

Obsah

Úvod	17
Proč číst tuto knihu?	18

ČÁST 1

Kapitola 1: Principy návrhu doménové struktury služby Active Directory	21
Kritéria návrhu doménové struktury služby Active Directory	22
Schéma	23
Aspekty návrhu schématu	24
Hranice zabezpečení	25
Hranice replikace	26
Společný globální katalog	26
Protokol Kerberos a vztahy důvěryhodnosti	27
Politické hranice a hranice správy	29
Výhody a nevýhody více doménových struktur	29
Úroveň funkčnosti doménové struktury v systému Windows 2003	33
Doporučené postupy návrhu doménové struktury	35
Jednoduchost: Začněte s jednou doménovou strukturou	35
Cílem je ideální návrh	35
Návrh s ohledem na zásady řízení změn	35
Oddělení extranetových aplikací do vlastní doménové struktury	36
Vytváření návrhu založeného na standardním použití doménové struktury	37
Další zdroje informací	37
Shrnutí	38
Kapitola 2: Principy návrhu domény služby Active Directory	39
Principy návrhu domény služby Active Directory	40
Definice požadavků na domény	40
Hranice domén	40
Hranice zásad účtů	41
Hranice replikace	42
Požadavky na definici stromů	42
Výhody a nevýhody více domén	42

Požadavky na službu DNS	43
Možnosti ověřování	43
Vztahy důvěryhodnosti mezi doménovými strukturami	44
Umístění řadiče domény	47
Fyzický přístup k řadičům domény	47
Umístění řadiče domény s ohledem na síť	47
Umístění globálního katalogu	48
Úrovně funkčnosti domény	48
Nastavení úrovně funkčnosti doménové struktury	52
Výhody nativního režimu	53
Doporučené postupy návrhu domén	56
Shrnutí	56
Kapitola 3: Principy návrhu služby DNS	57
<hr/>	
Vzájemná provázanost	57
Jak na překlad názvů	58
Různé typy zón	60
Primární zóny	60
Sekundární zóny	63
Zóny se zakázaným inzerováním (stub zone)	63
Jaký název dát zóně	65
Možnosti interních a externích názvů	65
Rozdílné obory názvů	65
Jediný obor názvů	66
Seznámení se stávající infrastrukturou DNS	66
Ten druhý server DNS	67
Distribuce změn	69
Doporučené postupy návrhu systému DNS	69
Shrnutí	70
Kapitola 4: Principy návrhu sítí, rolí hlavního serveru a globálního katalogu	71
<hr/>	
Určení topologie sítě	71
Seznámení se stávající síťovou infrastrukturou	73
Identifikace návrhu stávající síťové infrastruktury	73
Nastavení sítí k podpoře návrhu infrastruktury Active Directory	74
Návrh propojení sítí a přemostění propojení sítí	78
Propojení sítí	78
Přemostění propojení sítí	80
Volba umístění globálního katalogu	81

Volba umístění rolí hlavního serveru	83
Role hlavního serveru v doménové struktuře s jedinou doménou	83
Umístění sítě s rolemi hlavního serveru v doménové struktuře s více doménami	83
Hlavní server schématu	84
Hlavní názvový server domény	84
Hlavní server relativních identifikátorů (RID)	84
Hlavní server infrastruktury	84
Emulátor primárního řadiče domény	85
Doporučené postupy návrhu sítí	85
Shrnutí	86
Kapitola 5: Principy návrhu organizačních jednotek	87
<hr/>	
Návrh organizačních jednotek pro usnadnění správy	87
Možnosti návrhu organizačních jednotek	88
Organizační jednotky založené na umístění	88
Organizační jednotky založené na uspořádání	89
Organizační jednotky založené na funkci	89
Organizační jednotky založené na umístění a uspořádání	91
Volba nejvhodnějšího návrhu organizačních jednotek	93
Kritéria návrhu organizačních jednotek	93
Možnosti delegování řízení	93
Řízení viditelnosti objektů	96
Návrh organizačních jednotek pro Zásady skupiny	98
Možnosti využití v organizaci	100
Určení potřeb zabezpečení	102
Určení potřeb instalace softwaru	103
Určení uživatelských omezení	104
Vytvoření jednoduchého návrhu	105
Určení požadavků uživatelů	105
Minimalizace objektů Zásad skupiny	107
Identifikace možných potíží kompatibility	107
Zohlednění dědičnosti v návrhu	109
Možnosti připojení Zásad skupiny	112
Vytváření struktury organizačních jednotek	114
Určení požadavků na strukturu organizačních jednotek	114
Určení požadavků správy	115
Doporučené postupy návrhu organizačních jednotek	118
Shrnutí	118

