



Microsoft® **Windows** **2000** **Server**

Plánování a implementace sítě



VŠECHNY CESTY
K INFORMACÍM

Microsoft®

Microsoft® Windows 2000 Server

Plánování a implementace sítě

Computer Press
Praha
2000

Microsoft® Windows 2000 Server Plánování a implementace sítě

Copyright © Computer Press® 2000. Vydání první. Všechna práva vyhrazena.
Vydavatelství a nakladatelství Computer Press®,
Hornocholupická 22, 143 00 Praha 4, <http://www.cpress.cz>

ISBN 80-7226-291-2

Prodejní kód: K0385

Překlad: Karel Voráček

Odborná korektura: Bohdan Cafourek,

Ludvík Roubíček

Jazyková korektura: Barbora Antonová, Josef Novák

Vnitřní úprava: Petr Klíma, Jiří Matoušek

Sazba: Petr Klíma

Rejstřík: Tomáš Kuchař

Obálka: Jaroslav Novák

Komentář na zadní straně obálky: Ivo Magera

Odpovědný redaktor: Ivo Magera

Vedoucí technické redakce: Martin Hanslian

Produkce: Petr Baláš

Tisk: PBTISK

Copyright © 2000 by Microsoft Corporation.

Original English language edition Copyright © 2000 by Microsoft Corporation.

Translation: © Computer Press, 2000.

Autorizovaný překlad z originálního anglického vydání Microsoft® Windows® 2000 Server Resource Kit.

Originální copyright: © Microsoft Corporation Inc./Microsoft Corporation, 2000.

Překlad: © Computer Press, 2000.

Žádná část této publikace nesmí být publikována a šířena žádným způsobem a v žádné podobě bez výslovného svolení vydavatele.

Veškeré dotazy týkající se distribuce směřujte na:

Computer Press Brno, náměstí 28. dubna 48, 635 00 Brno-Bystrc,
tel. (05) 46 12 21 11, e-mail: distribuce@cpress.cz

Computer Press Bratislava, Hattalova 12, 831 03 Bratislava, Slovenská republika,
tel.: +421 (7) 44 45 20 48, 44 25 17 20, e-mail: distribucia@cpress.sk

Nejnovější informace o našich publikacích naleznete na adrese:

<http://www.cpress.cz/knihy/bulletin.html>.

Máte-li zájem o pravidelné zasílání bulletinu do Vaší e-mailové schránky, zašlete nám jakoukoli, i prázdnou zprávu na adresu bulletin@cpress.cz.



<http://www.vltava.cz>

Nejširší nabídka literatury, hudby, MP3,
multimediálního softwaru a videa za
bezkonkurenční ceny.



Vaše dotazy, vzkazy, náměty, připomínky ke knižní produkci
Computer Press přijímá 24 hodin denně naše horká linka:
knihy@cpress.cz

Obsah

Úvod	xlvi
O knize Microsoft Windows 2000 Server Plánování a implementace sítě	xlvi
Cíle tohoto průvodce	xlvi
Prvky průvodce	xlvi
Struktura průvodce	xlvi
Konvence dokumentů	xlvi
Grafické symboly	xlvi
Kompaktní disk sady Resource Kit	xlix
Zásady podpory sady Resource Kit	I

ČÁST I

Přehled plánování	1
--------------------------	----------

KAPITOLA 1

Úvod do plánování zavedení systému	3
Spuštění plánu	4
Efektivní používání této knihy	4
Jak začít plánování	5
Přehled rodiny produktů Windows 2000	6
Windows 2000 Professional	6
Rodina systémů Windows 2000 Server	7
Systém Windows 2000 Server Standard	8
Terminálové služby	9
Použití Windows 2000 pro zlepšení způsobů práce	9
Správce IT	10
Manažer oddělení	10
Prodejce	11

Příklady naplnění obchodních či výrobních potřeb systémem Windows 2000	11
Příklad 1: Severoamerický průmyslový výrobce	12
Existující prostředí IT	12
Cíle zavedení systému Windows 2000	12
Příklad 2: Velký mezinárodní výrobce	13
Existující prostředí IT	13
Cíle zavedení systému Windows 2000	14
Příklad 3: Nadnárodní korporace finančních služeb	14
Existující prostředí IT	15
Cíle zavedení systému Windows 2000	15
Příklad 4: Mezinárodní společnost vývoje softwaru	16
Existující prostředí IT	16
Cíle zavedení systému Windows 2000	17
Plánování charakteristických stránek systému Windows 2000 vaším obchodním či výrobním potřebám	18
Správa služeb infrastruktury	18
Řešení správy počítačů	19
Funkce zabezpečení	21
Publikování a sdílení informací	22
Podpora aplikací COM	22
Škálovatelnost a dostupnost	23
Práce v síti a komunikace	25
Správa ukládání	26
Plánování seznamu úloh pro mapování možností Windows 2000	27

KAPITOLA 2

Vytvoření cesty postupného zavádění	29
Vytvoření plánu projektu	30
Příprava procesu plánování projektu	31
Určení cílů	33
Návrh a vývoj funkcí	34
Pilotní program zavádění systému Windows 2000	34
Postupné zavádění do produkčního prostředí	35

Scénáře zavádění	36
Scénář 1: Mezinárodní finanční služby	36
Fáze 1: Vyhodnocení	36
Fáze 2: Návrh a technické řešení	38
Druhotný cíl	39
Fáze 3: Testování	40
Fáze 4: Migrace	41
Scénář 2: Mezinárodní výrobce spotřebního a průmyslového zboží.	41
Týmy zavádění	42
Tým zavádění serverů	43
Tým zavádění klientů	48
Technologické závislosti	50
Služba Active Directory a prostor názvů domén	50
Služba Active Directory a Exchange Server	51
Integrovaní systému Exchange Server	51
Vzdálená instalace operačního systému	51
Tipy plánování zavádění systému Windows 2000	52
Seznam úkolů plánování	55

KAPITOLA 3

Plánování zavedení	57
Vytvoření podrobností plánu projektu	58
Rozsah a cíle projektu	58
Požadavky na personál	59
Organizování týmů zavádění	59
Přiřazení rolí týmům Windows 2000	61
Současné počítačové prostředí	62
Vytvoření standardů a pravidel	64
Vykonání analýzy rozdílů	64
Testování a pilotní program zavádění systému Windows 2000	65
Vytvoření dokumentů plánování projektu	66
Správní dokumentace	66
Dokumenty zavádění	67
Funkční specifikace	68
Strategie komunikace	68

Plán vzdělávání a školení	69
Plánování kapacity	70
Vyhodnocení rizik	70
Řízení rizik.	71
Časový plán určený rizikovými faktory.	73
Zavádění systému Windows 2000	74
Seznam úkolů plánování zavádění	75

KAPITOLA 4

Vytvoření testovací laboratoře systému Windows 2000	77
Úvod do testovacího prostředí	78
Vytvoření testovacího prostředí	78
Použití laboratoře pro rizikový management.	78
Proces vývoje laboratoře	79
Testovací proces	81
Vytvoření předběžné laboratoře	82
Určení strategie laboratoře	82
Zvážení návratnosti nákladů	82
Použití laboratoře během životního cyklu projektu	83
Plánování	83
Vývoj	83
Zavádění.	84
Po zavedení systému	84
Vyhodnocení laboratorních modelů	85
Účelové laboratoře.	85
Změny managementu laboratoře	85
Výběr modelu laboratoře	86
Výběr umístění laboratoře	87
Testování v distribuovaném laboratorním prostředí	89
Studie 1: Funkční laboratorní sídla.	89
Studie 2: Laboratorní sídla pro případ nehody	89
Návrh laboratoře.	90
Předpoklady návrhu laboratoře	90
Návrh scénářů testování	90

Simulování navrhovaného serverového prostředí.	91
Simulování navrhovaného prostředí klientských počítačů.	93
Vytvoření rámce procesů testování	96
Dokumentování konfigurace laboratoře	98
Popis laboratoře	98
Diagramy laboratoře.	99
Vybudování laboratoře	102
Řízení laboratoře	103
Zodpovědnost řízení laboratoře	104
Vývoj pravidel laboratoře	104
Testování	105
Definice a eskalace plánů	106
Vytvoření plánu testování.	106
Rozsah a cíle	107
Metodologie testování.	107
Vyžadované zdroje.	107
Funkce a prvky	108
Rizika	109
Časový plán.	109
Návrh testovacích případů	109
Řízení testů	110
Dokumentování výsledků testů.	110
Testování po zavedení systému.	111
Použití laboratoře pro změnový management.	111
Definování role laboratoře v změnovém řízení	
Seznam úkolů plánování laboratorního testování	114
Seznam úkolů přípravy laboratoře	114
Seznam úkolů testování	115

KAPITOLA 5

Vykonání pilotního programu systému Windows 2000	117
Přehled vykonání pilotního programu	118
Pilotní proces.	118
Začnete v oddělení informačních technologií	118

Předpoklady pro vykonání pilotního programu v produkčním prostředí .	118
Vytvoření pilotního plánu	120
Rozsah a cíle	120
Rozsah pilotního programu	120
Cíle pilotního programu	121
Uživatelé a sídla pilotního programu	121
Plán školení pilotního programu.	122
Plán podpory pilotního programu	122
Komunikace.	123
Plán návratu pilotního programu	123
Časový plán	123
Příprava na pilotní program	124
Příprava pilotních sídel	124
Příprava pilotních uživatelů	125
Vytvoření včasné komunikace	125
Informování účastníků	125
Vývoj procesu postupného zavádění.	125
Zavádění pilotního programu	126
Vyhodnocení pilotního programu.	126
Sledování pilotního programu.	127
Zajištění zpětné vazby	127
Seznam úkolů plánování vykonání pilotního programu	128

ČÁST II

Předpoklady infrastruktury sítě	129
--	------------

KAPITOLA 6

Příprava infrastruktury sítě na systém Windows 2000	131
Dokumentování současného prostředí.	131
Inventář hardwaru a softwaru	132
Infrastruktura sítě	133
Fyzický diagram sítě.	134
Logický diagram sítě.	134
Konfigurace sítě.	136

Souborové, tiskové a webové servery	137
Obchodní či výrobní aplikace	137
Architektura adresářových služeb	138
Model správy domén	138
Zabezpečení	139
Příprava architektury sítě	140
Předběžné kroky	142
Stabilizace existující sítě	142
Zjištění síťových protokolů	142
Posudek fyzické infrastruktury	142
Příprava serverů	144
Příprava řadičů domén	144
Příprava členských serverů	145
Příprava infrastruktury zabezpečení	146
Příprava klientů	147
Úvahy o inovaci na systém Windows 2000 Professional	147
Příprava na spolupráci s jinými systémy	148
Seznam úkolů přípravy infrastruktury sítě	149

KAPITOLA 7

Určení strategií konektivity sítě	151
Přehled konektivity sítě	152
Síťové pozice	152
Metody vzdálené konektivity	152
Interní konektivita sítí LAN uvnitř pozic	152
Externí konektivita v organizaci	155
Návrh demilitarizované zóny	155
Konektivita sídel organizace	155
Konektivita vzdálených klientů	156
Protokol TCP/IP systému Windows 2000	157
Nové funkce v sadě TCP/IP systému Windows 2000	157
Konfigurace automatického privátního adresování IP	157
Podpora velkých datových rámců	158

Výběrové potvrzení	158
Zlepšený odhad času od odeslání požadavku do příchodu ozvěny	158
Úvahy o plánování protokolu Microsoft TCP/IP	158
Třídy adres IP	158
Masky podsítí a používání podsítí	159
Protokol TCP/IP a služba Windows Internet Name Service	160
Úvahy o návrhu systému WINS	160
Služba Směrování a vzdálený přístup	160
Nové funkce služby Směrování a vzdálený přístup systému Windows 2000.	161
Zásady vzdáleného přístupu	162
Úvahy o návrhu vzdáleného přístupu.	163
Zabezpečení sítí VPN	163
Výhody použití virtuálních soukromých sítí.	163
Sítě VPN využívající protokol Point-to-Point Tunneling Protocol	164
Sítě VPN využívající protokol L2TP ve spojení s protokolem IPSec	164
Úvahy o zavedení protokolu L2TP	164
Příklady protokolu L2TP	165
Zabezpečení sítí VPN protokolem IPSec	166
Služba Internet Authentication Service a centralizovaná správa	168
Systémy s více adresami	169
Infrastruktura směrování protokolu IP.	169
Staticky směrované sítě.	169
Návrh sítě s protokolem RIP pro IP	170
Návrh sítě s protokolem OSPF.	171
Struktura směrování protokolu IPX.	174
Návrh sítě s protokolem IPX	174
Struktura směrování protokolu AppleTalk.	175
Podpora vícesměrového vysílání	175
Překlad síťových adres.	176
Protokol DHCP systému Windows 2000.	177
Výhody používání protokolu DHCP	177
Nové funkce protokolu DHCP systému Windows 2000.	177
Vylepšené zprávy serveru	178
Podpora dalších oborů	178
Integrace DHCP a DNS.	178
Detekce neautorizovaných serverů DHCP.	178
Dynamická podpora klientů protokolu Bootstrap Protocol	179
Přístup pouze pro čtení ke Správci služby DHCP prostřednictvím konzole	179

Návrh protokolu DHCP ve vaší síti	179
Velikost infrastruktury sítě.	179
Technologie Asynchronous Transfer Mode v systému Windows 2000	180
Výhody používání ATM systému Windows 2000	181
Funkce ATM systému Windows 2000	181
Správce volání uživatelského síťového rozhraní ATM	181
Aktualizovaná podpora NDIS a hardwaru ATM	182
Emulace LAN na síti ATM	182
IP/ATM	183
Služba vícesměrového vysílání a překladu adres (MARS)	183
PPP/ATM	183
Úvahy o návrhu sítě ATM	184
Služba Quality of Service	185
Seznam úkolů plánování strategií práce v síti	186

KAPITOLA 8

Analýza infrastruktury sítě pomocí

serveru Systems Management Server	187
Analýza infrastruktury sítě	188
Práce se serverem Systems Management Server	188
Jak může server Systems Management Server	
urychlit zavádění systému Windows 2000	190
Rozdíly oproti serveru Systems Management Server 1.2.	191
Vytvoření inventáře.	192
Vyhodnocení současného stavu hardwaru	192
Kapacita hardwaru	192
Kompatibilita hardwaru	192
Práce s inventářem hardwaru serveru Systems Management Server	193
Vyhodnocení současného stavu softwaru	194
Použití inventáře k přípravě infrastruktury sítě	186
Vytváření sestav získaných dat	196
Ukázková sestava serveru Systems Management Server	
přípravenosti na systém Windows 2000	196
Použití podsystému kompatibility produktů	198
Analýzování a použití získaných dat.	200
Sledování sítě.	201

Zajištění kompatibility aplikací	201
Seznam úkolů plánování analýzy sítě	203
Další zdroje	203

ČÁST III

Infrastruktura služby Active Directory	205
---	------------

KAPITOLA 9

Návrh struktury služby Active Directory	207
Přehled služby Active Directory	206
Hlavní funkce služby Active Directory	208
Zajištění základů nových technologií	209
Plánování služby Active Directory	210
Obecné principy návrhu	211
Složení plánů struktury služby Active Directory	212
Plánování služby Active Directory	210
Obecné principy návrhu	211
Složení plánů struktury služby Active Directory	212
Vytvoření plánu doménových struktur	212
Proces plánování doménových struktur	214
Určení počtu doménových struktur v síti	214
Vytvoření prostředí s jedinou doménovou strukturou	214
Vytvoření prostředí s více doménovými strukturami	214
Nárůst nákladů na další doménové struktury	215
Vytvoření zásad řízení změn doménové struktury	217
Zásady změny schématu	217
Zásady změny konfigurace	218
Změna plánu doménových struktur po zavedení	218
Vytvoření plánu domén	218
Proces plánování domén	219
Určení počtu domén v jednotlivých doménových strukturách	220
Jak se změnilo vytváření domén	220
Kdy vytvořit více domén	221
Nárůst nákladů na další domény	228

Volba kořenové domény doménové struktury	228
Přiřazení názvů DNS a vytvoření hierarchie domén	229
Uspořádání domén do stromů	230
Doporučení vytváření názvů domén	232
Názvy domén a názvy počítačů	234
Plánování zavedení serverů DNS	234
Systém lokátoru řadiče domény	236
Umístěte autoritativní servery	237
Optimalizace ověřování pomocí explicitních vztahů důvěryhodnosti	237
Změna plánu domén po zavedení	238
Přidání nových domén a odstranění existujících domén	239
Slučování a rozdělování domén	239
Změna názvů domén	239
Vytvoření plánu organizačních jednotek	239
Struktura OU a struktura podniku	239
Proces plánování OU	241
Vytváření jednotek OU pro delegování správy	242
Úpravy seznamů řízení přístupu	242
Určení vytvořených jednotek OU	243
Vytváření jednotek OU pro skrývání objektů	247
Vytváření jednotek OU pro zásady skupiny	248
Změna plánu OU po zavedení	248
Vytvoření plánu topologie sídel	249
Proces plánování topologie sídel	250
Definování sídel a propojení mezi sídly	251
Vytváření sídel	251
Propojení sídel linkami	252
Umístění serverů do sídel	254
Umístění dodatečných řadičů domén	254
Umístění serverů globálního katalogu	255
Umístění serverů DNS	255
Změna topologie sídel po zavedení	256
Seznam úkolů plánování návrhu struktury služby Active Directory	257

KAPITOLA 10

Určení strategií migrace domén	259
Začátek procesu plánování migrace	260

Fáze procesu plánování	260
Určení postupné migrace	260
Cíle migrace	260
Koncepty migrace	262
Inovace klientů a serverů	263
Úvahy o migraci domén	264
Rozhodnutí o inovaci	264
Rozhodnutí o restrukturalizaci	265
Kompatibilita aplikací	265
Požadavky spolupráce	266
Požadavky objektů služby Active Directory na disková úložiště	267
Plánování inovace domén	267
Určení podporovaných cest inovace	269
Zjištění existující struktury domén	269
Vývoj plánu zotavení	270
Správa přechodu na doménovou strukturu systému Windows 2000	271
Úvahy o inovaci domén prostředků	271
Určení strategie inovace řadičů domény	273
Režimy domén systému Windows 2000	273
Inovace řadiče PDC systému Windows NT	275
Emulace řadiče PDC v systému Windows 2000	276
Součásti řízení přístupu	277
Určení pořadí inovace domén	278
Pokyny pro inovaci domén uživatelských účtů	278
Pokyny pro inovaci domén prostředků	279
Podřízené domény a vztahy důvěryhodnosti	279
Určení okamžiku přechodu na nativní režim	282
Důvody pro pokračování v kombinovaném režimu	283
Důvody pro přechod do nativního režimu	283
Popis skupin systému Windows 2000	284
Místní skupiny	284
Místní skupiny domény	284
Globální skupiny	284
Univerzální skupiny	284
Vkládání skupin	286
Rozšíření členství ve skupinách	286
Vliv inovace na skupiny	287
Používání systému NetBIOS v systému Windows 2000	287
Přechod na službu replikace souborů	288

Proces služby replikace systému LAN Manager	288
Proces služby FRS	289
Ponechání služby replikace systému LAN Manager v kombinovaném prostředí	290
Udržení dostupnosti služby replikace systému LAN Manager během inovace	291
Použití služby Směrování a vzdálený přístup v kombinovaném prostředí	292
Plánování restrukturalizace domén	292
Určení důvodů restrukturalizace domén	293
Určení okamžiku restrukturalizace domén	294
Zkoumání dopadů restrukturalizace domén	294
Přesun komitentů zabezpečení	295
Přesun uživatelů a globálních skupin	298
Přesun profilů a atributů SIDhistory	299
Přesun počítačů	300
Přesun členských serverů	301
Vytvoření vztahů důvěryhodnosti	301
Klonování komitentů zabezpečení	301
Scénáře restrukturalizace domén	301
Scénář #1: Postupná migrace uživatelů z Windows NT na Windows 2000	302
Scénář #2: Konsolidace domény prostředků do organizační jednotek.	303
Nástroje migrace domén	305
Nástroj ClonePrincipal	305
Program Netdom	306
Seznam úkolů plánování migrace	307

KAPITOLA 11

Plánování distribuovaného zabezpečení	309
Vývoj plánu zabezpečení sítě	310
Bezpečnostní rizika	311
Koncepty zabezpečení	312
Model zabezpečení	312
Model domény	312
Správa důvěryhodnosti	312
Zásady zabezpečení	312
Konfigurace a analýza zabezpečení	312
Šifrování symetrickým klíčem	313

Šifrování veřejným klíčem	313
Ověřování	313
Jediné přihlášení	313
Dvoufaktorové ověřování	313
Řízení přístupu.	314
Integrita dat.	314
Důvěrnost dat	314
Neodvolatelnost	314
Ověřování kódu.	314
Protokolování událostí	315
Fyzické zabezpečení.	315
Školení uživatelů	315
Strategie distribuovaného zabezpečení	315
Ověřování veškerého přístupu uživatelů	315
Úvahy o plánování	317
Ověřování protokolem Kerberos a důvěryhodnost	317
Fungování ověřování protokolem Kerberos.	317
Implementace ověřování protokolem Kerberos	318
Další úvahy o zabezpečení protokolem Kerberos	318
Přihlašování pomocí karet Smart Card	319
Fungování karet Smart Card	319
Požadavky na implementaci karet Smart Card	319
Implementace karet Smart Card	319
Další úvahy o kartách Smart Card	320
Vzdálený přístup	320
Fungování vzdáleného přístupu.	321
Zásady vzdáleného přístupu	321
Povolení vzdáleného přístupu	321
Další úvahy o vzdáleném přístupu.	321
Aplikování řízení přístupu.	322
Seznamy řízení přístupu.	323
Fungování seznamů ACL.	323
Požadavky na implementaci seznamů ACL	323
Implementace seznamů ACL	323
Skupiny se zabezpečením	324
Fungování skupin se zabezpečením	324
Typy skupin se zabezpečením.	324
Výchozí oprávnění skupin se zabezpečením	325
Požadavky na implementaci skupin se zabezpečením	326
Implementace skupin se zabezpečením	326
Další úvahy o skupinách se zabezpečením	326
Skupiny se zabezpečením a konflikty při replikaci.	327

Vytvoření vztahů důvěryhodnosti	328
Doménová důvěryhodnost	329
Fungování vztahu důvěryhodnosti	329
Požadavky na implementaci vztahů důvěryhodnosti	330
Implementace vztahů důvěryhodnosti	330
Další úvahy o vztazích důvěryhodnosti	330
Zavedení ochrany dat	331
Šifrovaný systém souborů – Encrypting File System (EFS)	331
Fungování systému EFS	332
Požadavky na implementaci systému EFS	332
Implementace systému EFS	332
Další úvahy o systému EFS	332
Zabezpečený protokol IP	333
Fungování protokolu IPSec	334
Požadavky na implementaci protokolu IPSec	334
Implementace protokolu IPSec	334
Další úvahy o protokolu IPSec	335
Nastavení jednotných zásad zabezpečení	336
Zásady skupiny	337
Fungování zásad skupin	337
Požadavky na implementaci zásad skupiny	337
Implementace zásad skupiny	337
Další úvahy o zásadách skupiny	338
Nastavení zabezpečení zásad skupiny	338
Zásady účtů	339
Zásady místního počítače	339
Zásady skupin s omezeným členstvím	340
Zásady systémových služeb	340
Zásady registru	340
Zásady systému souborů	341
Zásady veřejných klíčů	341
Zásady zabezpečení protokolu IP	341
Šablony zabezpečení	341
Fungování šablon zabezpečení	341
Požadavky na implementaci šablon zabezpečení	342
Implementace šablon zabezpečení	342
Další úvahy o šablonách zabezpečení	342
Zavádění zabezpečených aplikací	343
Authenticode a podepisování softwaru	344
Fungování Authenticode	344
Implementace sledování Authenticode	345

Další úvahy o Authenticode a podepisování softwaru	345
Zabezpečená elektronická pošta	345
Fungování zabezpečené elektronické pošty.	346
Další úvahy o zabezpečené elektronické poště	346
Zabezpečená webová sídla a komunikace	346
Další úvahy o zabezpečených webových sídlech.	347
Řízení správy	347
Delegování.	348
Skupiny se zabezpečením, zásady skupiny a seznamy řízení přístupu . . .	348
Zabudované skupiny se zabezpečením.	348
Průvodce delegováním řízení.	348
Průvodce delegováním správy.	348
Delegování řízení objektů zásad skupiny	349
Auditování	349
Fungování auditování.	349
Požadavky na implementaci funkce auditování	349
Implementace funkce auditování	349
Další úvahy o auditování	350
Seznam úkolů plánování distribuovaného zabezpečení	351

KAPITOLA 12

Plánování infrastruktury veřejných klíčů	353
Související informace v sadě Resource Kit.	353
Přehled infrastruktury veřejných klíčů	354
Fungování PKI	354
Požadavky na implementaci PKI.	355
Implementace PKI	356
Vytvoření místního certifikačního úřadu	356
Správa certifikátů	357
Použití webových stránek služby Certificate Services	357
Nastavení zásad veřejných klíčů v objektech zásad skupiny	357
Vytváření infrastruktury veřejných klíčů	358
Návrh infrastruktury veřejných klíčů	359
Určení požadavků na certifikáty.	359
Základní požadavky zabezpečení certifikátů	359
Určení typů vydávaných certifikátů	360
Definování zásad certifikátů a postupů certifikačního úřadu.	361
Zásady certifikátů.	362
Prohlášení o certifikačních postupech (CPS)	362

Definování strategie důvěryhodnosti certifikačních úřadů	362
Výhody hierarchií důvěryhodnosti certifikačních úřadů	363
Výhody seznamů důvěryhodných certifikátů	364
Další úvahy o strategiích důvěryhodnosti certifikačních úřadů	365
Definování požadavků na zabezpečení certifikačních úřadů	365
Definování životních cyklů certifikátů	366
Definování procesů zápisu a obnovení certifikátů	367
Definování zásad odvolávání certifikátů	367
Zásady odvolávání certifikátů	368
Zásady seznamů odvolaných certifikátů	368
Definování strategií údržby	368
Vývoj plánů obnovení po poškození	368
Nefungující certifikační úřad	368
Kompromitovaný certifikační úřad	369
Vývoj vlastních aplikací	369
Plánování prostředků	370
Zavedení infrastruktury veřejných klíčů	371
Plánování postupného zavedení	371
Instalace certifikačních úřadů	372
Instalace a konfigurace podpůrných systémů a aplikací	373
Konfigurace vystavovaných certifikátů	373
Příklady konfigurací	373
Seznamy řízení zabezpečeného přístupu šablon certifikátů	374
Konfigurace publikace seznamů odvolaných certifikátů	374
Konfigurace zásad skupiny z hlediska veřejných klíčů	375
Konfigurace obnovení a zápisu certifikátů	376
Začátek vystavování certifikátů	376
Seznam úkolů plánování infrastruktury veřejných klíčů	377

ČÁST IV

Inovace a instalace systému Windows 2000	379
---	------------

KAPITOLA 13

Automatizování instalace a inovace serveru	381
Rozhodování mezi inovací a čistou instalací	382

Řešení kritických problémů	382
Volba metody instalace	383
Příprava instalace	384
Vytváření distribučních složek	384
Vytvoření struktury distribuční složky	386
\i386	386
\OEM\$	386
\OEM\$\Textmode	388
\OEM\$\\\$.	388
\OEM\$\\1.	388
\OEM\$\\1\Pnpdrivers.	388
\OEM\$\\1\Sysprep	388
\OEM\$Písmeno_jednotky	388
Instalace zařízení hromadného ukládání dat	389
Instalace vrstev HAL (Hardware Abstraction Layer)	390
Instalace zařízení Plug-and-Play	391
Převod délky názvu souboru pomocí souboru \$\$Rename.txt	391
Přehled souboru odpovědí	392
Vytvoření souboru odpovědí	393
Vytvoření souboru odpovědí pomocí Správce instalace	393
Nastavení hesel pomocí souboru odpovědí	395
Rozšiřování oddílů pevného disku	395
Použití souboru odpovědí v Průvodci instalací služby Active Directory	396
Přehled příkazů instalačního programu systému Windows 2000	396
Winnt.exe	397
Winnt32.exe	397
Automatizování instalace serverových aplikací	398
Použití souboru Cmdlines.txt	398
Použití oddílu [GuiRunOnce] souboru odpovědí	399
Řízení instalace více aplikací pomocí dávkového souboru	400
Automatizování instalace systému Windows 2000 Server	401
Nové možnosti automatizované instalace	402
Metody automatizované instalace	403
Použití nástroje Syspart na počítačích s rozdílným hardwarem	403
Duplikování disků pomocí nástroje Sysprep	404
Přehled procesu Sysprep	405
Soubory nástroje Sysprep	406
Ruční spuštění nástroje Sysprep	409

Automatické spuštění nástroje Sysprep po dokončení instalačního programu	410
Rozšiřování diskových oddílů pomocí nástroje Sysprep	411
Použití serveru Systems Management Server	413
Použití spustitelného kompaktního disku	413
Příklad konfigurace instalace	414
Existující servery	414
Příklad 1: Windows NT Server se serverovými aplikacemi kompatibilními se systémem Windows 2000	414
Příklad 2: Počítače se systémem Windows NT Server 3.5 či dřívějším nebo servery s operačními systémy nepocházejícími od společnosti Microsoft.	416
Nové servery	416
Seznam úkolů plánování instalace	417

KAPITOLA 14

Zavádění systému Windows 2000 pomocí serveru Systems Management Server	419
Distribuce softwaru pomocí serveru Systems Management Server	420
Distribuce softwaru pomocí serveru Systems Management Server 2.0	421
Balíčky SMS.	421
Distribuce	422
Inzerování.	422
Doporučené postupy distribuce softwaru pomocí SMS	423
Jak vám server SMS pomůže se zavedením systému Windows 2000	423
Vytvoření balíčku systému Windows 2000 pro server Systems Management Server	425
Příprava balíčku inovace na systém Windows 2000 Server.	425
Umožnění zadání uživatelů během inovace.	428
Prohlídka definice balíčku systému Windows 2000 Server	429
Příprava balíčku inovace na systém Windows 2000 Professional	430
Inovace systému Windows 95 a Windows 98	430
Inovace systému Windows NT Workstation.	431
Distribuce balíčků systému Windows 2000	432
Příprava na distribuci balíčků	432
Kontrola stavu serverů sídel a distribučních bodů	432

Kontrola odpovídajícího počtu distribučních bodů na jednotlivých sídlech	432
Použijte skupiny distribučních bodů	433
Zajistěte správné ovládací prvky odesilatele	433
Zajistěte správnou funkci vějířovité distribuce	433
Vyberte testovací sídlo	434
Distribuce balíčků na sídla a distribuční body	434
Testování distribuce	435
Rozšíření distribuce	435
Distribuce pomocí fyzického dopravce	436
Sledování distribuce	436
Podsystem System Status	436
Hlášení stavu distribuce balíčku	438
Řešení problémů s distribucemi	439
Inzerování balíčků systému Windows 2000	439
Výběr inovovaných počítačů	440
Příprava klientů na příjem inzerátů	441
Inzerování balíčků počítačům	441
Rozšíření zabezpečení na distribučních bodech	442
Inovace počítačů	443
Vykonání inzerátu na jednotlivých počítačích	443
Stav inovace na jednotlivých počítačích	443
Sledování inzerátů	444
Podsystem System Status	444
Stav pro všechny inzeráty	444
Hlášení stavu inzerátu	446
Řešení problémů s inzeráty	447
Zjednodušení konsolidace a migrace domén pomocí serveru	
Systems Management Server	448
Rozdíly mezi servery Systems Management Server 1.2	
a Systems Management Server 2.0	448
Seznam úkolů plánování použití serveru	
Systems Management Server k zavedení systému Windows 2000	449
Další zdroje	450
 KAPITOLA 15	
Inovace a instalace členských serverů	451
Plánování inovace a instalace členských serverů	452

Proces instalace nebo inovace systému Windows 2000	452
Vytvoření plánu inovace a instalace	452
Vytvoření časového plánu	453
Scénář: Minimalizování doby výpadku sítě při inovaci serveru	454
Příprava členských serverů na inovaci nebo novou instalaci	454
Inventarizace existujícího hardwaru	455
Určení požadavků systému	455
Určení kompatibility a spolehlivosti existujícího softwaru	456
Určení kompatibility softwaru jiných výrobců	456
Vykonání úkolů před instalací	457
Vykonání inovace nebo instalace	457
Seznam úkolů před instalací	458
Inovace členských serverů	459
Vykonání nové instalace	459
Určení rolí serverů jednotlivých systémů Windows 2000 Server	459
Souborové servery	460
Svazky systému Macintosh	460
Svazky systému Novell NetWare	461
Testování míst sdílení souborů	462
Tiskové servery	462
Nastavení tiskového serveru	462
Instrukce pro nastavení prostředí síťového tisku	463
Integrace služby Active Directory s tiskovými službami systému Windows 2000	463
Testování míst sdílení tiskáren	463
Aplikační servery	464
Služby součástí systému	465
Terminálové služby	465
Databázový server	465
Webové servery	466
Proxy-servery	466
Vykonání úloh po inovaci a instalaci	467
Testování síťového připojení	467
Ladění síťových serverů	468
Nástroje pro správu systému	468
Seznam úkolů plánování členských serverů	469

KAPITOLA 16

Zavádění terminálových služeb	471
Přehled terminálových služeb	471
Licenční komponenty terminálových služeb	473
Microsoft Clearinghouse	473
Licenční server.	473
Terminálový server.	473
Klientské licence	474
Požadované licence	474
Volitelné licence terminálových služeb	475
Rozšíření od jiných výrobců	475
Vytváření plánu zavedení terminálových služeb	476
Proces zavedení terminálových služeb	476
Určení týmu terminálových služeb	476
Určení požadavků terminálových služeb.	477
Scénář 1: Vzdálená správa pomocí terminálových služeb	477
Scénář 2: Vzdálený přístup	478
Scénář 3: Obchodní aplikace	478
Scénář 4: Centrální zavádění kancelářských počítačů	479
Požadavky na zavedení.	480
Příprava počítačového prostředí.	481
Instalace licenčního serveru na řadič domény	481
Přístup přes rozsáhlou síť	481
Přístup k síťovým službám.	481
Propojení klienta a serveru terminálových služeb	481
Přístup k aktuálnímu prostředí.	482
Úvahy o zavádění aplikací	482
Vytváření návrhu zavedení terminálových služeb	483
Nastavení licenčního serveru	483
Povolení licenčního serveru	483
Aktivování licenčního server	484
Instalace licencí	485
Použití nástroje správy licencí terminálových služeb.	486
Zálohování licenčního serveru.	486
Návrh sítě pro přístup k terminálovému serveru.	487
Vyrovňování zatížení sítě and terminálové služby.	487
Návrh a vytvoření struktury domén.	488

Použití uživatelských profilů a cestovních uživatelských profilů systému Windows 2000	488
Cestovní uživatelské profily	489
Zásady skupiny	489
Přístup k aplikacím	490
Používání domovských adresářů	490
Plánování zabezpečení	491
Systém souborů NTFS	491
Práva uživatelů	492
Práva správce	492
Procedury automatického přihlašování	492
Šifrování	493
Další úvahy o zabezpečení	494
Vzdálený přístup	494
Terminálové služby přes Internet	494
Firewally	495
Konfigurování serverů na zavedení terminálových služeb	495
Příprava na zavedení klientů	496
Zavádění na terminály se systémem Windows CE	496
Zavádění na klientské počítače	497
Inovace na terminálové služby	498
Instalace a konfigurace aplikací	498
Zavádění aplikací z řadiče domény	499
Podpora vícejazyčných a mezinárodních uživatelů	499
Tisk z terminálových služeb	500
Tisk na místní tiskárnu pomocí protokolu RDP	500
Síťové sdílení tiskárny	500
Tisk přes síť WAN nebo telefonické připojení	501
Doporučené postupy konfigurace klientů	501
Plánování testování a pilotních programů	502
Úvahy o testovací laboratoři	502
Sledování výkonu	502
Vyhodnocení výkonu procesoru	502
Vyhodnocení výkonu paměti	503
Vyhodnocení výkonu sítě	503
Použití skupiny odborné pomoci a nástrojů správy	504
Vzdálené řízení	504

Nástroje pro správu	504
Seznam úkolů plánování zavádění terminálových služeb.....	505

ČÁST V

Pokročilá správa	507
-------------------------------	------------

KAPITOLA 17

Určení strategií zabezpečení sítě systému Windows 2000	509
Plánování zabezpečení sítě.....	510
Vyhodnocení rizik zabezpečení sítě	510
Určení velikosti a umístění serveru	512
Příprava personálu.....	512
Vývoj zásad a postupů zabezpečení	512
Vytvoření plánu zavedení technologií zabezpečení	513
Zjištění kategorií uživatelů a jejich potřeb a rizik zabezpečení	513
Vývoj strategií zabezpečených síťových připojení	513
Vytváření hranic zabezpečení.....	513
Zabezpečení proti všem	514
Použití programu Microsoft Proxy Server	515
Sledování zabezpečení sítě	515
Připojení k externím sítím	516
Zavádění technologií zabezpečení sítě	516
Příprava na technologie zabezpečení sítě systému Windows 2000	516
Směrování a vzdálený přístup	517
Zabezpečení služby Směrování a vzdálený přístup.....	518
Virtuální privátní sítě	519
Zavádění sítí VPN.....	520
Kapacita serveru VPN.....	524
Služba Internet Authentication Service.....	524
Zavádění strategií pro uživatele	524
Zavádění strategií pro partnery	526
Seznam úkolů plánování určení strategií zabezpečení sítě	527

KAPITOLA 18

Zajištění dostupnosti aplikací a služeb	529
Zajištění vysoké dostupnosti aplikací a služeb	530
Přehled systému Windows 2000 Advanced Server	530
Proces zajištění vysoké dostupnosti aplikací a služeb	531
Přehled clusteringu systému Windows	532
Určení strategií dostupnosti	532
Sestavení týmu plánování clusteringu	532
Zjištění potřeb vysoké dostupnosti aplikací a služeb	533
Určení hardwarové kompatibility pokročilých funkcí	535
Určení požadavků clusteringu	535
Plánování vyrovňování zatížení sítě	535
Proces plánování klastrů služby Vyrovňování zatížení sítě	537
Určení aplikací, které budou používat vyrovňování zatížení sítě	537
Zavádění klastrů terminálových serverů pomocí vyrovňování zatížení sítě	539
Konfigurování klastrů vyrovňování zatížení sítě pro servery se spuštěnými aplikacemi IIS/ASP a COM+	540
Určení síťových rizik	542
Plánování vyrovňování zatížení sítě	542
Určení požadavků na kapacitu serverů	544
Optimalizování klastrů služby Vyrovňování zatížení sítě	544
Požadavky na službu Vyrovňování zatížení sítě	544
Použití směrovače	545
Plánování služby Cluster Service	545
Proces plánování serverových klastrů	546
Volba aplikací běžících na serverovém klastru	547
Identifikace síťových rizik	548
Určení zásad překlopení a zpětného překlopení pro skupiny prostředků	549
Volba role serveru	550
Volba modelu serverového klastru	550
Plánování služby Cluster Service	557
Určení požadavků na kapacitu pro službu Cluster Service	561
Nástroje automatizace zavedení služby Cluster Service	563
Optimalizování clusterů	564
Plánování disků odolných proti chybám	564
Hardwarové pole RAID	564
Obnovení po chybě	565
Testování kapacity serveru	565

Plánování strategie zálohování a obnovení klastru	566
Seznam úkolů plánování clusterů systému Windows 2000	567
Další zdroje	568

KAPITOLA 19

Určení strategií správy úložišť systému Windows 2000	569
Zlepšení funkcí správy úložišť	570
Vytvoření plánu správy úložišť	570
Vyhodnocení potřeb ukládání dat	571
Výběr systému ukládání dat	572
Správa diskových prostředků	574
Správa disků	574
Základní a dynamická úložiště	575
Správa svazku	576
Body připojení svazku	577
Defragmentace disku	577
Úvahy o použití dynamického úložiště	578
Vyměnitelné úložiště	578
Vzdálené úložiště	579
Vztah mezi službou Vzdálené úložiště a službou Vyměnitelné úložiště. . .	580
Úvahy o použití služby Vzdálené úložiště	580
Optimalizace správy dat	580
Clustering systému Windows	581
Úvahy o použití klastrů ve strategii ukládání dat	582
Vylepšení systému souborů	582
NTFS	582
Správa kvót	583
Distribuovaný systém souborů	584
Úvahy o použití systému DFS ve strategii ukládání dat	586
Služba Indexing Service	586
Integrace se součástmi systému Windows 2000	587
Úvahy o použití služby Indexing Service ve strategii ukládání dat	588
Vylepšení ochrany dat	588
Odolnost proti chybám	589
Správa disků	589
Výběr strategie pole RAID	589

