-Lösung	318
DNS-Anforderungen für Active Directory	319
Vergleichen des DNS-Dienstes von Unix-BIND und Windows 2000	319
Integration des Speichers und der Replikation von Active Directory	319
Sichere dynamische Aktualisierung	320
Der Cacheauflösungsdienst	321
DNS-Snap-In	321
WINS-Integration	321
Unterstützung von UTF-8-Zeichen (Unicode)	322
Unterstützung der Alterung und des Aufräumvorgangs	322
Das Befehlszeilenprogramm DNSCDM	322
Aktualisierungsoptionen für eine Unix-DNS-Umgebung	323
Konfigurieren einer reinen Unix-DNS-Umgebung	325
Konfiguration von Unix-Servern	325
Konfiguration von Windows 2000 Server	330
Konfiguration von Windows 2000-DHCP-Server	331
Kompatible DHCP-Server	333
Windows 2000-Clients	333
Kompatible Clients	334
Zusätzliche Überlegungen	334
Server unter BIND 4.x und BIND 8.1.2	335
Domänencontroller und DHCP-Server unter Windows 2000	336
Zusammenfassung	336
Kapitel 8 Integrieren von Active Directory mit Exchange Server	337
Überblick über die Aktualisierungsstrategie	338
Profil des Unternehmens All-Terrain Trucking	339
Hintergrund des Projekts	339
Aktualisieren von Windows NT 4.0-Domänen auf Windows 2000	345
Zusammenfassung: Aktualisierung der Domäne ACCOUNTS	346
Zusammenfassung: Aktualisierung der Ressourcendomäne EXCHANGE	350
Reduzieren von Ressourcendomänen	351
Verzeichnisreplikation und -synchronisation	359
Active Directory Connector	360
Verwenden von Verbindungsabkommen zum Einrichten von Beziehungen	361

Replikation	362
Synchronisierung	363
Installieren und Konfigurieren von Active Directory Connector	364
Schritt 1: Überprüfen der Windows NT-Domänenstruktur sowie der Exchange Server-Standorttopologie	365
Schritt 2: Festlegen des für die Verwaltung der Objektidentität zu verwendenden Verzeichnisdienstes	366
Schritt 3: Durchführen von Active Directory-Schemaänderungen	367
Schritt 4: Festlegen von Objekten für die Verzeichnissynchronisation	367
Schritt 5: Zuordnen von Exchange Server-Standorten/-Containern zu Active Directory-Domänen/-Organisationseinheiten	369
Schritt 6: Festlegen der Attributzuordnung zwischen Active Directory und Exchange Server	370
Schritt 7: Einrichten von Active Directory-Verbindungen	372
Schritt 8: Erstellen von Verbindungsabkommen zur Datenübernahme von Exchange in Active Directory	373
Schritt 9: Erstellen eines Zeitplans für die Verzeichnisreplikation und -synchronisation	375
Schritt 10: Erstellen von Verbindungsabkommen zur Aufrechterhaltung der Verzeichnissynchronisation	377
Schritt 11: Sichern der Verzeichnisdienste zur Vermeidung von Kollisionen und zur Wahrung der Identität	381
Zusammenfassung: Active Directory Connector	384
Planen für Exchange 2000	385
Exchange 2000 verwendet Active Directory	386
Exchange 2000-ADC-Aktualisierung	386
Vor der Aktualisierung auf Exchange 2000	386
Zusammenfassung	387
Empfehlungen aus der Praxis	387
 Kapitel 9 Active Directory und Novell NetWare NDS (Novell Directory Services)	 391
Überblick über das Netzwerkverzeichnis	392
Schema: Objekte, Klassen und Attribute	394
Hierarchie und Container	395
Sicherheit und Delegierung	396
Replikation und Synchronisation	396
Partitionieren	397
Vergleich zwischen NDS und Active Directory	397
Containerobjekte	398
Kataloge	403
Replikationsüberblick	405

Multimaster-Aktualisierungen	406
Authentifizierung	407
Sicherheit und Vererbung	407
Internetstandards	408
Lösungen in Active Directory und NDS entwerfen	411
Regeln für das Aufbauen eines Verzeichnisses	411
Informationen zu Northwind	411
Der Designprozess	412
Synchronisierung zwischen Active Directory und NDS	423
Notwendigkeit der Synchronisierung	423
Herausgeber, Abonnenten und Sitzungen	424
Konfigurieren von MSDSS	425
Synchronisierungstypen	428
Verwaltung	428
Zusammenfassung	429

Teil III Verwaltung und Sicherheit 431

Kapitel 10 Scripting von Active Directory 433	433
Grundlagen	434
Info zu ADSI	434
Windows-Script-Host	435
Active Server Pages (ASP)	436
HTML-Anwendungen	437
Verwenden von Visual Basic für Anwendungen in Office 2000	437
Grundlagen von ADSI	438
Architektur	438
Herstellen einer Verbindung zu Active Directory	438
Lesen eines Objekts	440
Aktualisieren eines Objekts	440
Auflisten eines Containers	440
Suchen	440
Verwalten von Domänendaten	442
Extrahieren von Computerdaten	442
Vertrauensstellungen	444
Erstellen von Benutzerkonten	445
Erstellen von Gruppen	446
Verwalten der Unternehmenskonfigurationsdaten	449
Partitionen	449
Auflisten von Standorten	450
Erstellen von Standorten	452

Auflisten von Subnetzen	453
Erstellen von Subnetzen	454
Auflisten von Domänencontrollern	455
Standortverbindungen	457
Replikationsverbindungen	458
FSMO	460
Beispiele für IADSTools	461
WMI	463
Zusammenfassung	469
 Kapitel 11 Delegieren von Vorgängen in den Strukturen sowie der Gesamtstruktur	 471
Gründe für die Delegierung und deren Folgen	472
Hintergrund	473
Zentrales Büro	474
Stammdomänenverwaltung	474
Schemaverwaltung	474
Verfahren zur Vorbereitung der Erstellung untergeordneter Domänen	475
Standortverwaltung	481
Standortverknüpfungsverwaltung	482
Verwaltung des DNS-Stammes	483
Weitere Windows 2000-Dienste	484
Sicherheit	485
Zusammenfassung	488
 Kapitel 12 Erstellen einer Infrastruktur für öffentliche Schlüssel in Windows 2000	 489
Einführung in die Infrastruktur für öffentliche Schlüssel	489
Verschlüsselung	490
Digitale Signaturen	491
Digitale Zertifikate	491
Vertrauensstellungen und Zertifizierungsstellen	492
Kernkomponenten der Microsoft-Infrastruktur für öffentliche Schlüssel	493
Die Vorteile der Microsoft-Infrastruktur für öffentliche Schlüssel	495
Planen und Entwerfen einer Infrastruktur für öffentliche Schlüssel	495
Fallstudie: Trey Research	495
Analysieren der Geschäftsanforderungen	496
Festlegen einer Topologie der Infrastruktur für öffentliche Schlüssel	501
Spezifikationen der einzelnen Zertifizierungsstellen	508

Festlegen von Richtlinieneinstellungen für öffentliche Schlüssel (Gruppenrichtlinienobjekt)	517
Festlegen der Sicherheitsrichtlinie, des CPS (Certificate Practice Statement) sowie der Zertifikatsrichtlinien	520
Verwaltung und Instandhaltung der Infrastruktur für öffentliche Schlüssel	521
Zusammenfassung	524
Index	525