Kapitola 6: Požadavky na návrh při nasazení serveru Exchange	119
Změny	119
Příprava doménové struktury	120
Příprava domén	124
Vytvoření skupin pro správu	126
Automatické generování zobrazovaného jména	127
Rozšířené atributy	127
Doporučené postupy návrhu nasazení serveru Exchange	129
Shrnutí	129

Kapitola 7: Kapacita a umístění hardwaru	131
Určení specifikace a umístění řadičů domény	131
Určení specifikace řadičů domény	132
Určení umístění řadičů domény	133
Určení umístění globálního katalogu	134
Jednoduché určení kapacity a umístění hardwaru	135
Určení umístění rolí hlavních serverů	138
Role hlavního serveru v doménové struktuře s jedinou doménou	138
Umístění rolí hlavních serverů v doménové struktuře s více doménami	138
Doporučené postupy při určování kapacity a umístění hardwaru	140
Shrnutí	141

ČÁST 2

Kapitola 8: Nasazení	145
Definice názvů domén	145
Identifikace kořenové domény doménové struktury	146
Metody nasazení	147
Ruční instalace	147
Automatická instalace	148
Soubory odpovědí	148
Služba vzdálené instalace (Remote Installation Services, RIS)	149
Klonované bitové kopie	150
První řadič domény	150
Repliky řadiče domény	156
Počáteční naplnění	157
Replikace přes síť	157

Využití dat Stav systému	158
Automatické povýšení řadiče domény	161
Doporučené postupy nasazení	162
Shrnutí	163
Kapitola 9: Migrace a konsolidace domén	165
Zachování připojení	165
Možnosti migrace	166
Rozhraní nástroje ADMT	167
Příprava migrace	169
Požadavky nástroje ADMT	169
Plán zotavení	170
Migrace profilů	170
Pořadí migrace	171
Zachování jedinečnosti účtů	171
Ověření stavu účtů	171
Skriptování nástroje ADMT	172
Migrace hesel	172
Migrace ze systému Windows NT 4	174
Strategie migrace	174
Hlavní uživatelské domény	175
Domény prostředků	177
Řízení přetížení řadičů domény	178
Emulace záložního řadiče domény	179
Omezení emulace	180
Migrace ze systému Windows 2000	180
Příprava doménové struktury	181
Příprava domény	183
Potíže s aplikacemi	184
Upgrade nebo rekonstrukce	185
Další nástroje pro migraci	186
Doporučené postupy migrace a konsolidace domén	187
Shrnutí	187
Kapitola 10: Migrace systému NetWare	189
Příprava migrace	189
Stručný přehled migrace	191
Kompatibilita aplikací	191
Migrace dat	191

Migrace pošty	192
Mapovaná zařízení	192
Testovat, testovat, testovat	192
Zaškolení uživatelů	193
Použití služby Microsoft Directory Synchronization Services	194
Doporučené postupy migrace systému NetWare	194
Shrnutí	195