Zálohování	590
Strategie ochrany dat na podnikových sítích	590
Úvahy o návrhu systému ukládání dat odolného proti chybám	590
Zlepšení schopností zotavení po havárii	591
Vytváření zásad zálohování a ukládání dat mimo síťové sídlo	591
Zásady zálohování	591
Úvahy o ukládání mimo síťové sídlo	592
Vytváření plánu zotavení po havárii	592
Testování strategií obnovení systému	593
Praktikování postupů obnovení	593
Dokumentování postupu obnovení	593
Seznam úkolů plánování správy úložišť	594

KAPITOLA 20

Synchronizování služby Active Directory

s adresářovou službou programu Exchange Server	595
Přehled synchronizace adresářů	596
Proces synchronizace adresářů	596
Softwarové součásti systému Windows 2000 Server	596
Hlavní výhody použití ADC	598
Vytváření vztahů pomocí dohod o spojení	600
Vytvoření plánu dohody o spojení služby ADC	601
Sestavení týmu plánování zavedení	601
Získání informací o struktuře domény	
a topologii sídla Exchange Serveru	602
Příprava sítě na zavedení služby ADC	602
Zvážení specifických síťových požadavků	602
Požadavky na počítače	603
Doporučení zavádění	604
Strategie implementace služby ADC	605
Správa objektů	609
Správa objektů z Active Directory	610
Správa objektů z adresářové služby programu Exchange Server 5.5	610
Správa objektů z adresářové služby Active Directory	
i Exchange Serveru 5.5	610
Definování objektů synchronizace adresářů	611
Nastavení dohod o spojení	612

Návrh dohod o spojení	613
Model spojení ADC číslo 1: Jedna doména systému Windows 2000 Server s jediným sídlem programu Exchange Server	613
Model spojení ADC číslo 2: Jedna doména systému Windows 2000 Server s více sídly Exchange Server	614
Model spojení ADC číslo 3: Více domén systému Windows 2000 Server s jediným sídlem programu Exchange Server	615
Dokumentování plánu dohody o spojení ADC	621
Testování konfigurace dohod o spojení.	621
Určení časového plánu synchronizace adresářů	622
Ochrana před náhodnou ztrátou dat	623
Příklad 1: Zaplnění Active Directory novými objekty	624
Příklad 2: Zaplnění atributů (polí) existujících objektů	624
Seznam úkolů plánování synchronizace adresářů	625
Další zdroje	625

ČÁST VI

Zavádění klientů - systém Windows 2000 Professional 627

KAPITOLA 21

Testování kompatibility aplikací se systémem Windows 2000 . . . 629

Přehled testování aplikací.	630
Definice obchodní aplikace	630
Správa testování aplikací	631
Identifikování obchodních aplikací a určení jejich priorit	632
Určení aplikací.	632
Získávání informací o aplikacích	632
Zjednodušení aplikačního prostředí	633
Určení priority aplikací.	634
Příprava plánu testování aplikací	635
Určení rozsahu testování	636
Definování metodologie testování.	636
Studijní případ 1: Festivaly testování.	637
Studijní případ 2: Předběžný program	637
Určení požadavků na prostředky	637
Definování kritérií úspěchu a neúspěchu	638

Vytvoření časového plánu testování	638
Testování aplikací	639
Vývoj strategií testování	639
Strategie pro komerční aplikace	640
Strategie pro vlastní aplikace	640
Tipy testování	641
Obvyklé problémy kompatibility	643
Sledování výsledků testování	645
Volba systému zachytávání	645
Zachytávání dat	646
Hlášení výsledků	646
Řešení nekompatibility aplikací	647
Seznam úkolů plánování testování aplikací	648
Další zdroje	649

KAPITOLA 22

Definování strategie konektivity klientů	651
Přehled konektivity klientů	651
Základní konektivita klientů	653
Služby a protokoly systému Windows 2000	654
Síťoví klienti protokolu TCP/IP	654
Adresářová služba Active Directory	655
Síťoví klienti protokolu IPX	656
Klienti systému Windows na server systému Novell	657
Klienti systému Windows ve smíšeném prostředí systémů Novell NetWare a Windows 2000 Server	657
Tisk na tiskárny systému NetWare	658
Síťoví klienti systému UNIX	658
Pokročilá konektivita klientů	659
Režim asynchronního přenosu (ATM)	660
Přímo připojená síť ATM	660
Síť IP/ATM	660
Sada protokolů sdružení Infrared Data Association	660
Klienti vzdáleného přístupu	661
Telefonické připojení k privátní síti	661
Virtuální privátní síť	662

Metody vzdáleného připojení k síti	662
Sítě malé kanceláře	662
Konektivita sítě SOHO	663
Příklady SOHO	665
Střední až velké sítě	666
Směrování a vzdálený přístup	666
Telefonické připojení k privátní síti	667
Příklad střední až velké sítě	668
Seznam úkolů plánování konektivity klientů	670

KAPITOLA 23

Definování standardů správy a konfigurace klientů	671
Umožnění správy klientských systémů	672
Definování typů uživatelů	674
Vyhodnocení požadavků typů uživatelů	675
Definování softwarových standardů	676
Definování hardwarových standardů	677
Definování významných problémů technické podpory	678
Definování modelu správy a standardů	679
Shrnutí vašich cílů správy a konfigurace	680
Správa klientů pomocí zásad skupiny	680
Porovnání systémových zásad systému Windows NT 4.0	
a zásad skupiny systému Windows 2000	681
Aplikování zásad systému Windows NT 4.0 na systém Windows 2000 . . .	682
Delegování správy klientů pomocí služby Active Directory	684
Delegování správy zásad skupiny	685
Speciální možnosti implementování zásad skupiny	686
Porovnání samostatných funkcí správy s funkcemi správy	
využívajícími službu Active Directory	691
Používání zásad skupiny na samostatných počítačích	692
Konfigurování hardwaru	693
Podpora systému souborů	694
Hardwarové profily	694
Definování standardů uživatelského rozhraní	696
Řízení konfigurace pomocí zásad skupiny	697

Úprava procesů přihlašování a odhlašování	697
Omezení změn na pracovní ploše	698
Omezení změn v nabídce Start	699
Konfigurace možností pro vzdálené uživatele	699
Přidání vícejazyčných možností	700
Úvahy o volbě vícejazyčné verze	701
Inovace na vícejazyčnou verzi systému Windows 2000.	701
Plánování instalace vícejazyčné verze systému Windows 2000.	702
Správa jazyků uživatelského rozhraní pomocí zásad skupiny	704
Zajištění větší přístupnosti systémů	704
Konfigurování funkcí usnadnění systému Windows 2000	705
Použití zařízení jiných výrobců	705
Vyladění konfigurace usnadnění pomocí zásad skupiny	706
Seznam úkolů plánování klientských standardů	706

KAPITOLA 24

Aplikování správy změn a konfigurací	707
Vyhodnocení správy změn a konfigurací	708
Technologie používané k umožnění správy změn a konfigurací.	709
Identifikování potřeb a příležitostí správy změn a konfigurací.	710
Základní potřebné informace.	711
Doplnění funkcí IntelliMirror pomocí serveru Systems Management Server	712
Plánování vylepšené podpory klientů pomocí funkcí IntelliMirror	714
Umožnění funkce vzdálené instalace.	714
Definování požadavků uživatelů	715
Použití funkce vzdálené instalace	716
Konfigurování služeb vzdálené instalace.	718
Příprava obrazů klientských operačních systémů	719
Zlepšení správy softwaru pomocí zásad skupiny.	720
Příprava softwaru na distribuci	721
Když není vytváření nativních aplikací možné.	723
Používání transformací	724
Distribuce softwaru	725
Zacílení softwaru	725
Možnosti správy softwaru	726
Podpora cestujících uživatelů.	727
Podpora sdílených počítačů	727
Podpora mobilních pracovníků	728

Správa softwaru funkcemi IntelliMirror	728
Opravení existujícího softwaru.	730
Inovace existujícího softwaru.	730
Odstranění softwaru.	731
Převedení uživatelských dat a nastavení na síť	731
Zavedení cestovních uživatelských profilů	733
Pokyny pro nastavení cestovních uživatelských profilů.	733
Přesměrování složek	734
Pokyny pro konfiguraci přesměrování složek	734
Konfigurace synchronizování souborů offline	735
Pokyny pro konfiguraci souborů offline	736
Nastavení diskových kvót	736
Pokyny pro nastavení diskových kvót	737
Výběr možností správy změn a konfigurací vaší organizace	737
Přehled základních a pokročilých možností	737
Naplnění potřeb technických uživatelů	739
Naplnění potřeb stacionárních profesionálních uživatelů	739
Naplnění potřeb cestujících profesionálních uživatelů	740
Naplnění potřeb mobilních profesionálních uživatelů	741
Naplnění potřeb uživatelů s konkrétními úkoly	741
Souhrn	742
Seznam úkolů plánování správy změn a konfigurací	743

KAPITOLA 25

Automatizování instalace a inovace klientů	745
Rozhodnutí mezi inovací a čistou instalací	746
Řešení kritických problémů	746
Volba metody instalace	747
Příprava instalace	748
Vytváření distribučních složek	749
Vytvoření struktury distribuční složky.	750
Instalace zařízení hromadného ukládání dat	753
Instalace vrstev abstrakce hardwaru	754
Instalace zařízení Plug-and-Play	755
Převod délky názvu souboru pomocí souboru \$\$Rename.txt	756

Přehled souboru odpovědí	756
Vytvoření souboru odpovědí	757
Nastavení hesel pomocí souboru odpovědí	759
Rozšiřování oddílů pevného disku	760
Přehled příkazů instalačního programu systému Windows 2000	760
Winnt.exe	761
Winnt32.exe	761
Automatizování instalace klientských aplikací	762
Použití souboru Cmdlines.txt	762
Použití oddílu [GuiRunOnce] souboru odpovědí	763
Použití programů instalace aplikace	764
Řízení instalace více aplikací pomocí dávkového souboru	764
Použití instalační služby Windows Installer	765
Terminologie služby Windows Installer	765
Soubor balíčku služby Windows Installer	766
Automatizování instalace systému Windows 2000 Professional	766
Nové možnosti automatizované instalace	766
Metody automatizované instalace	767
Použití nástroje Syspart na počítačích s rozdílným hardwarem	768
Duplikování disků pomocí nástroje Sysprep	769
Přehled procesu Sysprep	770
Soubory nástroje Sysprep	771
Ruční spuštění nástroje Sysprep	774
Automatické spuštění nástroje Sysprep po dokončení instalačního programu	775
Rozšiřování diskových oddílů pomocí nástroje Sysprep	776
Použití serveru Systems Management Server	778
Použití spustitelného kompaktního disku	778
Použití vzdálené instalace operačního systému	779
Dopady zavedení serveru RIS na zatížení sítě	779
Optimalizace výkonu	780
Protokol DHCP a Servery DHCP	780
Řízení výběru serveru RIS a vyrovnávání zatížení	781
Práce se směrovači	783
Příklady konfigurace instalace	783
Existující klientské počítače	784
Příklad 1: Windows NT Workstation 4.0 s klientskými aplikacemi kompatibilními se systémem Windows 2000	784

Příklad 2: Počítače se systémem Windows NT Workstation 3.5 či dřívějším
a klientské počítače s operačními systémy nepocházejícími od společnosti
Microsoft. 785

Nové klientské počítače 786

Seznam úkolů plánování instalace 787

ČÁST VII

Přílohy. 789

PŘÍLOHA A

Ukázkové listy plánování 791

Použití této přílohy 791

Úvod do plánování zavádění systému Windows 2000 793

Služby infrastruktury správy 793

Řešení správy počítačů 795

Funkce zabezpečení 796

Publikování a sdílení informací 797

Podpora aplikací COM 797

Škálovatelnost a dostupnost 798

Práce v síti a komunikace 800

Správa úložišť 801

Vytváření testovací laboratoře systému Windows 2000 802

Příprava infrastruktury sítě na systém Windows 2000 804

Určení strategií migrace domén 805

Plánování distribuovaného zabezpečení 806

Automatizování instalace a inovace serveru. 807

Inovace a instalace členských serverů 809

Pracovní list plánování členských serverů 810

Plán zálohování dat serveru a zotavení po havárii 811

Určení nových hardwarových požadavků 812

Zaznamenání specifikací serverů 812

Tiskové servery 812

Souborové servery 813

Aplikační servery 814

Webové servery 814

Naplánování inovace nebo čisté instalace	814
Určení priorit zavedení každého členského serveru	814
Zajištění dostupnosti aplikací a služeb	815
Určení potřeb vysoké dostupnosti	815
Specifikace aplikace a služby.	815
Plánování vyrovňování zatížení sítě	818
Synchronizování služby Active Directory s adresářovou	
službou programu Exchange Server	820
Vytvoření dohod o spojení	820
Vytvoření časového plánu synchronizace adresářů.	823
Záznam kontaktů synchronizování adresářů.	824
Skupina správců schéma.	824
Správce domény systému Windows 2000	824
Správce sídla programu Exchange Server 5.5.	824
Testování kompatibility aplikací se systémem Windows 2000.	824
Definování standardů správy a konfigurace klientů.	826
Definování požadavků zásad skupiny	828
Aplikování správy změn a konfigurací.	831
Automatizování instalace a inovace klientů.	833

PŘÍLOHA B

Příkazy instalačního programu	835
Instalace systému Windows 2000 pomocí příkazů instalačního programu.	835
Syntaxe příkazu Winnt32	836
Winnt.	839

PŘÍLOHA C

Příklady souborů odpovědí pro bezobslužnou instalaci	841
Formát souboru odpovědí	841
Klíče a hodnoty souboru odpovědí	842
Ukázkové soubory odpovědí	842
Příklad 1 – Výchozí soubor Unattend.txt.	842

Příklad 2 – Bezobslužná instalace systému Windows 2000 Professional z disku CD-ROM	844
Příklad 3 – Instalace a konfigurace systému Windows 2000 a konfigurace aplikace Microsoft Internet Explorer nastaveními proxy	845
Příklad 4 – Instalace a konfigurace systému Windows 2000 Server se dvěma síťovými adaptéry	849
Příklad 5 – Instalace systému Windows 2000 Advanced Server s vyrovnáváním zatížení sítě	851
Příklad 6 – Instalace systému Windows 2000 Advanced Server se službou Windows Clustering	854

PŘÍLOHA D

Nástroje zavádění	859
Další zdroje	867

PŘÍLOHA E

Možnosti usnadnění pro postižené osoby	869
Přehled možností usnadnění systému Windows 2000	869
Výhody usnadnění v systému Windows 2000	870
Úvahy před inovací na systém Windows 2000	871
Zavádění systému Windows 2000 s možnostmi usnadnění	872
Technologie Active Accessibility	872
Výrobky a služby jiných společností	872
Logo „Certified for Windows“	873
Použití funkce Posloupnost kláves s doplňkovým hardwarem a softwarem	873
Úprava počítače pro možnosti usnadnění	874
Vzdálená instalace a bezobslužná instalace z disku CD	874
Služba Windows Installer	874
Zásady skupiny	875
Vytvoření více uživatelských profilů	875
Možnosti správy	875
Reset (vypršení) usnadnění	875
Systém Active Desktop	876

Konfigurace možností usnadnění v systému Windows 2000	877
Konfigurace možností usnadnění pomocí	
Průvodce funkcemi usnadnění	878
Konfigurace možností usnadnění pomocí ovládacího panelu	879
Nastavení možností usnadnění podle typu postižení	879
Možnosti pro uživatele s postižením rozpoznávání	879
Formát Synchronized Accessible Media Interchange	880
Možnosti pro uživatele s postižením sluchu	880
Upravitelná zvuková schémata	880
Úprava hlasitosti	880
Funkce Zobrazení zvuku	880
Funkce Popis zvuku	881
Formát Synchronized Accessible Media Interchange	881
Možnosti pro uživatele s fyzickým postižením	881
Možnosti klávesnice	881
Možnosti myši	883
Možnosti pro uživatele se záchvaty	884
Vzory časování	884
Zvuková schémata	884
Nastavení barvy a kontrastu	885
Možnosti pro uživatele s postižením zraku	885
Narrator	885
Zvuková signalizace klávesnice	885
Lupa	885
Schémata velikosti a barvy	886
Barevná schémata s vysokým kontrastem	887
Nové ukazatele myši	887
Další zdroje	887
Glosář	889
Rejstřík	945

Úvod

Vítá vás kniha *Microsoft Windows 2000 Server Plánování a implementace sítě*.

Sada *Microsoft Windows 2000 Server Resource Kit* se skládá z pěti svazků a dvou kompaktních disků (CD) obsahujících nástroje, další referenční materiály a online verzi všech knih. Objeví-li se nové informace, budou vydány dodatky sady *Windows 2000 Server Resource Kit*, a aktualizace a informace se budou průběžně objevovat také na síti WWW.

O knize Microsoft Windows 2000 Server Plánování a implementace sítě

Kniha *Microsoft Windows 2000 Server Plánování a implementace sítě* poskytuje jak instrukce pro plánování implementace systému, tak i strategie zavádění různých technologií, které tvoří systém Microsoft Windows 2000. Tento průvodce upozorňuje na body důležitých rozhodnutí a nabízí technické informace, které vám pomohou určit pořadí a procesy zavádění. Průvodce také poskytuje podrobné procedury automatizace instalací serverů i klientů. V dalších svazcích sady *Windows 2000 Server Resource Kit* najdete podrobnější informace o jednotlivých technologiích systému Windows 2000 včetně jejich funkce a údržby ve vaší organizaci.

Cíle tohoto průvodce

Tento průvodce je vytvořen tak, aby pomáhal týmům plánování projektu, které mají na starosti zavedení systémů Microsoft Windows 2000 Server a Microsoft Windows 2000 Professional. Jsou tu informace pro management, architekty sítě, správce systému a další členy organizace informačních technologií (IT), kteří se budou účastnit plánování zavádění systému Windows 2000.

Základními cíli tohoto průvodce je pomoci vám:

- určit současný stav sítě, stav, jakého chcete dosáhnout, a způsoby, jakými lze žádaného stavu docílit pomocí systému Windows 2000,
- určit, co musíte zvážit na všech úrovních plánování od svých obchodních či výrobních cílů postupného zavádění systému Windows 2000 až po laboratorní testování,
- vytvořit dokumenty plánování, které budou představovat cestu hladkého zavádění nové infrastruktury sítě,
- začít s instalací systému Windows 2000 a s využíváním mnoha jeho funkcí.

Prvky průvodce

Struktura tohoto průvodce je navržena tak, aby usnadnila organizacím s různými potřebami vyhledání obsahu, který nejlépe odpovídá jejich cílům zavádění systému Windows 2000.

Struktura průvodce

Tento průvodce je strukturován tak, že k jeho obsahu můžete přistupovat různými způsoby. Můžete procházet kapitolami postupně a začít částí 1 s celkovým přehledem všech problémů a procesů plánování zavádění. Pak můžete přejít do další fáze uvedené v části 2, kde se dozvíte o tom, jak připravit současnou infrastrukturu sítě a zajistit co nejhladší přechod na systém Windows 2000. Následně se můžete věnovat buď plánování služby Active Directory nebo přejít až do části 4 „Inovace a instalace systému Windows 2000“ a seznámit se s podrobnými postupy instalace serverů. Nebo se můžete rovnou věnovat části 6, pokud vás zajímá především zavádění klientů. Na začátku každé části najdete přehled jejího obsahu.

Struktura kapitol

Nejvíce informací z kapitol načerpáte, když si je přečtete od začátku do konce a když se zaměříte na jejich dále popsané součásti.

Cíle kapitoly

Na začátku každé kapitoly je oddíl „Cíle kapitoly“. Tyto cíle identifikují dokumenty plánování, které vám kapitola pomůže vytvořit. Kapitoly uvádějí doporučení a postupy získávání informací potřebných k vytvoření uvedených dokumentů plánování.

Vývojové diagramy

První oddíl každé kapitoly také uvádí vývojový diagram úkolů. Jedná se o doporučené základní úkoly, které byste měli vykonat v zájmu vytvoření plánu nebo plánů pro určitou fázi zavádění, jako je například plán zavedení adresářové služby Active Directory nebo plán vybudování testovací laboratoře. Obsah kapitoly je uvedený v pořadí úkolů ve vývojovém diagramu.

Body důležitých rozhodnutí

V určitých fázích plánování zavádění budete muset učinit závažná rozhodnutí, která budou mít významné dopady na náklady, či dobu zavádění, nebo na oba tyto prvky. Rozhodnutí učiněná v takových bodech mohou ovlivnit nejen zavádění systému Windows 2000, ale také budoucí produktivitu vaší organizace a následně její ziskovost. Tyto body rozhodnutí, které ovlivňují samotné základy celého systému, se objevují v různých kapitolách.

Seznamy úkolů plánování

Každá kapitola končí tabulkou, jež uvádí úkoly popsané v kapitole. Můžete ji využít jako kontrolní seznam a s její pomocí se ujistit, že jste se zabývali všemi důležitými otázkami.

Pracovní listy plánování

Mnoho kapitol vás také odkazuje na přílohu „Ukázkové listy plánování“ v této knize. Ty vám pomohou s vývojem dokumentů plánování, ale můžete je použít také jako základní šablony při vytváření svých vlastních formulářů. Budete totiž potřebovat nějaký formalizovaný způsob získávání a sběru informací pro účely plánování.

Konvence dokumentů

V celém tomto průvodci se používají následující konvence stylů a terminologie.




Prvek	Význam
Tučné písmo	Znaky, které zapíšete přesně tak, jak je uvedeno, včetně příkazů a přepínačů. Tučně jsou označeny také prvky uživatelského rozhraní.
<i>Kurzíva</i>	Proměnné, které musíte nahradit nějakou hodnotou. Například označení <i>Nazev_souboru.pri</i> může pro daný případ představovat libovolný platný název soubor.
Neproporcionální písmo	Ukázka kódu.
%SystemRoot%	Složka, v níž je instalovaný systém Windows 2000.

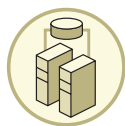
Upozornění pro čtenáře	Význam
Tip	Upozorňuje vás na dodatečné informace, které však nejsou k dokončení daného úkolu podstatné.
Poznámka	Upozorňuje vás na dodatečné informace.
Důležité	Upozorňuje vás na dodatečné informace, které jsou podstatné pro dokončení daného úkolu.
Upozornění	Upozorňuje vás na možnou ztrátu dat, narušení zabezpečení nebo jiné závažnější problémy.
Varování	Upozorňuje vás, že vykonání nebo naopak nevykonání určitých akcí vám může způsobit fyzickou újmu nebo poškodit zařízení.
Důležité rozhodnutí	Upozorňuje vás na rozhodnutí, které lze jen velmi obtížně později změnit.

Grafické symboly

Tabulka I.1 obsahuje grafické symboly používané v obrázcích v celém svazku. Můžete ji používat při studování diagramů v tomto průvodci.

Tabulka I.1 Grafické symboly

Symbol	Význam	Symbol	Význam	Symbol	Význam
	<i>Token přístupu.</i> Objekt, který obsahuje informace o uživateli a používá se pro účely zabezpečení.		<i>Automatizovaná knihovna.</i> Páskové nebo diskové knihovny, které obsahují kolekci médií a jednu nebo více jednotek.		<i>Klient.</i> Počítač, který přistupuje ke sdíleným síťovým prostředkům poskytovaným jiným počítačem.



Klaster. Skupina nezávislých počítačů, které společně pracují jako jediný systém.



Databáze. Libovolná kolekce dat uspořádaná pro ukládání a přístup pomocí počítačů.



Dokument. Libovolná samostatná část práce vytvořená nějakým aplikačním programem a uložená na disk.



Doména. V systému Windows 2000 je to kolekce počítačů definovaných administrátorem, které sdílejí společnou databázi adresářů.



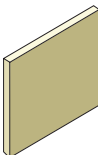
Elektronická pošta. Výměna textových zpráv a počítačových souborů přes nějakou komunikační síť.



Selbání. Neschopnost počítačového systému nebo souvisejícího zařízení na svou chybu upozornit během určité doby.



Složka souborů. Adresář nebo podadresář.



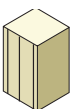
Firewall. Část systému zabezpečení používaná k zabránění neoprávněného přístupu na síť.



Obecný server. Počítač se spuštěným softwarem správy.



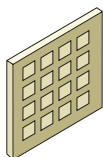
Pevný disk. Zařízení používané k magnetickému ukládání dat.



Hostitel. Hlavní počítač v systému počítačů nebo terminálů propojených komunikačními linkami.



Hostitel. Hlavní počítač v systému počítačů nebo terminálů propojených komunikačními linkami.



Filtr I/O. Sada definic indikujících směrovač typ provozu povoleného na jednotlivých rozhraních.



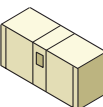
Internet. Představuje celosvětovou kolekci sítí, které vzájemně komunikují.



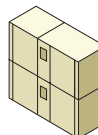
Notebook nebo přenosný počítač. Malý, přenosný osobní počítač.



Klient systému Macintosh. Osobní počítač v síti vyrobený společností Apple Computer Corporation.



Mainframový počítač. Počítač vysoké úrovně navržený pro nejintenzivnější úkoly.



Mainframový počítač. Počítač vysoké úrovně navržený pro nejintenzivnější úkoly.



Doména v kombinovaném režimu. Režim, v němž v jedné doméně existují zároveň řadiče domény se systémy Windows 2000 a Windows NT.



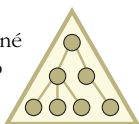
Modem. Komunikační zařízení umožňující počítači přenášet informace přes standardní telefonní linku.



Modemová banka. Kolekce modemů připojených k jedinému serveru.



Síťový adaptér. Rozšiřující karta nebo jiné zařízení sloužící pro připojení počítače k místní síti.



Organizační útvar (jednotka). Struktura v doméně.



Organizační útvar (jednotka). Logický kontejner obsahující uživatele, skupiny, počítače a další organizační útvary.



Pakety. Jednotky síťového přenosu pevné maximální velikosti.



Tiskárna. Tiskové zařízení, které je přímo připojené k síti.



Spojení vzdáleného přístupu. Telefonické spojení mezi servery, řadiči domén a sídly.



Kořen. Nejvyšší neboli nejhornější úroveň v hierarchicky uspořádaných sadě informací.



Směrovač. Prostřednické zařízení, které směruje a optimalizuje síťový provoz.



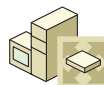
Klíč zabezpečení. Popisovač zabezpečení, který obsahuje místní zásady zabezpečení.



Serverová farma. Skupina serverů, které zajišťují služby pro síť.



Sídlo. Jedna nebo více dobře propojených podsítí TCP/IP.



Směrovač. Počítač fungující jako prostřednické zařízení na komunikační síti.



Přepínač nebo brána. Zařízení spojující dvě sítě, které je schopno předávat nebo blokovat pakety.



Páska nebo pásková záloha. Formát páskové kazety používaný k zálohování dat.



Pásková jednotka. Zařízení pro čtení a zápis pásků.



Terminál. Zařízení skládající se z grafické karty, monitoru a klávesnice, které samo prakticky nic nepracovává a je připojeno k počítači přes komunikační linku.



Tunel. Logická cesta, kterou procházejí zabalené pakety přenosovými sítěmi.



Doména systému Windows NT. Síťová sada počítačů, na kterých běží systém NT 4.0 a které sdílejí databázi SAM, jež lze spravovat jako skupinu.



Systém Windows 2000 Server. Server zajišťující centralizované řízení sítě.



Zdroj nepřerušitelného napájení. Zařízení mezi zdrojem napájení a počítačem, které zajišťuje nepřetržité napájení počítače.

Kompaktní disk sady Resource Kit

Doprovodný disk CD sady *Windows 2000 Server Resource Kit* obsahuje různé nástroje a prostředky, které vám pomohou pracovat se systémem Windows 2000 efektivněji.

Poznámka Nástroje obsažené na CD jsou vytvořeny pro severoamerickou verzi systému Windows 2000, na které jsou také otestovány. Použití těchto nástrojů na jiných verzích systému Windows 2000 nebo na verzích systému Microsoft Windows NT může mít nepředvídatelné výsledky.

Doprovodné CD sady *Resource Kit* obsahuje tyto položky:

Online knihy sady Windows 2000 Server Resource Kit

Tištěné knihy ve verzi nápovědy HTML. Tyto knihy používejte k vyhledání stejných podrobných informací o systému Windows 2000, které se nacházejí také v tištěné verzi. Chcete-li najít nejvhodnější informace potřebné pro dokončení určitého úkolu, prohledejte všechny knihy.

Nápověda nástrojů sady Windows 2000 Server Resource Kit

Více než 200 softwarových nástrojů, dokumentace a dalších prostředků, které vám pomáhají ovládat moc a sílu systému Windows 2000. Tyto nástroje použijte ke správě služby Active Directory, ke správě funkcí zabezpečení, pro práci s registrem, při automatizování opakujících se činností a při mnoha jiných důležitých činnostech. Více se o použití nástrojů pro správu dozvíte v dokumentaci nápovědy k nástrojům.

Popisy sady Windows 2000 Resource Kit

Sada popisů ve formě nápovědy HTML:

- **Error and Event Messages Help** (nápověda k chybovým hlášením a hlášením událostí) obsahuje většinu chybových hlášení a hlášení událostí generovaných systémem Windows 2000. U každého hlášení je podrobné vysvětlení a navrhovaná akce uživatele.
- **Technical Reference to the Registry** (technický popis registru) poskytuje podrobný popis obsahu registru systému Windows 2000, jako jsou podstromy, klíče, podklíče a položky, s nimiž se mohou seznámit pokročilí uživatelé. Je tu také mnoho nastavení, která nelze změnit pomocí nástrojů nebo programovacích rozhraní systému Windows 2000.
- **Performance Counter Reference** (popis čítačů výkonu) popisuje všechny objekty a čítače výkonu, jejichž použití umožňuje modul snap-in Výkon (Performance) systému Windows 2000. Tento popis použijte, chcete-li se dozvědět více o tom, jak vám mohou hodnoty čítačů pomoci při diagnostikování problémů či detekování úzkých míst ve vašem systému.
- **Group Policy Reference** (popis zásad skupiny) obsahuje podrobný popis nastavení zásad skupiny v systému Windows 2000. Tyto popisy vysvětlují vliv povolení, zákazu nebo nenakonfigurování jednotlivých zásad i vysvětlení, jak spolu související zásady pracují.

Zásady podpory sady Resource Kit

Software dodaný v sadě *Windows 2000 Server Resource Kit* není podporován. Společnost Microsoft nezaručuje výkon nástrojů sady *Windows 2000 Server Resource Kit* a nezavazuje se do nějaké doby reagovat na otázky ani řešení chyb v těchto nástrojích. Umožňujeme však zákazníkům, kteří si zakoupí sadu *Windows 2000 Server Resource Kit*, hlásit chyby a v některých případech také získávat jejich řešení. Toho dosáhnete odesláním zprávy elektronické pošty na adresu rkinput@microsoft.com. Tato adresa elektronické pošty slouží pouze pro problémy související se sadou *Windows 2000 Server Resource Kit*. Problémy související s operačním systémem Windows 2000 řešte prosím v souladu s informacemi o podpoře, které jsou součástí vašeho produktu.

ČÁST I

Přehled plánování



Určení nejlepšího postupu akcí zavádění systému Microsoft Windows 2000 ve vaší organizaci vytváří základní předpoklady úspěchu. Část 1 poskytuje informace o plánování, které vám pomohou určit funkce systému Windows 2000 vhodné pro vaši organizaci, vytvořit plán zavádění, připravit testovací laboratoř a vykonat pilotní projekt.

V této části:

Úvod do plánování zavedení systému 3

Vytvoření cesty postupného zavádění 29

Plánování zavedení 57

Vytvoření testovací laboratoře systému Windows 2000 77

Vykonání pilotního programu systému Windows 2000 117

KAPITOLA 1

Úvod do plánování zavedení systému Windows 2000



Kniha *Microsoft Windows 2000 Server Plánování a implementace sítě* je nástroj, který můžete používat během návrhu, plánování a vývoje postupu zavádění systému Microsoft Windows 2000. Při čtení této knihy získáte přehled o tom, jak je zavedení zapotřebí naplánovat – na úrovni správy projektu i na úrovni jednotlivých funkcí. V této knize najdete informace o plánování, které vám pomohou začít, jako jsou informace o vytvoření testovací laboratoře a spuštění pilotního programu, i důležitá technická pojednání, jež vám pomohou se zaváděním různých technologií systému Windows 2000.

V této kapitole začnete proces plánování. Obsahuje úvod k této knize a krátký přehled systému Windows 2000 a jeho funkcí. Dále najdete studie ukazující, jak čtyři různé společnosti začaly svůj proces plánování zavedení. V kapitole najdete také přehled funkcí z hlediska informačních technologií (IT). Právě tímto přehledem můžete začít svůj proces plánování zavedení.

V této kapitole

Spuštění plánu 4

Přehled rodiny produktů Windows 2000 6

Použití Windows 2000 pro zlepšení způsobů práce 9

Příklady naplnění obchodních či výrobních potřeb systémem Windows 2000 11

Přizpůsobování funkcí systému Windows 2000

vašim obchodním či výrobním potřebám 18

Plánování seznamu úloh pro mapování možností Windows 2000 27

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Seznam produktů Windows 2000 pro vaši organizaci
- Plán přiřazení funkcí systému Windows 2000 vašim obchodním či výrobním potřebám

Související informace v sadě Resource Kit

- Další informace o započítí procesu plánování zavedení najdete v kapitole „Vytvoření cesty postupného zavádění“ v této knize.
- Další informace o plánování zavedení najdete v kapitole „Plánování zavedení“ v této knize.

Spuštění plánu

Zavedení nového operačního systému, jakým je systém Windows 2000, v podnikovém prostředí je úkol vyžadující nejen schválení výkonným managementem a finanční zajištění, ale také značně rozsáhlé plánování. Na začátku plánování musíte porozumět rodině produktů Windows 2000. Dále se musíte seznámit s jejich funkcemi a s možnostmi jejich využití v zájmu zvýšení produktivity práce a snížení celkových nákladů na pořízení (Total Cost of Ownership – TCO) ve vaší organizaci. Následující dva oddíly představují přehled procesu plánování popsaného v této kapitole a úvod do používání této knihy.

Efektivní používání této knihy

Tato kniha vám pomůže s návrhem, plánováním a implementací zavedení systémů Microsoft Windows 2000 Professional a Microsoft Windows 2000 Server. Poskytuje postupy a možnosti řešení důležitých obchodních či výrobních potřeb pomocí hlavních funkcí systému Windows 2000. Obsahuje také podrobné instrukce pro automatizování instalací systémů Windows 2000 Server a Windows 2000 Professional pomocí nástrojů, jakými jsou bezobslužná instalace, skripty a server Microsoft Systems Management Server. Informace jsou uvedeny v logickém pořadí, které můžete využít v začátku zavádění.

Dosažení těchto cílů zajišťují tři různé typy kapitol:

- Plánovací kapitoly poskytují informace, které vám umožní úspěšné naplánování postupného zavádění; patří sem kapitoly testování a plánování.
- Kapitoly technických návrhů nabízejí informace, které vám budou pomáhat s implementací specifických funkcí systému Windows 2000, jako je adresářová služba Active Directory, a s návrhem takové sítě systému Windows 2000, která naplní potřeby vaší organizace.
- Kapitoly o automatizované instalaci uvádějí podrobné informace o instalování systémů Windows 2000 Server a Windows 2000 Professional pomocí takových nástrojů, jako je server Systems Management Server.

Tabulka 1.1 uvádí všech šest částí této knihy a kapitoly, které do jednotlivých částí patří.

Tabulka 1.1 Kapitoly knihy Microsoft Windows 2000 Server Plánování a implementace sítě

Číslo	Název části/kapitoly	Typ
Část 1: Přehled plánování		
Poskytuje informace, které vám pomohou s určitými aspekty plánování zavádění, a obsahuje informace o testování a pilotních programech.		
1	Úvod do plánování zavedení systému Windows 2000	Plánování
2	Vytvoření cesty postupného zavádění	Plánování
3	Plánování zavádění	Plánování
4	Vytvoření testovací laboratoře systému Windows 2000	Plánování
5	Vykonání pilotního programu systému Windows 2000	Plánování

Část 2: Předpoklady infrastruktury sítě

Poskytuje informace, které vám pomohou s vyhodnocením současné sítě a s plánováním inovace sítě.

6	Příprava infrastruktury sítě na systém Windows 2000	Technický návrh
7	Určení strategií konektivity sítě	Technický návrh
8	Analýza infrastruktury sítě pomocí serveru Systems Management Server	Technický návrh

Část 3: Infrastruktura služby Active Directory

Poskytuje informace, které vám budou pomáhat s plánováním zavedení specifických technických funkcí.

9	Návrh struktury služby Active Directory	Technický návrh
10	Určení strategií migrace domén	Technický návrh
11	Plánování distribuovaného zabezpečení	Technický návrh
12	Plánování infrastruktury veřejných klíčů	Technický návrh

Část 4: Inovace a instalace systému Windows 2000

Poskytuje informace o inovace a instalace serverů, členských serverů a terminálových služeb.

13	Automatizování instalace a inovace serveru	Automatizovaná instalace
14	Zavádění systému Windows 2000 pomocí serveru Systems Management Server	Automatizovaná instalace
15	Inovace a instalace členských serverů	Automatizovaná instalace
16	Zavádění terminálových služeb	Technický návrh

Část 5: Pokročilá správa

Poskytuje informace, které vám pomohou s plánováním pokročilejších funkcí.

17	Určení strategií zabezpečení sítě systému Windows 2000	Technický návrh
18	Zajištění dostupnosti aplikací a služeb	Technický návrh
19	Určení strategií správy úložišť systému Windows 2000	Technický návrh
20	Synchronizování služby Active Directory s adresářovou službou programu Exchange Server	Technický návrh

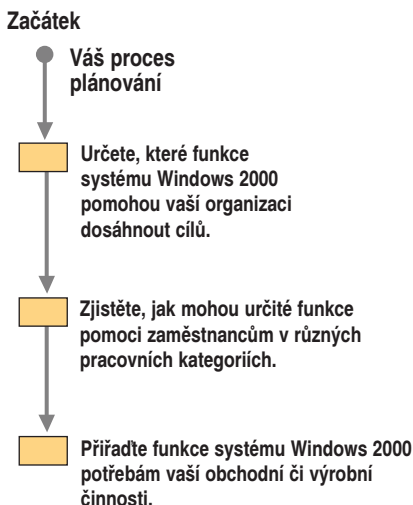
Část 6: Zavádění klientů – systém Windows 2000 Professional

Poskytuje informace, které vám pomohou naplánovat a zavést klienty systému Windows 2000 Professional.

21	Testování kompatibility aplikací se systémem Windows 2000	Technický návrh
22	Definování strategie konektivity klientů	Technický návrh
23	Definování standardů správy a konfigurace klientů	Technický návrh
24	Aplikování správy změn a konfigurací	Technický návrh
25	Automatizování instalace a inovace klientů	Automatizovaná instalace

Jak začít plánování

Plánování instalace nebo inovace operačního systému vyžaduje mnoho kroků a značné znalosti. V této kapitole najdete informace, které vám pomohou začít s procesem plánování. Obrázek 1.1 ilustruje kroky plánování popsané v této kapitole.



Obrázek 1.1 Jak začít plánování

Přehled rodiny produktů Windows 2000

Udržet si konkurenceschopnost v nové digitální ekonomice vyžaduje pokročilou počítačovou infrastrukturu vycházející z konfigurace klient/server, která snižuje náklady a umožňuje vaší organizaci rychle se přizpůsobovat změnám. Platforma Microsoft Windows 2000 – kombinace systémů Windows 2000 Professional a Windows 2000 Server – přináší organizacím všech velikostí následující výhody:

- Nižší celkové náklady na pořízení (TCO)
- Spolehlivou platformu práce s počítači 24 hodin denně a 7 dní v týdnu
- Digitální infrastrukturu, která se dokáže přizpůsobovat rychlým změnám

Celá rodina produktů je vytvořena tak, aby podporovala služby práce v síti, aplikací, komunikací a sítě WWW se zvýšenou spravovatelností, spolehlivostí, dostupností, možnostmi spolupráce, škálovatelností a zabezpečením. K naplnění potřeb práce s počítači organizací všech velikostí slouží několik produktů Windows 2000. Následující oddíly popisují jednotlivé produkty, které jsou součástí rodiny systémů Windows 2000.

Windows 2000 Professional

Systém Windows 2000 Professional umožňuje uživatelům zvýšení produktivity při různých pracích a v různých situacích (například u mobilních a vzdálených uživatelů), zajišťuje nejvyšší úroveň zabezpečení uživatelských dat a poskytuje výkon nezbytný pro novou generaci osobních aplikací produktivity. Systém Windows 2000 Professional pomáhá snížit celkové náklady na vlastnictví prostřednictvím těchto technik:

Zlepšené možnosti správy klientů

Systém Windows 2000 umožňuje vašim správcům plně řídit klientská data a aplikace a nastavení systému, což pomáhá snížit počet zásahů technické podpory. Zajišťuje také, že uživatelé nemohou náhodně poškodit svůj systém, a dovoluje vašim uživatelům

přístup k nástrojům, které potřebují ke své práci, po 24 hodin denně, i když pracují na počítači někoho jiného.

Široká podpora nástrojů správy

V zájmu zlepšení spravovatelnosti informačních technologií obsahuje systém Windows 2000 Professional „klientské agenty“, kteří umožňují efektivně pracovat významným řešením správy, jako je například systém Systems Management Server.

Snadné použití

Uživatelské rozhraní bylo upraveno tak, aby zajišťovalo snazší přístup k informacím pomocí vlastních nabídek a seznamů naposledy použitých položek. (Operační systém sleduje, které úkoly vykonáváte nejčastěji, a ty pak zobrazuje ve viditelné části každé nabídky.)

Vyšší úroveň stability

Systém Windows 2000 Professional je vytvořen jako nejspolehlivější nabízený klientský a mobilní operační systém. Klienti mohou nyní pracovat déle, což zajišťuje vyšší úroveň produktivity.

Větší podpora zařízení

Systém Windows 2000 Professional podporuje více než 7000 zařízení; patří sem také rozšířená podpora mnoha zařízení, která nebyla v systému Microsoft Windows NT Workstation verze 4.0 podporována, jako je řada starších tiskáren, skenery a digitální fotoaparáty. To představuje 60procentní nárůst počtu zařízení podporovaných v systému Windows NT 4.0. Systém Windows 2000 Professional také podporuje technologii Microsoft DirectX verze 7.0, sadu programovacích rozhraní aplikací (API) pracujících na nízké úrovni, které na počítačích se systémem Windows umožňují přístup k výkonné akceleraci médií.

Poznámka Další informace o podporovaných zařízeních najdete v odkazu Microsoft Windows Hardware Compatibility List (HCL) stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Snazší konfigurace

Noví průvodci zjednodušují konfiguraci a nastavení systému Windows 2000 Professional.

Více jazykových možností

Technologie MultiLanguage (podpory více jazyků) nabízí nevídané vícejazyčné možnosti koncovým uživatelům a správcům.

Další informace o systému Windows 2000 Professional najdete v kapitolách části 6 této knihy.

Rodina systémů Windows 2000 Server

Rodina systémů Windows 2000 Server má dva členy: Standard a Advanced. Edice Standard nabízí základní funkce důležitých služeb (včetně souborových, tiskových, komunikačních a webových serverů a serverů infrastruktury) vhodných pro malé a střední organizace s mnoha pracovními skupinami a pobočkami. Edice Advanced slouží k naplnění velmi důležitých (mission-critical) potřeb, jako je tomu u velkých datových skladů, elektronické komerce nebo služeb webového hostování středních a velkých organizací a poskytovatelů připojení k Internetu (Internet Service Provider – ISP).

Systém Windows 2000 Server Standard

Jádrem systému Windows 2000 Server je úplná sada služeb infrastruktury vycházející z adresářové služby Active Directory. Active Directory zjednodušuje správu, posiluje zabezpečení a rozšiřuje možnosti spolupráce (interoperability). Poskytuje centralizovanou metodu správy uživatelů, skupin, služeb zabezpečení a síťových prostředků. Navíc má služba Active Directory řadu standardních rozhraní, což umožňuje její spolupráci s různými aplikacemi a zařízeními.

Systém Windows 2000 Server poskytuje rozsáhlou sadu internetových služeb, které umožňují organizacím využívat nejnovější webové technologie. Tato integrovaná, flexibilní webová platforma má velký rozsah služeb, které lze využít k zavedení intranetů a webových řešení. Patří sem hostování webových sídel, pokročilé webové aplikace a podpora datových proudů.

Systém Windows 2000 Server rozšiřuje aplikační služby nabízené systémem Microsoft Windows NT Server verze 4.0. Integrovaním aplikačních služeb, jako jsou služby Component Services, podpora transakcí a řazení zpráv a podpora jazyka Extensible Markup Language (XML), se systém Windows 2000 Server stává ideální platformou jak pro řešení nezávislých výrobců softwaru tak i pro vaše vlastní obchodní aplikace.

V několika posledních letech těžilo mnoho společností z rychlého vývoje, jakého dosáhli výrobci v rychlostech mikroprocesorů. Aby bylo možné zvýšit výkon systému pomocí rychlejších procesorů, systém Windows 2000 Server také podporuje jednoprocesorové systémy a systémy čtyřcestného symetrického multiprocessingu (symmetric multiprocessing – SMP) s až 4 gigabajty (GB) fyzické paměti.

Obchodní či výrobní server s operačním systémem Windows 2000 má víceúčelové schopnosti vyžadované klienty i servery jak v tradičním modelu klient/server tak i v pracovních skupinách. Vaše organizace může také vyžadovat další zavedení souborových a tiskových serverů, aplikačních serverů, webových serverů a komunikačních serverů v jednotlivých odděleních. Mezi klíčové funkce operačního systému, které vám budou pomáhat s instalací a konfigurací serverů vykonávajících tyto různé role, patří:

- Služba Active Directory
- Funkce IntelliMirror a zásady skupiny
- Ověřování protokolem Kerberos a zabezpečení infrastrukturou veřejných klíčů (Public Key Infrastructure – PKI)
- Terminálové služby (Terminal Services)
- Služby Component Services
- Vylepšené internetové a webové služby
- Podpora až čtyřcestného SMP

Systém Windows 2000 Advanced Server

Systém Windows 2000 Advanced Server je novou verzí systému Windows NT Server 4.0, Enterprise Edition. Nabízí rozsáhlou infrastrukturu clusteringu zajišťující vysokou dostupnost a škálovatelnost aplikací a služeb včetně podpory hlavní paměti až do velikosti 8 gigabajtů (GB) na systémech Page Address Extension (PAE). Systém Advanced Server je vytvořen pro náročné podnikové aplikace a podporuje nové systémy pomocí až osmicestného symetrického multiprocessingu (SMP). SMP umožňuje každému z více procesorů v počítači zpracovávat libovolný tok operačního systému nebo aplikace zároveň s ostatními procesory v systému. Systém Windows 2000 Advanced Server se

dobře hodí k náročné práci s databázemi a nabízí clustering serverů s vyrovnáváním zatížení, který zaručuje vysokou dostupnost systému a aplikací.

Systém Windows 2000 Advanced Server obsahuje všechny funkce systému Windows 2000 Server, k nimž přidává vysokou dostupnost a škálovatelnost vyžadovanou řešeními na úrovni oddělení podniků a na vyšších úrovních. Mezi klíčové funkce systému Advanced Server patří:

- Všechny funkce systému Windows 2000 Server
- Vyrovnávání zatížení sítě (TCP/IP)
- Vylepšený serverový klastr se dvěma uzly vycházející z technologie Microsoft Windows Cluster Server (MSCS) v systému Windows NT Server 4.0 Enterprise Edition
- Až 8 GB hlavní paměti na systémech PAE
- Až osmicestný SMP

Terminálové služby

Funkce terminálových služeb (Terminal Services) systému Microsoft Windows 2000 Server přináší systém Windows 2000 Professional a nejnovější aplikace systému Windows na počítače, na kterých nemůže systém Windows obvykle pracovat. Terminálové služby nabízejí také režim vzdálené správy umožňující správcům přistupovat ke klientům, spravovat je a řešit jejich problémy. Prostřednictvím emulace terminálu umožňují terminálové služby provozování stejné sady aplikací na odlišných typech počítačového hardwaru. Organizacím, které chtějí zvýšit svou flexibilitu v zavádění aplikací a řídit náklady na správu počítačů, nabízí architektura terminálových služeb důležité vylepšení tradiční dvou- nebo třívrstvé architektury klient/server vycházející ze serverů a plně funkčních osobních počítačů. Další informace o terminálových službách najdete v kapitole „Zavádění terminálových služeb“ v této knize.

Použití Windows 2000 pro zlepšení způsobů práce

Při plánování migrace na systém Windows 2000 ve vaší organizaci se mnoho uživatelů nejprve zeptá: „Co mi to přinese?“ Z výhod migrace na systém Windows 2000 budou těžit jak správci, tak i uživatelé. Vaši správci budou schopni poskytovat větší mobilní podporu, jednodušší instalace klientů a budou muset vykonávat méně dodatečných činností správy. Pracovníci ve vaší organizaci budou moci využívat jednodušší uživatelské rozhraní a zvýšenou spolehlivost a dostupnost. Jednotliví uživatelé se také setkají s konkrétními zlepšeními podle typu své práce.

Seznámíte-li se s tím, jak může platforma Windows 2000 ovlivnit tři různé kategorie činností – správce informačních technologií (IT), manažera oddělení a prodejce – pomůže vám to zodpovědět otázky týkající se zlepšení práce ve vaší organizaci pomocí systému Windows 2000. Následující oddíly nepředstavují úplný výčet funkcí, které bude každá z uvedených kategorií činností používat. Je to jen ukázka, která vám pomůže s plánováním.

Správce IT

Jako správci IT vám systém Windows 2000 poskytuje centralizované řízení všech klientů ve vaší organizaci. Správce bude také moci využívat aplikace napsané tak, aby přímo podporovaly nové funkce systému Windows 2000. Tyto aplikace se budou snáze zavádět, budou spravovatelnější a spolehlivější. Důsledkem bude poskytování lepších služeb. Následující funkce systému Windows 2000 jsou příklady nových technologií systému Windows 2000 Server, které vám umožní pracovat efektivněji.

Funkce IntelliMirror a služba Active Directory

Tyto funkce vám umožňují používat zásady skupiny ke konfiguraci klientů tak, aby naplňovala potřeby jednotlivých skupin uživatelů. Můžete například zajistit, aby měly všechny osoby ve finančním oddělení k dispozici potřebné aplikace tabulkového kalkulátoru, textového procesoru a vytváření prezentací. Podobně můžete přiřadit software sledování prodeje týmům prodeje. Navíc můžete nastavit zásady umožňující uživatelům zobrazení jejich preferovaného uspořádání na libovolném počítači na síti. Chcete-li omezit počet zásahů technické podpory, můžete počítače uživatelů zabezpečit, takže nebude možné měnit jejich nastavení.

Technologie vzdálené instalace

Technologie vzdálené instalace (Remote Install – RI) vám umožňují využívat zásady skupiny k vykonání automatizované čisté instalace operačního systému Windows 2000 Professional na klienta. Tuto technologii můžete použít k instalaci operačního systému Windows 2000 Professional z centrálního místa (nástroj RIPrep je k dispozici na CD operačního systému Windows 2000 Server). RI můžete zkombinovat s technologiemi Microsoft IntelliMirror a vytvořit bitovou kopii celého systému. Používáte-li zároveň cestovní profily, tato kombinace funkcí vám také výrazně pomůže v procesu zotavení po havárii.

Program certifikace aplikací Windows 2000 Logo

Program Windows 2000 Logo je specifikace společnosti Microsoft, která pomáhá vývojářům s vývojem aplikací využívajících službu Active Directory, software Windows Installer a další funkce systému Windows 2000, jež usnadňují správu aplikací v rámci celého podniku. Pomocí informací v těchto specifikacích můžete vyvinout aplikace využívající funkce systému Windows 2000 k omezení nákladů TCO, které navíc budou dobře spolupracovat s dalšími aplikacemi používanými ve vaší organizaci. Další informace o specifikaci aplikací Windows 2000 Logo najdete v odkazu MSDN Online stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/res-kit/webresources>.

Terminálové služby a mobilní zařízení

Tyto funkce vám umožňují spravovat služby z libovolného místa sítě. Jestliže například obdržíte informace o problému s přenosovou šířkou pásma někde na síti v okamžiku, kdy jste na návštěvě v nějaké pobočce, můžete pro přístup k centralizovaným nástrojům správy sítě, diagnostiku problému a jeho vyřešení použít bezdrátově připojený osobní počítač.

Manažer oddělení

Jako manažer oddělení zodpovídáte za koordinaci mnoha projektů a zaměstnanců. Důsledkem zlepšeného přístupu k informacím je, že nyní můžete snáze shromažďovat

a analyzovat informace. Dále jsou uvedeny příklady toho, jak vám konkrétní funkce systému Windows 2000 usnadní úlohu řídicího pracovníka.

Terminálové služby a technologie správy změn a konfigurací

Pomocí technologií správy změn a konfigurací vám může správce zajistit dostupnost softwaru, dat a nastavení pracovní plochy, která potřebujete, bez ohledu na to, kde na síti se přihlásíte. Jste-li na návštěvě v oddělení účetnictví a potřebujete-li se podívat na nějakou zprávu, můžete se pomocí terminálových služeb připojit k zařízení citlivého klienta a pracovat, jako byste byli ve své kanceláři.

Podpora programu NetMeeting, služby Quality of Service a technologie USB

Program Microsoft NetMeeting umožňuje vzájemné zobrazení více uživatelů na síti přes video-spojení a jejich spolupráci na dokumentech v reálném čase. Aby byla zajištěna dostatečná kvalita video-spojení, podpora služby Quality of Service (QoS) integrovaná do služby Active Directory umožňuje správci přiřadit uživatelům a aplikacím, které to potřebují, větší šířku pásma. Podpora univerzální sériové sběrnice (Universal Serial Bus – USB) umožňuje uživatelům rychle instalovat zařízení, která se jen připojí k počítači a ihned fungují, jako jsou například videokamery. Chcete-li tak zřídit videokonferenci, stačí jen připojit kameru a klepnout na příslušná jména v adresáři.

Prodejce

Prostřednictvím technologií správy změn a konfigurací může správce zajistit, že budete mít vždy k dispozici potřebný software, a proto také jednoduchý přístup ke svým nástrojům a aplikacím. Další schopnosti jsou určené uživatelům, kteří tráví většinu času mimo svou hlavní kancelář. Existuje několik funkcí systému Windows 2000, které vám pomohou lépe zhodnotit čas – ať už jste na cestách nebo jednáte ve své kanceláři.

Správce synchronizace

Správce synchronizace (Synchronization Manager) vám umožňuje pracovat s informacemi offline, jako byste pracovali na síti. Můžete si tak sebou vzít například soubory o zákazníkovi, pracovat s nimi v terénu a synchronizovat je s jejich síťovými verzemi při svém dalším přihlášení. Podobně si můžete nahrát webové stránky z intranetového sídla vaší společnosti a pracovat na nich offline. Po svém dalším přihlášení k síti můžete aktualizovat intranetové informace na svém notebooku a záznamy o zákazníkovi uložené na síti.

Cestovní uživatelské profily

Cestovní uživatelské profily vám umožňují používat svá upravená nastavení pracovní plochy a přistupovat ke všem svým dokumentům z libovolného místa na síti. Při cestování se můžete přihlásit k síti z libovolného místa a stále mít přístup ke všem svým datům. V zájmu zajištění přístupu k důležitým datům se již nemusíte starat o přenos dat na diskety nebo elektronickou poštou.

Příklady naplnění obchodních či výrobních potřeb systémem Windows 2000

Organizace přistupují k zavádění z mnoha různých perspektiv, podle plánu implementace nového operačního systému do svého prostředí. Většina organizací zavádí operační systém postupně (neboli ve fázích), aby nedocházelo k výpadkům uživatelů a aby bylo zajištěno úspěšné naplnění důležitých kroků v rámci tohoto procesu.

Následující oddíly uvádějí určité studie a příklady přístupu různých organizací k zavádění z hlediska funkcí produktu. Tyto příklady obsahují informace o tom, jak některé významné organizace vyřešily své naléhavé obchodní či výrobní problémy. Informace poskytnuté v tomto oddílu vám pomohou se zlepšením a zajištěním vyšší efektivity používání systému Windows 2000 ve vaší organizaci.

Příklad 1: Severoamerický průmyslový výrobce

Hlavní činností této organizace je výroba. K výrobě produktů dochází na mnoha různých místech v Severní Americe, obchodní kanceláře jsou však rozmístěny po celém světě a vytvářejí tak vysoce distribuované globální počítačové prostředí. Existuje tu několik hlavních oddělení produktů s více řadami produktů. Mnoho interních celosvětově distribuovaných týmů vyžaduje různé úrovně přístupu k dokumentům o zákaznících a k interním dokumentům. Uživatelé v každém oddělení požadují vysokou úroveň klientských úprav. Navíc je tu mnoho prodejců a kontraktorů, z nichž někteří potřebují přístup k interní síti za firewall a jiným stačí jen externí přístup. Správci sítě musí zajistit různé úrovně zabezpečení podle potřeb jednotlivých interních a externích týmů.

Existující prostředí IT

V současné době tato organizace podporuje kombinované síťové operační prostředí se systémy Windows NT Server 4.0 Service Pack (SP) 4 a UNIX a kombinované klientské prostředí systémů Microsoft Windows 95 (85 procent), Windows NT Workstation 4.0 (10 procent) a UNIX (5 procent). Informační technologie jsou centrálně spravovány, přičemž řízení aplikací a prostředků je distribuováno na manažery IT na nižších úrovních. Organizace vyžaduje velké přenosové šírky pásma a potřebuje silnou správu klientů. Globálně nejdůležitější aplikací zajišťující komunikaci a časové plánování je v současné době systém Microsoft Exchange Server.

Cíle zavedení systému Windows 2000

Společnost chce standardizovat jediný operační systém a jediný klientský systém, aby se snížily náklady na podporu. Bude také integrovat adresářovou službu Exchange Serveru se službou Active Directory, aby se vytvořil společný adresář umožňující zlepšení spolupráce týmů. V zájmu spolupráce a sdílení informací také plánují používat multi-mediální síť.

Tabulka 1.2 shrnuje cíle oddělení IT této organizace a uvádí důvody, proč k jejich dosažení zvolila organizace systém Windows 2000.

Tabulka 1.2 Cíle IT severoamerického průmyslového výrobce

Cíle	Co nabízí systém Windows 2000
Podpora a instalace jediného standardního klientského operačního systému zajišťující rychlou instalaci a konfiguraci i nenákladné zavedení.	Poskytuje funkce správy klientů, jako jsou IntelliMirror a technologie automatizované instalace a inovace klientů (například služby vzdálené instalace a Systems Management Server).
Instalace síťového operačního systému, který je zabezpečený, ale přitom dostatečně flexibilní a robustní, aby mohl fungovat na různém hardwaru.	Poskytuje bezpečnostní funkce ověřování protokolem Kerberos a zabezpečený protokol Internet Protocol Security (IPSec). Nabízí více hardwarových možností uvedených v seznamu HCL. Podporuje funkce Plug-and-Play.

Omezení nákladů na zavádění a správu zavedením jediného serverového obrazu (bitové kopie). Podpora jen jedné společné serverové platformy a konsolidace menších serverů do větších serverů.

Udržení stálé funkčnosti Exchange Serveru, protože je to aplikace pro celou organizaci naprosto zásadní (mission-critical).

Vytvoření centralizovaného modelu správy, který umožňuje vytvoření distribuovaného řízení v doménách nižší úrovně.

Zajištění spolupráce se současnými servery systému UNIX a použití společného zabezpečeného protokolu.

Podpora dalšího zabezpečení mezi platformami v podniku.

Použití síťového operačního systému a struktury domén, která bude odrážet obchodní či výrobní potřeby.

Vytvoření jediného rozsáhlého podnikového počítačového adresáře.

V zájmu spolupráce a sdílení informací používat multimediální síť.

Funkce systému Advanced Server zajišťují počítačové potřeby celé organizace, protože podporují clustering, vyrovnávání zatížení a možnosti podpory dalších procesorů.

Systém Windows 2000 poskytuje stabilní platformu operačního systému pro Exchange Server.

Služba Active Directory umožňuje správcům na vyšší úrovni delegovat řízení konkrétních prvků v rámci Active Directory jednotlivcům nebo skupinám. Není tak zapotřebí, aby mělo úplné řízení celé domény k dispozici více správců. Služba Active Directory umožňuje společnosti vymodelovat své síťové prostředí podle své obchodní či výrobní struktury.

Spolupráci zajišťuje protokol dynamické aktualizace systému Domain Name System (DNS). Zabezpečení Kerberos funguje na obou platformách.

Distribuované zabezpečení zahrnující protokol IPSec, ověřování protokolem Kerberos a infrastrukturu PKI.

Systém Windows 2000 je dostatečně flexibilní, abyste mohli vytvořit domény a hranice zabezpečení podle struktury své obchodní či výrobní činnosti – strukturu svého podniku tak nemusíte organizovat podle omezení daných serverovým operačním systémem.

Umožňuje vám slučovat data služby Active Directory s daty Exchange Serveru a vytvářet společný adresář.

Program NetMeeting umožňuje konverzaci skupinám v různých částech světa. Služba QoS vám umožňuje vyhradit pro multimediální data potřebnou šířku pásma. Technologie Plug-and-Play zjednodušuje připojování multimediálních kamer.

Příklad 2: Velký mezinárodní výrobce

Tato mezinárodní organizace má ústředí v Evropě a kanceláře ve více než 190 zemích. Společnost roste expanzí na další trhy, zvyšováním prodeje produktů a sloučením a nákupy jiných společností. Společnost vyrábí mnoho různých produktů včetně spotřební a průmyslové elektroniky, počítačů a dalších přístrojů. Všechny oddělené výrobní závody pracují jako nezávislé společnosti pod záštitou mateřské korporace. Existuje tu více než 130 samostatně fungujících společností, přičemž každá má svou vlastní strukturu vytváření zpráv a hlavní finanční, informační a výkonné ředitele. To má vliv na dynamiku společnosti v jejím rámci i vně, protože každá organizace IT má jiné cíle, rozpočet a omezení. Mateřská společnost musí zajišťovat podporu a pokyny pro spolupráci různých oddělení IT.

Existující prostředí IT

Neexistuje tu žádná centrální skupina operací IT a k dispozici je jen málo společných standardů IT mezi jednotlivými společnostmi jak z hlediska síťových či klientských ope-

račních systémů, tak i z hlediska klientských aplikací produktivity. Za směrnice a standardy platící v rámci celé společnosti zodpovídá centrální oddělení IT.

Cíle zavedení systému Windows 2000

V roce 1998 oddělení IT této společnosti sponzorovalo projekt návrhu globální architektury služby Active Directory systému Windows 2000 – jednotící koncept všech decentralizovaně fungujících společností. Skupiny zástupců několika společností se soustředily na architekturu a zavádění systémů Windows 2000 Server a Windows 2000 Professional, které pak ve vhodnou dobu integrovaly. Mateřské společnosti bylo uloženo vyvinout společný rámec, který bude podle potřeby přijat jednotlivými samostatně fungujícími společnostmi.

Tabulka 1.3 shrnuje cíle oddělení IT této organizace a uvádí důvody, proč k jejich dosažení zvolila organizace systém Windows 2000.

Tabulka 1.3 Cíle IT velkého mezinárodního výrobce

Cíle	Co nabízí systém Windows 2000
Vytvoření společné metodiky IT, kterou budou moci skupiny IT ze všech fungujících společností použít k vytvoření globálního modelu s více operátory.	Architektura doménových struktur služby Active Directory nabízí bod jediného přihlášení a schopnosti globálního katalogu.
Zavedení jediné společné adresářové služby, kterou budou moci využívat všechny společnosti.	Služba Active Directory je flexibilní, rozšiřitelná a upravitelná, takže dokáže pojmut potřeby IT i obchodní či výrobní potřeby samostatně fungujících společností.
Vytvoření jediného společného modelu migrace z prostředí systému Windows NT na systém Windows 2000.	K dispozici jsou technologie vzdálené instalace a další nástroje vzdálené nebo automatizované instalace, jako je například Systems Management Server.
Vykonání pilotního postupného zavedení, které lze použít jako standard implementace ve všech skupinách IT v samostatných společnostech.	Možnost klonovat komitenty zabezpečení z jiné domény systému Windows NT a funkce historie identifikátorů zabezpečení (Security Identifier – SID), které umožňují bezpečný přechod do pilotního prostředí s možností návratu k původnímu prostředí.
Zavedení jednoho společného klientského operačního systému, který budou využívat všechny samostatně fungující společnosti.	Společný model zabezpečení kancelářských i přenosných počítačů. Možnosti technologie Plug-and-Play. Společná podpora hardwaru. Zásady skupiny, funkce IntelliMirror a další nástroje správy klientů řízené pomocí služby Active Directory.

Příklad 3: Nadnárodní korporace finančních služeb

Nadnárodní organizace poskytující finanční služby se skládá z několika samostatně fungujících společností a má hlavní ústředí v Severní Americe, Evropě, Malé Asii a v Jiho-východní Asii. Více než 50 hlavních regionálních poboček nabízí plný rozsah finančních služeb (investice a osobní bankovní služby, správa aktiv a pojištění). Každá fungující společnost je autonomní obchodní jednotkou, na místní úrovni však mohou jednotlivé společnosti sdílet kanceláře s dalšími společnostmi.

Tato společnost pracuje pod přísným regulačním dohledem v mnoha zemích a pod jejich jednotlivými statuty souvisejícími se soukromím finančních operací, pravidly ob-

chodu a fungováním a zabezpečením IT. Je tedy zapotřebí zajistit zabezpečené a stabilní systémy jak na úrovni síťového operačního systému tak i na úrovni operačního systému kancelářských počítačů.

Existující prostředí IT

Není tu žádná centrální skupina IT pro všechny fungující společnosti, takže také neexistují souhrnné standardy IT pro celou organizaci. Každá fungující společnost si vytvořila své vlastní standardy, a proto má každá společnost svou vlastní infrastrukturu IT. V některých oblastech sdílejí fungující společnosti jednu síť. V jiných místech odpovídá počet sítí počtu fungujících společností, které sdílejí dané místo. Místní kanceláře, zejména místa spotřebitelského a maloobchodního prodeje, mají své vlastní souborové a tiskové servery. Regionální pobočky obvykle mají řadiče domén a jejich funkce IT je jinak omezená.

Určité finanční služby vyžadují operační systém UNIX. V současné době jsou všechny služby infrastruktury, jako je protokol Dynamic Host Configuration Protocol (DHCP) a služba DNS, spravovány v prostředí systému UNIX. Protokol dynamické aktualizace DNS systému Windows 2000 se bude používat, zatímco bude společnost zkoumat možnost migrace vlastních aplikací pracujících na serverech systému UNIX na systém Windows 2000.

Jejich současné síťové prostředí operačního systému běží z 95 procent na systému Windows NT Server 4.0 a z pěti procent na systému Novell NetWare Bindery. Mezi aktuálně používané klientské operační systémy v jednotlivých fungujících společnostech patří 80 procent systému Windows NT Workstation 4.0, přibližně 15 procent systému Windows NT Workstation 3.51 a asi 5 procent systému Windows 95. Někteří profesionálové finančních služeb používají klienty systémů UNIX i Windows NT 4.0.

Cíle zavedení systému Windows 2000

Jedna ze samostatně fungujících společností vyvíjí svou vlastní strukturu služby Active Directory s cílem vytvoření návrhu společného globálního adresáře pro celou organizaci. Iniciativa mateřské společnosti IT řízená skupinou profesionálů IT reprezentujících všechny fungující společnosti také zajišťuje vývoj celopodnikové struktury služby Active Directory.

Organizace plánuje po instalaci systému Windows 2000 opustit prostředí NetWare Bindery. V budoucnosti bude síť používat systémy Windows 2000 a UNIX.

Tabulka 1.4 shrnuje cíle oddělení IT této organizace a uvádí důvody, proč k jejich dosažení zvolila organizace systém Windows 2000.

Tabulka 1.4 Cíle IT nadnárodní korporace finančních služeb

Cíle	Co nabízí systém Windows 2000
Společný klientský operační systém v celém prostředí, který umožní standardizaci,lepší spravovatelnost a možnosti správy, a omezí náklady TCO.	Zlepšená podpora hardwaru umožňuje širší výběr standardních počítačů společnosti (kancelářských i přenosných). Zlepšená správa napájení umožňuje zpřístupnění síťových informací na přenosných počítačích na úrovni kancelářských počítačů. Zásady skupiny a další nástroje správy lze zavést v celém rozsahu prostředí IT.

Společné síťové operační systémy nabízející škálovatelnost a dostupnost pro prostředí IT s různými potřebami ve všech fungujících společnostech.	Nabízí clustering, vyrovňování zatížení a možnost používat rozsáhlé datové sklady a komplexní objekty. Jediný bod správy vyžaduje jen jednu sadu správců. Zásady skupiny umožňují dokonalou správu všech klientů.
Klientské zabezpečení na všech kancelářských a přenosných počítačích.	Může zajistit přenosný počítač stejně jako kancelářský.
Potřeba více monitorů na jednotlivých kancelářských počítačích, aby bylo možné zároveň sledovat prodej a přistupovat k informacím o zákaznících.	Umožňuje jednomu procesoru podporovat více monitorů.
Omezení nákladů na pořízení (TCO) při nižší správě klientů a zvýšené úrovni služeb.	Zlepšené zásady skupiny a integrace se serverem Systems Management Server.
Omezení vlastního vývoje softwaru a souvisejících nákladů.	Služba Component Services a další nástroje, jako je Windows Installer, které jsou součástí systému Windows 2000 Server, umožňují snazší vytváření nástrojů a snižují čas investovaný do vývoje vlastních aplikací.
Společný adresář pro všechny fungující společnosti.	Služba Active Directory má dostatečnou flexibilitu, aby dokázala obsáhnout všechny fungující společnosti.
Umožnění všem samostatným společnostem vlastnictví své vlastní podřízené domény nebo domén.	Návrh služby Active Directory využívá název domény nejvyšší úrovně jako základní doménu a umožňuje tak všem samostatným společnostem vlastnit svou vlastní podřízenou doménu nebo domény.
Sdílení společného adresáře mezi Exchange Serverem a systémem Windows 2000 Server.	Synchronizování adresáře systému Microsoft Exchange Server verze 5.5 se službou Active Directory pomocí nástroje Active Directory Connector.
Vzdálená správa služeb.	Terminálové služby jsou nakonfigurovány ve zjednodušené verzi režimu správy a nikoli v režimu aplikačního serveru. To dává správcům další možnosti správy, aniž by to mělo negativní vliv na výkon serveru.

Příklad 4: Mezinárodní společnost vývoje softwaru

Hlavní společnost vývoje softwaru počítačových operačních systémů a aplikací pro spotřebitele i obchod či výrobu má své hlavní ústředí na západě Spojených států. Kanceláře prodeje, podpory a vývoje softwaru se nacházejí na 180 místech celého světa. Oddělení informačních technologií (IT) má dvě hlavní oblasti zodpovědnosti:

- Poskytování a údržba systémů a řešení IT, které pomáhají zaměstnancům efektivně a výkonně pracovat.
- Spolupráce se skupinami vývoje produktů při testování a zavádění beta-produktů do podnikového prostředí.

Existující prostředí IT

Současné prostředí IT této společnosti je homogenní prostředí systému Windows NT Server 4.0 s různými kombinacemi klientů systémů Windows NT 4.0, Windows 95 a Microsoft Windows 98. Patří sem také mnoho počítačů v kancelářích uživatelů, na nichž často běží beta-verze softwaru. IT zajišťuje centralizované:

- adresářové služby,

- poštovní služby a služby spolupráce,
- správu služeb zabezpečení systému Windows NT Server 4.0, síťových účtů, webových služeb a práce v síti.

Uživatelé jsou geograficky rozptýleni po celém světě. 80 až 90 procent zaměstnanců si sami řeší problémy se svými počítači. Velký počet uživatelů přistupuje k síti vzdáleně a vyžaduje stabilní služby vzdáleného přístupu. Oddělení IT také podporuje zaměstnance pracující doma a nikoli v sídle a zaměstnance, kteří vyžadují k síti společnosti mezinárodní přístup.

Cíle zavedení systému Windows 2000

Hlavním cílem této společnosti je inovovat všechny servery a uživatele na systém Windows 2000 v příštích 12 měsících. Během migrace musí skupina IT udržet služby důležitých aplikací a zároveň slučovat domény prostředků do geograficky určených hlavních uživatelských domén. Zrušení mnoha domén prostředků by mělo snížit počet serverů na síti, zjednodušit správu a zároveň omezit náklady na podporu hardwaru a softwaru.

Oddělení IT musí také zajistit synchronizaci informací o uživatelských atributech mezi adresářovou službou Active Directory, adresářovou službou systému Exchange Server 5.5 a dalšími systémy používanými ve společnosti. Vše, co je převedeno online a používá službu Active Directory, musí spolupracovat. Je také zapotřebí vytvořit společný strom konzoly a společný adresář.

Tabulka 1.5 shrnuje cíle oddělení IT této organizace a uvádí důvody, proč k jejich dosažení zvolila organizace systém Windows 2000.

Tabulka 1.5 Cíle IT mezinárodní společnosti vývoje softwaru

Cíle	Co nabízí systém Windows 2000
Konsolidace globálních serverů v zájmu zlepšení spravovatelnosti a snížení nákladů na podporu.	Konsolidaci serverů umožňují schopnosti velmi výkonné správy paměti a podpory více procesorů systému Advanced Server. Tyto funkce zlepšují škálovatelnost platformy a činí z ní vhodný základ pro konsolidaci serverů.
Nákup nového výkonného hardwaru, s jehož pomocí se vytvoří nová vysokorychlostní síť společnosti.	Nové technologie v systému Windows 2000 Server integrují pokroky v architektuře počítačů a mikročipů; patří sem Advanced Power Management, zařízení USB, rozhraní FireWire, čtečky karet Smart Card a podpora infračervené komunikace.
Standardizace jediného klienta, jež umožní lepší řízení správy a delegování oprávnění a zajistí více možností vzdálené instalace a správy.	Dosáhnout lepší správy kancelářských počítačů pomocí zásad skupiny a organizačních útvarů (jednotek), což umožňuje služba Active Directory, funkce IntelliMirror a další technologie správy změn a konfigurací.
Dosažení 50% nárůstu výkonu a spolehlivosti oproti systému Windows NT 4.0 Server na všech systémech Advanced Server.	Zásadní vylepšení na úrovni jádra operačního systému umožňuje zlepšení správy paměti, ukládání do mezipaměti a preemptivního multitaskingu.
Přechod ze středně složitého prostředí systému Windows NT Server 4.0 na výrazně zjednodušené prostředí systému Windows 2000.	Služba Active Directory umožňuje ukládat více objektů a zajišťuje detailnější správu serverů a klientů a zlepšení zjednodušeného návrhu domén s využitím systému Domain Name System (DNS) a protokolu dynamické aktualizace systému DNS.

Změna struktury domén systému Windows NT Server 4.0 na model služby Active Directory s doménami a doménovými strukturami.	Služba Active Directory nabízí flexibilnější strukturu domén, která dokáže pojmut současně i budoucí potřeby organizace.
Zlepšení zabezpečení, sdílení informací a podpory transakcí ve společnosti i s ostatními podniky a zákazníky.	Umožňuje vytvoření virtuální privátní sítě pomocí pokročilých funkcí práce v síti a zabezpečení systému Windows 2000 Advanced Server.
Zlepšení zabezpečení elektronické pošty.	Použití infrastruktury PKI a certifikátů.
Udržení plně funkční podnikové sítě v celém přechodném období.	Simultánní správu a auditování serverů se systémem Windows NT Server 4.0 a Windows 2000 Advanced Server. Sem patří všechny tiskové, souborové, proxy a interní webové servery společnosti i servery vzdáleného přístupu. Spolupráce s klienty systémů Windows 95, Windows 98 a Windows NT 4.0.

Plánování charakteristických stránek systému Windows 2000 vašim obchodním či výrobním potřebám

Předcházející oddíly se zabývaly funkcemi a výhodami platformy Windows 2000 z hlediska obchodních či výrobních potřeb, ukázkových společností a uživatelů a funkcí produktu. V tomto oddílu se seznámíte se specifickými funkcemi s cílem určit technologie, které jsou pro vaši organizaci nejdůležitější. Tyto funkce si prostudujte z hlediska krátkodobých, střednědobých i dlouhodobých plánů vaší organizace. Kapitoly v této knize, které se zaměřují na návrh, se podrobně zabývají integrací jednotlivých technologií s ostatními technologiemi systému Windows 2000 a také dalšími závislostmi návrhu.

Následující oddíly obsahují tabulky uvádějící mnoho funkcí systému Windows 2000, které budete ve své organizaci zavádět a konfigurovat. Vyhodnoťte přínosy uvedených funkcí a určete jejich relativní priority ve vaší organizaci. Pak můžete vyvinout plán zavedení, který bude efektivní jak z hlediska času tak i z hlediska nákladů.

Všechny tabulky v tomto oddílu jsou obsaženy v příloze „Ukázkové listy plánování“ v této knize. Tabulky v příloze jsou naformátovány tak, abyste do nich mohli zadat své vlastní komentáře o možných rolích jednotlivých funkcí ve vaší organizaci. Tyto pracovní listy použijte pro přípravu upraveného výkonného souhrnu funkcí systému Windows 2000 vyžadovaných vaší organizací.

Poznámka Následující tabulky uvádějí hlavní výhody systémů Windows 2000 Server a Windows 2000 Professional a nejsou úplným popisem všech funkcí. Další informace o konkrétní funkci najdete v souborech nápovědy produktu nebo v příslušné knize a kapitole sady *Microsoft Windows 2000 Server Resource Kit*.

Správa služeb infrastruktury

Služby infrastruktury správy systému Windows 2000 Server dodávají oddělením IT nástroje umožňující poskytování nejvyšších dostupných úrovní služeb a omezení nákladů na vlastnictví. Tabulka 1.6 popisuje služby infrastruktury správy systému Windows 2000 Server a jejich přínos.

Tabulka 1.6 Služby infrastruktury správy

Funkce	Popis	Přínos
Adresářové služby	Služba Microsoft Active Directory ukládá informace o všech objektech v síti, což činí tyto objekty snadno vyhledatelnými. Poskytuje flexibilní adresářovou hierarchii, podrobné delegování zabezpečení, výkonné delegování oprávnění, integrované služby DNS, programovací rozhraní na vysoké úrovni a rozšiřitelné úložiště objektů.	Zajišťuje jedinou sadu rozhraní pro vykonávání úkolů správy, jako je přidávání uživatelů, správa tiskáren a vyhledávání prostředků jen jediným přihlášením. Uspadňuje vývojářům vytvářet aplikace, které budou konkrétní adresář podporovat.
Služby správy	Nástroj Microsoft Management Console (MMC) poskytuje správcům systému společnou konzolu pro sledování síťových funkcí a používání nástrojů správy. Konzola MMC je plně upravitelná.	Konzola MMC standardizuje sadu nástrojů správy, snižuje nutný čas na zaškolení a zvyšuje produktivitu nových správců. Také zjednodušuje vzdálenou správu a umožňuje delegování úkolů.
Zásady skupiny	Zásady skupiny (Group Policy) umožňují správci definovat a řídit stav počítačů a uživatelů. Zásady skupiny lze zadat na libovolné úrovni adresářové služby, včetně síťových sídel, domén a organizačních jednotek (útvarů). Zásady skupiny lze také filtrovat na základě členství ve skupinách se zabezpečením.	Zásady skupiny dávají správcům možnost řídit, kteří uživatelé mají přístup k určitým počítačům, funkcím, datům a aplikacím.
Instrumentační služby	Pomocí služby Windows Management Instrumentation (WMI) mohou správci vytvářet vztahy mezi daty a událostmi z více zdrojů v místě nebo v celé organizaci.	WMI vám umožňuje vytvářet vlastní aplikace a moduly snap-in, protože zajišťuje přístup k objektům systému Windows 2000.
Skriptové služby	Nástroj Windows Script Host (WSH) podporuje přímé vykonávání skriptů jazyků Microsoft Visual Basic Script, Java a dalších z uživatelského rozhraní nebo z příkazového řádku.	WSH umožňuje správcům a uživatelům automatizovat různé akce, mezi něž patří také připojení k síti a odpojení od sítě.

Další informace o návrhu a vytváření adresářových služeb a zásad skupiny systému Windows 2000 najdete v kapitolách „Návrh struktury služby Active Directory“, „Plánování distribuovaného zabezpečení“, „Definování standardů správy a konfigurace klientů“ a „Aplikování správy změn a konfigurací“ v této knize.

Řešení správy počítačů

Řešení správy počítačů jsou funkce umožňující vám snížit celkové náklady na vlastnictví (TCO) ve vaší organizaci tím, že usnadňují instalaci, konfiguraci, správu a použití klientských počítačů. Tyto funkce jsou také navrženy jako nástroje usnadňující použití

počítačů. Tabulka 1.7 uvádí funkce správy počítačů systémů Windows 2000 Server a Windows 2000 Professional, které zvyšují produktivitu uživatelů.