ČÁST 3

Kapitola 11: Zálohování a zotavení po havárii	199
Reaktivně vs. proaktivně	199
Zálohování řadičů domény	200
Zálohování dat Stav systému	200
Vytvoření zálohy dat Stav systému	201
Omezení nástroje Zálohování	201
Obnovení služby Active Directory	202
Režim obnovení adresářové služby	202
Heslo správce režimu DSRM	203
Primární obnovení	203
Normální obnovení	205
Autoritativní obnovení	205
Označení neplatnosti objektu	206
Automatické obnovení systému	207
Zálohování dat pro automatické obnovení systému	207
Obnovení dat funkce Automatické obnovení systému	208
Doporučené postupy při zotavení po havárii	209
Shrnutí	210
Kapitola 12: Optimalizace databáze služby Active Directory	211
Konfigurace diagnostického protokolování	211
Použití nástroje ADSI Edit k prohlížení oddílů adresářové služby	213
Použití nástroje NTDSUTIL k odstraňování potíží a opravám služby Active Directory	214
Provádění transakcí s databází	215
Kontrola integrity databáze	216
Komprimace databáze	217
Přesunutí databáze	218

Přesunutí souborů protokolu	219
Odstranění osamocených objektů	220
Odstranění osamocených metadat domény	220
Odstranění osamocených metadat řadiče domény	221
Údržba účtů zabezpečení	224
Doporučené postupy pro optimalizaci služby Active Directory	225
Shrnutí	225
Kapitola 13: Odstraňování potíží s replikací služby Active Directory	227
<hr/>	
Přehled replikace	227
Určení příčin potíží serveru DNS	228
Ověření replikace	231
Použití nástroje RepAdmin	232
Použití nástroje ReplMon	233
Použití nástroje DCDiag	235
Řízení replikace v rozsáhlých organizacích	235
Doporučené postupy pro odstraňování potíží s replikací služby Active Directory	236
Shrnutí	237
Kapitola 14: Údržba služby DNS	239
<hr/>	
Metody překladu názvů pomocí služby DNS	239
Vysoká dostupnost záznamu SRV kořenné domény	243
Active Directory Application Mode	244
Diagnostické nástroje	246
Doporučené postupy při údržbě služby DNS	250
Shrnutí	251
Kapitola 15: Odstraňování potíží se službou FRS	253
<hr/>	
Přehled služby FRS	253
Potíže se službou FRS	254
Oříznutí žurnálu	254
Adresáře s upravenými názvy	255
Potíže s pracovní oblastí	255
Paralelní slučování vektorů verzí	256
Nástroje pro odstraňování potíží se službou FRS	256
Použití nástroje FRSDIAG.EXE	256

Použití nástroje Ultrasound	257
Microsoft Operations Manager	261
Nápověda k nástroji Ultrasound	262
Řešení běžných potíží se službou FRS	262
Doporučené postupy pro odstraňování potíží se službou FRS	263
Shrnutí	264
Kapitola 16: Odstraňování potíží s přihlašováním	265
<hr/>	
Auditování potíží s přihlašováním	265
Acctinfo.dll	269
Protokolování modulu Kerberos	271
Potíže s přihlašováním v nativním režimu	271
Potíže s uzamčením účtů	272
Potíže se vzdáleným přístupem	276
Jak rozpoznat útok	277
Řízení komunikace přes linky WAN	277
Doporučené postupy pro odstraňování potíží s přihlášením a uzamčením účtů	278
Shrnutí	278
Kapitola 17: Odstraňování potíží s rolemi hlavního serveru	279
<hr/>	
Role hlavního serveru a jejich důležitost	279
Hlavní server schématu	280
Hlavní názvový server domény	280
Hlavní server infrastruktury	280
Hlavní server relativních identifikátorů (RID)	281
Emulátor primárního řadiče domény	282
Přesunutí a převzetí rolí hlavního serveru	283
Identifikace stávajícího držitele role	283
Integrované nástroje služby Active Directory	284
Active Directory Schema	284
ReplMon	286
Nástroje pro příkazový řádek	286
Přesunutí role na jiný řadič domény	287
Převzetí role rezervním řadičem domény	288
Doporučené postupy pro odstraňování potíží s rolemi hlavního serveru	289
Shrnutí	290