Tabulka 1.7 **Řešení správy počítačů**

Funkce	Popis	Přínos
Funkce IntelliMirror	Microsoft IntelliMirror je skupina funkcí, které lze použít k tomu, aby data, aplikace a upravená nastavení operačního systému následovala uživatele při přesunu na jiný počítač v organizaci.	Uživatelé mají přístup ke všem svým informacím a aplikacím, ať už jsou připojeni k síti, nebo nejsou. Správci také nemusejí opakovaně navštěvovat jednotlivé počítače při inovacích aplikací nebo operačního systému.
Služba Windows Installer	Služba Windows Installer řídí instalaci, úpravu, opravu a odebrání softwaru. Poskytuje model pro zabalení instalačních informací a rozhraní API pro aplikace, které se službou Windows Installer spolupracují.	Správcům systému umožňuje vzdálené zavádění a údržbu aplikací. Omezuje počet konfliktů dynamicky připojitelných knihoven (Dynamic Link Library – DLL). Podporuje automatickou opravu aplikací.
Vzdálená instalace	Technologie vzdáleného spuštění založená na službě DHCP instaluje operační systém na pevný disk klienta ze vzdáleného zdroje. Síť lze inicializovat buď prostředím PXE nebo síťovou kartou podporující standard PXE, specifickým funkčním tlačítkem nebo disketou vzdáleného spuštění u klientů bez podpory PXE.	Správce nemusí při instalaci operačního systému navštívit cílový počítač. Funkce vzdálené instalace OS také poskytuje řešení rozšiřování a údržby společného obrazu (bitové kopie) kancelářských počítačů ve vašem podniku.
Cestovní uživatelské profily	Cestovní uživatelské profily kopírují hodnoty registru a informace dokumentů na nějaké místo na síti, aby byla nastavení uživateli dostupná na všech místech, kde se přihlásí.	Uživatelé mohou cestovat a přitom mít stále k dispozici své dokumenty a systémové informace.
Správce součástí systému	Instalační program systému Windows 2000 Server vám umožňuje pomocí instalačního modulu zabalit a nainstalovat doplňkové komponenty během nastavování systému nebo po něm.	Omezuje dobu potřebnou pro zavedení systému a snižuje počet nutných návštěv u jednotlivých počítačů.
Duplikování disku	Stačí vám nastavit jen jedinou instalaci systému Windows 2000 Server nebo Windows 2000 Professional a tu pak zkopírovat na podobné počítače.	Klonování vám při zavádění velkého počtu serverů nebo klientů ušetří mnoho času.

Poznámka Pro doplnění technologií systému Windows 2000 správy kancelářských počítačů můžete použít server Microsoft Systems Management Server (SMS).

Další informace o zavádění řešení správy systému Windows 2000 Server a Windows 2000 Professional najdete v kapitolách „Definování standardů správy a konfigurace klientů“ a „Aplikování správy změn a konfigurací“ v této knize.

Funkce zabezpečení

Zabezpečení na úrovni podniku musí být flexibilní a robustní, aby správci mohli nakonfigurovat pravidla možné zodpovědnosti za zabezpečení, aniž by přitom docházelo ke zbytečnému bránění volnému toku potřebných informací. Tabulka 1.8 uvádí funkce zabezpečení systému Windows 2000.

Tabulka 1.8 Funkce zabezpečení

Funkce	Popis	Přínos
Šablony zabezpečení	Umožňují správcům nastavovat různá globální a místní nastavení zabezpečení včetně citlivých (z hlediska zabezpečení) hodnot registru, řízení přístupu k souborům a k registru a zabezpečení systémových služeb.	Umožňují správcům definovat šablony konfigurace zabezpečení a následně tyto šablony aplikovat jedinou operací na vybrané počítače.
Ověřování Kerberos	Hlavní protokol zabezpečení pro přístup v rámci domény systému Windows 2000 nebo mezi doménami. Poskytuje vzájemné ověřování klientů a serverů a podporuje delegování a autorizování pomocí mechanismů proxy.	Zvyšuje výkon, protože omezuje zatížení serverů při vytváření připojení. Můžete je použít také pro přístup k jiným počítačovým platformám v podniku, které podporují protokol Kerberos.
Infrastruktura veřejných klíčů (PKI)	Integrovanou strukturu PKI můžete používat pro zajištění vysokého zabezpečení ve více internetových a podnikových službách systému Windows 2000 včetně extranetových komunikací.	Prostřednictvím PKI mohou různé obchodní či výrobní jednotky zabezpečeně sdílet informace, aniž by přitom musely vytvářet mnoho jednotlivých účtů systému Windows 2000. Umožňuje také použití karet Smart Card a zabezpečené elektronické pošty.
Infrastruktura karet Smart Card	Systém Windows 2000 obsahuje standardní model připojení čteček karet Smart Card k počítačům a rozhraní API nezávislá na zařízení podporující aplikace, které umějí s kartami Smart Card pracovat.	Technologie karet Smart Card systému Windows 2000 lze využít k vytvoření řešení zabezpečení v intranetových, extranetových i veřejných webových sídlech.
Správa zabezpečeného protokolu IP (Internet Protocol security – IPSec)	Protokol IPSec podporuje ověřování na úrovni sítě, integritu dat a šifrování, čímž zabezpečuje intranetové, extranetové a internetové webové komunikace.	Transparentně zabezpečuje podnikové komunikace, přičemž není zapotřebí interakce uživatelů. Existující aplikace mohou také pro zabezpečenou komunikaci používat protokol IPSec.
Šifrování systému souborů NTFS	Systém NTFS s využíváním veřejného klíče lze povolit na úrovni jednotlivých souborů nebo adresářů.	Umožňuje správcům a uživatelům šifrovat data pomocí náhodně generovaných klíčů.

Další informace o zavádění služeb zabezpečení systému Windows 2000 najdete v kapitolách „Plánování distribuovaného zabezpečení“ a „Určení strategií zabezpečení sítě systému Windows 2000“ v této knize.

Publikování a sdílení informací

Technologie publikování a sdílení informací v systému Windows 2000 usnadňují sdílení informací přes Internet, intranet nebo extranet. Tabulka 1.9 shrnuje funkce publikace a sdílení informací.

Tabulka 1.9 Publikování a sdílení informací

Funkce	Popis	Přínos
Integrované webové služby	Webové služby integrované do systému Windows 2000 Server vám umožňují používat různé webové publikační protokoly.	Flexibilní příležitosti publikování informací na extranet, intranet nebo síť WWW.
Služba Indexing Service	Integrovaná indexová služba umožňuje uživatelům vykonávat fulltextové hledání v souborech různých formátů a jazyků.	Zlepšuje produktivitu.
Podpora multimédií	Skládá se ze serverových nástrojů a součástí přenášení audia, videa, ilustrovaného audia a dalších typů multimédií přes síť.	Nové příležitosti školení, spolupráce a sdílení informací zvyšují produktivitu.
Tisk	Systém Windows 2000 zpřístupňuje všechny sdílené tiskárny v doméně službě Active Directory.	Umožňuje uživatelům rychle vyhledat nejvhodnější tiskový prostředek.

Další informace o zavádění služeb publikování a sdílení informací systému Windows 2000 najdete v kapitole „Inovace a instalace členských serverů“ v této knize a v knize *Microsoft Internet Information Services 5.0 Resource Kit*.

Podpora aplikací COM

Jako vývojová platforma nabízí systém Windows 2000 podporu modelu Component Object Model (COM) a Distributed COM (DCOM), který rozšiřuje schopnosti vývojových týmů výkonně vytvářet škálovatelnější aplikace se součástmi. Tabulka 1.10 uvádí hlavní funkce podpory aplikací COM.

Tabulka 1.10 Zavedení podpory aplikací COM

Funkce	Popis	Přínos
Řazení komponent do fronty	Vývojáři a správci mohou vybrat vhodný komunikační protokol (DCOM nebo asynchronní) používaný při zavádění.	Pro vývojáře je jednodušší využívat úložiště a předávat dál služby nabízené službami řazení zpráv do fronty integrované v systému Windows 2000 Server, aniž by bylo zapotřebí vytvářet nějaký kód.
Publikování a odebrání	Funkce COM Events poskytuje všem aplikacím systému Windows 2000 Server jednotný mechanismus publikování a odebrání.	Vývojáři nemusejí znovu vymýšlet a programovat základní služby.
Transakční služby	Poskytují aktualizace informací voláním aplikace na mainframovém počítači nebo odesláním zprávy do fronty zpráv a jejím přijetím z fronty zpráv.	Poskytuje vývojářům možnost zaručit správnost jejich aplikací při aktualizaci více zdrojů dat.
Služby řazení zpráv	V podnikovém prostředí zajišťuje úplné dokončení transakce nebo její bezpečné vrácení do předchozího stavu.	Poskytuje vývojářům prostředky pro vytvoření a zavedení aplikací, které spolehlivě pracují na nespolehlivých sítích a spolupracují s dalšími aplikacemi běžícími na jiných platformách.
Služby webových aplikací	Vývojáři mohou k vytvoření webového rozhraní svých existujících serverových aplikací použít technologii Active Server Pages.	Služby webových aplikací umožňují správu vzdálených serverů pomocí webového prohlížeče s minimálními náklady na konektivitu.

Další informace o zavádění služeb Component Application Services a rozhraní Microsoft Security Support Provider Interface systému Windows 2000 najdete v kapitole „Určení strategií zabezpečení sítě systému Windows 2000“ v této knize. Další informace pro vývojáře najdete v odkazu MSDN Platform SDK stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Poznámka Tyto funkce a jejich potenciální význam pro vaši společnost byste měli diskutovat se členy týmu vývoje aplikací. Jejich znalosti vám pomohou určit možnou hodnotu těchto technologií ve vaší organizaci.

Škálovatelnost a dostupnost

Kdysi byly rychlejší procesory a síťové karty tradičními zárukami vysokého výkonu sítě. V budoucnosti budou stejně důležitými charakteristikami síťové architektury výkonnější možnosti čtení a zápisu, zvýšený výkon vstupů a výstupů a rychlejší přístup k disku. Prostředí vyžadující použití velmi důležitých (mission-critical) počítačů mohou nyní využívat tyto rozšířené možnosti systému Windows 2000. Tabulka 1.11 uvádí funkce systému Windows 2000, které vám pomohou zlepšit škálovatelnost a dostupnost sítě.

Tabulka 1.11 Škálovatelnost a dostupnost

Funkce	Popis	Přínos
Architektura paměti	Systém Windows 2000 Advanced Server umožňuje procesorům přístup k až 32 Gigabajtům (GB) paměti.	Umožňuje aplikacím, které vykonávají podporu zpracování transakcí nebo rozhodování na velkých datových sadách, ukládat více dat do paměti a tak zvyšovat výkon.
Zlepšená škálovatelnost symetrického multiprocesingu (SMP)	Systém Windows 2000 Advanced Server byl optimalizován pro osmicestné servery SMP.	Umožňuje organizacím plně využít rychlejší procesory.
Klastrová služba	Umožňuje dvou nebo více serverům fungovat společně jako jediný systém.	Dovoluje větší dostupnost, spolehlivost, stabilitu a zabezpečení s jednodušší správou.
Podpora inteligentních vstupů a výstupů (I2O)	Technologie I2O zbavuje hostitele úkolů I/O náročných na přerušení, protože se zatížení odstraňuje z hlavních procesorů.	Zlepšuje výkon operací vstupů a výstupů v aplikacích pracujících se širokým pásmem.
Terminálové služby	Pomocí emulace terminálu umožňují terminálové služby běžet jedné sadě aplikací na různých typech klientského hardwaru včetně tenkých klientů, starších počítačů a klientů neobsahujících systém Windows. Tyto služby lze také používat ke vzdálené správě.	Umožňuje centralizovanou správu aplikací a počítačů pracovníků s konkrétními úkoly. Poskytuje technologie převedení existujících počítačů do plného prostředí Microsoft Win32. Poskytuje vzdáleným uživatelům výkon na úrovni místní sítě při použití telefonického připojení vzdáleného přístupu. Také zajišťuje grafickou vzdálenou správu libovolného systému Windows 2000 Server.
Vyrovňování zatížení sítě	Kombinuje až 32 serverů se spuštěným systémem Windows 2000 Advanced Server do jediného klastru s vyrovňováním zatížení. Nejčastěji se používá k distribuci příchozích webových požadavků do klastru aplikací internetového serveru.	Zlepšuje dostupnost a škálovatelnost webových serverů, serverů protokolu File Transfer Protocol (FTP), serverů datových proudů a dalších důležitých programů zkombinováním funkcí dvou nebo více hostitelských počítačů (serverů, které jsou členy klastru).
Funkce IntelliMirror	Funkce IntelliMirror umožňuje uživatelům, aby je jejich data, aplikace a nastavení následovala při jejich připojení k síti.	Data jsou vždy k dispozici a uživatelské zobrazení počítačového prostředí je konzistentní, ať už je klient připojený k síti, nebo není.

Další informace o zavádění klastrové služby systému Windows 2000 najdete v kapitole „Zajištění dostupnosti aplikací a služeb“ v této knize.

Další informace o terminálových službách najdete v kapitole „Zavádění terminálových služeb“ v této knize.

Práce v síti a komunikace

Chcete-li zlepšit možnosti práce v síti, zamyslete se nad použitím technologií systému Windows 2000 uvedených v tabulce 1.12, které rozšíří vaše možnosti řízení šířky pásma, zajistí zabezpečený vzdálený přístup k síti a nativní podporu nové generace komunikačních řešení.

Tabulka 1.12 Práce v síti a komunikace

Funkce	Popis	Přínos
Protokol dynamické aktualizace DNS	Eliminuje nutnost ručně upravovat a replikovat databázi DNS.	Omezuje náklady na správu a vybavení, protože snižuje počet serverů DNS potřebných k podpoře sítě.
Služba Quality of Service (QoS)	Protokoly a služby QoS poskytují zaručený expresní systém dodávek mezi dvěma body provozem IP.	Umožňuje vám nastavit prioritu síťového provozu a zajistit tak vykonání kritických procesů a dodání dat rychle a přesně.
Protokol Resource Reservation Protocol (RSVP)	Signalizační protokol, který umožňuje odesílateli a příjemci vytvořit rezervovanou cestu přenosu dat s určenou kvalitou služeb.	Zlepšuje spolehlivost spojení a přenos dat.
Režim asynchronního přenosu (Asynchronous Transfer Mode – ATM)	Síť ATM může simultánně přepřevodovat velké množství různého síťového provozu včetně hlasu, dat, obrázků a videa.	Unifikace více typů provozu na jediné síti může výrazně snížit náklady.
Služby multimediálních proudů	Serverové součásti a nástroje pro přenos multimediálních souborů přes síť.	Multimediální proudy mohou výrazně snížit náklady na cestování, spolupráci týmů a školení, protože nabízejí online schůzky a sdílení informací.
Technologie Fibre Channel	Technologie Fibre Channel poskytuje přenosy dat rychlostí jednoho gigabitu za sekundu tím, že se mapují obvyklé přenosové protokoly a síťové a vysokorychlostní vstupy a výstupy se slučují do jediné kolekce.	Zlepšená flexibilita, škálovatelnost, spravovatelnost, kapacita a dostupnost technologií rozhraní (Small Computer System Interface – SCSI) pro náročné aplikace.
Telefonování přes IP	Telefonické rozhraní API 3.0 (TAPI) unifikuje tradiční a IP telefonování.	Vývojáři mohou pomocí TAPI vytvářet aplikace fungující přes Internet či intranet stejně jako přes tradiční telefonní síť.

Další informace o práci v síti a komunikačních funkcích systému Windows 2000 najdete v kapitole „Příprava infrastruktury sítě na systém Windows 2000“ a „Určení strategií konektivity sítě“ v této knize.

Správa ukládání

Systém Windows 2000 Server poskytuje služby úložišť určené jak ke zlepšení spolehlivosti tak i přístupu uživatelů. Tabulka 1.13 uvádí tyto služby.

Tabulka 1.13 Správa ukládání

Funkce	Popis	Přínos
Vzdálené úložiště	Sleduje množství prostoru dostupného na místním pevném disku. Když volný prostor na primárním pevném disku klesne pod úroveň nezbytnou pro spolehlivé fungování, služba Vzdálené úložiště (Remote Storage) odstraní místní data, která byla zkopírována na vzdálené úložiště.	Umožňuje správcům spravovat množství volného diskového prostoru migrováním souborů do knihovny pásků, kde soubory zůstávají z pohledu uživatele aktivní.
Vyměnitelné úložiště	Umožňuje správcům spravovat zařízení a funkce vyměnitelných úložišť. Správci mohou vytvářet fondy médií, které vlastní a používá nějaká konkrétní aplikace.	Umožňuje správcům optimalizovat výkon sítě řízením míst ukládání dat. Dovoluje také více aplikacím sdílet stejné prostředky médií úložišť.
Vylepšení systému souborů NTFS	Podporuje vylepšení výkonu, jako je šifrování souborů, schopnost přidat diskový prostor ke svazku NTFS bez restartování, distribuované sledování odkazů a kvóty svazků pro jednotlivé uživatele, které jsou určeny ke sledování a omezování použití diskového prostoru.	Šifrování souborů omezuje riziko vystavení důvěrných dat neautorizovaným uživatelům. Protože lze rychle rozšiřovat oddíly, omezují se výpadky serverů a sítě a také riziko ztráty dat.
Diskové kvóty	Pomáhají správcům plánovat a implementovat používání disků.	Omezují potřeby správy hardwaru a snižují náklady na správu.
Zálohování	Pomocí programu Zálohování (Backup) si mohou uživatelé zálohovat data na různá ukládací média včetně pevných disků a magnetických a optických médií.	Pomáhá ochránit data před náhodnou ztrátou způsobenou selháním hardwaru nebo média úložiště.
Podpora distribuovaného systému souborů (DFS)	Umožňuje správcům vytvořit jediný adresářový strom obsahující více souborových serverů a míst sdílení souborů a umožňují spolupráci (interoperabilitu) mezi klienty systému Windows 2000 a libovolným souborovým serverem s odpovídajícím protokolem.	Systém DFS usnadňuje správcům a uživatelům vyhledávání a správu dat na síti. DFS také poskytuje místo sdílení odolné proti chybám pro důležité síťové soubory.

Další informace o zavádění technologií správy úložišť systému Windows 2000 Server najdete v kapitole „Určení strategií správy úložišť systému Windows 2000“ v této knize.

Plánování seznamu úloh pro mapování možností Windows 2000

Seznam úkolů plánování uvedený v tabulce 1.14 použijte na začátku procesu plánování zavedení systému Windows 2000.

Tabulka 1.14 Plánování seznamu úloh pro mapování možností Windows 2000

Úkol	Umístění v kapitole
Seznamte se s tím, jak vám struktura této knihy bude pomáhat v procesu plánování zavedení.	Spuštění plánu
Seznamte se s rodinou produktů systému Windows 2000.	Přehled rodiny produktů Windows 2000
Určete, jak lze jednotlivé funkce použít ke zvýšení produktivity pracovníků.	Zlepšení způsobu práce pomocí systému Windows 2000
Seznamte se s funkcemi systému Windows 2000 v kontextu svých obchodních či výrobních cílů.	Přiřazování funkcí systému Windows 2000 vašim obchodním či výrobním potřebám

KAPITOLA 2

Vytvoření cesty postupného zavádění



Plánování projektu zavedení je důležitý krok v logickém postupu implementování systému Microsoft Windows 2000. Protože systém Windows 2000 je vytvořen tak, aby umožňoval postupné zavádění (na základě specifických obchodních či výrobních potřeb a možností oddělení informačních technologií (IT) organizace libovolné velikosti), musíte určit, které funkce jsou pro vaši organizaci vhodné. Musíte také zvážit závislosti technického a projektového řízení funkcí systému Windows 2000, které jste vybrali k zavedení. Musíte se také zamyslet nad požadavky spolupráce nebo společné funkce vašeho existujícího prostředí IT.

Tato kapitola představuje celkový proces řízení projektu a identifikuje klíčové fáze zavádění, čímž vám pomáhá s vytvořením plánu projektu (cesty postupného zavádění), který bude váš tým plnit při zavádění systému Windows 2000 ve vaší organizaci.

V této kapitole

Vytvoření plánu projektu 30

Scénáře zavádění 36

Technologické závislosti 50

Tipy plánování zavádění systému Windows 2000 52

Seznam úkolů plánování 55

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Plán projektu
- Proces řízení projektu vhodný pro vaši organizaci

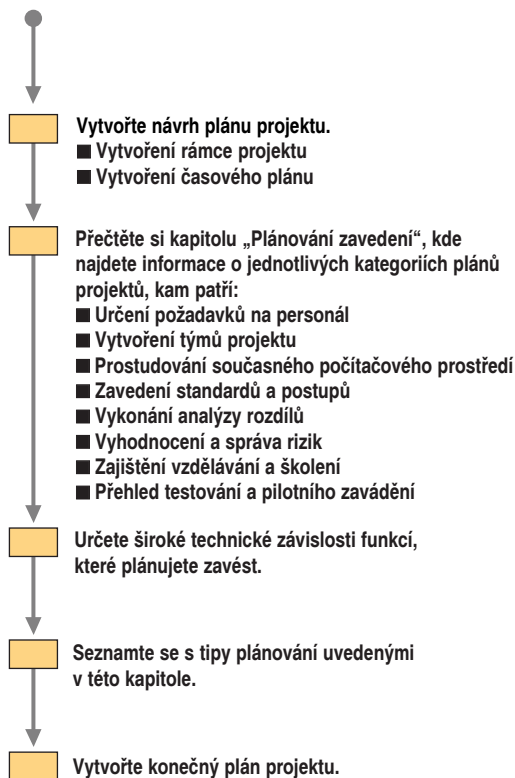
Související informace v sadě Resource Kit

- Další informace o vývoji plánu projektu zavedení najdete v kapitole „Plánování zavedení“ v této knize.
- Další informace o tom, jak spustit úspěšný pilotní projekt zavedení systému Windows 2000, najdete v kapitole „Vykonání pilotního programu systému Windows 2000“ v této knize.
- Další informace o návrhu testovací laboratoře a vyhodnocení funkcí systému Windows 2000 najdete v kapitole „Vytvoření testovací laboratoře systému Windows 2000“ v této knize.

Vytvoření plánu projektu

Vytvoření plánu projektu zavedení systému Windows 2000 zajistí úspěšné zavedení. Třebaže budete vytvářet plán projektu, který bude jedinečným způsobem naplňovat vaše obchodní či výrobní požadavky a požadavky IT, existují určité obecné prvky, jež musí být v plánu obsaženy, aby představoval skutečně efektivní cestu postupného zavádění vašeho projektu. Tato kapitola se soustřeďuje na integraci předběžných rozhodnutí o technologiích do plánu řízení projektu, který použijete k zavedení systému Windows 2000. Další informace o specifických problémech řízení projektu, kterými se musíte zabývat při přípravě plánu projektu, najdete v kapitole „Plánování zavedení“ v této knize. Obrázek 2.1 ilustruje některé kroky, které můžete využít při vytváření plánu projektu.

Začátek



Obrázek 2.1 Vytvoření plánu projektu

Použijete-li plán projektu efektivně, může zřetelně označovat jednotlivé fáze procesu zavedení a poskytovat jasnou a funkční cestu zavádění. Není sice zapotřebí postupovat v procesu zavádění naprosto přesně (jako je tomu u procedury instalace), proces zavedení infrastruktury však poskytuje koncepční rámec pro váš projekt zavedení systému Windows 2000 a usnadňuje vašim týmům zavádění vyhodnocování postupu.

Mnoho organizací již používá nějaké metody a struktury řízení projektů. Maximalizace úspěchu zavedení systému Windows 2000 dosáhnete, budete-li postupovat podle struktury řízení projektů používané a vhodné ve vaší organizaci. Následující oddíly představují ukázkovou strukturu řízení projektů a následně popisují struktury řízení projektů používané dvěma ukázkovými společnostmi.

Při čtení této kapitoly budete nacházet odkazy na tým zavádění, dokumenty plánování projektu, vytvoření a použití testovací laboratoře a pilotní testování systému Windows 2000. Tabulka 2.1 je seznam kapitol v této knize obsahujících další informace, které vám pomohou s vývojem plánu projektu.

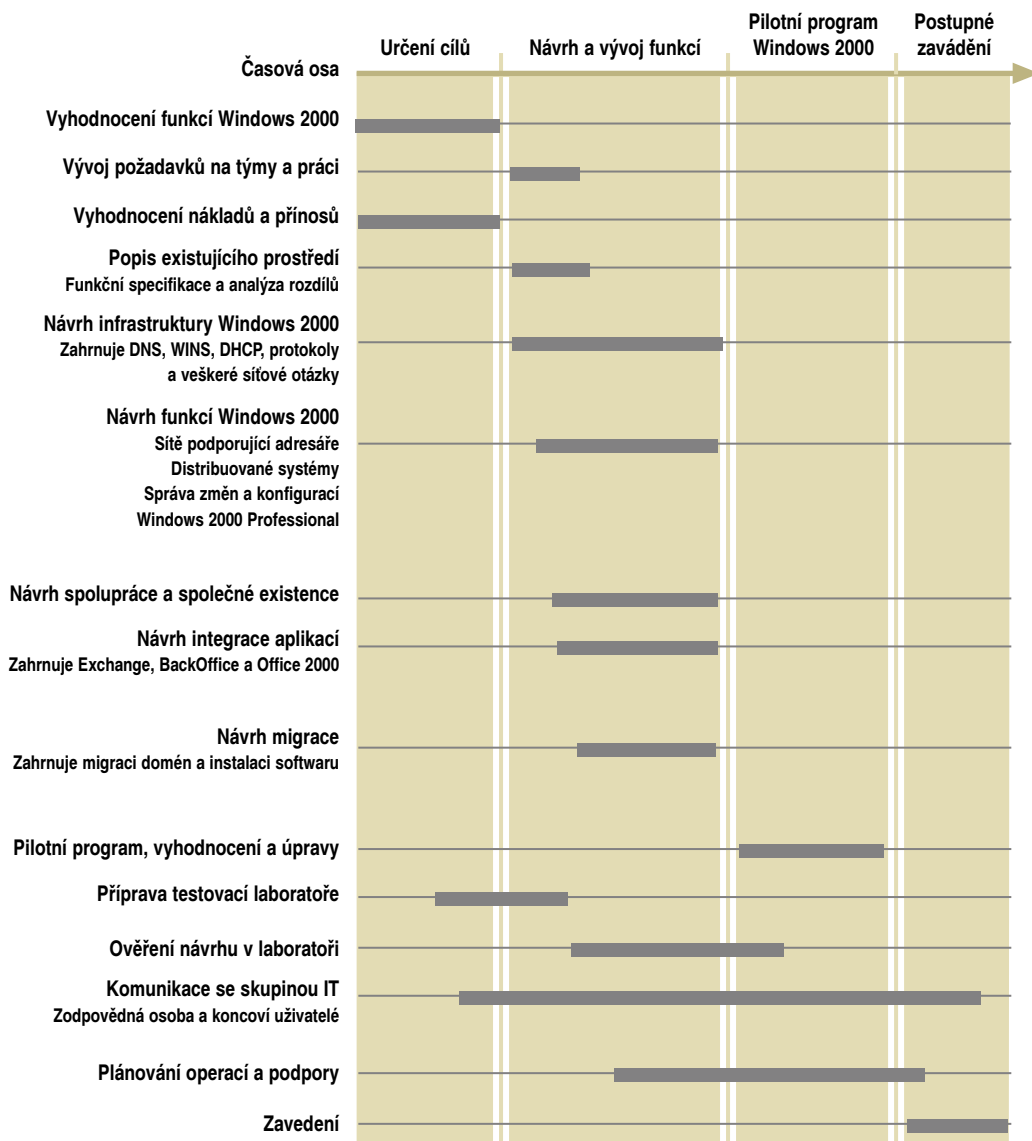
Tabulka 2.1 **Informace o plánování zavedení obsažené v této knize**

Kapitola	Popis
Plánování zavádění	Obsahuje informace o analýze současného počítačového prostředí, vykonání analýzy rozdílů, požadavcích na personál, plánování úkolů, dokumentech plánování zavádění, plánování kapacity, vyhodnocení rizik a vzdělávání a školení.
Vytvoření testovací laboratoře systému Windows 2000	Obsahuje informace o návrhu, vytvoření a správě testovací laboratoře, testování zavádění a testování po zavedení.
Vykonání pilotního programu systému Windows 2000	Obsahuje informace o úspěšném vykonání pilotního projektu systému zavedení Windows 2000.
Testování kompatibility aplikací se systémem Windows 2000	Obsahuje informace o testování kompatibility aplikací (vlastních i zakoupených) s vaší konfigurací systému Windows 2000.

Příprava procesu plánování projektu

Každý projekt zavádění prochází určitým životním cyklem, tedy procesem zahrnujícím určení cílů IT, návrh a vývoj funkcí, vykonání pilotního projektu a instalaci nového operačního systému do produkčního prostředí. Hlavním smyslem procesu plánování projektu je sestavit pořadí, v jakém váš tým zavádění určuje, implementuje, testuje a vykonává požadované činnosti.

Obrázek 2.2 ilustruje ukázkový proces řízení projektu zavedení systému Windows 2000. Jednotlivé fáze jsou uvedeny v horní části obrázku. Hlavní část obrázku obsahuje úkoly, které je zapotřebí dokončit v různých fázích zavádění, a navrhuje technologie systému Windows 2000, které by mohlo být vhodné zavést.



Obrázek 2.2 Ukázkový proces řízení projektu zavádění systému Windows 2000

Dvě linie ve spodní části obrázku souvisejí s testovací laboratoří. Testování je integrální součástí zavádění systému Windows 2000 a budete je používat v celém procesu zavádění.

Všechny čtyři kroky řízení projektu uvedené v obrázku 2.2 jsou popsány v následujících oddílech.

Určení cílů

V této fázi vyhodnoťte funkce systému Windows 2000 ve vztahu k potřebám vaší organizace. V této době musíte také zajistit podporu a financování ze strany zodpovědných složek vaší společnosti, vytvořit přesně určené cíle a sestavit tým zavádění. Nakonec začnete zkoumat funkce systému Windows 2000 v testovací laboratoři.

Prvním důležitým mezníkem je potvrzení celkového plánu zavádění systému Windows 2000 ve vaší organizaci jejími odpovědnými osobami. Při definování plánu načrtněte obchodní či výrobní cíle a cíle IT vašeho zavádění, aby byl dán jasný směr implementace. Také zřetelně definujte, které funkce systému Windows 2000 budou součástí jednotlivých fází zavádění.

Mezi otázky, které musíte zodpovědět v této fázi, patří:

- Proč vaše organizace zavádí systém Windows 2000?
- Jaké výhody získá vaše organizace přechodem na systém Windows 2000?
- Jaké výhody v oblasti IT získá vaše organizace přechodem na systém Windows 2000?
- Jaké jsou rozdíly mezi současným prostředím IT vaší organizace a prostředím, kterého chcete dosáhnout?
- Kdy musí být tento projekt dokončen a jaký je časový plán?
- Co patří do rámce a mimo rámec tohoto projektu?
- Jaké uživatele tento projekt ovlivní?
- Jaké jsou kritické faktory úspěchu?
- Jaká jsou rizika?
- Které skupiny, organizace a jednotlivci se budou tohoto procesu účastnit?

Mezi dokumenty, které bude možná zapotřebí vytvořit v rámci této fáze, patří:

- Dokument cílů
- Popis současného prostředí včetně profilů uživatelů
- Vyhodnocení rizik
- Analýza rozdílů

Další informace o vyhodnocení rizik a analýze rozdílů najdete v kapitole „Plánování zavedení“ v této knize.

Tato fáze je důležitá pro vytvoření cesty postupného zavádění. Jakmile definujete své cíle, je mnohem jednodušší určit funkce systému Windows 2000, které k jejich naplnění potřebujete, a jejich vztah k současnému prostředí. Vaše analýza vám také pomůže porozumět důležitým technologickým závislostem. Ve svém vyhodnocení sice musíte být přesní, tuto fázi však lze dokončit v poměrně krátké době. Fáze cílů vám pomůže vytvořit vizi projektu, kterou budou sdílet oddělení IT, koncoví uživatelé i management a která vám pomůže dosáhnout úspěšného zavedení.

Poznámka Vaše organizace možná již touto fází prošla, ať formálně nebo neformálně. I když se management již rozhodl pro zavedení systému Windows 2000, přesto musíte vytvořit dokument cílů a nechat si jej formálně potvrdit. Pak je teprve možné přejít do fáze návrhu a vývoje funkcí.

Návrh a vývoj funkcí

Během fáze návrhu a vývoje funkcí vytváříte vlastní návrh – někdy označovaný za funkční specifikaci – funkcí systému Windows 2000, které budete ve vaší organizaci implementovat. V této době také určíte, jak budou vybrané funkce skutečně pracovat v produkčním prostředí.

V této fázi jsou důležitější technické závislosti funkcí systému Windows 2000, takže různé týmy zavádění musejí spolupracovat a sdílet svá pojetí schopností, funkčnosti a vzájemných závislostí jednotlivých funkcí. S určením způsobu zavádění konkrétních funkcí ve vaší organizaci vám pomohou kapitoly technického návrhu ve zbývajících částech této knihy.

Specifikace funkčního návrhu je úplná sada návrhů, které budete testovat a doladovat. Můžete mít například více variant návrhu oboru názvů služby Active Directory vycházejících z různých obchodních či výrobních požadavků nebo požadavků IT – každý z nich bude vyhodnocen z hlediska kritérií obchodní či výrobní činnosti a kritérií IT odpovídajících vaší organizaci. Po technických testech a analýzách budete nakonec připraveni k implementování jednoho oboru názvů služby Active Directory v organizaci. Je důležité uvědomit si, že tento proces a jeho výsledky budou pro vaší organizaci specifické.

Iterační proces návrhu a testování začíná v této fázi tím, že každý z vašich týmů zavádění vytvoří své vlastní plány a ty se pak vzájemně synchronizují, aby došlo k vytvoření zevrubné specifikace návrhu. V této fázi je také důležitá testovací laboratoř, protože musíte otestovat různé konfigurace a určit, jak lze použít funkce systému Windows 2000 k naplnění cílů vašeho projektu.

Specifikace funkčního návrhu musí poskytovat vašim projektovým týmům dostatek podrobností o funkcích a prvcích, které bude vaše organizace zavádět, což jim pomůže snadno určit požadavky a vazby na prostředky potřebné pro implementování vaší infrastruktury systému Windows 2000.

Během této fáze také vytvoříte plán projektu obsahující funkční specifikaci (kombinovaný plán jednotlivých týmů) a časový plán. S implementací plánu projektu můžete začít, jakmile od výkonných složek obdržíte povolení začít se zaváděním. Mezi předběžné položky, které můžete zahrnout do svého plánu, patří:

- Specifikace funkčního návrhu
- Aktualizovaný plán řízení rizik
- Hlavní plán projektu a hlavní časový plán projektu
- Plán funkcí uvádějící funkce patřící a nepatřící do rámce vašeho zavádění

Pilotní program zavádění systému Windows 2000

Jakmile dokončíte návrh a vývoj funkcí a dokonale otestujete konfigurace funkcí, můžete začít s vykonáváním pilotního projektu. Tým zavádění musí určit řadu průběžných cílů, z nichž každý zahrnuje vývoj řešení, testování, vyhodnocení vzhledem k předem specifikovaným kritériím výkonu a změnu návrhu. Sledování problémů zavádění a jejich efektivní řešení je zásadní podmínkou dosažení cílů zavádění při současném dodržení časového plánu a nepřekročení vyhrazených finančních prostředků.

Jakmile váš pilotní projekt stabilně běží, osoby financující tento plán a tým zavádění se mohou sejít a vyhodnotit funkčnost nové infrastruktury systému Windows 2000 a ověřit správnost plánů postupného zavádění do produkčního prostředí a plánů zajištění

technické podpory. V této fázi mohou být základními milníky a dokumenty zavádění tyto položky:

- Dokončené technologické vyhodnocení
- Dokončená a stabilní funkční specifikace
- Dokončené potvrzení koncepce
- Dokončený test použití v produkčním prostředí
- Dokončený pilotní projekt
- Aktualizovaný plán řízení rizik

Mezi další dokumenty, které můžete vyvinout, patří:

- Plán školení
- Plán technické podpory
- Plán převodu operací
- Plán zotavení po havárii
- Seznam nástrojů

V této fázi upravitě své návrhy podle výsledků pilotního testování. Potřebných změn si všimnete, protože spojujete všechny návrhy jednotlivých zaváděných funkcí dohromady a následně testujete jejich řádnou integraci.

Další informace o vyhodnocování a testování plánu zavádění systému Windows 2000 Server pomocí laboratorního testování a pilotního programu potvrzení koncepce najdete v kapitolách „Vytvoření testovací laboratoře systému Windows 2000“ a „Vykonání pilotního programu systému Windows 2000“ v této knize.

Další informace o testování kompatibility aplikací se systémem Windows 2000 Professional najdete v kapitole „Testování kompatibility aplikací se systémem Windows 2000“ v této knize.

Postupné zavádění do produkčního prostředí

Poslední fází projektu systému Windows 2000 je postupné zavádění do obchodního či výrobního prostředí. V tomto okamžiku již máte laboratorně otestovány všechny návrhy a vykonali jste pilotní program, který dále doladil váš plán a znovu návrhy otestoval. Nyní jste připraveni na postupné zavádění systému Windows 2000 do celého podniku. V případě některých společností je počáteční pilotní projekt první fází postupného zavádění. Jiné společnosti instalace pilotního projektu zruší a postupné zavádění do produkčního prostředí začnou čistými instalacemi.

Během fáze postupného zavádění do produkčního prostředí jsou stále velmi důležité činnosti testování a technické podpory, protože iterační cykly zavedení, testování, ověřování a podpory jsou nyní zásadní. Nová infrastruktura systémů Windows 2000 Server a Windows 2000 Professional se formálně převede na skupiny operací a podpory v okamžiku úspěšného dokončení zavádění. Nyní je čas projekt vyhodnotit. Mezi základní milníky a dokumenty zavádění, které můžete vytvořit v této fázi, patří:

- Plán postupného zavádění do produkčního prostředí
- Plán uvedení systému Windows 2000 Server, systému Windows 2000 Professional, nebo obou
- Informační systém operací a technické podpory (databáze znalostí, procedury a postupy technické podpory včetně výsledků testů a testovacích nástrojů)

- Sady obrazů (bitových kopií) a instalační skripty
- Archivace dokumentů (archivují se papírové a elektronické kopie všech dokumentů projektu včetně poznámek k zavádění)
- Školící materiál pro koncové uživatele, správce, technickou podporu a personál operací
- Zpráva o dokončení projektu
- Plán zotavení po havárii

Jakmile je zavádění dokončeno a vy jste připravili zprávu o dokončení projektu pro výkonné a finanční složky společnosti, můžete vykonat přehled projektu. V přehledu projektu můžete objektivně vyhodnotit silné a slabé stránky celého projektu a analyzovat, jak lze zlepšit budoucí zavádění infrastruktury pomocí znalostí nabytých v praxi.

Scénáře zavádění

Každá společnost si podle svých obchodních či výrobních potřeb a postupů řízení projektu vytvoří svůj vlastní plán projektu. Následující scénáře uvádějí příklady převodu cílů několika velkých organizací na postupné cíle a kritéria výkonu. Tyto scénáře vycházejí ze zkušeností společností, které se účastnily programu Joint Development Program systému Windows 2000.

Scénář 1: Mezinárodní finanční služby

Tato organizace má devět samostatně fungujících společností – každá z nich má svou vlastní organizaci IT a neexistují tu žádné společné standardy IT. Tato organizace má problémy se zásadami zabezpečení, strukturou domén a konfiguracemi sítí. Na většině jejích serverů v současné době běží systém Microsoft Windows NT Server 4.0. Klíčovými cíli, kterých chce tato organizace dosáhnout, je vytvořit:

- nové prostředí IT s funkcemi systému Windows 2000,
- společný adresář pro všech devět fungujících společností.

Tým zavádění identifikoval několik klíčových problémů, které určují fáze zavádění systému:

- Fáze 1: Vyhodnocení
- Fáze 2: Návrh a technické řešení
- Fáze 3: Testování
- Fáze 4: Migrace (zavedení)

Fáze 1: Vyhodnocení

Během fáze vyhodnocení souhlasí management IT jednotlivých společností s potřebou vytvoření společného oboru názvů. Jednotlivé fungující společnosti sice již mají zaregistrovaných několik názvů systému Domain Name System (DNS), je však zapotřebí najít jeden název, který se bude používat jako kořenový název pro všechny společnosti. Tento jediný „všezahrnující“ název musí odpovídat následujícím kritériím:

- Musí přesně definovat kořen stromu všech devíti samostatně fungujících společností.
- Musí být nový (nikdy jej nepoužila žádná ze společností, interně ani externě).

Management IT definuje globální technické týmy, které jsou rozděleny do osmi pracovních skupin podle plánů základní konfigurace, kterou lze otestovat, změnit a upravit pro jednotlivé společnosti. Tabulka 2.2 ukazuje týmy zavádění a jejich zodpovědnost.

Tabulka 2.2 **Týmy plánování zavedení**

Tým zavádění	Zaměření
Návrh serverů a infrastruktury	Zodpovídá za celkový návrh, iterace návrhu a konečné technické provedení.
Služba Active Directory	Návrh domén a stromů pod hlavní doménovou úrovní a neustále probíhající správa služby Active Directory a jejich domén, zejména v souvislosti s privilegii zabezpečení a správy.
Návrh přenosných a kancelářských počítačů	Vývoj konfigurací systémů Windows 2000 pro všechny kancelářské a přenosné počítače a určení příslušných zásad skupiny a funkcí Microsoft IntelliMirror používaných pro správu těchto konfigurací.
Zabezpečení	Oprávnění, členství ve skupinách a delegování správy (poskytují vstup pro skupinu služby Active Directory ohledně návrhu organizačních útvarů).
Migrace	Migrace systému Windows NT Server 4.0 na prostředí systému Windows 2000 Server. Zaměřuje se na možnosti spolupráce (interoperability), migraci a společné existenci paralelních domén během přechodného období do úplného dokončení migrace.
Certifikační služby	Šifrování souborů a infrastruktura PKI.
Volný pohyb	Vývoj konfigurace systému Windows 2000 umožňující volný pohyb klientů a určení příslušných zásad skupiny a funkcí IntelliMirror, které se budou používat pro správu těchto konfigurací.
Řízení aplikací	Zajištění kompatibility všech používaných aplikací se systémem Windows 2000. Určení nejlepší metody zavádění systému Windows 2000 na kancelářské a přenosné počítače (pomocí vlastních vyvinutých instalačních programů instalace nevyžádaných aplikací nebo pomocí instalačních nástrojů systému Windows 2000). Určení sdílených komponent používaných za běhu programu. Studium mechanismu ochrany systémových souborů. Současné spouštění existujících aplikací v zájmu minimalizování údržby.

Tým určí, že obchodní či výrobní potřeby a potřeby IT budou v zásadě naplněny těmito položkami:

- Služba Active Directory
- Nový návrh domén
- Funkce IntelliMirror
- Distribuovaný systém souborů
- Řízení diskových kvót

- Vzdálená instalace operačního systému
- Synchronizace služby Active Directory s adresářovými službami Exchange

Fáze 2: Návrh a technické řešení

Hlavním problémem v této fázi je určit, zda má být název kořenové domény viditelný neboli přístupný z Internetu, nebo zda má být dostupný pouze interně. Celá skupina fungujících společností má již vytvořenou prezentaci na Internetu, takže intranetový název musí být odlišný. Je tedy vytvořen interní kořenový název, aby bylo možné vytvářet jednotlivé domény pro každou z devíti fungujících společností. Každá společnost si ponechává autonomii v oblastech, jako je vytvoření konfigurace, správa a zabezpečení.

Tuto fázi organizace používá také k návrhu a testování konfigurace jednotlivých funkcí. Týmy pak spolupracují a určí, jak se vybrané funkce systému Windows 2000 vzájemně ovlivňují. Také se vytváří školicí dokumentace a začíná se vyvíjet plán technické podpory.

Hlavní cíle

Návrh služby Active Directory a domén musí jako základní důvod migrace na systém Windows 2000 naplnit následující obchodní či výrobní kritéria a kritéria IT. Jen tak bude přijatelný pro všechny fungující společnosti:

- Je nezbytná jedna kořenová doména, aby mohly být všechny fungující společnosti účastny v jednom společném adresáři.
- Každá obchodní či výrobní jednotka si chce zachovat plné řízení správy celé své organizace včetně všech samostatných domén a struktury systému Windows NT Server 4.0 a chce být zcela nezávislá na jiných fungujících společnostech.
- Návrh domén a adresáře musí být dostatečně flexibilní, aby umožňoval nákupy jiných společností, rozdělování a reorganizaci existujících samostatně fungujících společností.
- Jednotlivé fungující společnosti samy zodpovídají za svou doménu a vše, co se pod ní nachází na základě svých specifických potřeb.

Během vývoje návrhu služby Active Directory musí tým migrace zvážit otázky klonování počítačů a porovnat je s inovacemi počítačů. Klonování počítačů je proces, ve kterém vytvoříte jednu instalaci a konfiguraci nových instalací operačního systému a tuto konfiguraci pak zkopírujete na všechny nově instalované počítače.

Jelikož jsou rozhodnutí o oboru názvů velmi důležitá k naplnění cílů společnosti, je vytvořena skupina oboru názvů se zástupci ze skupin IT všech samostatně fungujících společností. Vyšší management a organizace IT jednotlivých společností se musejí dohodnout na konečném návrhu oboru názvů. Mezi zvažované faktory návrhu oboru názvů patří:

- Vliv na model domén systému Windows 2000
- Vliv na existující obor názvů systému Windows NT Server 4.0
- Konflikty s existujícím oborem názvů DNS

Společnost považuje jak návrh domén, tak i návrh systému DNS za důležitá rozhodnutí inovace ze systému Windows NT Server 4.0 na systém Windows 2000 ze dvou důvodů:

- Jestliže navrhovaná struktura domén systému Windows 2000 zrcadlí existující strukturu domén systému Windows NT Server 4.0, pak se mohou inovovat přímo domény Windows NT na domény Windows 2000.
- Je-li rozhodnuto použít stejnou strukturu domén systému Windows 2000, jaká byla použita v systému Windows NT Server 4.0, pak musí existovat dvě paralelní struktury domén. Prostředí systému Windows NT také musí být zachováno až do doby stabilizace nového prostředí systému Windows 2000.

Tým určí, že rozhodnutí o inovaci nebo migraci bude určeno těmito položkami:

- Existující struktura domén
- Existující funkce
- Nové funkce, které se budou implementovat kvůli systému Windows 2000

Tým si dále uvědomí, že určení prvků existujících v jednotlivých doménách vyžaduje analýzu následujících položek:

- Vyhodnocení problémů v současném návrhu domén systému Windows NT Server 4.0.
- Určení funkcí systému Windows NT Server 4.0, které je zapotřebí zachovat v návrhu domén systému Windows 2000.
- Určení nových funkcí systému Windows 2000, které se budou implementovat na základě jimi dosažených vylepšení nové struktury domén.
- Zjištění, zda tu existuje nativní prostředí systému Windows NT Server 4.0, nebo zda bylo nějakým způsobem změněno nebo upraveno (buď vlastními vývojovými týmy nebo nezávislými poskytovateli řešení či vývojáři).

Tato organizace například používá svůj vlastní skriptový nástroj, který přiřazuje uživatelům specifické aplikace. Tento nástroj vykonává publikování aplikací podobné nástroji Windows Installer v systému Windows 2000, takže je zapotřebí rozhodnout, zda se bude nadále používat vlastní vyvinutý nástroj nebo Windows Installer. Použitím nástroje Windows Installer se sníží náklady na interní vývoj a tedy i celkové náklady na vlastnictví (TCO). Proto se rozhodne používat Windows Installer.

Další informace o návrhu domén služby Active Directory najdete v kapitole „Návrh struktury služby Active Directory“ v této knize. Další informace o migraci domén najdete v kapitole „Určení strategií migrace domén“ v této knize.

Druhotný cíl

Druhotným cílem je určit další funkce systému Windows 2000, které budou do prostředí přinášet výhody, jež však třeba nebyly součástí systému Windows NT Server 4.0. Následně se vyvine plán, určující zda jsou tyto nové funkce pro dané prostředí vhodné. Tato ukázková organizace se například rozhodne, že její obchodní či výrobní požadavky a požadavky IT naplňují následující funkce:

Soubory přístupné offline

Uživatelé přenosných počítačů mohou mít přístup k datům na síti na cestách, protože mají své osobní a síťové soubory na místních počítačích. Necestujícím koncovým uživatelům tato funkce zajistí produktivitu i v případě výpadku služeb sítí LAN nebo WAN, protože potřebné soubory jsou uloženy na místním pevném disku uživatele.

Distribuovaný systém souborů odolný proti chybám

Pomocí distribuovaného systému souborů (Distributed File System – DFS) je možné vytvořit jediný strom adresářů zahrnující mnoho souborových serverů a míst sdílení souborů skupin, oddělení i podniků. To umožňuje uživatelům jednoduše vyhledávat soubory a složky distribuované v síti. Systém DFS odolný proti chybám je propojen s cestovními uživatelskými profily, které se již používají v infrastruktuře systému Windows NT Server 4.0. Soubory tak lze ukládat na síť, což zajišťuje lepší replikaci mezi partnery společnosti.

Řízení diskových kvót

Řízení diskových kvót umožňuje společnosti používat svazky naformátované systémem souborů NTFS ke sledování a omezování množství diskového prostoru serveru dostupného jednotlivým uživatelům. Mohou také definovat reakce na situace, kdy uživatelé překročí zadané limity. V minulosti musela společnost používat nástroje nezávislých výrobců. Nyní přechází na nativní nástroje systému Windows 2000, čímž se snaží omezit náklady na vývoj a celkové náklady na vlastnictví.

Vzdálená instalace operačního systému

V organizaci je již vytvořen vylepšený skriptový proces instalace, skripty je však při každé změně základní konfigurace klientského počítače zapotřebí upravit. K prvotní instalaci systému Windows 2000 Professional se tedy použije funkce vzdálené instalace OS systému Windows 2000, která bude také sloužit k rychlým inovacím nesprávně fungujících počítačů. Organizace plánuje používat vzdálenou instalaci OS ve spojení s funkcemi IntelliMirror, čímž se zrychlí a zjednoduší náhrada počítačů a tedy se také sníží náklady TCO.

Integrace adresářové služby Exchange se službou Active Directory

Tato organizace plánuje synchronizovat adresář systému Exchange 5.5 pomocí nástroje Active Directory Connector (ADC) a po inovaci na následující verzi Exchange tyto adresářové služby plně integrovat.

Fáze 3: Testování

Ukázková organizace vytvoří v zájmu testování funkcí a pilotního testování laboratoř. Chce simulovat skutečné podmínky migrace produkčního prostředí. Jakmile laboratorní a pilotní testy ověří proces migrace, organizace bude připravena na postupné zavádění do produkčního prostředí. Během fáze testování budou personálu IT předány předběžné pilotní programy návrhu, aby mohli své návrhy otestovat a doladit.

Mezi počáteční problémy návrhu, které organizace plánuje otestovat a vyhodnotit, patří:

- Návrh služby Active Directory (základní doména a čtyři podřízené domény)
- Standardní klientská konfigurace

Cíle pilotního projektu zahrnují:

- Vyhodnocení systému Windows 2000 a navrhovaného modelu služby Active Directory ve skutečném produkčním prostředí
- Použití nových technologií nativních systému Windows 2000 v co nejvyšší možné míře
- Sloučení standardních klientských stacionárních a mobilních konfigurací

- Představení navrhovaných budoucích konfigurací obchodním či výrobním jednotkám v celé organizaci a zaznamenání jejich konstruktivní kritiky
- Konsolidace a změna zaměření izolovaných projektů systému Windows 2000 v rámci celé organizace

V této fázi tým zavádění testuje návrhy tak dlouho, dokud není dosaženo shody. Nový návrh musí splňovat následující kritéria přijatelnosti:

- Zvyšuje stabilitu
- Zajišťuje lepší síťové prostředí
- Lze jej spravovat současnými a novými nebo dodatečnými prostředky správy
- Nepřekračuje rozpočet

Po dokončení testování návrhu domén podepíše každý globální tým technického zabezpečení v organizaci daný návrh domén. Návrh pak musí být schválen vyšším managementem IT ve všech devíti samostatně fungujících společnostech.

Fáze 4: Migrace

Protože organizace vyžaduje zachování cestovních uživatelských profilů, rozhodne se během přechodného období zachovat dvě paralelní prostředí. Mnoho cestujících uživatelů, kteří inovují na systém Windows 2000 doma, zjistí, že jejich pracovní prostředí ještě nebylo inovováno. Zachováním paralelních prostředí bude infrastruktura podporovat všechny uživatele a umožní jim přístup k jejich souborům bez ohledu na operační systém, který používají.

K migraci však musí dojít co nejdříve. Organizace plánuje zachovat duální prostředí systémů Windows NT Server 4.0 a Windows 2000 po 12 až 24 měsíců. Uživatelé budou moci zůstat v obou prostředích, až dokud nebude prostředí IT ve všech devíti samostatně fungujících společnostech plně převedeno na systém Windows 2000.

V případě této organizace je zrušení prostředí systému Windows NT Server 4.0 nejkritičtější rozhodnutím celé migrace. Organizace si chce být jista, že vykonala dostatečné laboratorní a pilotní testování a že se vyřešily všechny významné problémy, které mohly být důsledkem nevhodného návrhu. Pomocí odpovídajícího testování se chce vyhnout výpadkům sítí. Po dokončení testování se bude pokračovat s migrací na systém Windows 2000 ve všech fungujících společnostech a nakonec se zruší prostředí systému Windows NT Server 4.0.

Scénář 2: Mezinárodní výrobce spotřebního a průmyslového zboží

Scénář 2 vychází z vysoce decentralizované obchodní a výrobní organizace s distribuovaným prostředím IT skládajícím se ze 175 samostatně fungujících organizací. Výroba a montáž probíhá ve 49 zemích na šesti kontinentech. Společnost má přibližně 390 000 zaměstnanců po celém světě, kteří hovoří asi 120 různými jazyky. V zájmu zjednodušení přechodu všech fungujících společností a omezení nákladů na zavádění je zapotřebí společný proces rozhraní a implementace. Všechny fungující společnosti se chtějí zabývat následujícími společnými problémy:

- Poskytovat zákazníkům snadný přístup k obecné sadě znalostí souvisejících se společnostmi a jejich obchodní a výrobní činností.
- Omezit náklady na správu IT a zlepšit služby vytvořením jediné doménové struktury.

- Konsolidovat servery se systémem Windows NT 4.0 pro inovaci.
- Zajistit společné prostředí IT všem fungujícím společností.
- Vytvořit doporučené postupy zavádění systému Windows 2000 platné v celé organizaci, které zajistí stabilní prostředí IT a zabrání jednotlivým skupinám v zavádění samostatných produktů nebo funkcí, které nejsou podporovány centrálním oddělením IT.
- Vzájemně se informovat o problémech IT.
- Efektivně navrhnout strukturu služby Active Directory, jelikož na ní závisí mnoho dalších funkcí systému Windows 2000.

Týmy zavádění

Tato organizace vytvoří tým zavádění skládající se ze serverového a klientského týmu. Každý tým má zástupce ze všech hlavních samostatně fungujících společností. Jejich cílem je vyvinout model pro serverová i klientská operační prostředí, který lze aplikovat a používat ve všech společnostech. To znamená, že jejich cílem je vlastně vytvořit a ověřit proces návrhu a zavedení, který lze použít ve všech samostatně fungujících společnostech – nikoli tedy zavádět systém Windows 2000 v produkčním prostředí. Svůj plán rozdělí do tří fází:

- Fáze 1: Návrh a vývoj infrastruktury páteřního spojení
 - Vytvoření základních služeb hlavní domény společnosti
 - Zavedení serverů v hlavních kancelářích společnosti
- Fáze 2: Plánování zavedení v samostatně fungujících společnostech
 - Vytvoření pilotních domén v samostatně fungujících společnostech
 - Konfigurování sídel a mostů spojujících sídla
 - Vytvoření uživatelských účtů
 - Zřízení vztahů důvěryhodnosti mezi doménami systémů Windows NT Server 4.0 a Windows 2000
 - Pilotní zavedení systému Windows 2000 Professional ve více samostatně fungujících společnostech
- Fáze 3: Migrace základních služeb ze systému Windows NT Server 4.0 na systém Windows 2000 Server
 - Služba Windows Internet Name Service (WINS)
 - Protokol Dynamic Host Configuration Protocol (DHCP)
 - Tisk
 - Webové servery používající službu Windows Internet Information Services (IIS)

Jedním z prvních úkolů, které tým splní, je vytvoření seznamu základních otázek a rizik celkového projektu. Tento seznam zahrnuje:

- Poznání, že koordinace potřebná k vytvoření globálního podniku musí dosahovat vysokých úrovní. (Zavedení nějakého operačního systému na servery i klienty ve všech samostatně fungujících společnostech trvá průměrně tři roky.)
- Příprava na společnou existenci s unixovými a mainframovými obchodními aplikacemi podle požadavků. (Mnoho samostatně fungujících společností má například server Sun RISC 6000 obsahující účetní program pracující v prostředí operačního systému Windows NT Server 4.0.)

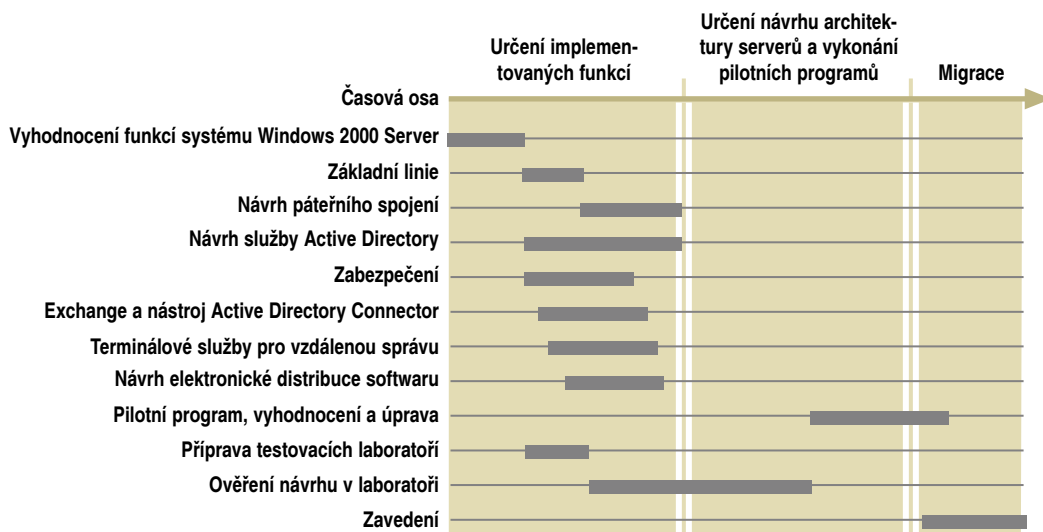
- Zajištění nástrojů pro přesun a sloučení částí doménové struktury v případě potřeby na základě interních změn společností a častých nákupů jiných společností, slučování a rozdělování.
- Obsazení místa prvního správce domén, který:
 - dokáže rychle reagovat na požadavky změn a technickou podporu kořenové domény,
 - je schopen efektivně delegovat podřízené domény a vytváření sídel.
- Poznání, že jediné schéma nemusí naplňovat konfigurační požadavky všech samostatně fungujících společností. K zajištění spolupráce mezi společnostmi tedy může být zapotřebí nástroj synchronizace adresářů.
- Odhalení závislostí protokolu Internet Protocol (IP) společnosti, jako jsou:
 - Firewally
 - Výkon sítě

Tým zavádění serverů

Tým zavádění serverů zodpovídá za plánování a návrh procesu zavádění serverů, který vychází z fází definovaných týmem celkového zavádění. Tým zavádění serverů je dále rozdělen do týmů zaměřených na technické plánování, službu Active Directory, logistiku a migraci. Strategické cíle určené týmem serverů jsou:

- Definovat služby Active Directory systému Windows 2000, které mohou využívat všechny samostatně fungující společnosti.
- Vyvinout plán migrace ze současného prostředí systému Windows NT Server 4.0 na prostředí systému Windows 2000.
- Vyvinout krátkodobé přípravné kroky.
- Implementovat pilotní program páteřního spojení společnosti.
- Implementovat zásady a modely systému Windows 2000 pro všechny společnosti.

Obrázek 2.3 ilustruje rámec řízení projektu, který tým serverů používá k zavedení systému Windows 2000.



Obrázek 2.3 Proces zavádění serverů v mezinárodní výrobní společnosti

Serverová fáze 1: Určení implementovaných funkcí

Hlavním cílem týmu zavádění serverů je vytvořit standardy zavádění společného adresáře a modelu domén, které budou moci používat všechny samostatně fungující společnosti. Také potřebují sestavit globální infrastrukturu systému Windows 2000 podporující všechny samostatně fungující společnosti. Tým se nejprve zaměří na návrh infrastruktury páteřního spojení využívajícího hlavní body páteře IP společnosti po celém světě. Toto páteřní spojení je logické páteřní spojení kořenového oboru názvů a řadičů domén a nikoli fyzické síťové páteřní spojení. Pomocí infrastruktury systému Windows 2000 musí tým vyvinout páteřní spojení, k němuž se mohou připojit všechny samostatně fungující společnosti. Každá společnost potřebuje mít rozhraní ke kořenu doménové struktury a sdílet společný globální katalog.

Následně tým začne na základě obchodních či výrobních potřeb identifikovat jednotlivé technologie, které bude podnik potřebovat. Protože angličtina je například společným jazykem všech správců systémů po celém světě, vícejazykové (MultiLanguage) možnosti nejsou na úrovni serverů zapotřebí. Mezi konkrétní problémy, na které se zaměří, patří:

- Návrh domén a sídel
- Návrh organizačních útvarů (jednotek)
- Určení překladu názvů systémem DNS nebo WINS
- Porozumění replikaci a kontejnerům služby Active Directory
- Synchronizace adresářové služby Exchange se službou Active Directory
- Návrh služby Active Directory systému Windows 2000
- Vývoj standardů společné konfigurace serverových operačních systémů
- Návrh kritérií logického i fyzického umístění serverů řadičů domén a globálního katalogu

Tabulka 2.3 uvádí seznam činností, které společnost vyvinula, aby bylo možné určit okamžik dokončení cílů první fáze týmu serverů.

Tabulka 2.3 Seznam dokončení úkolů první fáze

Dokončeno	Položka
	<p>Vytvoření pilotních zavedení čtyř až šesti serverů minimálně na třech místech.</p> <p>Získání souhlasu s použitím názvu <název_domény>.net/<doména>.int kořenové domény.</p> <p>Instalace systému Windows 2000 Server v zadaném počtu bodů IT společnosti.</p> <p>Definování struktury <společnost.XXX> DNS včetně:</p> <ul style="list-style-type: none"> Konfigurování integrovaného serveru DNS dynamické aktualizace pro doménu <společnost.XXX> v evropském místě X. Konfigurování integrovaného serveru DNS dynamické aktualizace v americkém místě A. Inovace základní serverů IT novými informacemi o doménách. Ověření sériového řazení záznamů a přenosu zóny se základním provozním sídlem. Spuštění přímého hostitele <společnost.XXX> dne dd/mm/rrrr. Definování základních provozních konfigurací včetně: <ul style="list-style-type: none"> Vytvoření globálních katalogů v evropských místech X a Z. Identifikování podsítí. Vytvoření počtu X sídel. Vytvoření spojení sítí mezi evropskými místy X a Z. Vylepšení možnosti správy instalováním terminálových služeb systému Windows 2000 v režimu vzdálené správy. Umožnění elektronické distribuce softwaru nakonfigurováním páteřních sídel na replikaci verzí systému Windows 2000 do evropského místa Z. Vytvoření adresářové služby v pilotním scénáři pomocí: <ul style="list-style-type: none"> Naplnění pilotní adresářové služby daty adresáře společnosti (200 000 a více názvů a jmen). Ověření replikace a zatížení systému. Odstranění obsahu po dokončení testu.

Serverová fáze 2: Příprava konečného návrhu architektury serverů a vykonání pilotních programů

Tým se nyní může zaměřit na druhou fázi a začít vytvářet různé domény samostatně fungujících společností pro pilotní program. Některé domény jsou nové, zatímco jiné budou migrovány ze systému Windows NT Server 4.0. Konkrétní problémy, na které se tým zaměří, zahrnují:

- Navrhnout strukturu Active Directory a ověřit ji v testovací laboratoři.
- Vyvinout plány migrace ze systému Windows NT Server 4.0 na systém Windows 2000 Server.

- Vyvinout standardní instalační proces zavádění serverů.
- Vytvořit laboratoř podnikové integrace.
- Definovat specifikace dalších funkcí systému Windows 2000.
- Aktivovat plán komunikace s koncovými uživateli včetně oddělení IT v ostatních společnostech, správců IT a uživatelů kancelářských počítačů.

Tabulka 2.4 uvádí seznam činností, které společnost vyvinula, aby bylo možné určit okamžik dokončení cílů druhé fáze týmu serverů.

Tabulka 2.4 Seznam dokončení úkolů druhé fáze

Dokončeno	Položka
	<p>Určení deseti míst pilotního zavedení, čtyř v USA, pěti v Evropě a jedné evropské klientské laboratoře.</p> <p>Zavedení 18 až 24 serverů v pilotním prostředí.</p> <p>Zavedení 30 až 40 pracovních stanic v pilotním prostředí.</p> <p>Vytvoření páteřního spojení IP společnosti přes virtuální privátní síť (Virtual Private Network – VPN) nakonfigurováním firewallů pro přístup VPN mezi společnostmi a vhodnými místy páteřního spojení společnosti.</p> <p>Definování delegování správy včetně:</p> <ul style="list-style-type: none"> ■ Předběžné vytvoření domén pro samostatně fungující společnosti. ■ Delegování společností do zón DNS. <p>Vytvoření domény pro samostatně fungující společnosti včetně:</p> <ul style="list-style-type: none"> ■ Instalování domén společností v pěti evropských a čtyřech amerických místech. ■ Identifikování podsítí účastnících se společností. ■ Vytvoření sídel a delegování správy sídel. ■ Vytvoření spojení mezi sídly samostatně fungujících organizací a sídly páteřního spojení. ■ Zavedení globálního katalogu na každém zúčastněném sídle (nikoli společnosti). <p>Definování delegování pro každou společnost včetně:</p> <ul style="list-style-type: none"> ■ Vytvoření struktury organizačních útvarů v doméně samostatně fungující společnosti. ■ Delegování správy organizačních útvarů. <p>Určení uživatelských účtů a vytvoření účtů členů týmů zavádění serverů a klientů.</p> <p>Připojení klientských počítačů patřících týmu zavádění systému Windows 2000 do domén samostatných společností.</p> <p>Vytvoření vztahu důvěryhodnosti ve stylu systému Windows NT Server 4.0 jako produkční domény prostředků pro danou společnost.</p> <p>Integrace služby WINS v páteřním spojení společností podle potřeby.</p> <p>Integrace systému Microsoft Exchange Server nakonfigurováním nástroje Active Directory Connector v každé samostatné společnosti a zajištění jednosměrné synchronizace zaručující aktualizaci informací služby Active Directory.</p>

Vytvoření certifikačního úřadu.

Vytvoření replikace adresářové služby.

Zavedení systému Windows 2000 Professional koordinovaně s týmem zavádění klientů prostřednictvím:

Vývoje bezobslužné instalace prototypů klientů v různých doménách.

Použití zásad skupiny pro všechny klienty ve všech doménách.

Instalace balíčků MultiLanguage na klientský prototyp se třemi zkušebními jazyky.

Umožnění cestování mezinárodním klientům.

Instalace a používání standardního softwaru jednotlivých společností na všech sídlech používajících objekty zásad skupiny.

Zajištění přístupu pracovních stanic k prostředkům systému Windows 2000 přes existující služby vzdáleného přístupu systému Windows NT 4.0.

Definování uživatelů pomocí:

Použití zásad skupiny pro uživatele ve všech doménách.

Zajištění správné funkce uživatelů přesunujících se mezi různými doménami (výchozí klientský jazyk musí být identický).

Zajištění správné funkce uživatelů přesunujících se mezi různými státy (různé výchozí klientské jazyky).

Zajištění fungujícího přístupu k prostředkům v jiných doménách po celém světě.

Serverová fáze 3: Představení migračních plánů samostatným společností

Třetí fáze se zaměřuje na migraci služeb ze systému Windows NT Server 4.0 na systém Windows 2000. Služby budou migrovány podle vyhodnocení rizik navržených k omezení vlivu na existující obchodní či výrobní systémy. Jakmile tým získá určité zkušenosti při migrování klíčových komponent, úroveň složitosti se zvýší, čímž se zase zvýší rizika. Tým zavedení představí tyto plány samostatně fungujícím společnostem, které je budou používat jako prototypy poté, co tým dokončí zevrubné testování. Činnosti v této fázi zahrnují:

- Představení strategie migrace.
- Úvod do konceptů systému Windows 2000 a návrhů předložených samostatným společností.
- Zdůvodnění předkládaného návrhu výkonnému ředitelství.
- Zdůvodnění projektu a předkládaného návrhu koncovým uživatelům.
- Příprava plánu zotavení po havárii, který zajistí nepřetržitou činnost společnosti, zejména:
 - Strategie zálohování
 - Strategie návratu k systému Windows NT 4.0 po migraci na systém Windows 2000

Tabulka 2.5 uvádí seznam činností, které společnost vyvinula, aby bylo možné určit okamžik dokončení cílů třetí fáze týmu serverů.

Tabulka 2.5 Seznam dokončení úkolů třetí fáze

Dokončeno	Položka
	Určení míst migrací sídel v různých geografických oblastech včetně Severní Ameriky, Evropy a Asie.
	Určení počtu serverů migrovaných v jednotlivých doménách a sídlech.
	Určení počtu klientských počítačů migrovaných v jednotlivých doménách a sídlech.
	Vykonání migrace systému WINS zavedením serveru WINS systému Windows 2000 do existujícího prostředí.
	Vykonání migrace protokolu DHCP zavedením serveru DHCP systému Windows 2000 do existujícího prostředí.
	Vykonání migrace tiskových serverů vybráním určitého počtu serverů, které nejsou řadiči domén systému Windows NT Server 4.0, a jejich inovací na systém Windows 2000.
	Vykonání migrace internetových serverů implementováním webového sídla zavádění systému Windows 2000 pomocí IIS 5.0 a vytvořením odkazu na toto sídlo z existujícího centrálního sídla. Replikování obsahu ze zkušebního sídla na nějaké nové sídlo. Přidání záznamů DNS tohoto serveru.
	Omezení domén prostředků výběrem nějaké domény prostředků systému Windows NT 4.0 a její migrací na systém Windows 2000 Server.
	Vytvoření nových domén účtů migrací primárního řadiče domény účtů na systém Windows 2000 Server.

Tým zavádění klientů

Největší výzvou týmu zavádění klientů je spolupráce s ostatními nezávisle fungujícími společnostmi při vytváření jediné klientské konfigurace, se kterou budou všichni souhlasit. Existující klientské operační systémy v organizaci zahrnují systémy Windows 95, Windows 98 a Windows NT 4.0 Workstation. Dalšími klientskými problémy zvažovanými tímto týmem jsou:

- Omezení počtu celopodnikově používaných aplikací. V současné době tu existuje více než 1000 aplikací, jejichž podpora je pro tým IT velmi náročná.
- Změna zaměření IT z cestujících počítačů na cestující uživatele.
- Prostudování, zda je vhodné změnit existující metodu zavádění softwaru používanou v systému Windows NT Server 4.0.
- Zajištění větší hardwarové podpory přenosných počítačů.

Tým potřebuje vyvinout určitý návrh, který pomůže samostatným společnostem rozhodnout, zda mají nejprve inovovat své klienty nebo raději infrastrukturu serverů. Tým si sice uvědomuje, že možné jsou obě cesty, jeho členové však rozhodnou, že pro jejich organizace platí následující podmínky upřednostňující prvotní inovování infrastruktury serverů:

- Centralizovanější řízení klientských počítačů.
- Omezení možností uživatelů změnit konfigurace klientských počítačů.

- Použití nástrojů systému Windows 2000 k instalaci.
- Získání globálního katalogu přístupného všem uživatelům.

Tým zjistí, že většina samostatných společností v organizaci chce nejprve inovovat své servery a jakmile bude možné používat službu Active Directory a globální katalog, pak zavést zásady skupiny a další nástroje správy změn a konfigurací umožňující detailnější správu klientských počítačů. Také si uvědomí, že rozhodnutí o prvotní inovaci serverů je zejména důležité, pokud tým plánuje doporučit zavádění softwaru pomocí zásad skupiny systému Windows 2000. Tým bude muset prostudovat, jak použití zásad skupiny ovlivní službu Active Directory.

Organizace stanovila týmu architektury klientů následující cíle:

- Vyvinout standardní klientskou konfiguraci jako modulární produkt pro všechny samostatně fungující společnosti.
- Vytvořit referenční instalaci včetně hardwaru, softwaru a operací.
- Navrhnout rámec globálního modelu, který umožní uživatelům přihlásit se z libovolného místa na světě.
- Vyvinout model školení a technické podpory.

Práce týmu klientů je rozdělena do dvou fází:

- Fáze 1: Problémy standardní klientské konfigurace
- Fáze 2: Logistika softwaru

Fáze 1: Problémy standardní klientské konfigurace

V zájmu naplnění cílů možnosti práce po celém světě se tým klientů rozhodne použít standardizovanou konfiguraci zahrnující:

- Klienty systému Windows 2000 Professional
- Sadu Microsoft Office 97 nebo Office 2000
- Antivirový software
- Webový prohlížeč
- Klienta elektronické pošty
- Podporu více jazyků
- Podporu terminálových služeb systému Windows (zajišťuje, že návrh klientů je vhodný pro terminálové služby)
- Umožnění cestování klientů, aby se mohli uživatelé připojit (například telefonicky) k pátečnímu spojení IP společnosti z libovolného místa na světě a přistupovat k:
 - osobním nastavením pracovní plochy a aplikacím,
 - osobním dokumentům a elektronické poště,
 - celopodnikovému standardnímu softwaru.

Fáze 2: Logistika softwaru

Během druhé fáze se tým zaměří na vývoj strategie přenesení konfigurací nového operačního systému a klientů jak na stacionární tak i na mobilní klienty nějakým stabilním a výkonným způsobem. Tým identifikuje následující problémy:

- Vytvoření instalačních balíčků pro:
 - Podnikové aplikace
 - Společné aplikace všech samostatných společností
 - Vlastní aplikace jednotlivých samostatných společností (podle potřeby)
- Vytvoření pokynů pro instalační balíčky zahrnující:
 - Standardizovaný vývoj balíčků používaný celosvětově ve všech společnostech
 - Zvláštní instalační balíčky jednotlivých aplikací používané celosvětově pro ne-standardní software
 - Opakované vytvoření balíčků podle potřeb jednotlivých společností
- Přiřazování instalačních balíčků:
 - Všem uživatelům
 - Skupinám uživatelů podle funkcí nebo organizací
 - Klientům se specifickými potřebami
- Instalování aplikací podle požadavků uživatelů

Tým zavádění klientů zjistil, že management chce nadále provozovat praxi instalování nových klientských operačních systémů a konfiguračních obrazů ve spojení se současným nákupem nového hardwaru. Průměrná doba zavádění operačního systému v této organizaci je tři roky. Interní studie nákladů TCO ukazují, že vydání peněz na lepší hardware a následná inovace obrazu (bitové kopie) nové klientské konfigurace ještě před instalováním nového hardwaru na systémy uživatelů snižuje TCO.

Výrazné přínosy v oblasti klientů pro správce systémů a profesionály IT vycházejí z nových funkcí a vylepšené funkčnosti, uživatelé a řídicí pracovníci však potřebují jasný důkaz zvýšení produktivity. Proto je zapotřebí přesvědčit jak odpovědné osoby činící rozhodnutí tak i koncové uživatele – pak se teprve může projekt dostat do fáze zavádění v jednotlivých samostatně fungujících společnostech.

Technologické závislosti

Protože systém Windows 2000 Server je víceúčelový síťový operační systém vybavený samostatně použitelnými, přesto však integrovanými funkcemi, které lze zavádět postupně, existuje tu mnoho technologických závislostí, které musíte zvážit během plánování zavádění. Následující příklady ilustrují některé z těchto technologických závislostí.

Služba Active Directory a prostor názvů domén

Vaše struktura služby Active Directory a systému Domain Name System (DNS) musí být spolu s plány infrastruktury služby Windows Internet Name Service (WINS), protokolu Dynamic Host Configuration Protocol (DHCP), síťovými protokoly, soubory, tiskem, multimediálními datovými proudy a dalšími aplikacemi náročnými na šířku pásma vytvořena tak, aby naplnila požadavky obchodních či výrobních činností a vyhovovala možnostem IT. Vyžaduje-li vaše obchodní či výrobní činnost řadu podpůrných prvků

a podporu cestujících nebo vzdálených uživatelů, pak musíte zvážit použití technologií organizačních útvarů, zásad skupiny, zabezpečení a funkcí IntelliMirror. Chcete-li nabídnout podporu zabezpečeného intranetu nebo extranetu, pak budou pro váš návrh důležité součásti IP Security (IPSec) a PKI.

Budete-li zavádět Windows 2000 Professional jako základní operační systém kancelářských i přenosných počítačů, pak můžete zvážit použití různých instalačních možností, podpory více jazyků, zabezpečení, služby Active Directory a dalších technologií správy změn a konfigurací. Pracujete-li v heterogenním prostředí zahrnujícím také jiné síťové operační systémy než Windows NT a Windows 2000, budete se muset zamyslet nad možnostmi jejich spolupráce a současné existence.

Služba Active Directory a Exchange Server

Možná plánujete zavedení služby Active Directory v geograficky roztroušeném prostředí, kde je obtížné zajistit centralizované řízení IT, jelikož se používají pomalá propojení WAN a není zajištěno stabilní a zabezpečené připojení. Přesto však můžete požadovat stabilní, zabezpečený a společný systém elektronické pošty a spolupráce mezi různými samostatně fungujícími společnostmi zahrnující také geograficky vzdálená sídla. Musíte se zamyslet nad vztahem mezi službou Active Directory a adresářovou službou Exchange Serveru 5.5 ve spojení se zásadami skupiny, protokolem IPSec a virtuálními privátními sítěmi (VPN). Naplánujte synchronizaci dat s adresářem Exchange pomocí nástroje Active Directory Connector (ADC).

Musíte se také zamyslet nad návrhem systému DNS, zejména máte-li více organizací a pomocných funkčních jednotek, z nichž každá má svůj vlastní internetový název domény, struktury domén a stromů, požadavky na zabezpečení a různé síťové operační systémy nebo standardy IT. Návrh DNS je důležitý zejména v případě, kdy za obor názvů DNS zodpovídají jiné skupiny než tým systému Windows 2000, jako je tomu v mnoha organizacích IT využívajících systém UNIX.

Integrovaní systému Exchange Server

Vyžadujete-li společný standard elektronické pošty a společný adresář, jestliže však vaše organizace nepoužívá systém Exchange Server 5.5, pak budete možná muset implementovat Exchange Server 5.5 ještě před zavedením systému Windows 2000 – pak budete moci vykonávat synchronizaci se službou Active Directory pomocí ADC. Alternativně můžete tento úkol odložit až na dobu po dokončení zavedení systému Windows 2000 a následně zavést další verzi Exchange.

Vzdálená instalace operačního systému

Jiná situace může nastat u uživatelských lokacích s omezenou podporou ale vynikající konektivitou, kde se instalace místních klientů v minulosti vykonávala ručně. Pomocí technologií vzdálené instalace OS a IntelliMirror máte nyní možnost vykonávat instalaci vzdáleně a tímto způsobem také řešit problémy, aniž byste museli na takovém sídle vytvářet skupinu technické podpory.

Další informace o technologických závislostech najdete v jednotlivých kapitolách technického plánování v této knize. Pamatujte si, že každá zaváděná funkce musí mít svůj vlastní návrh, aby ji bylo možné formálně otestovat v laboratorních i pilotních prostředích.

Tipy plánování zavádění systému Windows 2000

Vaším konečným cílem při vytváření dokumentů plánování a formulování plánu zavedení je úspěšně zavést systém Windows 2000 pomocí technik řízení projektů fungujících ve vaší organizaci. Dále uvedené oddíly uvádějí seznam položek, které musíte při plánování zavedení zvážit.

Obecné doporučené postupy

Následující seznam obsahuje obecné doporučené postupy identifikované společnostmi, které již mají se zaváděním systému Windows 2000 první zkušenosti.

- Použijte organizační diagram a seznamte se s tím, jak struktura řízení ve vaší organizaci odpovídá potřebám vaší organizace i síťovým spojením LAN. Na základě těchto úvah vytvořte infrastrukturu služby Active Directory.
- Určete, jaké úrovně mezinárodní funkčnosti chcete dosáhnout a k jakým kompromisům jste ochotni, abyste tento požadavek naplnili.
- Naplánujte dodatečnou úroveň složitosti v testování produktu.
- Naplánujte instalaci aplikací pomocí služby Windows Installer.
- Určete, jak rozdělíte zodpovědnost správců systému za vaše aplikace a určete, komu budou udělena oprávnění správce.
- Rozhodněte, jaké zásady budou vynuceny na systému typického uživatele.
- Využijte nové součásti nabízené systémem Windows 2000. Moudře je integrujte, aby se minimalizoval jejich dopad na výkon vaší aplikace.
- Naplánujte si dostatečný čas pro instalaci serveru se systémem Windows 2000, což je několikahodinový proces.
- Na seznam problémů se systémem Windows 2000 přidejte problémy s mezinárodní podporou a otestujte sledovací systémy.
- Vyvíňte „pracovní skupiny“, které budou studovat rozhodnutí architektury podle jednotlivých úkolů.
- Napište dobrý plán testování a vytvořte testovací laboratoř, která přesně zrcadlí vaše produkční prostředí z hlediska používaného typu hardwaru a softwaru.
- Nejprve inovujte konzervativně. Rychlost tohoto procesu a postup zavádění můžete zvýšit, jakmile budete dosahovat úspěchů.

Fáze zavádění

Určete celkově nejlepší pořadí zavádění systému Windows 2000 ve vašich organizacích. Jedna ze společností použila tento postup:

- Definujte současné prostředí určením, jaké serverové a klientské operační systémy se v současné době ve vaší společnosti používají. Prostudujte si jejich funkce a účel, kterému slouží.
- Zjistěte, zda se bude počet uživatelů pravděpodobně měnit díky sloučením, akvizicím, reorganizacím nebo růstu.
- Prostudujte potřebu škálování serverového prostředí (určete potřeby clusteringu a vyrovnávání zatížení i zavedení terminálových služeb).
- Navrhněte strukturu služby Active Directory včetně oboru názvů DNS.
- Inovujte infrastrukturu sítě a členské servery.
- Implementujte službu Active Directory a správu úložišť.