Kapitola 18: Zásady skupiny	291
Nástroje pro odstraňování potíží	292
Group Policy Results	292
Group Policy Verification	293
Software Installation Diagnostics	295
Odstraňování potíží pomocí konzoly Group Policy Management	295
Group Policy Modeling	295
Group Policy Results	296
Karta Summary	298
Karta Settings	299
Karta Policy Events	299
Metodologie odstraňování potíží	300
Objekt Zásad skupiny nebyl použit	300
Objekt Zásad skupiny byl použit, i když neměl být	302
Protokolování pomocí nástroje User Environment	303
Další faktory	305
Užitečné skripty	307
Doporučené postupy pro Zásady skupiny	308
Shrnutí	308

ČÁST 4

Kapitola 19: Zabezpečení operačního systému	311
Zabezpečení řadiče domény před fyzickým přístupem	311
Zabezpečení řadiče domény před vzdáleným přístupem	312
Nastavení zásad auditování řadiče domény	312
Konfigurace přiřazení uživatelských práv	313
Možnosti zabezpečení řadičů domény	314
Ochrana systému v průběhu instalace	319
Doporučené postupy zabezpečení operačního systému	319
Bezpečné umístění instalace	320
Zakázání automatického generování názvů ve formátu 8.3	320
Zabezpečení dobře známých účtů	320
Zabezpečení účtů služeb	321
Použití nástroje Syskey k zabezpečení hesel	321
Definice komunikace řadiče domény pomocí filtrů protokolu IPSec	321
Nastavení výchozích služeb	324
Doporučené postupy pro zabezpečení řadičů domény	326

Shrnutí	327
Kapitola 20: Zabezpečení služby DNS	329
Zajištění fungování systému	329
Omezení dynamických aktualizací	330
Monitorování datových přenosů	330
Samostatné obory názvů	330
Nastavení kvót	331
Zakázání rekurze	333
Použití vhodného směrování	334
Zajištění správnosti informací	335
Použití protokolu IPSec	335
Zabezpečení záznamů DNS	335
Zabránění znehodnocení mezipaměti	336
Zajištění vhodného přístupu	337
Zóny integrované se službou Active Directory	338
Zóny neintegrované se službou Active Directory	338
Uzamčení přenosů	338
Doporučené postupy pro zabezpečení služby DNS	339
Shrnutí	340
Kapitola 21: Správa oprav	341
Monitorování bulletinů zabezpečení a oznámení	341
Určení, zda oznámená chyba zabezpečení může ohrozit vaše systémy	342
Testování oprav v zabezpečeném prostředí	344
Vytvoření plánu nasazení	344
Integrace oprav do provozního prostředí	347
Windows Update	347
Nasazení oprav pomocí služby Software Update Services	348
Použití serveru SMS se sadou SUS Feature Pack k nasazení oprav	351
Řešení jiných výrobců	352
Doporučené postupy pro správu oprav	352
Shrnutí	353
Kapitola 22: Zabezpečení služby Active Directory	355
Umístění souborů databáze služby Active Directory	355
Zajištění dostatečného místa pro databázi	356
Auditování řadičů domény	356
Auditování oddílů adresáře schématu	357

Auditování oddílů konfigurace adresáře	359
Auditování oddílů domény	362
Údržba účtů správců služeb	365
Vytvoření základního nastavení	365
Použití metod bezpečné správy	366
Sekundární přihlašování	366
Důvěryhodný personál	367
Ověřování dvou osob	367
Řízení ukládání přihlašovacích informací do mezipaměti	367
Doporučené postupy pro zabezpečení služby Active Directory	368
Shrnutí	369
Příloha A: Zdroje informací o skriptování	371
<hr/>	
Od společnosti Microsoft	371
Z jiných zdrojů	372