- Inovujte nebo migrujte klienty na systém Windows 2000 Professional.
- Implementujte řízení kancelářských počítačů pomocí nástrojů správy změn a konfigurací.

Problémy instalování aplikací

Následující typy plánování použijte při plánování instalací aplikací ve vaší organizaci.

- Včas investujte do procesu vytváření instalací. Čas na vytvoření procesu instalace si vyhraďte již na počátku cyklu zavádění produktu.
- V procesu vytváření instalací využijte vývojáře. Zajistíte tím včasné odhalení závislostí.
- Buďte si vědomi toho, že vyhodnocování nástroje Windows Installer mohou ovlivnit výkon vaší aplikace.
- Kdykoli je to možné, vyhněte se restartům během instalace.
- Nepřidávejte položky do souborů Win.ini, System.ini, Autoexec.bat ani Config.sys.
- Od všech, kdo budou vaše aplikace testovat, vyžadujte jejich instalaci pomocí služby Windows Installer.
- Pamatujte, že správce může inzerovat váš produkt v nabídce **Start** nebo na pracovní ploše uživatelů, aniž by zatím došlo k jeho plné instalaci. Aplikace se nainstaluje, když uživatel poklepe na daného zástupce nebo otevře dokument takového typu, který má daná aplikace na starosti.
- Seznamte se s problémy „ochrany systémových souborů“ a naplánujte jejich řešení.

Mezinárodní problémy

Následující typy vám pomohou naplánovat mezinárodní instalace.

- Vyhýbejte se jakémukoli předpokládání jazykových verzí operačního systému, na němž vaše aplikace běží.
- Vyhýbejte se předpokládání místních nastavení, kódových stránek a uživatelského rozhraní daného uživatele nebo počítače.
- Používejte Windows Installer. Je k dispozici v sadách ANSI i Unicode.
- Určete potřebná písma. Často k podpoře mezinárodních funkcí stačí jen správná písma.
- Používejte nejnovější ovladače tiskáren pro systém Windows 2000. Zajistí nejlepší podporu mezinárodních funkcí.
- Při řešení problémů s mezinárodním nastavením prověřte jak danou aplikaci tak i operační systém.

Problémy s výkonností

Udržení vysokého výkonu je důležitým předpokladem naplnění cílů většiny zavádění. Následující typy vám pomohou naplánovat zlepšení výkonu.

- Zpozděte všechny inicializace při spuštění, které můžete.
- Zjednodušte spouštěcí obrazovky, aby se přes síť odesílalo méně grafických bitů.
- Naplánujte řešení záležitostí souvisejících s výpadky sítě a obecnými problémy s výkonem.
- Používejte vrstvu mezipaměti nabízenou Windows 2000 v systému souborů pro případ výpadky sdíleného místa.

Cestující uživatelé a terminálové služby

Následující tipy vám pomohou naplánovat podporu cestujících uživatelů a instalace terminálových služeb.

- Naplánujete-li scénář cestujících uživatelů pečlivě, dosáhnete tím také podstatné části implementace terminálových služeb.
- Podporujte oddělení cestovních uživatelských profilů a států.
- Oddělte nastavení jednotlivých uživatelů od nastavení jednotlivých počítačů.
- Nevyžadujte přístup se zápisem k nastavením jednotlivých počítačů.
- Pamatujte, že normální uživatelé systému Windows 2000 mají možnost upravovat data jen ve svých uživatelských profilech. Vaše aplikace nebude moci měnit části podstromu HKEY_LOCAL_MACHINE registru.
- Spusťte svou aplikaci, když jste přihlášení jako uživatel (nikoli jako správce), a otestujte ji na počítačích, kde nemají uživatelé práva správce. Včas tak odhalíte možné problémy.

Správa

Při vytváření svého plánu použijte následující tipy správy, které vám usnadní správu instalace systému Windows 2000.

- Zajistěte, aby byly funkce správy vaší aplikace co nejjednodušší, aby však poskytovaly všechny potřebné funkce. To napomůže zavádění aplikace v malých až středních organizacích, kde nejsou vyvinuty vlastní nástroje.
- Ve své aplikaci podporujte využití skriptů. Jedna z možných strategií: Napišete-li poskytovatele pro Windows Management Instrumentation (WMI), umožní vám to nenákladně zajistit jednoduchou podporu skriptů ve vaší aplikaci.
- Podporujte požadavky OnNow/ACPI. Zpracovávejte upozornění a požadavky režimu spánku a probuzení.
- Pamatujte, že výchozí nastavení zabezpečení jsou pro normální uživatele výrazně bezpečnější, než byly v systému Windows NT 4.0. Funkce, které normálním uživatelům pracovaly v systému Windows NT 4.0, mohou v systému Windows 2000 vyžadovat zařazení do skupiny Power Users.

Seznam úkolů plánování

Tabulka 2.6 shrnuje úkoly, které je zapotřebí vykonat při vytváření cesty postupného zavádění systému Windows 2000.

Tabulka 2.6 Seznam úkolů postupného zavádění

Úkol	Umístění v kapitole
Definujte proces řízení projektu, který bude určovat klíčové milníky a cíle vaší organizace.	Příprava procesu plánování projektu
Při určování specifických zaváděných funkcí prostudujte jejich technologické závislosti na jiných funkcích a technologiích systému Windows 2000.	Návrh a vývoj funkcí
Zjistěte všechna omezení řízení projektu, která mohou mít vliv na zavádění. Například omezení lidských nebo finančních prostředků nebo logistiku organizace, jako je období dovolených nebo problémy konce fiskálního roku.	Určení cílů
Vyvíňte proces vyhodnocení rizik a připravte zevrubnou analýzu rizik.	Určení cílů
Definujte pořadí postupného zavádění.	Scénáře zavádění
Vytvořte plán projektu pro vaši organizaci se zaměřením na funkce systému Windows 2000, týmy zavádění, časové plány a související závislosti.	Scénáře zavádění

Další informace o řízení projektu najdete v odkazu Microsoft Solutions Framework stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

KAPITOLA 3

Plánování zavedení

Jakmile určíte strukturu řízení projektu použitou při plánování zavedení, musíte se začít zabývat podrobnostmi svého plánu. Tato kapitola poskytuje informace o vytváření specifických oddílů plánu projektu. Například manažeri projektu musí určit své požadavky na personál, týmy zavádění, typy vytvářených dokumentů zavádění, analýzu rozdílů a funkční specifikaci.

Společnost Microsoft sice zjistila, že metody popsané v této kapitole přispívají k úspěšnému zavedení, jedná se však pouze o doporučení, která je zapotřebí přizpůsobit potřebám a struktuře vaší organizace.

V této kapitole

Vytvoření podrobností plánu projektu 58

Testování a pilotní program zavádění systému Windows 2000 65

Vytvoření dokumentů plánování projektu 66

Zavádění systému Windows 2000 74

Seznam úkolů plánování zavádění 75

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Rozsah a cíle projektu
- Požadavky na personál a týmy projektu
- Analýza rozdílů
- Plány správy
- Strategie komunikace
- Plán vzdělávání a školení
- Matice vyhodnocení rizik

Související informace v sadě Resource Kit

- Další informace o vývoji plánu projektu najdete v kapitole „Vytvoření cesty postupného zavádění“ v této knize.
- Další informace o spuštění úspěšného pilotního projektu systému Microsoft Windows 2000 najdete v kapitole „Vykonání pilotního programu systému Windows 2000“ v této knize.
- Další informace o návrhu testovací laboratoře a vyhodnocení funkcí systému Windows 2000 najdete v kapitole „Vytvoření testovací laboratoře systému Windows 2000“ v této knize.

Vytvoření podrobností plánu projektu

Chcete-li pomocí systému Windows 2000 dosáhnout největších přínosů, musíte jeho zavedení pečlivě naplánovat. Celkový plán projektu bude zahrnovat různé aspekty infrastruktury vaší obchodní či výrobní činnosti i sítě. Na začátku se zamyslete nad kroky popsány v následujících oddílech.

Rozsah a cíle projektu

Prvním krokem plánování zavedení je definování cílů projektu. Právě v tomto kroku identifikujete konkrétní obchodní či výrobní cíle, kterých chcete dosáhnout, a způsob, jak vám systém Windows 2000 k jejich dosažení může pomoci. Tato strategie vám také pomůže vybrat nejužitečnější funkce systému Windows 2000.

V cílech projektu naznačte konkrétní obchodní či výrobní problémy, kterými se musíte zabývat. Zahrňte sem specifické krátkodobé cíle, jako například „zavést systém Windows 2000 na 2500 počítačů ke konci tohoto čtvrtletí“, i obecnější dlouhodobé cíle, jako je „omezit stálé náklady na distribuci softwaru“.

Své cíle určete, ještě než budete pokračovat v plánování zavádění, protože ovlivňují co děláte a jak to děláte. Jasně cíle vám pomohou nevybočit z kurzu.

Při dokumentování rozsahu projektu naznačte oblasti, funkce a prostředí, kterých se bude vaše implementace systému Windows 2000 týkat. Může vás například zajímat aktualizace staršího souborového serveru, nikoli však implementace služby Active Directory v rozsahu celé infrastruktury.

Tabulka 3.1 shrnuje některé obvyklé obchodní či výrobní otázky a cíle projektu související se zaváděním systému Windows 2000. Tato tabulka však slouží jen jako ukázka – své vlastní cíle musíte odvodit z konkrétních obchodních či výrobních zájmů. Můžete přijít na to, že jeden obchodní či výrobní zájem lze řešit mnoha cíli projektu, nebo že jediný cíl projektu může naplnit řadu obchodních či výrobních zájmů.

Tabulka 3.1 Ukázka obchodní či výrobní zájmů a cílů projektu souvisejících se systémem Windows 2000

Obchodní či výrobní zájem	Cíl projektu
Omezit celkové náklady na vlastnictví rozšířením životnosti starších systémů.	Použití terminálových služeb k zajištění přenosu prostředí kancelářských počítačů se systémem Windows 2000 na systémy, které by jinak vyžadovaly inovaci.
Uspadnit uživatelům vyhledávání a přístup k prostředkům na síti.	Použití služby Microsoft Active Directory k ukládání informací o všech objektech na síti.
Podporovat cestující uživatele zajištěním jejich přístupu k dokumentům a systémovým informacím z více počítačů.	Použití cestovních uživatelských profilů ke zkopírování nastavení pracovní plochy a dokumentů na nějaké místo na síti, aby byly uživateli daná nastavení a dokumenty k dispozici, kdykoli se přihlásí.

Požadavky na personál

Zorganizujte týmy zavádění a pak členům týmů přiřadte specifické role. Podle velikosti své organizace a složitosti zavádění můžete také vytvořit podtýmy.

Vyhodnoťte kompetence personálu informačních technologií (IT). Také vyhodnoťte jeho schopnosti s ohledem na technologie systému Windows 2000. Pak se rozhodněte, jak budete řešit případné nedostatky. Následující seznam uvádí možnosti, které můžete zvážit s ohledem na řízení otázek školení:

- Zavádění odložte až na dobu, kdy bude váš personál plně proškolen v nových technologiích.
- Slabé body svého zavádění svěřte externím organizacím. Váš personál ať získá potřebné znalosti a zkušenosti od najmutých pracovníků nezávislých společností.
- Zavádění, podporu a údržbu systému v podniku svěřte externí organizaci.

Důležité Velmi důležité pro úspěch je obvykle určení výkonného pracovníka, který dokáže jasně stanovit celkové potřeby organizace související s tímto projektem. Tato osoba může týmu zavádění pomoci pochopit a dosáhnout potřebné cíle.

Organizování týmů zavádění

Požadavky na personál mohou být sice při plánování a zavádění systému Windows 2000 různé, zavádění operačního systému však obvykle vyžaduje několik členů týmu. V případě velké organizace zařadte do svého centralizovaného týmu alespoň dva nebo tři správce operačního systému. Nezapomeňte ani na personál technické podpory. Hned od začátku projektu zavádění se snažte využít osoby se značným rozsahem znalostí o společnosti a poskytněte jim přehled systému Windows 2000 a jeho přínosů – tito lidé vám pomohou dosáhnout širších potřeb vaší organizace. Je-li vaše organizace mezinárodní, doporučujeme vám zařadit do týmu také klíčové osoby z míst v jiných zemích. Najděte osoby, které jsou proškoleny v operačním systému Windows 2000 a které dokonale rozumí vašemu síťovému prostředí.

Členové základního týmu tvořeného experty v oblastech zabezpečení, práce v síti, spolupráce a testování aplikací mohou pracovat také jako vedoucí podtýmů v rámci svých zaměření. Členové týmu musejí disponovat schopnostmi řízení podrobných projektů, vlastními technickými zkušenostmi a schopnostmi inovace a rychle a nezávisle se seznamovat s novými technologiemi. Členové týmu také musejí mít silné analytické schopnosti, aby byli schopni spojit vize projektu s detaily potřebnými k jejich dosažení.

Jako základního průvodce používejte dokument rozsahu projektu a jeho cílů a určete, které podtýmy budou zodpovídat za plánování a testování zavádění vybraných funkcí. Můžete také základní tým zavádění rozdělit na serverový tým a klientský tým a dále delegovat zodpovědnost podtýmům jako v následujícím seznamu:

- Základní serverový tým
 - Služba Active Directory
 - Systém Domain Name System (DNS)
 - Návrh práce v síti
 - Protokol Dynamic Host Configuration Protocol (DHCP) a služba Windows Internet Name Service (WINS)
 - Zabezpečení

- Nástroje pro správu
- Systém Microsoft Exchange Server a elektronická pošta
- Základní klientský tým
 - Funkce klientů a počítačů, jako jsou Microsoft IntelliMirror, instalace operačního systému a aplikací a existující aplikace.
 - Problémy přenosných počítačů a notebooků, jako je řízení spotřeby, ukládání do doků, vzdálený přístup a cestovní profily.

Týmy naplánujte tak, aby odrážely vaši interní strukturu, obchodní či výrobní potřeby, zaváděné funkce a služby systému Windows 2000 a způsob jejich zavádění. Uspořádání vašich týmů zavádění bude odrážet výše uvedené role.

Jeden ze způsobů, jakým můžete uspořádat tým zavádění, je uveden v tabulce 3.2.

Tabulka 3.2 Příklad týmů zavádění

Tým	Zodpovědnost
Řízení	Vedoucí všech ostatních týmů se budou starat o celkovou koordinaci a komunikaci. Použijte strategické plánovače, kteří se v organizaci vyznají, například osoby, které vědí, jaké systémy se v současné době používají a proč jsou zapotřebí.
Plánování a koordinace	Stará se o technickou podporu a školení, obchodní či výrobní plánování, plánování před migrací, velmi důležité systémy a konzultace s nezávislými společnostmi.
Servery	Testuje a vyvíjí řešení v oblastech: clusteringu, systému Hierarchical Storage Management (HSM), zálohování, zotavení po havárii, terminálových služeb, integrace a požadavků na hardware.
Návrh infrastruktury	Řeší problematiku modelu domén, služby Active Directory, místních sítí (LAN), telekomunikací, systému Distributed File System (DFS), globálního přístupu k souborům, systému Domain Name System (DNS) a vzdáleného přístupu.
Zabezpečení	Vyvíjí standardy pro internetové, intranetové a extranetové služby i zabezpečení domén a implementaci zásad.
Spolupráce	Integrace architektury Systems Network Architecture (SNA), propojení protokolu Kerberos s mainframem a systémem UNIX, integrace UNIX/mainframe a integrace/společná existence systémů NetWare a OS/2.
Integrace aplikací	Integruje aplikace a sady práce se zprávami, databázemi a pracovními skupinami, internetové nástroje, obchodní aplikace a aplikace nezávislých společností.
Práce v síti	Zkoumá, testuje a vyvíjí síťová řešení podporující adresáře.
Klienti	Testuje a řeší problémy aplikací, inovace/migrace, hardwaru a přenosných počítačů.
Správa počítačů	Testuje a vyvíjí plán správy změn a konfigurací organizace zahrnující zásady skupiny, instalaci softwaru a správu uživatelských dat a nastavení.
Výbor požadavků komentářů	Skládá se z členů uživatelské komunity. Zajišťuje zpětnou vazbu ohledně rozhodnutí učiněných týmy zavádění.

Přirazení rolí týmům Windows 2000

Činnosti zavádění systému Windows 2000 lze rozdělit do mnoha kategorií. V projektech malých implementací může jediná osoba zastávat několik rolí a v projektech velkých implementací může být jednotlivým rolím přirazeno více osob.

Pamatujte, pokud umožníte používání adresářových služeb, systém Windows 2000 se bude výrazně odlišovat od prostředí nepoužívajících adresářové služby. Chcete-li používat adresářové služby, musí být organizace IT vzdělána v tomto směru a postupně migrována do nové struktury podpory a správy. Jedná se o změnu, která ovlivňuje celou organizaci a která vyžaduje ještě vyšší úroveň řízení vzdělávání než typická inovace.

Tabulka 3.3 popisuje proměnné role, odpovědnosti, požadavků a pracovního zatížení personálu systému Windows 2000, které musíte zvážit při určování potřeb personálu.

Tabulka 3.3 Role řízení Windows 2000

Role a odpovědnost	Požadavky
<p>Řízení IT a výkonná složka</p> <p>Určuje priority infrastruktury systému Windows 2000. Vytváří obchodní či výrobní projektový případ. Definuje vizi zavádění a zajišťuje financování. Funguje jako zástupce týmů i organizace. Odstraňuje překážky, zajišťuje rovnoměrnost zavádění funkcí a časového plánu a zodpovídá za plány komunikace.</p>	<p>Znalost obchodní či výrobní problematiky organizace a řešení, která bude systém Windows 2000 poskytovat. Znalost základních funkcí a schopností systémů Windows 2000 Server a Windows 2000 Professional.</p>
<p>Řízení projektu</p> <p>Činí kritická rozhodnutí potřebná k vytvoření infrastruktury systému Windows 2000. Vymýšlí řešení a s týmem zavádění definuje rozsah zavádění. Se členy ostatních týmů vytváří funkční specifikaci. Zajišťuje každodenní koordinaci nezbytnou k zavedení systémů Windows 2000 podle standardů organizace a cílů spolupráce. Činí celková kritická rozhodnutí.</p>	<p>Znalost podrobností fungování systémů Windows 2000 Server a Windows 2000 Professional. Schopnost koordinovat cíle výkonného řízení s cíli týmu projektu.</p>
<p>Zavádění/Návrh</p> <p>Vyhodnocuje technická řešení, která se použijí v návrhu a vývoji infrastruktury systému Windows 2000. Definuje strategii všech funkcí systému Windows 2000 uvedených během zavádění. Hraje základní roli v návrhu počáteční infrastruktury. Navrhuje a vytváří infrastrukturu nezbytnou pro implementaci.</p>	<p>Zkušenosti s vývojem složitých služeb operačního systému. Znalosti technických požadavků na existující a novou infrastrukturu sítě.</p>

Předmět/Techničtí experti

Zodpovídá za návrh a vývoj strategie příslušných oblastí. Zajišťuje vedení podtýmů.

Testování

Pomáhá při vývoji počátečního návrhu řešení. Zajišťuje, že týmu jsou známy všechny problémy a že jsou vyřešeny ještě před postupným zaváděním do produkčního prostředí. Navrhuje a vytváří testovací laboratoř a vykonává všechny procedury testování a vyhodnocování před postupným zaváděním do produkčního prostředí. Vykonává analýzu škálovatelnosti a testování výkonu.

Dokumentace

Pomáhá s vývojem projektové dokumentace včetně dokumentů plánování, hlášení a základních popisů. Může obsahovat spisovatele, redaktory a osoby z produkčního prostředí.

Vzdělávání uživatelů/školení

Funguje jako zástupce uživatelů. Vyhodnocuje požadavky uživatelů, určuje cíle školení a vyvíjí programy vzdělávání a školení, které uživatelům umožní maximalizovat využití infrastruktury systému Windows 2000.

Řízení logistiky

Skupinám operací a podpory včetně technické podpory a školení zajišťuje hladké postupné zavádění, instalace a migraci.

Vyšší úroveň technických znalostí v jednotlivých expertních oblastech a operačního systému Windows 2000. Schopnosti řízení projektu s ohledem na detaily.

Dobrá znalost systému Windows 2000 Server a souvisejícího síťového hardwaru nebo konektivity systému Windows 2000 Professional. Zkušenosti s návrhem, spouštěním a laděním testů. Zkušenosti s testováním aplikací.

Znalost odpovídajících technologií. Schopnosti komunikace, psaní a redaktorské práce i znalosti technologické dokumentace.

Dobrá znalost systému IT organizace, infrastruktury sítě a funkcí systému Windows 2000. Znalosti samostatně použitelných řešení a prezentačního softwaru. Schopnosti komunikace a školení.

Dobré znalosti funkcí a možností systémů Windows 2000 Server a Windows 2000 Professional.

Při zjišťování požadavků na správu můžete přijít na to, že současnou strukturu organizace je zapotřebí upravit. Využijte tuto příležitost a seznámte se se současným stavem řízení a zjistěte, zda by nebylo přínosné jej reorganizovat. Jestliže například systémy Microsoft Exchange a Microsoft Windows NT spravují dva samostatné týmy, bude vhodné vytvořit samostatný tým pro správu systému Windows 2000.

Současné počítačové prostředí

Ještě než navrhnete prostředí systému Windows 2000, musíte se dokonale seznámit se současným počítačovým prostředím. Zdokumentování existujícího počítačového prostředí vám pomůže porozumět struktuře organizace a její podpoře uživatelů. Také vám to pomůže při návrhu plánu zavádění systému Windows 2000. Ke znázornění složitých konceptů, jako jsou sítě, se nejlépe hodí diagramy. Kdykoli je to možné, takové diagramy vytvořte a zahrňte je do dokumentace vašeho plánu projektu.

Další informace o síťových diagramech najdete v kapitolách „Příprava infrastruktury sítě na systém Windows 2000“ a „Určení strategií konektivity sítě“ v této knize.

Při zjišťování aktuálního počítačového prostředí nezapomeňte zdokumentovat následující položky:

Organizace obchodní či výrobní činnosti a geografické požadavky

Popište umístění a organizaci obchodních či výrobních jednotek. Jsou velké skupiny zaměstnanců umístěny v široce rozptýlených geografických oblastech nebo jsou poblíž? Souvisejí spolu vaše obchodní či výrobní jednotky nebo mají výrazně odlišné požadavky a potřeby?

Klíčové obchodní či výrobní procesy

Jestliže upravujete klíčové obchodní či výrobní procesy, vytvořte také diagramy ilustrující tyto procesy a skutečnost, jaký na ně má nová infrastruktura IT vliv. V některých organizacích může být například klíčovým cílem zavádění systému Windows 2000 Server používání služby Active Directory k distribuci správy na místní správce. Distribucí správy umožňujete správcům lépe a rychleji reagovat na požadavky místních uživatelů. Je-li to také váš případ, vytvořte model ilustrující, jak celkový plán tohoto cíle dosáhne.

Architektura informací

Při zakreslování klíčových obchodní či výrobní procesů do diagramů také ilustrujte, jak budou informace potřebné k učinění důležitých rozhodnutí dostupné v pravý okamžik na správném místě. Jsou například osoby z oddělení prodeje a marketingu schopny potvrdit přesná data vyřízení objednávek zákazníků? V koncepčním návrhu se přesvědčte, že klíčové datové sklady jsou dobře uspořádány a snadno přístupné.

Požadavky na aplikace

Vykonejte úplnou inventuru aplikací, které se ve vaší organizaci používají. Zahrňte sem také všechny vlastní (samostatně vyvinuté) aplikace. Při dokumentování počítačového prostředí si také poznamenejte různé úkoly, ke kterým zaměstnanci počítače používají, a zaznamenejte, jak přechod na systém Windows 2000 ovlivní jejich práci. Jestliže zaměstnanci například používají starší obchodní aplikaci, která závisí na určitých konkrétních verzích Open Database Connectivity (ODBC), obchodní aplikaci je zapotřebí otestovat a ujistit se, že bude fungovat i v novém prostředí.

Architektura technologií

Při dokumentování architektury sítě nezapomeňte na topologii, velikost, typ a vzory provozu. Všechny významné plánované změny architektury technologií, jako je hardware, práce v síti a služby, musí být ilustrovány v diagramech vyšší úrovně.

Současné a budoucí standardy IT

Časem síťové a aplikační standardy v mnoha organizacích zastarají a dojde k jejich fragmentaci. To je obvyklé zejména v organizacích, které se sloučily s jinými společnostmi nebo je přímo zakoupily. Rozdílné systémy vytvořené v různých dobách, navržené různými lidmi a často geograficky oddělené představují potenciální riziko pro úspěšné zavedení. Audit existujících systémů přispěje k úspěchu týmu zavádění.

Model správy

Prozkoumáním existujícího modelu správy zjistíte úkoly správy, které personál IT vykonával ve všech oblastech vaší organizace. To vám pomůže určit, zda je zapotřebí změnit nějaký aspekt existujícího návrhu operací správy v zájmu podpory nově zaváděných funkcí systému Windows 2000.

Vytvoření standardů a pravidel

Mnoho organizací zjišťuje, že vytvoření standardů a pravidel systému Windows 2000 šetří čas a peníze. Je tomu tak proto, že standardní prostředí omezuje potenciál příliš mnoha konfiguračních kombinací, čímž se úkoly správy a architektury výrazně zjednodušují. Tyto standardy musejí vycházet z toho, jak zaměstnanci používají počítače. Například uživatel využívající počítač ke konstruktérské činnosti (CAD) má vyšší požadavky než zaměstnanec používající obvyklé kancelářské aplikace.

Nejlepších výsledků dosáhnete, když vytvoříte standardní konfigurace pro klienty a servery. Určete také minimální a doporučené parametry procesoru, paměti RAM a pevného disku. Nezapomeňte ani na příslušenství, jako jsou jednotky CD-ROM a zdroje nepřerušitelného napájení.

Vytvořte standardní softwarové konfigurace používané v organizaci. Jedná se o operační systémy a další aplikační software a pokyny pro distribuci, podporu a omezení použití příslušného softwaru.

Vytvořte standardy pro síťové operační systémy a protokoly používané v organizaci. Nezapomeňte na standardní konfigurace všech síťových součástí (jako jsou směrovače, rozbočovače a opakovací). Vytvořte pokyny pro podporu a údržbu těchto konfigurací.

Vytvořte také nové standardy a pokyny potřebné pro systém Windows 2000 včetně standardů správy a sledování schéma, návrhu sídel a vytváření názvů.

Vykonání analýzy rozdílů

Porovnejte své současné počítačové prostředí s budoucím prostředím podle cílů vašeho projektu. Rozdíly mezi existujícím prostředím a vašimi cíli vám pomohou určit, které funkce systému Windows 2000 budete zavádět. Základní kroky vykonání analýzy rozdílů jsou uvedeny dále:

- Určete rozdíl mezi způsobem, jakým zaměstnanci pracují v současné době, a způsobem, jakým budou pracovat po zavedení systému.
Počítače a operační systémy mají pro vaši obchodní či výrobní činnost nějakou hodnotu jen v případě, kdy jsou vašim zaměstnancům užitečné. Úspěšné zavedení omezuje rozdíly mezi způsobem, jakým zaměstnanci pracují dnes, a způsobem, kterým budou moci zaměstnanci pracovat s novým systémem po jeho zavedení. Až bude později tým vyhodnocovat úspěšnost, jeho základním měřítkem bude, nakolik se zlepšila práce těch uživatelů, kteří nový systém využívají.
- Prostudujte dokumenty, pokud nějaké existují, z předchozích inovací počítačů a sítí. Takové dokumenty vám mohou kromě užitečných informací o současném počítačovém prostředí nabídnout také šablonu, podle které budete moci postupovat procesem rozhodování.
- Seznamte se s dokumenty získanými od prodejců hardwaru nebo softwaru. Dokumenty související se současným hardwarem a softwarem ve vaší infrastruktuře vám pomohou rozhodnout, zda je zapotřebí inovovat nebo nahradit počítačové prostředky.
- Identifikujte úkoly a určete požadavky jednotlivých úkolů s ohledem na prostředky. Po určení úkolů a prostředků potřebných k jejich naplnění můžete rozhodnout, které skupiny v organizaci je zapotřebí do projektu zapojit a zda nebudete potřebovat dodatečné prostředky nepocházející z vaší organizace.

- Aktualizujte všechny dokumenty, jako jsou pracovní listy nebo časové plány s přiřazením plánování, prací a prostředků. Budete-li udržovat dokumenty aktuální, snáze se vám budou rozvrhovat časové plány prací a přiřazovat prostředky.
- Dokumenty analýzy rozdílů odešlete příslušným řídicím pracovníkům v organizaci, kteří je musejí schválit. Po schválení je možné spustit projekt. Nedosáhnete-li schválení, musíte dokumenty potřebným způsobem upravit a znovu projít procesem schvalování – pak teprve můžete začít s implementováním.

Konkrétní pravidla plánování a návrhu najdete v rozsahu celé této knihy.

Testování a pilotní program zavádění systému Windows 2000

Před zavedením systému Windows 2000 musíte otestovat jeho návrh v laboratoři. V počátečních fázích plánování musíte vybrat testovací a pilotní sídla a vyhodnotit hardwarové požadavky. Jakmile je laboratoř funkční, můžete ji využít k lepšímu seznámení s produktem, potvrzení konceptů a ověření funkčnosti řešení. Očekávejte vývoj prostředí laboratoře během postupu projektu.

Obecně platí, že do dokumentů plánu testování musíte zahrnout co nejvíce podrobností, aby měly vaše týmy testování a zavádění všechny informace potřebné pro dosažení úspěchu. V plánu testování popište rozsah, cíle, metodologii, časový plán a prostředky (hardware, software, personál, školení a nástroje). Jednotlivé týmy a podtýmy si musí pro své oblasti technické expertízy vytvořit své vlastní plány testování a napsat testovací případy. Testovací případy popisují, jak se testování uskuteční. To umožňuje zopakovat a porovnat výsledky testů.

V počátečních fázích projektu se testování soustředí na součásti, přičemž ověří jejich návrh. Později se testování soustředí na spolupráci komponent a zajištění společné funkce všech součástí. Musíte také otestovat kompatibilitu aplikací se systémem Windows 2000. Začněte s testováním funkcí, které jsou pro vaši organizaci nejdůležitější a jejichž návrh by bylo drahé a časově náročné měnit.

Vyvíňte také plán předání vzniklých problémů osobám, které je dokáží vyřešit. Jasný proces předávání pomáhá týmu soustředit se na řešení a okamžitě činit nápravné akce.

Zavádíte-li službu Active Directory, nezapomeňte otestovat aplikace ve spojení s touto adresářovou službou.

Jakmile ověříte zavádění systému Windows 2000 v laboratorním prostředí, ještě před celkovým zaváděním vykonajte alespoň jeden pilotní projekt. Pilotní projekt udává tón konečného zavádění, takže je důležité důkladně se připravit na všechny jeho aspekty. Musíte určit dobu potřebnou k instalaci, osoby a nástroje umožňující a usnadňující tento proces a dodržení celkového časového plánu. Pilotní program vám umožňuje otestovat plány zavádění. Pilotní projekt také nabízí příležitost proškolení pracovníky technické podpory a vyhodnotit reakce uživatelů na daný produkt, což vám pomůže odhadnout budoucí potřeby technické podpory.

Další informace o vytvoření testovací laboratoře najdete v kapitole „Vytvoření testovací laboratoře systému Windows 2000“ v této knize. Další informace o pilotních projektech najdete v kapitole „Vykonání pilotního programu systému Windows 2000“ v této knize.

Poznámka Pilotní projekt dokončete, ještě než se pustíte do plného zavádění do produkčního prostředí. Při dokončení jednotlivých fází pilotního projektu zdokumentujte výsledky, ověřte, že jste naplnili požadavky projektu, a v případě potřeby plán přepracujte. Před přechodem do fáze plného zavádění vyřešte všechny zásadní problémy. Nezapomeňte do pilotního projektu zahrnout všechny aspekty vašeho produkčního prostředí. Bude-li například zavádění probíhat v mezinárodním měřítku zahrnujícím několik jazyků, musíte ve svém pilotním programu úspěšně vyřešit problémy s různými jazyky.

Vytvoření dokumentů plánování projektu

V rámci celého projektu zavádění musíte vytvářet různé dokumenty definující vaše vize, zlepšující podporu, vedoucí a shrnující proces zavádění. Ať už jsou tyto informace zachyceny v několika málo dokumentech nebo v mnoha dokumentech, měly by obsahovat položky popsané v následujících odstavcích.

Správní dokumentace

Dokumenty správy jsou součástí plánu projektu. Pomáhají vám určovat a definovat cíle. Pomáhají vám udržet organizovanost a dodržet časový plán. Do dokumentů správy zahrňte následující informace:

Rozsah a cíle

Jak již bylo řečeno, zajistěte, aby váš plán jasně stanovoval cíle projektu, definoval jeho rozsah a zajišťoval metody měřící postup a úspěšnost.

Fáze a milníky

Vytvořte fáze projektu, aby měl váš personál čas zorientovat se a pomoci vám ověřit předpoklady přijaté ve fázi plánování. Očekávejte, že některé procesy budou iterační. Vytvořte a sledujte milníky postupného zavádění, aby se projekt neodchyloval od kurzu. Další informace najdete v kapitole „Vytvoření cesty postupného zavádění“ v této knize.

Rozpočet

Identifikujte a sledujte očekávané náklady a omezení výdajů nákladů na projekt včetně vývoje, hardwaru, nástrojů, školení, personál, testování a zavádění. Identifikujte záložní finanční zdroje umožňující pokrytí nečekaných výdajů. Zajistěte jasnou vizi projektu ve společnosti, aby bylo jasné i rozdělování fondů.

Personál

Plánujte, jak obsadíte sídla systému Windows 2000 personálem. Užitečný bude dokument naznačující strukturu hlášení, odpovědnosti, četstost schůzek, strategie komunikace a celkové vlastníky úkolů a funkcí. Další informace najdete v oddílu „Přiřazení rolí týmům Windows 2000“ dříve v této kapitole.

Prostory

Určete požadavky na prostory a komunikujte s příslušnými skupinami v organizaci. Definujte své požadavky na prostory a potřebná místa si zajistěte včas, aby se minimalizovala pravděpodobnost, že se tyto problémy stanou překážkami zavádění.

Celkový odhad rizika

Identifikujte rizika projektu existující mimo oblast zavádění. Mezi možná rizika může patřit dostupnost prostředků, chýějící se sloučení nebo ztráta klíčového personálu.

Strategie komunikace

Managementu a uživatelům představte projekt zavádění tím, že budete své plány konzultovat s jinými skupinami v organizaci. S vytvářením podpory a přijímání projektu začněte brzy – předávejte své plány manažerům a klíčovým osobám v dohodnutých intervalech. Další informace najdete v oddílu „Strategie komunikace“ dále v této kapitole.

Dokumenty zavádění

Následující doporučené dokumenty zavádění můžete vytvořit jako součást plánu projektu:

Přehled současného síťového prostředí

Vytvořte popis vyšší úrovně současného síťového prostředí včetně infrastruktury sítě, hardwaru, zásad, počtu a typu uživatelů a geografických míst.

Návrh zavádění

Podrobně specifikujte, jak se přechod na systém Windows 2000 uskuteční, včetně strategie inovace a migrace serverových a klientských počítačů, kdy a jak se tyto inovace uskuteční a koho se budou týkat. Vezměte v úvahu také existující systémy a aplikace, jako je vliv změny operačního systému na existující aplikace a schopnosti ukládacího prostoru a hardwaru.

Analýza rozdílů

Zabývejte se konkrétními rozdíly mezi existujícím prostředím a cílem projektu. Pak vytvořte seznam specifických změn, které jsou zapotřebí pro podporu cílů projektu. Další informace najdete v oddílu „Vykonání analýzy rozdílů“ dříve v této kapitole.

Plán kapacity

Identifikujte problémy a nahodilosti, kterými se budete muset zabývat v zájmu zajištění dostatečné kapacity hardwaru a sítě pro zaváděné funkce systému Windows 2000 (například replikační provoz způsobovaný službou Active Directory nebo vzdálená instalace operačního systému). Musíte si být jisti, že nedojde ke snížení úrovně základních služeb během zavádění a po jeho dokončení. Další informace najdete v oddílu „Plánování kapacity“ dále v této kapitole.

Vyhodnocení rizik

Ve svém plánu identifikujte rizika a vytvořte kontingenční plány jejich řešení. Neustále opakovaně vyhodnocujte plán zavádění a po dokončení jednotlivých fází projektu vytvořte formální vyhodnocení. Další informace najdete v oddílu „Vyhodnocení rizik“ dále v této kapitole.

Plán eskalace problémů

Určete cestu předávání, kterou budou lidé ve vaší organizaci používat k řešení a postupování problémů podle potřeb. Jednotlivé typy problémů nebo situace předávejte lidem, kteří si s nimi dokáží nejlépe poradit. Tento proces eskalace umožňuje týmu soustředit se na vyřešení problémů.

Pilotní plán

Určete cíle pro servery a klienty, kteří se budou účastnit prvotního postupného zavádění, jaké funkce se budou zavádět a jaké mechanismy budete používat k získávání informací od účastníků pilotního projektu. Další informace o přípravě na pilotní program a jeho vykonání najdete v kapitole „Vykonání pilotního programu systému Windows 2000“ v této knize.

Strategie testování a zavádění

Naplánujte, jak budete testovat a zavádět systém Windows 2000. Další informace najdete v oddílu „Testování a pilotní program zavádění systému Windows 2000“ dříve v této kapitole.

Funkční specifikace

Funkční specifikace podrobně popisuje implementované funkce operačního systému a jejich konfiguraci a zavádění. Všechny tyto prvky musí odpovídat rozsahu a cílům projektu zavádění.

Popište různé typy uživatelů, jimi vykonávané klíčové úkoly, jak se tyto úkoly vykonávají v současné době a jak se zlepší výkon v novém síťovém prostředí. Je-li vaše organizace velká a má-li více sídel, nebo jedná-li se o mezinárodní organizaci, musíte se také podrobně věnovat geografickým otázkám.

Mnoho funkcí systému Windows 2000 vzájemně souvisí, což je důležité zejména, plánujete-li zavádět službu Active Directory. Z tohoto důvodu je velmi zásadní matice závislostí a lze ji považovat za primární dokument.

Týmy zavádění musejí spolupracovat a identifikovat úkoly potřebné k integrování jednotlivých součástí a určit dobu potřebnou k dokončení těchto úkolů. Identifikujte všechny problémy a otázky, kterých si členové týmu a management musí být vědomi. Zejména důležité je zjistit závislosti ovlivňující jiné týmy. Můžete například zjistit, že práce řady týmů zahrnuje strukturu systému Domain Name System (DNS) a že jejich úkoly je zapotřebí koordinovat, aby se zbytečně nevykonávaly dvakrát.

Strategie komunikace

Podrobný plán komunikace může zlepšit efektivitu vašeho projektu zavádění. Při řádné komunikaci se podaří vaši práci s plánováním a zaváděním systému Windows 2000 doplnit a integrovat s prací jiných týmů zavádějících nové projekty IT. To umožňuje managementu pomáhat projektovým týmům v překonávání překážek a také přípravu je uživatele na využívání výhod nové infrastruktury.

Efektivní strategie komunikace identifikuje potřeby několika typů uživatelů, jako jsou výkonný management, projektové týmy, organizace IT a uživatelé na všech úrovních. Budete-li uživatele neustále informovat, budou se projektu také účastnit. Pomocí strategie komunikace zajistíte podporu projektu zavádění, nových technologií systému Windows 2000 a obchodních či výrobních procesů, které tyto technologie umožňují.

Při vytváření plánu komunikace je důležité zabývat se následujícími otázkami:

Jak budou distribuovány informace o zavádění?

Tradičnější média, jako je tisk, můžete doplnit využitím elektronické pošty a intranetů. Vytvoření intranetového sídla, které lze snadno aktualizovat hlášením o stavu zavádění, je jedním z nejlepších způsobů, jak zajistit informovanost uživatelů. Zkušenosti uži-

vatelů se zvyšují, když si dokáží své problémy vyřešit sami. Omezuje se tak zmatení a snižují se náklady na technickou podporu.

Jaké informace se budou oznamovat?

Vysvětlíte, jak nová infrastruktura zjednoduší uživatelům práci a jak bude sloužit obchodním či výrobním potřebám organizace. Stav zavádění je jednou z nejdůležitějších informací, kterou můžete předávat uživatelům a členům týmů zavádění. Zvýrazněte úspěchy ale přiznejte také překážky a neúspěchy.

Jak často se budou informace distribuovány?

Pro koncové uživatele mohou být měsíční aktualizace dostatečné. Pro manažery však budou zapotřebí častější aktualizace, zejména když se přiblížíte pilotnímu zavádění a zavádění do produkčního prostředí. Členové týmu IT, ať už jsou v procesu zavádění přímo zapojeni nebo ne, potřebují týdenní aktualizace. Zaváděné změny mají přímý dopad na způsob, jakým své funkce vykonává personál IT, a proto musí podrobně sledovat postup projektu zavádění.

Jaký typ mechanismu zpětné vazby budete implementovat?

Ve svých plánech podrobně určete zpětné předávání zkušeností uživatelů. Vytvoření mechanismu zpětné vazby, kterým mohou uživatelé vyjadřovat svoje připomínky a nespokojenost s některými prvky, je pro celkový úspěch velmi důležité. Obousměrný komunikační kanál umožní uživatelům účastnit se projektu a fungovat jako členové týmu poskytující hodnotné informace, které mohou přispět úspěchu vašeho projektu.

Plán vzdělávání a školení

Ještě před začátkem zavádění předejte uživatelům informace o funkcích a prvcích systému Windows 2000. Můžete také zajistit formální školení a vyvinout mechanismus zpětné vazby.

Program Microsoft Official Curriculum (MOC) pro systémy Microsoft Windows 2000 Professional a Windows 2000 Server nabízí počítačovým profesionálům školení v oblasti zavádění, správy a technické podpory sítí systému Windows 2000. Tento technický program zahrnuje kurzy předávající účastníkům znalosti a dovednosti potřebné k:

- pochopení funkcí a prvků systému Windows 2000,
- instalaci, konfiguraci a inovaci na systém Windows 2000,
- správu sítě systému Windows 2000,
- aktualizaci dovedností technické podpory ze systému Microsoft Windows NT verze 4.0 na systém Windows 2000,
- navržení infrastruktury adresářových služeb systému Windows 2000,
- navržení infrastruktury síťových služeb systému Windows 2000,
- navržení infrastruktury správy změn a konfigurací.

Další informace o programu MOC pro systém Windows 2000 najdete v odkazu Microsoft Training and Certification – Microsoft Official Curriculum stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Plánování kapacity

Plánování kapacity zajišťuje solidní základy pro plánování a řízení počítačového prostředí. Jakmile určíte počítačové prostředky potřebné k naplnění vašich obchodních či výrobních požadavků, získáte následující výhody:

- Jsou naplněny cíle služeb.
- Zlepší se produktivita.
- Je možné vyvinout a udržet škálovatelnost.
- Jsou řízeny nebo sníženy celkové náklady na vlastnictví (Total Cost of Ownership – TCO).

Jedním z nejdůležitějších úkolů při plánování kapacity je zkonstruovat reprezentativní základní linii pracovního zatížení a počítačových prostředků. Plánovači kapacity a plánovači obchodní či výrobní činnosti musejí spolupracovat na identifikaci součástí obchodní či výrobní činnosti, které závisejí na počítačových prostředcích, a předpovídat požadavky zatížení. Klíčovým prvkem vykonání inventarizace hardwaru je řízení aktiv. Potřebujete-li nahradit nějaký hardware, ještě před inovací pečlivě zjistěte, co je zapotřebí nahradit.

Některé organizace se spoléhají na zkušenosti manažerů s plánováním kapacity, jiné používají analytické modelování, simulace, měření výkonu nebo v kritických situacích reálné experimenty s plánováním kapacity. Bez ohledu na použité techniky vyžaduje úspěšné řízení počítačového prostředí aktivní přístup.

Dobrým výchozím bodem je vytvořit profil různých aktivit, k nimž dochází na vaší síti nebo podsítích každou hodinu, každý den nebo měsíc, jako jsou tyto údaje:

- Počet změn hesel
- Počet přihlašování uživatelů
- Počet požadavků DNS
- Počet změn hesel účtů počítačů

Následně vyhodnoťte minimum, maximum a průměr pro všechny výše uvedené položky. Potřebujete vědět, ke kolika takovým událostem dochází, jakou šířku pásma zabírají na síti a kolik výkonu procesoru a diskového prostoru spotřebovávají na serveru.

Zjistěte, jaké kladou stejné činnosti požadavky v novém produktu. Tyto informace pak můžete použít k optimalizaci serverů a k naplánování struktury domén a sídel.

Další informace o plánování kapacity a funkcích systému Windows 2000 najdete v jednotlivých kapitolách v této knize zabývajících se technologiemi, jejichž zavádění plánujete.

Vyhodnocení rizik

Při plánování zavádění operačního systému a infrastruktury sítě počítejte také s neočekávanými událostmi. Dokonce i ty nejlepší plány zavádění mohou být výrazně ovlivněny změnami obchodních či výrobních potřeb, ekonomiky, požadavků uživatelů nebo dalšími narušeními, jakými jsou výpadky napájení a bouřky.

Plán řízení rizik vám pomůže s určením potenciálních rizik ještě než dojde k jejich výskytu a umožní vám rychle reagovat, pokud skutečně takové situace nastanou. Dobře promyšlený plán řízení rizik pojatý aktivně vám pomůže:

Omezit pravděpodobnost, že se nějaký rizikový faktor skutečně projeví.

Bude-li vaší infrastruktura zabezpečení plně rozumět jen jediná osoba personálu, pak může mít ztráta této osoby uprostřed procesu zavádění velmi vážné důsledky. Toto riziko můžete omezit výškolením zálohy všech klíčových expertů a zajištěním přístupu k aktuální dokumentaci.

Omezit rozsah ztrát při výskytu rizikového faktoru.

Máte-li dojem, že projekt zavádění systému Windows 2000 Server není dostatečně financován, můžete identifikovat několik záložních prostředků, které mohou pokrýt neočekávané výdaje.

Změnit následky rizikového faktoru.

Náhlá reorganizace, nákup jiné organizace nebo rozdělení organizace uprostřed procesu zavádění může vážně narušit vaše plány. Pokud vytvoříte proces zajištění aplikování náhlých změn, můžete tyto potřeby naplnit jen s minimálními dopady na časový plán projektu.

Připravit se na zmírnění rizik během zavádění.

Toho dosáhnete strategickým plánováním instalace a postupného zavádění. Můžete například začít přidáváním nových řadičů domény se systémem Windows 2000 do existující domény systému Windows NT 4.0. Alternativně můžete vybudovat novou doménu systému Windows 2000, vytvořit vztahy důvěryhodnosti s existující doménou účtů a následně klonovat účty uživatelů. Nebo můžete do své domény nainstalovat nové řadiče domény systému Windows NT 4.0, přesunout je na privátní síť a pak je inovovat na instalaci nové domény. Ve všech těchto případech se můžete jednoduše v případě potřeby vrátit k předchozímu prostředí.

Řízení rizik

Chcete-li efektivně řídit rizika, musí váš plán řízení rizik:

- identifikovat nejdůležitější (mission-critical) aplikace,
- identifikovat a analyzovat potenciální rizika,
- kvantifikovat potenciální dopady těchto rizik,
- podrobně popisovat procesy eskalace,
- identifikovat řešení,
- být předáván vyššímu managementu a členům projektu,
- být součástí každodenního řízení projektu,
- být aktualizován.

Řízení rizik musí být součástí pravidelných činností vašeho týmu a musí se zabývat všemi klíčovými lidmi, procesy, obchodními či výrobními činnostmi a technologickými oblastmi vašeho zavádění systému Windows 2000. Musíte:

Vyhodnotit rizika ve všech oblastech, která mohou ovlivnit váš projekt.

Požádejte jednotlivé týmy o identifikaci a řízení potenciálních rizik souvisejících s různými oblastmi jejich zodpovědnosti, jako je zabezpečení, práce v síti, pomocné nástroje, technická podpora a školení.

Seřadit rizika podle priority.

Rizika se mohou výrazně lišit svými dopady a svou pravděpodobností. Určete, která rizika představují pro vaši organizaci největší hrozbu. Primárními rizikovými faktory se zabývejte nejprve.

Setkat se s lidmi, kteří zajišťují podporu obchodních a existujících aplikací.

Starší a vlastní obchodní či výrobní aplikace představují speciální rizika. Včas se setkejte s lidmi, kteří mají s takovými aplikacemi rozsáhlé zkušenosti. Zodpovídá-li za něj takovou aplikaci jiná společnost, co nejdříve ji zapojte do celého procesu.

Vyhýbat se vyhodnocení životaschopnosti pouze na základě počtu nevyřešených rizikových faktorů.

Projekt se 20 identifikovanými rizikovými faktory nemusí být o nic stabilnější než projekt se 40 identifikovanými rizikovými faktory. Vyhodnocení identifikující vyšší počet rizik může být jen důkladnější než vyhodnocení s méně rizikovými faktory. Tento dokument použijte k označení rizik, která mohou projekt velmi závažně narušit, i rizik, která mají menší vliv.

Vytvořte takové prostředí, kde nebudou lidé identifikující rizikové faktory hodnocení negativně.

Pracovníci, kteří skutečně vykonávají určité činnosti v organizaci, často rozpoznají problémy dříve než jejich nadřízení. Pokud nebudou ochotni tyto špatné zprávy předávat, může dojít k narušení vyhodnocení rizik. Zvažte zavedení programu odměn pro ty, kdo identifikují rizika, i pro ty, kteří jsou schopni takto zjištěná rizika vyřešit.

Matice vyhodnocení rizik

Abyste plně identifikovali potenciální rizika, musíte dokonale porozumět vzájemným závislostem mezi různými prvky zavádění. Matice rizik vám pomůže identifikovat a propojit tyto prvky.

Tabulka 3.4 obsahuje ukázkovou matici vyhodnocení rizik, která uvádí otázky, jako je pravděpodobnost vzniku rizika, stupeň vlivu konkrétního rizika na projekt a strategii potřebnou ke snížení rizika.

Tabulka 3.4 Ukázková matice vyhodnocení rizik

Riziko	Pravděpo- dobnost	Vliv	Vlastník	Datum vyřešení	Strategie omezení
Zvažuje se slou- čení s jinou spo- lečností.	Střední	Vysoký	Manažer týmu zavádění	dd/mm/rr	Vytvoření strategie rychlé integrace s přísluš- nými týmy v jiných organizacích.
Před zavedením systému Windows 2000 nebudou mít všichni uživatelé počítač splňující minimální požá- davky systému Windows 2000.	Střední	Střední	Týmy manage- mentu progra- mu, technické podpory a lo- gistiky	dd/mm/rr	Rozhodnout se, zda inovovat hardware v době instalace nebo zda počkat na inovaci hardwaru v celé organizaci.

Tuto matici vytvořte včas ve fázi plánování a aktualizujte ji v pravidelných intervalech nebo při změnách v časovém plánu, specifikacích, managementu, týmu, rozsahu nebo strategii postupného zavádění.

Časový plán určený rizikovými faktory

Jen málo prvků zavádění dokáže vytvořit více rizikových faktorů, než špatně zformovaný časový plán. Jestliže například vaše organizace zmrazí ve čtvrtém kvartálu projekty zavádění, pokusy o vykonání příliš mnoha kroků na poslední chvíli mohou znamenat snížení kvality testování a postupného zavádění. Naplánujete-li zavádění nejjednodušších komponent jako prvních a složitější a nejriskantnější součásti si necháte až na konec, omezíte si tím čas dostupný k řešení složitějších problémů.

Časový plán, který zvažuje rizikové faktory, může minimalizovat pravděpodobnost vážných problémů. Následující pokyny vám pomohou s vytvořením časového plánu určeného rizikovými faktory:

Časový plán musí vycházet z odhadů na úrovni úkolů.

Začněte s odhady na úrovni úkolů a postupujte výše časovými plány týmů. Nakonec integrujte časové plány více týmů. Bude-li váš časový plán vycházet z nejnižších úrovní jednotlivých úkolů, budete muset při jeho vytváření identifikovat a vyřešit všechny problémy, které mohou projekt zpomalit nebo dokonce zastavit.

Nejprve vyviňte nejrizikovější součásti.

Nejprve se zabývejte nejrizikovějšími prvky zavádění. Důsledky zpoždění, změn návrhu a dalších problémů mají na zbytek procesu menší dopad, když se jim budete věnovat včas.

Stanovte hlavní a postupné kontrolní body.

Kontrolní body postupu se ověřují testováním. Časté postupné milníky vám umožní znovu vyhodnotit postup s využitím nových informací již na počátku procesu, čímž se omezí rizika nesplnění hlavních milníků.

Vyhradte čas pro neočekávané situace.

Jen málo větších zavedení se podaří dokončit, aniž by došlo k nějakým událostem narušujícím časový plán, jako je nemoc klíčových osob, zpožděné dodávky hardwaru nebo problémy se zajištěním finančních prostředků. Ve svém časovém plánu počítejte s časem pro tyto neočekávané situace.

Naplánujte čas pro řízení projektu.

Určitý čas trvá definování vize, zajištění finančních prostředků a vykonání všech dalších úkolů řízení projektu. Vyhradte příslušný čas pro řízení projektu.

Použijte nástroj časového plánování projektu.

Nástroje časového plánování projektu vám umožní rychle propojit úkoly se závislostmi a vzájemnými závislostmi a určit vlastníky úkolů a stavy plnění úkolů. Tyto nástroje jsou také užitečné při sledování postupu různých týmů a jejich úkolů a zajištění plnění časového plánu projektu.

Zajistěte aktualizaci časového plánu.

Časový plán aktualizujte, kdykoli se změní okolnosti obchodní či výrobní činnosti nebo zavádění, přidají se nové aktivity a dosáhne se určitých milníků.

Informujte vedoucí projektů o potřebných změnách časového plánu.

Definování cílů umožní lidem poznat, kdy je zapotřebí projekt zavádění zastavit. Pokud jste například zavedli systém Windows 2000 na deset počítačů a zjistili jste, že nelze nadále používat službu nějaké jiné společnosti, bude před pokračováním zapotřebí tento problém vyřešit.

Zavádění systému Windows 2000

Poslední fází plánování zavádění je definování, jak se zajistí hladký přechod z pilotního programu do produkčního prostředí. Vaším cílem je zavést systém Windows 2000 úspěšně a výkonně s minimálním dopadem na uživatele, síť a základní funkce vaší organizace.

Zavádění systému Windows 2000 do produkčního prostředí sdílí mnoho charakteristik se zaváděním systému Windows 2000 v pilotní fázi. Mezi doporučené kroky zajišťující úspěch patří:

Rozdělte činnosti zavádění do fází.

Postupné zavádění vám umožní omezit rizika a minimalizovat narušení normálních funkcí.

Vytvořte plán zálohování zavádění.

Spolehlivý a otestovaný plán zálohování vám umožní rychlé a snadné zotavení či obnovení v případě, kdy se během zavádění setkáte s nějakými problémy.

Vytvořte plán zálohování/obnovení.

Protože velká havárie počítače nebo sídla může překonat i ty nejlepší strategie ochrany dat, potřebujete mít plán zotavení systému po havárii. Další informace o vytváření plánů zotavení po havárii najdete v kapitole „Určení strategií správy úložišť systému Windows 2000“ v této knize.

Zajistěte potřebné školení.

Ujistěte se, že jsou vaše týmy technické podpory a správy plně vyškoleny a připraveny na zavádění.

Informujte koncové uživatele.

Informujte a vzdělávejte koncové uživatele systému Windows 2000 ještě před jeho zavedením na počítače. Některé organizace vyžadují školení koncových uživatelů před zavedením jakékoli nové technologie. Zvažujete-li tuto strategii, počítejte s dalšími prostředky a náklady.

Zajistěte, aby týmy byly trvale informovány.

Ujistěte se, že týmy si uvědomují plány zavádění jako celek, rozsah své zodpovědnosti a všechny změny plánu a časového plánu.

Hlavní činnosti zavádění naplánujte mimo pracovní hodiny.

Vliv na uživatele a síť můžete minimalizovat promyšleným časovým naplánováním hlavních činností systému Windows 2000. Zavedení systému Windows 2000 určité skupině odložte až na dobu, kdy splní důležitý termín nebo jiný velký projekt.

Seznam úkolů plánování zavádění

Tabulka 3.5 shrnuje úkoly, které musíte vykonat při plánování zavádění systému Windows 2000.

Tabulka 3.5 Seznam úkolů plánování zavádění

Úkol	Umístění v kapitole
Definujte rozsah projektu a krátkodobé i dlouhodobé cíle.	Rozsah a cíle projektu
Přiřadte funkce systému Windows 2000 cílům projektu.	Rozsah a cíle projektu
Zdokumentujte současné počítačové prostředí.	Současné počítačové prostředí
Vykonejte analýzu rozdílů.	Vykonání analýzy rozdílů
Definujte role personálu a čas potřebný ke splnění úkolů.	Požadavky na personál
Vytvořte standardy konfigurací hardwaru, softwaru a sítě.	Vytvoření standardů a pravidel
Vytvořte dokumenty správy.	Dokumenty správy
Vytvořte dokumenty zavádění.	Dokumenty zavádění
Vytvořte návrh zavádění.	Návrh zavádění
Vytvořte strategii komunikace.	Strategie komunikace
Vyhodnoťte požadavky na kapacitu.	Plánování kapacity
Identifikujte rizika.	Vyhodnocení rizik
Vytvořte a spravujte časový plán.	Časový plán určený rizikovými faktory
Vytvořte plán vzdělávání a školení.	Plán vzdělávání a školení
Vytvořte plán testování.	Testování a pilotní program zavádění systému Windows 2000
Naplánujte pilotní projekt.	Testování a pilotní program zavádění systému Windows 2000
Naplánujte hladký přechod na systém Windows 2000.	Zavádění systému Windows 2000

KAPITOLA 4

Vytvoření testovací laboratoře systému Windows 2000



Ještě než zavedete i třeba jen pilotní program systému Microsoft Windows 2000, musíte otestovat předpokládaný návrh v prostředí, které simuluje a chrání vaše produkční prostředí. Svůj návrh můžete prověřit vymyšlením a vykonáním testů odrážejících podmínky v cílovém prostředí.

Tato kapitola nabízí manažeru testování i týmům projektu zavádění obecné úvahy o návrhu a provozování testovací laboratoře, která naplní konkrétní potřeby vaší organizace. Problémy s testováním určitých funkcí systému Windows 2000 najdete také v ostatních kapitolách této knihy.

V této kapitole

Úvod do testovacího prostředí 78

Určení strategie laboratoře 82

Návrh laboratoře 90

Vybudování laboratoře 102

Řízení laboratoře 103

Testování 105

Testování po zavedení systému 111

Seznam úkolů plánování laboratorního testování 114

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Popis laboratoře
- Diagram laboratoře
- Plán předávání problémů
- Plán testování
- Testovací případy

Související informace v sadě Resource Kit

- Další informace o plánování testování aplikace najdete v kapitole „Testování kompatibility aplikací se systémem Windows 2000“ v této knize.
- Další informace o plánování pilotního programu v produkčním prostředí najdete v kapitole „Vykonání pilotního programu systému Windows 2000“ v této knize.

Úvod do testovacího prostředí

Klíčovým faktorem úspěchu projektu zavádění systému Windows 2000 je zevrubné testování vycházející z realistických scénářů. Realistické scénáře vyžadují testovací prostředí, které simuluje v co největší možné míře vaše produkční prostředí. V tomto testovacím prostředí si mohou členové týmu plánování ověřit své předpoklady, odhalit problémy zavádění a optimalizovat návrh zavádění i zlepšit své vlastní znalosti jednotlivých technologií. Takové činnosti omezují riziko chyb a minimalizují doby výpadků v produkčním prostředí během zavádění a po něm.

Vytvoření testovacího prostředí

Testovací prostředí zahrnuje všechna místa podporující testování bez ohrožení sítě společnosti. Mnoho velkých organizací distribuuje svá testovací prostředí do mnoha fyzických a dokonce i geografických oblastí, kde se testují různé technické, obchodní či výrobní nebo politické souvislosti. Následující faktory ovlivňují rozhodování o testovacím prostředí:

- Vaše metodologie testování
- Funkce a součásti, které budete testovat
- Personál, který bude testování vykonávat

Testovací prostředí může zahrnovat jednu nebo více laboratoří a jedna laboratoř může představovat jedno nebo více míst. Termín laboratoř se v této kapitole používá k označení sítě, která je vytvořena pro testování a která je izolována od sítě společnosti.

V případě svého projektu systému Windows 2000 se můžete rozhodnout vytvořit několik nezávislých laboratoří, které budou testovat různé funkce. Můžete mít například jednu laboratoř pro testování infrastruktury sítě a serverů a jinou laboratoř pro testování klientských počítačů a aplikací. Podobně se může jedna laboratoř skládat z několika míst. Můžete tak například vytvořit laboratoř infrastruktury sítě s více místy propojenými rozlehlou sítí (WAN), která se bude používat k testování různých rychlostí linek. Zavádíte-li najednou systémy Microsoft Windows 2000 Server a Microsoft Windows 2000 Professional, vaše rozhodnutí, zda mají mít tyto projekty samostatné laboratoře nebo jednu společnou, ovlivňuje mnoho faktorů. Mezi tyto faktory patří:

- Složitost zavádění (jako je různorodost v produkčním prostředí a nových funkcí, které plánujete implementovat).
- Velikost, umístění a struktura týmů projektu.
- Dostupné finanční prostředky.
- Dostupnost fyzických míst.
- Umístění testovacích pracovníků.
- Využití laboratoře po skončení testování.

Úvahy v této kapitole platí pro laboratoře navržené k testování systému Windows 2000 Server nebo systému Windows 2000 Professional.

Použití laboratoře pro rizikový management

Dobře navržená laboratoř poskytuje řízené prostředí pro různé testy po celý cyklus životnosti projektu – od experimentování s technologiemi přes porovnávání řešení návrhu až po vyladování procesu postupného zavádění do produkčního prostředí. Dobrá

laboratoř nemusí být nutně velkou investicí; může mít rozsah od několika kousků hardwaru v malé místnosti až po plnohodnotnou síť v prostředí datového střediska.

Testovací laboratoř je investice, která se mnohokrát zaplatí omezením nákladů na podporu a opakované zavádění, jež jsou důsledkem špatně otestovaných řešení. Je to důležitá součást plánu řízení rizik projektu systému Windows 2000. Rizika můžete identifikovat v laboratoři, když testy odhalí problémy jako tyto:

- Hardwarové nebo softwarové nekompatibility
- Chyby návrhu
- Problémy s výkonem
- Problémy se spoluprací různých systémů
- Omezené znalosti nových technologií
- Nevýhodné prvky provozu nebo zavádění

Jestliže testování odhalí podobné problémy, laboratoř může poskytnout prostředky pro vývoj a ověření alternativních řešení. V laboratoři lze také vykonávat následující činnosti:

- Navrhovat a ověřovat plány návratu zpět, čímž se omezuje riziko narušení obchodních či výrobních úkolů během pilotního zavádění a zavádění do produkčního prostředí.
- Naučit se optimalizovat proces zavádění a omezit tak čas a náklady potřebné na činnosti zavádění.
- Vyvinout výkonné postupy správy a omezit tak čas a personál potřebný pro stálou údržbu po dokončení zavedení.
- Ověřit postup podle plánu projektu a vyladit časový plán projektu.

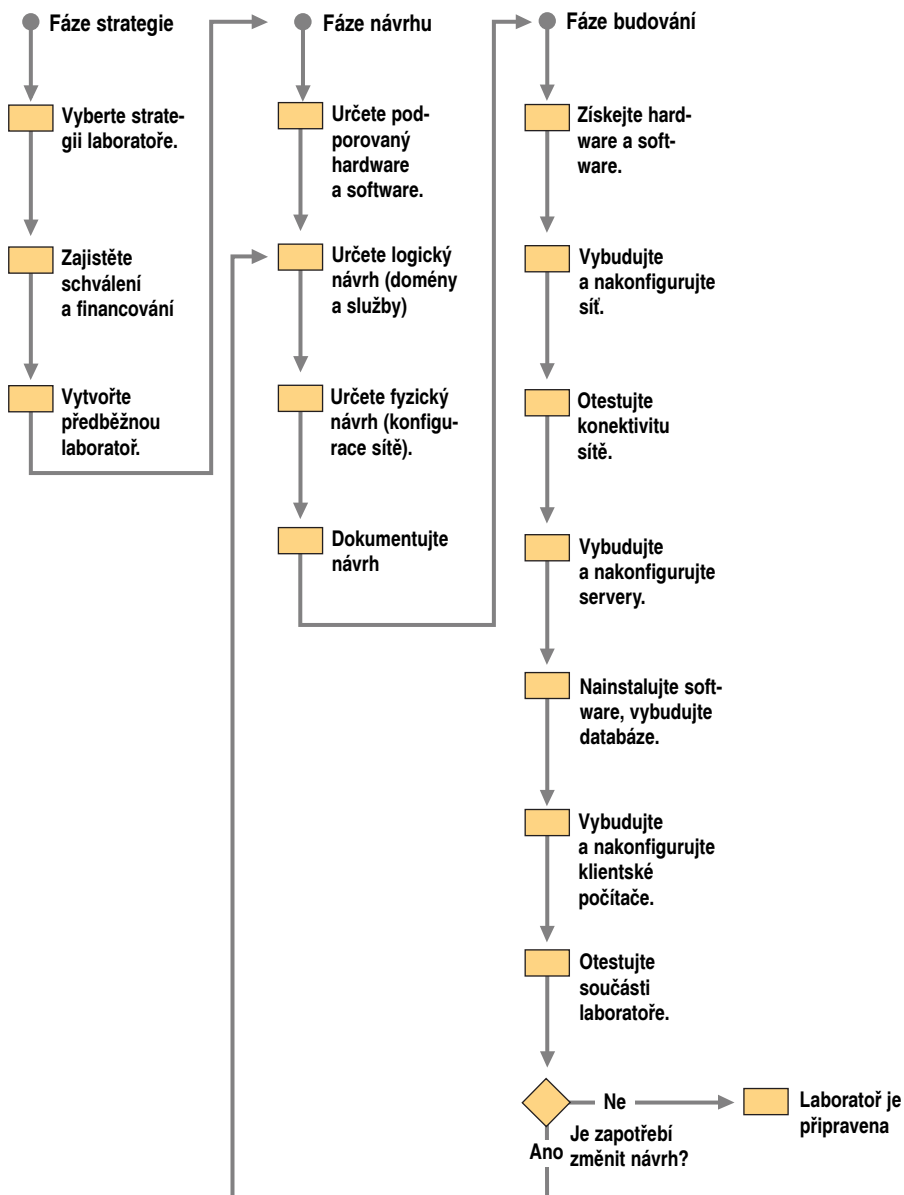
Proces vývoje laboratoře

Obrázek 4.1 je vývojový diagram ilustrující jednotlivé fáze přípravy laboratoře na testování. Ve fázi strategie vytvoříte cíle a obecný přístup k problematice laboratoře. Rozhodnutí učiněná v této fázi ovlivňují rozhodnutí ve fázi návrhu.

Ve fázi návrhu plánujete a dokumentujete logickou a fyzickou strukturu laboratoře. Rozhodnutí učiněná ve fázi návrhu určí, co vytvoříte ve fázi budování.

Ve fázi budování vytváříte laboratoř a ještě před začátkem testování systému Windows 2000 testujete síťové součásti. Fáze návrhu a budování jsou iterační: jak se zvyšují vaše zkušenosti, vyvíjejí se požadavky a mění se zaměření testování, tak musíte opakovaně navrhovat nebo budovat součásti v laboratoři. Součásti musíte přebudovat také v případě, kdy akumulované změny hardwaru, softwaru nebo metodologie testování začínají ovlivňovat výsledky testů.

Začátek



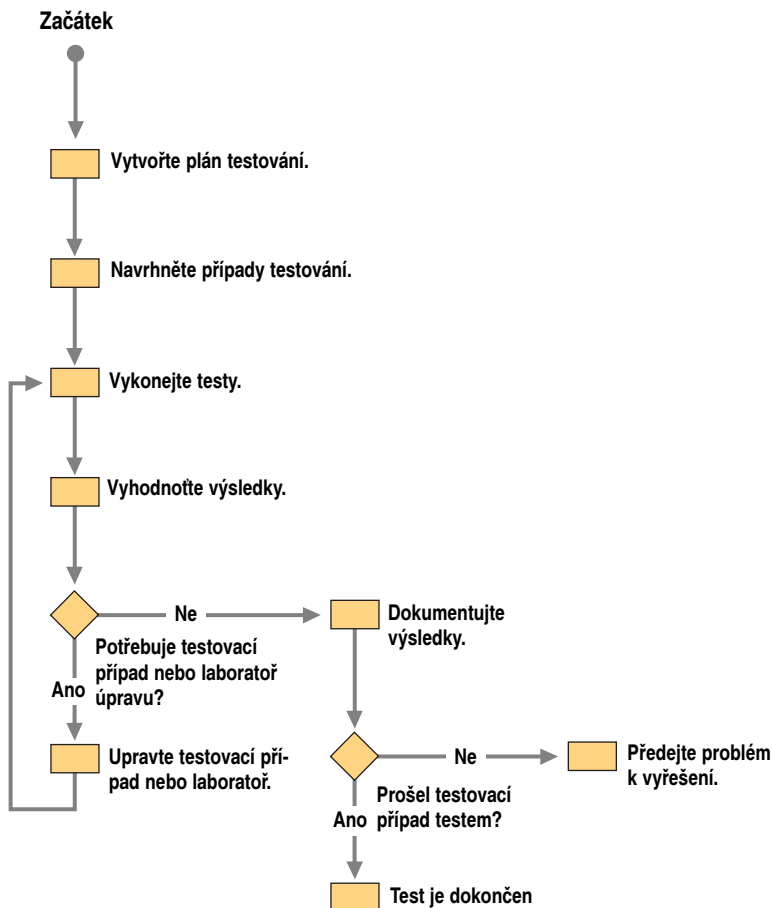
Obrázek 4.1 Proces vytvoření testovací laboratoře

Testovací proces

Obrázek 4.2 je vývojový diagram, který ilustruje fáze plánování a vykonávání testů v laboratoři.

Základními činnostmi jsou:

- Vytvoření plánu testování popisujícího rozsah, cíle a metodologii.
- Návrh testovacích případů, popisujících vykonávání testů.
- Vykonání testů a vyhodnocení výsledků.
- Dokumentování výsledků testů.
- Předání problémů příslušným lidem k řešení.



Obrázek 4.2 Proces plánování a vykonávání testů

Vytvoření předběžné laboratoře

Pokud ještě žádnou laboratoř nemáte, je důležité začít na ní pracovat co nejdříve v rámci projektu zavádění systému Windows 2000. Laboratoř budete velmi brzy potřebovat ve fázi plánování pro seznámení se s produktem, ověření konceptů, testování různých scénářů v souvislosti s obchodním či výrobním modelem a vyhodnocování řešení. Velmi brzy v projektu můžete vybrat umístění, začít odhadovat hardwarové požadavky, překonfigurovat existující laboratorní zařízení a třeba začít nakupovat nebo shromažďovat hardware pro laboratoř.

Včasné plánování se vyplatí v době vykonávání testů, kdy nabídnete odpovídající prostor nezbytnému zařízení a řádnou konfiguraci pro vlastní testy. Rozhodování ohledně požadavků na hardware, software a personál pro testování dokumentujte v plánu testování. Další informace o plánu testování najdete v oddílu „Testování“ dále v této kapitole.

Plánujete-li vytvořit trvalou laboratoř, budete potřebovat schválení managementu a zajištění financování nezávisle na projektu zavádění systému Windows 2000. Je-li tomu tak, začněte s procesem schvalování co nejdříve.

Již v počátcích plánování vám laboratoř pomůže vytvořit základní návrh oboru názvů a plán zavádění vyšší úrovně, který můžete dále použít jako základní linii pro další testování a vývoj. Použijete-li laboratoř jako základní konfiguraci a budete-li postupně rozšiřovat její funkce, vyhnete se problémům souvisejícím s nezávisle vyvinutými návrhy.

Abyste mohli hned začít se zkoušením testování, můžete si vybudovat laboratoř se dvěma nebo třemi servery a klientskými počítači, použít existující laboratoř, nebo vytvořit konfiguraci server/klient v nějaké kanceláři. Když se pak rozhodnete ohledně návrhu vyšší úrovně, začněte skládat dohromady formální laboratoř.

I když se laboratoř v celém projektu vyvíjí a odráží změny v zaměření testování, musí být plně vybavena a stabilní již před testováním předběžné pilotní integrace.

Určení strategie laboratoře

Možná již máte vytvořenou laboratoř, kterou plánujete použít pro testování systému Windows 2000, nebo si myslíte, že by bylo lepší vytvořit pro tento projekt novou laboratoř. Bez ohledu na vaši současnou situaci je vhodné promyslet si cíle laboratoře a její dlouhodobý účel. Můžete se rozhodnout, že nyní je vhodná doba pro inovaci laboratoře vytvořené pro jiné účely, kterou budete moci v budoucnosti používat k řízení změn v prostředí systému Windows 2000.

Máte-li již trvalou laboratoř, kterou plánujete využívat k testování návrhu zavedení systému Windows 2000, můžete přejít přímo do oddílu „Návrh laboratoře“ dále v této kapitole.

Zvážení návratnosti nákladů

Rozhodnete-li se pro testování zavádění systému Windows 2000 vytvořit novou laboratoř, budete muset před výkonnými pracovníky projektu ospravedlnit tuto investici. Pomůže vám, když zvážíte širší pohled na všechny související výdaje. Testování vykonané v laboratoři vede k čistším implementacím a snížení nákladů na technickou podporu. Jestliže v laboratoři vyvinete výhodné operační činnosti, jako jsou automatizované nástroje správy a vzdálené procedury, snížíte tím celkové náklady na vlastnictví pro organizaci. Z dlouhodobého hlediska tedy budou náklady na vybudování a údržbu labo-

ratoře pravděpodobně velmi výrazně nižší než náklady na řešení problémů v produkčním prostředí, opakované zavádění špatně vymyšlených či špatně otestovaných řešení nebo na správu produkčního prostředí procesy vyžadujícími značné prostředky.

V organizacích, které budují samostatné laboratoře pro různé projekty, je možné také rozsah laboratoře ekonomicky zdůvodnit. Konsolidací laboratoří a formalizací použití a údržby nové laboratoře lze dosáhnout toho, že několik projektů může se sníženými náklady sdílet jedinou laboratoř. Rozhodnete-li se však sdílet laboratoř, pokuste se vybrat projekty s kompatibilními časovými plány a požadavky na vybavení. Je jednodušší a levnější přidat v rámci inovace laboratoře v nějakém projektu jen několik nových součástí, než ji začínat pokaždé budovat znovu od začátku.

Čím víceúčelovější bude vaše laboratoř, tím snáze budete moci obhájit finanční výdaje na prostory, zařízení a podporu nezbytnou k jejímu vytvoření a provozování. Laboratoř může sloužit účelům od prvotních školení až k řešení problémů po zavedení systému. Laboratoř můžete považovat za svou počáteční investici do školení. Můžete ji dokonce použít pro vzdělávací účely, jako je demonstrování funkcí nebo procesů zavádění managementu a dalším skupinám.

Použití laboratoře během životního cyklu projektu

V zájmu ospravedlnění nákladů na laboratoř musíte zvážit řadu způsobu, jak ji bude možné v celém průběhu projektu využívat. Tento oddíl obsahuje příklady možných využití laboratoře.

Plánování

V počátečních fázích plánování využívají členové týmu projektu laboratoř k získání zkušeností: zvyšují své znalosti technologií, testují si své hypotézy a odhalují problémy s implementací a požadavky na zavádění. To je také dobrá doba k vyhledání způsobů zlepšení současných operačních procesů, jako je identifikace úkolů, které lze automatizovat nebo vykonávat vzdáleně.

Při postupu návrhu mohou členové týmu používat laboratoř k vyzkoušení nových technologií, modelů a procesů řešení požadavků obchodních či výrobních činností. Takové vytváření prototypů a modelování vede k rozhodnutím o způsobu implementování funkcí a prvků systému Windows 2000.

Vývoj

Během vývoje poskytuje laboratoř řízené prostředí testování a vyhodnocování různých problémů a otázek, jako jsou tyto:

- Funkce systému Windows 2000
- Kompatibilita infrastruktury sítě
- Možnost spolupráce s jinými síťovými operačními systémy
- Hardwarová kompatibilita
- Kompatibilita aplikací
- Plánování výkonu a kapacity
- Dokumentování instalace a konfigurace
- Administrativní postupy a dokumentace
- Postupné zavádění do produkčního prostředí (procesy, skripty a soubory, plány návratu zpět)

- Základní vzory provozu (objemy provozu bez aktivity uživatelů)
- Nástroje (systému Windows 2000, jiných společností nebo vlastní)
- Výkonnost operací

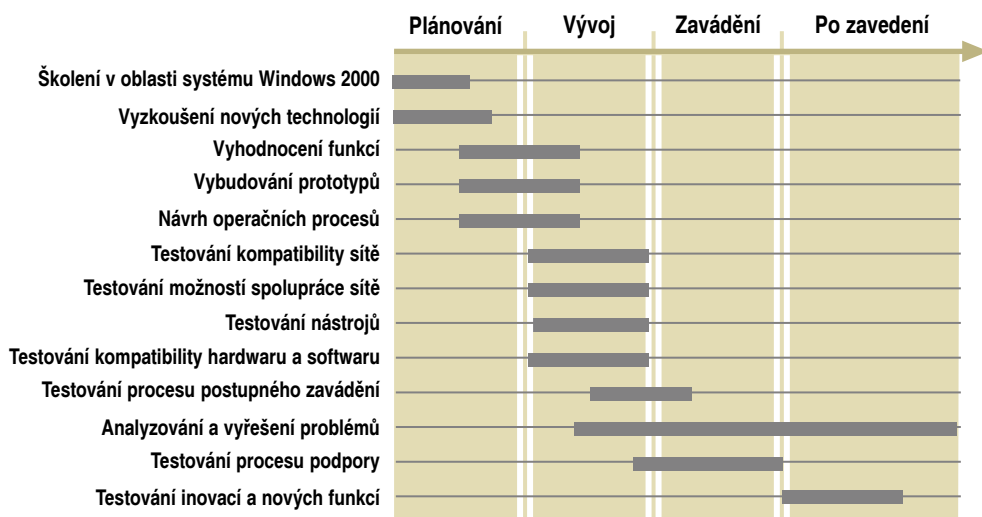
Zavádění

Během pilotního zavádění nabízí laboratoř operačním týmům (jako je technická podpora a personál operací) místo, kde mohou začít plánovat strukturu podpory. Laboratoř lze během pilotního programu a zavádění do produkčního prostředí používat také k izolování, reprodukování, analyzování a nápravě problémů s procesy zavádění.

Po zavedení systému

Po zavedení systému může tým podpory využívat laboratoř k reprodukování a řešení problémů zjištěných v produkčním prostředí. Laboratoř nabízí také bezpečné místo pro testování změn, jako jsou servisní balíčky, opravy, nové aplikace nebo nové konfigurace počítačů, které jsou součástí procesu řízení změn.

Obrázek 4.3 ilustruje různá využití laboratoře a fáze projektu, při nichž může docházet k určitým aktivitám. Časové rámce jsou jen odhady a nepředstavují skutečné zavádění.



Obrázek 4.3 Role laboratoře v životním cyklu projektu

Laboratoř není jediným místem, kde dochází k testování. Členové týmů projektu mohou také testovat funkčnost na svých samostatných testovacích počítačích. V testovací laboratoři se však ověřuje spolupráce součástí a funkcí v integrovaném prostředí, které simuluje vaše cílové produkční prostředí. Simulované prostředí musí odrážet jak přechodné období, kdy se používá kombinace různých funkcí, tak i konec projektu, kdy došlo k úplné implementaci nových funkcí.

Vyhodnocení laboratorních modelů

Mnoho organizací vytváří účelové laboratoře, kdykoli potřebují otestovat nástroje nějakého nového projektu. Jiné organizace vytvářejí trvalé laboratoře, které jsou škálovatelné pro různé projekty, a používají je k řízení změn. Jak účelové laboratoře tak i laboratoře řízení změn mají své výhody a nevýhody.

Účelové laboratoře

Účelové laboratoře se vytvářejí pro specifické projekty. Jakmile je projekt dokončen, zařízení laboratoře se použijí jinde. Zařízení tak lze použít například v produkčním prostředí, lze je převést do inventáře nebo po zapůjčení vrátit prodejci.

Krátkodobé náklady na vytvoření účelové laboratoře mohou být nižší než náklady na vytvoření trvalé laboratoře, protože veškeré jejich zařízení se opakovaně používá někde jinde. Takový pohled na náklady je však krátkozraký, protože pro každý další projekt je zapotřebí vybudovat novou laboratoř. Účelové laboratoře mohou vést k následujícím problémům:

- Je-li pro každý projekt zapotřebí vytvořit novou laboratoř, kritickým faktorem se stává čas. Protože týmy potřebují laboratoř velmi brzy, musejí se řešit následující problémy:
 - Dokážete včas zajistit příslušný hardware a softwarové licence?
 - Může náhrada softwaru nebo hardwaru vést k neadekvátnímu testování?
 - Dokážete najít výrobce, modely a verze potřebné k odpovídajícímu otestování kombinace hardwaru a softwaru v produkčním prostředí?
 - Můžete rezervovat fyzické prostory potřebné k vytvoření síťových konfigurací a vykonání testů?
 - Způsobí čas strávený budováním a laděním laboratoře omezení času na testování, což může mít za následek nedokončení testování?
- Když hardware a softwarové licence vyhledává příliš mnoho týmů, je obtížné sledovat, kdo co používá a kdo povoluje nákupy. Výsledný nedostatek zodpovědnosti může vést ke zbytečným výdajům a nárůstu nákladů.

Změny managementu laboratoře

Problémy zmíněné v předchozím oddílu představují zásadní důvody pro vytvoření trvalé, formalizované laboratoře. Po zavedení systému Windows 2000 můžete používat trvalou laboratoř k testování změn prostředí, jako jsou tyto:

- Inovace sítě
- Servisní balíčky a opravy softwaru
- Kompatibilita obchodních či výrobních aplikací
- Konfigurace kancelářských počítačů
- Nové hardwarové platformy
- Procesy správy a podpory
- Nástroje řízení klientských počítačů

Plně vybavená trvalá laboratoř používaná k řízení změn má následující výhody:

Z dlouhodobého hlediska šetří náklady.

Vezmete-li všechny projekty jako celek, náklady na trvalou laboratoř budou pravděpodobně mnohem rozumnější než náklady na účelově vytvářené laboratoře, jejichž nákupy se nesledují tak podrobně nebo je u nich rozptýlena finanční zodpovědnost.

Omezuje rizika pro vaši obchodní či výrobní činnost.

Laboratoře omezují rizika pro vaše produkční prostředí, protože důkladné testování vede k čistším implementacím. Je například lákavé vůbec netestovat zjevně nevýznamnou změnu v testovací laboratoři, která není ihned připravena. Avšak i malá změna může zastavit celý obchodní či výrobní proces. Budete-li mít trvalou laboratoř sloužící účelům řízení změn, bude velmi jednoduché otestovat i ty nejmenší změny. Čím více bude laboratoř odrážet produkční prostředí, tím platnější všechny testy budou.

Šetří čas projektu.

Nastavení a ladění se minimalizuje, protože inovace existující laboratoře jsou rychlejší než vytvoření nové laboratoře. Šetření časem je kritické, pokud plánujete používat laboratoř k trvalému vytváření prototypů vývoje. Používáte-li laboratoř k vývoji i testování, máte k jejímu vytvoření méně času.

Pomáhá odpovídajícím způsobem vybavit laboratoř.

Může pro vás být jednodušší ospravedlnit nákup vybavení potřebného k naplnění určitých potřeb testování, plánujete-li zároveň vytvořit laboratoř řízení změn. V případě účelových laboratoř se vybavení pravděpodobně převede z jiného využití nebo se nakoupí tak, aby splnilo konkrétní specifikace svého budoucího použití – nemusí tedy odpovídat požadavkům na testování.

Navíc je pravděpodobnější, že se vám podaří udržet kombinaci zařízení, které přesně odpovídá produkčnímu prostředí. Časem si můžete ponechat originální vybavení a obdržet nové vybavení, které bude odrážet neustále se měnící, různorodé produkční prostředí. Udržení vhodné kombinace vybavení v laboratoři zajišťuje zevrubné testování možnosti návratu zpět během procesů řízení změn.

Pomáhá vytvořit konzistentní metodologii.

Máte-li trvalou laboratoř, můžete pro její podporu určit vyhrazený personál. V případě trvalé laboratoře a kontinuity řízení laboratoře můžete vytvořit jednotné testovací procesy a postupy, které budou podávat konzistentní výsledky, jež bude možno vzájemně porovnávat.

Výběr modelu laboratoře

Rozhodování o typu vybrané laboratoře, účelové nebo k řízení změn, ovlivňuje mnoho faktorů. Vaše rozhodnutí ovlivní následující faktory:

- Rozpočet
- Čas a personál dostupný k vybudování laboratoře
- Existující laboratoře
- Fyzický prostor a omezení prostředí
- Fungování společnosti
- Cíle projektu nebo společnosti

Prvním krokem v tomto rozhodnutí je vyhodnotit dlouhodobé cíle testování a řízení rizik. Pak zvažte výhody a nevýhody jednotlivých modelů ve vztahu k vašim cílům.

Můžete určit, že některý z modelů vyhovuje vašim cílům nejlépe, okolnosti však mohou diktovat jiný přístup. Můžete například chápat výhody dlouhodobé laboratoře, kterou budete moci využívat pro testování oprav softwaru a inovací, vaše organizace však nemá na vybudování trvalé laboratoře prostředky. Musíte porovnat možné výsledky různých řešení a možná se vám podaří najít kreativní způsoby podpory vašeho ideálního řešení. Sami si položte třeba následující otázky:

- Jaký bude mít toto rozhodnutí vliv na kvalitu testování?
- Jak toto rozhodnutí ovlivní školení týmů a podporu návrhů?
- Přispěje laboratoř také jiným existujícím projektům?
- Mohou ostatní projekty zkombinovat činnosti a rozpočty a sdílet jedinou laboratoř?
- Můžete laboratoř vytvářet ve fázích, přičemž začnete nejpodstatnějšími součástmi a dále ji budete rozšiřovat podle dostupných finančních prostředků?
- Bude prodejce hardwaru souhlasit s nějakou zvláštní dohodou?

Může vám prodejce například poskytnout vybavení na splátky nebo je poskytnout výměnou za to, že bude moci používat název vaší organizace pro účely marketingu?

Výběr umístění laboratoře

Vaše rozhodnutí ohledně modelu laboratoře a jejího umístění budou pravděpodobně vzájemně souviset. Umístění trvalé laboratoře používané mnoha různými skupinami vyžaduje důkladnější rozvahu, než jak je tomu v případě krátkodobé laboratoře používané jen několika skupinami. Jedním z důležitých ohledů, se kterým musíte počítat v plánu dlouhodobé laboratoře, je například prostor pro budoucí růst. S těmito rozhodnutími vám pomohou následující otázky:

- Jaké laboratoře již existují? Jsou odpovídající? Jak snadno je lze upravit, aby odpovídaly požadavkům testování?
- Lze konsolidovat existující laboratoře?
- Jaký je rozsah a složitost implementace?
- Jak se bude rozdělovat rozpočet laboratoře? Zvažte tyto položky:
 - Náklady na nástroje a pracovní prostor (místo, topení, ventilace, klimatizace, napájení, kabely, serverové stojany a pracovní stoly).
 - Hardware a software.
 - Technická podpora a další personál laboratoře.
- Musí být laboratoř připojena k produkčnímu prostředí nebo k jiným laboratořím? Jestliže musí být připojena k produkční síti, jak budete toto připojení regulovat a jak nakonfigurujete směrovače v zájmu ochrany produkční sítě?

Další informace o připojení laboratoře k produkční síti najdete v oddílu „Simulování navrhovaného serverového prostředí“ dále v této kapitole.

Mezi další otázky, které je zapotřebí zvážit při výběru umístění laboratoře, patří:

Inovování nebo vytvoření nové

Rozhodnete-li se použít existující laboratoř, mohou k testování systému Windows 2000 postačovat jen menší úpravy a inovace. Bude například zapotřebí inovovat servery na

stejně množství paměti a kapacitu pevného disku a na stejné typy a rychlosti procesorů, jaké budou obsahovat zaváděné servery.

Přístupnost

Laboratoř musí být přístupná všem skupinám, které ji chtějí používat. Implementujete-li program, podle kterého si lidé mimo projektový tým mohou přijít otestovat své vlastní aplikace, laboratoř musí mít prostředky umožňující takové návštěvy, například parkovací místa.

Zabezpečení

Zajistěte, abyste mohli fyzicky zabezpečit laboratoř a zabránit neoprávněnému využívání zařízení.

Prostor

Ať už budete budovat novou laboratoř nebo inovovat tu existující, důležitým prvkem je dostupný prostor. Samotný systém Windows 2000 nevyžaduje ke svému provozování složité a drahé zařízení. Protože je však zapotřebí simulovat do co největší možné míry produkční prostředí, složitost takového prostředí přímo ovlivňuje složitost laboratoře.

Mezi faktory současného a navrhovaného produkčního prostředí, které mohou určit složitost a tedy také prostorové požadavky laboratoře, patří:

- Počet a kombinace funkcí a prvků, které plánujete implementovat.
Plánujete implementovat doménu, která zahrnuje více sídel? Plánujete implementovat virtuální privátní síť (Virtual Private Network – VPN)?
- Množství různorodosti v produkčním prostředí.
Máte nebo plánujete zavést do produkčního prostředí standardní vybavení, aplikace a konfigurace? Nebo budete používat mnoho výrobců, modelů, verzí a konfigurací?
- Úroveň složitosti síťové konfigurace.
Máte ve své produkční síti více typů topologií? Plánujete zavedení rozhraní mezi systémem Windows 2000 Server a mainframem, systémem Macintosh, nebo systémem UNIX?

Kromě faktorů v produkčním prostředí mohou složitost vaší laboratoře ovlivnit také některé testované situace. Můžete například potřebovat další servery, abyste mohli izolovat určité typy testování, jak je popsáno dále v této kapitole.

Požadavky na prostor jsou také ovlivněny počtem lidí, kteří se pravděpodobně budou účastnit testování. Zamyslete se nad tím, kolik lidí bude v laboratoři pracovat najednou.

Podmínky prostředí

Umístění laboratoře musí zajišťovat odpovídající podmínky prostředí, jako je teplota, vlhkost a čistota. Tyto požadavky se podobají požadavkům kladeným na datové středisko. Umístění laboratoře musí také podporovat vaše požadavky na napájení, kabeláž a síťovou konektivitu.

Počet míst

V některých případech můžete požadovat, aby se laboratoř skládala z více vzájemně propojených míst v zájmu otestování vlivu geograficky oddělených síťových segmentů. Jestliže například plánujete implementovat adresářovou službu Microsoft Active Directory na více sídlech Active Directory, musíte otestovat replikaci přes podobná interne-

tová spojení nebo spojení WAN. Další informace o sídlech služby Active Directory a replikaci najdete v kapitole „Návrh struktury služby Active Directory“ v této knize.

V jiných případech můžete požadovat více nezávislých laboratoří, které se budou využívat různými způsoby. Můžete potřebovat samostatnou laboratoř pro testování aplikací a třeba samostatné laboratoře pro testování systémů Windows 2000 Server a Windows 2000 Professional.

Testování v distribuovaném laboratorním prostředí

Laboratorní prostředí může být distribuováno v mnoha fyzických nebo i geografických místech. Studie případů uvedené dále popisují, jak se dvě organizace rozhodly používat laboratoře tímto způsobem.

Studie 1: Funkční laboratorní sídla

Společnost velkého výrobce hardwaru je organizována podle funkcí. Její regionální pobočky jsou umístěny v různých geografických sídlech vybraných tak, aby se nacházely v blízkosti dodavatelů a prodejců, kteří podporují konkrétní funkce každého regionu. Tento výrobce vyvinul laboratoř zahrnující tři hlavní sídla v jihozápadních a západních státech Spojených států. Každé umístění laboratoře je navrženo tak, aby testovalo funkce a konfigurace používané v obchodní či výrobní činnosti daného sídla. Všechny laboratoře jsou trvalé a používají se k řízení změn produkčního prostředí.

Organizace plánuje nakonec laboratoř rozšířit, aby zahrnovala také vzdálená mezinárodní místa, jako jsou města na Vzdáleném východě, Středním východě, ve Východní Evropě a na Britských ostrovech. Organizace použije tato vzdálená sídla k návrhu a testování řešení výzev globálního podnikání, jako je:

- Konektivita v řízených zemích
- Pomalá spojení
- Dočasně dostupná spojení
- Více jazyků
- Více časových zón
- Mezinárodní měny
- Rozdíly v počítačovém a síťovém hardwaru

Studie 2: Laboratorní sídla pro případ nehody

Jiná organizace si myslí, že je důležité být připraven a na havárii. Tato organizace chce, aby její geograficky oddělená sídla byla připravena fungovat v roli centralizovaného oddělení informačních technologií (IT), bude-li to nutné. V této organizaci se jedná o trvalou laboratoř řízení změn, která se používá také pro testování zotavení po havárii.

V případě havárie se produkční přístroje ve vybraných místech použijí k vykonávání funkcí oddělení IT. Aby byly stále připraveny, organizace vykonává testování v laboratořích a ujišťuje se, že všechny potřebné hardwarové a softwarové součásti v alternativním místě jsou dostupné a mohou řádně fungovat. Mezi tyto testy patří:

- Nahrávání aplikací a databází
- Nastavování konfigurací
- Spouštění aplikací

Návrh laboratoře

Ještě než navrhnete laboratoř, musíte mít plán zavádění vyšší úrovně. Musíte například znát předpokládaný návrh oboru názvů. Musíte také znát architekturu domén a konfiguraci serverů takových služeb, jako jsou Domain Name System (DNS), protokol Dynamic Host Configuration Protocol (DHCP) a služba Windows Internet Name Service (WINS). Chcete-li zajistit, že návrh laboratoře bude skutečně odrážet požadavky na testování, podtýmy projektu by vám měly poskytnout informace o hardwaru, softwaru a konfiguracích, které potřebují.

Rozhodnete-li se vybudovat trvalou laboratoř, kterou budete moci využívat k řízení změn po zavedení systému Windows 2000, váš návrh by měl být dostatečně flexibilní jak z hlediska prostoru tak i rozvržení, aby dokázal naplnit i budoucí požadavky.

Čím více se budete věnovat návrhu laboratoře, tím více testů bude přesně odrážet skutečnou implementaci.

Předpoklady návrhu laboratoře

Protože laboratoř musí simulovat prostředí, kde budete zavádět systém Windows 2000, potřebujete ještě před vytvořením návrhu laboratoře informace o současném a navrhovaném prostředí. Se sběrem informací o současném systému vám může pomoci server Microsoft Systems Management Server (SMS). Další informace o používání serveru SMS k inventarizaci systému najdete v kapitole „Analýza infrastruktury sítě pomocí serveru Systems Management Server“ v této knize. Informace o navrhovaném prostředí by měly být k dispozici v dokumentech plánování vytvořených týmem projektu. Pro důkladné pochopení funkcí a prvků systému Windows 2000 navíc potřebujete tyto informace:

- Současný návrh sítě (logický a fyzický).
- Předpokládaný návrh systému Windows 2000.
- Seznam funkcí, které je zapotřebí vyhodnotit a prostudovat.
- Inventář existujícího hardwaru (serverů, klientských počítačů a přenosných počítačů).
- Seznam hardwaru navrhovaného pro systém Windows 2000.
Tento seznam se může během testování vyvíjet, potřebujete však nějaký výchozí stav pro vybavení laboratoře.
- Seznam nástrojů správy (Windows 2000, jiné nezávislé společnosti a samostatně vyvinutých).
- Seznam inovací, jako jsou servisní balíčky, ovladače a systém BIOS, které musíte nainstalovat při přípravě na systém Windows 2000.

Návrh scénářů testování

Snažte se navrhnout flexibilní laboratoř. Navíc se přinejmenším pokuste splnit tato kritéria:

- Simulujte navrhované prostředí – určete, co budete testovat.
- Zajistěte podmínky pro vykonání procesu testování – určete, jak budete testovat.

Můžete se sice rozhodnout použít jedinou laboratoř pro testování jak klientských tak i serverových počítačů, tento oddíl však popisuje návrh laboratoří samostatně.

Simulování navrhovaného serverového prostředí

Naplánujte otestování co největší části navrhovaného logického a fyzického produkčního prostředí včetně hardwaru počítačů, topologie sítě, spojení WAN, architektury domén, služeb, databází, obchodních aplikací, nástrojů pro správu, modelu zabezpečení, metodologie zavádění aplikací a serverových ukládacích metod.

Tento oddíl obsahuje určité úvahy o návrhu laboratoře k testování systému Windows 2000 Server. Zde uvedené problémy nemusejí platit pro všechny implementace systému Windows 2000 Server. Zaměřte se na úvahy, které platí pro váš návrh.

Serverový hardware a ovladače

Použijte stejný typ hardwarových součástí a ovladačů, které používáte nebo plánujete používat na serverech v produkčním prostředí. Nezapomeňte si obstarat inovovaný systém BIOS, který bude kompatibilní se systémem Windows 2000.

Služby a konfigurace

Použijte stejné služby a konfigurace, které použijete také ve vlastním zavedení. Duplikujte například konfigurace DNS, DHCP a WINS. Neplánujete-li používat služby DNS a DHCP zabudované do systému Windows 2000, použijte služby jiných společností, které budete zavádět.

Uživatelské účty

Budete-li migrovat ze systému Microsoft Windows NT 4.0, nastavte řadiče domén jako repliky vašich řadičů domén produkčního prostředí pomocí kopií účtů uživatelů z produkčního prostředí. Ke zkopírování uživatelů z produkčního prostředí do testovací domény můžete použít nástroj ClonePrincipal. Další informace o strategiích migrování účtů uživatelů a používaných nástrojích najdete v kapitole „Určení strategií migrace domén“ v této knize. Každé kopírování produkčních dat do databází laboratoře koordinujte s oddělením zabezpečení IT.

Struktura domén

Jestliže implementujete službu Active Directory, simulujte hierarchii domén. Použijte například doménovou strukturu s více stromy, strom s nadřazenými a podřízenými doménami a přenosné a jednosměrné vztahy důvěryhodnosti podle potřeby. V organizačním útvaru reflektujte svou centralizovanou nebo decentralizovanou správu IT. Podle potřeby použijte sídla služby Active Directory.

Serverová strategie

Zahrňte souborové a tiskové servery, aplikační servery, webové servery, databázové servery a další servery, které se nacházejí, nebo budou nacházet v produkčním prostředí. Plánujete-li k zavádění systému Windows 2000 použít server SMS, zapojte jej do laboratoře.

Smišená prostředí

Chcete-li podporovat jak kombinované prostředí během postupného zavádění tak i prostředí systému Windows 2000 po dokončení zavádění, naplánujte vytvoření domén následujících typů:

- Nativního režimu
- Kombinovaného režimu
- Současného produkčního operačního systému

Simulováním přechodného stavu určité funkční problémy, k nimž může dojít během postupné implementace. Servery s jiným operačním systémem než Windows 2000 Server musejí zrcadlit služby v současném produkčním prostředí.

Konfigurace klientských počítačů

Použijte stejnou kombinaci klientských počítačů, jaká se vyskytuje v produkčním prostředí. Plánujete-li nejprve zavést systém Windows 2000 Server a teprve později systém Windows 2000 Professional, použijte operační systém klientských počítačů, který se bude používat až do zavedení systému Windows 2000 Professional.

Plánujete-li zavádět nejprve systém Windows 2000 Professional, otestujte, jak dlouho se bude zavádět rozšířená funkce serverů do vašeho prostředí během zavádění infrastruktury.

Plánujete-li postupné zavádění, použijte stejnou kombinaci, k níž dojde během zavádění. Použijte tak například klientské počítače se systémem Microsoft Windows 95 a klientské počítače se systémem Windows 2000 Professional.

Topologie sítě a protokoly

Co nejlépe zrcadlete topologii sítě a protokoly používané v produkčním prostředí. Jestliže například produkční síť používá jak Ethernet tak i Token Ring, laboratoř musí obsahovat obě tyto technologie.

Spojení WAN

Máte-li síť WAN, laboratoř musí mít směrovače testující zpoždění sítě. Máte-li k dispozici potřebné nástroje a finance, vytvořte v nějakém vzdáleném místě druhou laboratoř, abyste mohli otestovat fungování sítě přes spojení WAN. Měli byste například otestovat replikaci řadičů domén a globálního katalogu přes toto spojení. Pokud pracujete v nadnárodní organizaci, doporučujeme vám vytvořit druhou laboratoř v jiné části světa, abyste vyzkoušeli reálné problémy se zpožděním.

Nemáte-li druhou laboratoř, kde byste mohli otestovat spojení WAN, můžete kabelem v jedné laboratoři spojit dva směrovače a k otestování spojení použít simulátor.

Vzdálená připojení

Zajistěte stejné typy vzdáleného připojení, jako je služba Směrování a vzdálený přístup (Routing and Remote Access Service) a VPN, abyste mohli otestovat protokol Point-to-Point Tunneling Protocol (PPTP), Internet Protocol Security (IPSec), protokol Layer 2 Tunneling Protocol (L2TP) a směrování telefonického připojení na požádání.

Periferie

Zahrňte reprezentativní vzorek typů periferií zařízení používaných v produkčním prostředí. Použijte například shodné typy tiskáren a skenerů společně s odpovídajícími ovladači.

Spolupráce

Plánujete-li implementovat systém Windows 2000 Server tak, že bude spolupracovat se sítími nebo počítači využívajícími jiný operační systém, zkopírujte infrastrukturu spolupráce. Zahrňte sem například připojení k mainframovým hostitelům, systémům UNIX a dalším síťovým operačním systémům. Abyste udrželi spravovatelnost konfigurace laboratoře a testovací sady, určete, které scénáře spolupráce jsou pro vaši organizaci nejdůležitější a zaměřte se na ně.

Administrativní nástroje

Zahrňte také nástroje (systému Windows 2000, jiných společností i samostatně vyvinuté), které v současné době používáte nebo plánujete používat k naplnění serverových úkolů správy. Musíte otestovat kompatibilitu a výhodnost použití těchto nástrojů v novém prostředí.

Techniky odolnosti proti chybám

Otestujte všechny techniky odolnosti proti chybám, které plánujete použít v produkčním prostředí. Plánujete-li například používat clustering, umístěte do laboratoře klastr serverů.

Terminálové služby

Plánujete-li implementovat terminálové služby, nainstalujte na server příslušnou kombinaci aplikací. Musíte porozumět důsledkům provozování aplikací ve víceuživatelském prostředí. Možná bude v případě určitých aplikací zapotřebí upravit výchozí operační prostředí, aby bylo zajištěny požadované funkce. Další informace o terminálových službách najdete v kapitole „Zavádění terminálových služeb“ v této knize.

Poznámka Jestliže máte obavy, že některé vaše důležité aplikace nebudou kompatibilní se systémem Windows 2000 Professional, zvažte instalování terminálových služeb. Terminálové služby můžete nainstalovat na server se systémem Windows NT 4.0 a nastavit své klientské počítače se systémem Windows 2000 tak, aby k problematickým aplikacím přistupovaly z daného serveru. Toto pojetí však považujte jen za možnost, jak se na poslední chvíli vyhnout nesplnění časového plánu.

Připojitelnost produkční sítě

Testovací laboratoř musíte izolovat od sítě společnosti. Musíte-li zajistit spojení z laboratoře do sítě společnosti, naplánujte způsoby regulování a řízení připojení a vymyslete možnosti rychlého ukončení připojení.

Navrhněte konfigurace směrovačů, které budou chránit produkční síť. Zvažte například použití směrovače s více adresami, se dvěma síťovými adaptéry, který bude připojovat laboratoř k produkční síti v zájmu specifických a řízených použití. Směrovač nakonfiguruje tak, aby mohla produkční síť přistupovat k laboratorní síti, aby však testovací síť nemohla přistupovat k produkční síti. Toto pojetí ochraňuje produkční prostředí před všemi událostmi v laboratoři, umožňuje však uživatelům v produkčním prostředí přistupovat k prostředkům v laboratoři. Uvedené pojetí můžete například využít k otestování přihlašovacích skriptů na laboratorním serveru s menším počtem uživatelů ještě před převedením skriptů do pilotního projektu v produkčním prostředí.

Simulování navrhovaného prostředí klientských počítačů

Laboratoř klientských počítačů navrhňte tak, abyste mohli otestovat stejné funkce a prvky, jaké používáte v produkčním prostředí. Použijte stejné typy hardwaru, aplikací a síťových konfigurací. Tento oddíl popisuje určité úvahy o vytváření laboratoře pro testování systému Windows 2000 Professional. Zde uvedené problémy nemusejí platit pro všechny implementace systému Windows 2000 Professional. Zaměřte se na úvahy, které platí pro váš návrh.

Hardware klientských počítačů

Použijte alespoň jeden klientský počítač jednotlivých výrobců a modelů, který bude pracovat v produkčním prostředí systému Windows 2000. Používá-li vaše organizace

přenosné počítače, dokovací stanice nebo replikátory portů, nezapomeňte také zahrnout všechny příslušné výrobce a modely. Získejte aktualizovaný BIOS kompatibilní se systémem Windows 2000.

Doporučujeme vám jako součást projektu zavádění vyvinout standardní hardwarové konfigurace pro systém Windows 2000 Professional. Laboratorní testování vám pomůže takovou standardní konfiguraci definovat a vyladit. Při definování hardwarových konfigurací ověřte, že jsou všechny komponenty kompatibilní se systémem Windows 2000. Bude zapotřebí ověřit například kompatibilitu následujících součástí:

- Adaptéry univerzální sériové sběrnice (USB)
- Ovladače kompaktních disků (CD) a digitálních video-disků (DVD)
- Zvukové karty
- Síťové adaptéry
- Grafické karty
- Adaptéry rozhraní Small Computer System Interface (SCSI)
- Řadiče zařízení hromadného ukládání dat
- Zařízení vyměnitelných úložišť
- Polohovací zařízení (myši, trackbally, tablety)
- Klávesnice

Kompatibilitu určíte tak, že příslušné komponenty vyhledáte v seznamu Microsoft Hardware Compatibility List (HCL), který najdete na adrese <http://www.microsoft.com> po vyhledání klíčového slova „HCL“. Seznam HCL obsahuje veškerý hardware, který společnost Microsoft podporuje. Není-li váš hardware uveden na tomto seznamu, kontaktujte jeho výrobce a zjistěte, zda poskytuje nový ovladač. Používají-li vaše součásti 16bitové ovladače, musíte si obstarat 32bitový ovladač.

Kompatibilitu hardwaru můžete také prověřit pomocí instalačního programu systému Windows 2000 Professional. Spusíte instalační program v režimu kontroly aktualizace – získáte tak protokol záznamu indikující nekompatibilitu hardwaru a softwaru a ovladače zařízení, které je zapotřebí inovovat. Formát příkazového řádku režimu kontroly inovace je:

```
winnt32 /checkupgradeonly
```

Na počítačích se systémem Windows 9x, najdete soubor záznamu protokolu nazvaný Upgrade.txt v instalační složce systému Windows. Na systémech Windows NT je soubor protokolu nazvaný Winnt32.log umístěn také v instalační složce.

Nejsou-li aktualizované ovladače vašich zařízení součástí systému Windows 2000, kontaktujte prodejce těchto zařízení a obstarejte si nejnovější ovladače.

Jakmile určíte standardní hardwarovou konfiguraci, inventarizujte počítače v produkčním prostředí a určete, které je zapotřebí před zavedením systému Windows 2000 inovovat. Informace o použití serveru SMS k vykonání této inventarizace najdete v kapitole „Zavádění systému Windows 2000 pomocí serveru Systems Management Server“ v této knize.

Další informace o vývoji standardů klientských počítačů najdete v kapitole „Definování standardů správy a konfigurace klientů“ v této knize.

Připojitelnost sítě

Zajistěte konektivitu ke stejným typům sítí, jaké se používají v produkčním prostředí, jako jsou místní sítě (LAN), rozlehlá síť nebo Internet.

Plánujete-li používat v produkčním prostředí službu Směrování a vzdálený přístup (Routing and Remote Access) nebo síťovou službu proxy, zaveďte tyto typy připojení také do laboratoře.

Serverové služby

Nakonfigurujte servery na zajištění služeb používaných v produkčním prostředí. Použijte například tyto služby:

- DNS, WINS a DHCP
- Adresářové služby (jako je X.500 a NetWare)
- Sdílení souborů
- Síťový tisk
- Serverové obchodní či výrobní aplikace, centralizované i decentralizované
- Funkce IntelliMirror

Pamatujte na zajištění služeb správy, jako jsou:

- Vzdálená instalace operačního systému
- Serverové zavádění aplikací
- Nástroje pro správu klientských počítačů (například SMS)

Ověřování v doméně

Pokud vaše organizace používá nebo plánuje používat ověřování v doméně, simulujte tuto konfiguraci ověřování v laboratoři. Pokud migrujete ze systému Windows NT 4.0 na systém Windows 2000 Server, naplánujte ověřování v kombinovaném prostředí, k němuž bude docházet během postupného zavádění.

Služby řízení sítě

Zahrňte také síťové služby používané ve vašem prostředí, jako je například protokol Simple Network Management Protocol (SNMP).

Síťové protokoly

Použijte protokoly, které plánujete nasadit do produkčního prostředí. Protokoly používané na klientských počítačích prověřte, ještě než tyto klienty připojíte na produkční síť.

Aplikace

Potřebujete licence a přístup k softwaru všech aplikací, samostatných i serverových, které musejí být podporovány na klientských počítačích se systémem Windows 2000 Professional. Další informace o testování aplikací v laboratoři najdete v kapitole „Testování kompatibility aplikací se systémem Windows 2000“ v této knize.

Periferie

Použijte také reprezentativní vzorek typů periferií, jako jsou tiskárny a skenery aplikované v produkčním prostředí.

Spolupráce se serverovou platformou

Simulujte serverové platformy, k nimž budou přistupovat klientské počítače se systémem Windows 2000 Professional. Máte-li samostatnou laboratoř serverů, zvažte její pro-

pojení s laboratoří klientských počítačů – nebudete pak muset instalovat servery do laboratoře klientských počítačů. Možná bude zapotřebí zajistit konektivitu k následujícím systémům:

- Systém Windows 2000 Server
- Systém Windows NT
- Mainframy podporující emulaci 3270
- Systém UNIX
- Další síťové operační systémy

Plánujete-li zavádět systém Windows 2000 Professional zároveň se systémem Windows 2000 Server, použijte všechny typy serverů, ke kterým klientské počítače přistupují během období zavádění, pokud tedy tyto testy nemá na starosti tým systému Windows 2000 Server.

Konfigurace stolních počítačů

Jako součást projektu systému Windows 2000 Professional se vaše organizace může rozhodnout vyhodnotit standardní klientské konfigurace a zásady skupin pro jejich řízení. Laboratorní testy mohou poskytnout informace doporučující konkrétní konfigurace a objekty zásad skupiny k řízení. Rozhodnete-li se vykonat tento typ vyhodnocovacího testování, proveďte také vzájemná porovnání různých konfigurací a nastavení zásad skupiny.

Naplánujte si dostatečný počet počítačů stejného modelu, abyste mohli jednotlivé varianty porovnávat. Klientské konfigurace vyhodnoťte na základě výkonu, jednoduchosti použití, stability, kompatibility hardwaru a softwaru, funkčnosti a modelu zabezpečení. Objekty zásad skupiny vyhodnoťte prověřením, že poskytují požadované výsledky, zejména když pro jednu konfiguraci platí více zásad, a že je výsledná doba přihlašování přijatelná.

Výkon

Pomocí laboratoře začněte vyhodnocovat dopady na síťový provoz na vaší síti. Otestujte změny základních vzorů provozu bez činnosti uživatelů. Další informace o koncepcích výkonu a nástrojích sledování najdete v kapitole „Přehled sledování výkonu“ v knize *Microsoft Windows 2000 Server Správa systému*.

Připojitelnost produkčního prostředí

Laboratoř klientských počítačů musí být podobně jako serverová laboratoř izolována od sítě společnosti. Potřebujete-li zajistit spojení z laboratoře na síť společnosti, určete, jak pomocí směrovačů tyto sítě oddělíte.

Vytvoření rámce procesů testování

Protože některé testy mění prostředí laboratoře, mohou nechtěně ovlivnit také další testy. Je tedy zapotřebí věnovat velkou pozornost izolování, koordinování a řízení těchto typů testů. Například testy inovace serverů mění stav serverů. V návrhu domén laboratoře se zabývejte těmito scénáři. Další scénáře může být zapotřebí zpracovat v procedurách řízení laboratoře. Například změny schémat ovlivňují celou doménovou strukturu, takže tento typ testu musíte dobře naplánovat a oznámit všem ostatním uživatelům laboratoře.

Pamatujte si, že laboratoř se musí často měnit, aby odrážela aktuální změřený testování. Základní konfigurace si zálohujte, aby mohli testovací pracovníci rychle obnovit po-

čítač do původního stavu. Nezapomeňte otestovat také tento proces obnovování. Záložní soubory dokumentujte a ukládejte je na bezpečné, přístupné místo.

Návrh domén pro testování

Navrhněte strukturu domén laboratoře tak, aby byla zaručena konzistentní instalace a konfigurace. Pracovníci testování se pak budou moci spolehnout na infrastrukturu, jejíž stav jim bude znám. Vyhradte tedy například jednu doménu pro testování migrace a funkce kombinovaného režimu. Učiníte-li tak, doména by se měla vždy nacházet v kombinovaném režimu s výjimkou naplánovaných časových období, kdy se vrátí do předchozího stavu a otestuje se proces migrace. Uživatelé laboratoře pak budou vždy vědět, co mohou očekávat.

Abychom všechno shrnuli: Měli byste navrhnout takovou hierarchii domén laboratoře, která zajistí oddělení testů do samostatných domén. Příklady testů, které mohou vyžadovat samostatné domény, jsou:

- Systém DNS
- Nativní režim
- Kombinovaný režim
- Proces migrace
- Replikace produkčních dat

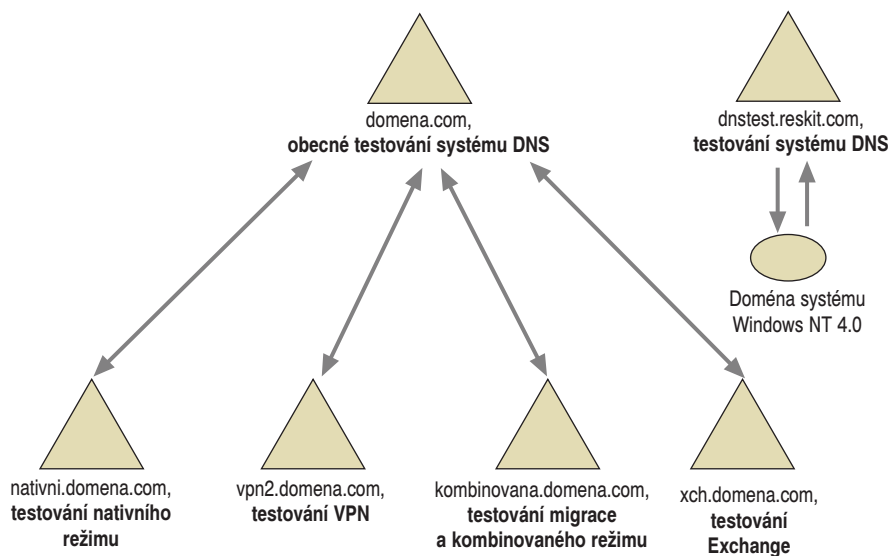
Studijní případ návrhu testovacích domén

Velká výrobní společnost navrhla svou laboratoř pro přesně určené účely testování. Obrázek 4.4 ilustruje logickou strukturu domén laboratoře.

Tato společnost vytvořila kořenovou doménu se čtyřmi podřízenými (dceřinnými) doménami. Struktura domén umožnila projektovému týmu používat samostatné domény pro následující typy testů:

- Funkce systému Windows 2000 Server v doméně pracující v nativním režimu včetně zajištění tisku.
- Virtuální privátní síť.
- Spolupráce v kombinovaném režimu a proces migrace.
- Integrace systému Microsoft Exchange Server se systémem Windows 2000.

Jedna izolovaná doména umožnila týmu testovat systém DNS, aniž by to mělo vliv na jiné testy.



Obrázek 4.4 Příklad logického návrhu domén testovací laboratoře

Dokumentování konfigurace laboratoře

Při návrhu musíte laboratoř dokumentovat jak textovými popisy, tak i diagramy. Diagramy vystavte v laboratoři, čímž zajistíte jednoduchý přístup k informacím o laboratoři a budete moci uživatele laboratoře okamžitě informovat o změnách návrhu. Pracovníci testování mohou používat popis laboratoře a diagramy při návrhu testovacích případů. Zajistí tak zevrubnost plánu testování a reprodukovatelnost testů.

Popis laboratoře

Do popisu laboratoře zahrňte následující informace:

- Strukturu domén včetně:
 - hierarchie doménových struktur a stromů,
 - objektů zásad skupiny,
 - smyslu jednotlivých domén,
 - metody zaplnění uživatelských účtů daty,
 - vztahů důvěryhodnosti (přenosných a explicitních).
- Řadiče domén včetně:
 - primárních řadičů domén (Primary Domain Controller – PDC) a záložních řadičů domén (Backup Domain Controllers – BDC), pokud migrujete ze systému Windows NT 4.0,
 - serverů, které budou povýšeny na řadiče domén, pokud migrujete z nějakého jiného operačního systému.
- Členské servery včetně služeb, které na nich poběží.

- Klientské počítače včetně:
 - výrobce a modelu počítače,
 - množství paměti,
 - typu a rychlosti procesoru,
 - kapacity pevného disku,
 - grafických karet (typu, rozlišení a barevné hloubky).
- Použití návrhu laboratoře ke specifickým testům včetně:
 - testování kombinovaného a nativního režimu,
 - testování telefonického a jiného vzdáleného připojení,
 - testování spolupráce (UNIX, mainframy a další systémy),
 - testování replikace a sídel služby Active Directory,
 - testování spojení WAN.

Diagramy laboratoře

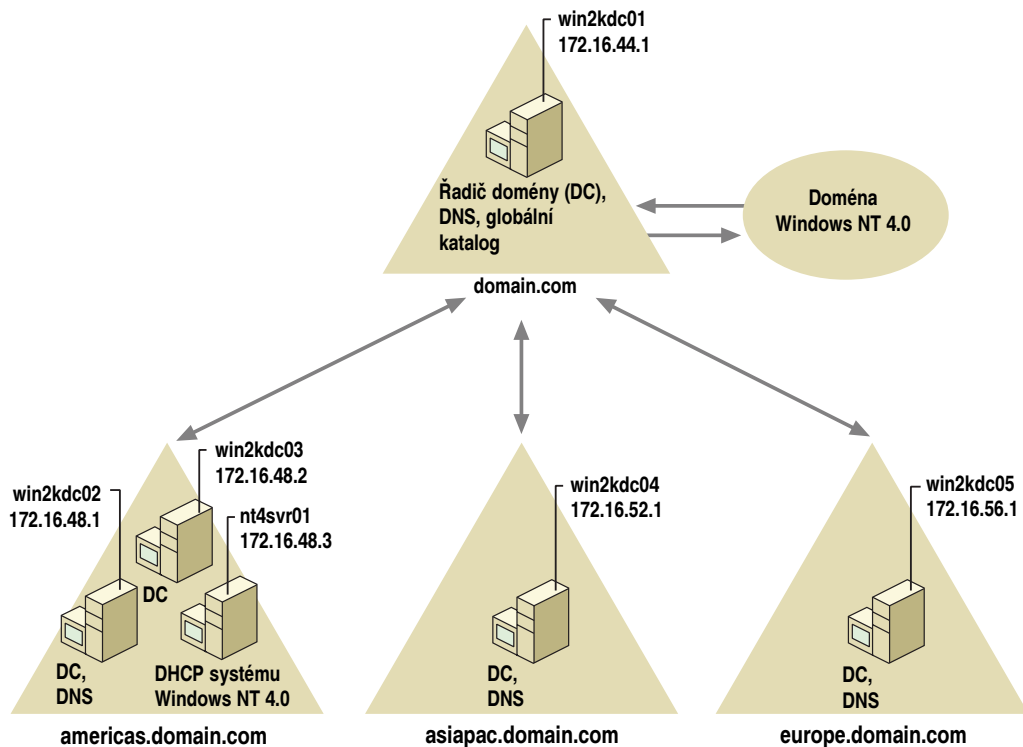
Diagramy laboratoře musí ukazovat logickou i fyzickou strukturu laboratoře. V závislosti na složitosti sítě laboratoře lze logické a fyzické zobrazení zkombinovat do jednoho diagramu.

Logický diagram

Do logického diagramu uveďte:

- hierarchii domén včetně doménových struktur a stromů,
- názvy domén,
- sídla služby Active Directory,
- speciální servery služeb (řadiče domén, globální katalog, DNS, DHCP a WINS) s těmito informacemi:
 - název počítače,
 - adresa protokolu Internet Protocol (IP),
 - funkce serveru,
- přenosné (tranzitivní) vztahy důvěryhodnosti,
- explicitní jednosměrné vztahy důvěryhodnosti.

Obrázek 4.5 je příkladem logického diagramu. Tato laboratoř má jeden strom, který se skládá z kořene a tří podřízených domén. Spojení se dvěma šipkami označují přenosné vztahy důvěryhodnosti mezi doménami systému Windows 2000. Doména systému Windows NT 4.0 má explicitní jednosměrný vztah důvěryhodnosti se stromem Windows 2000. Tato laboratoř nemá sídla služby Active Directory. Ve fázi testování obsahuje laboratoř řadiče domén, mezi něž patří servery DNS podporující protokol dynamické aktualizace, servery DHCP a jeden server globálního katalogu.



Obrázek 4.5 Příklad logického diagramu testovací laboratoře

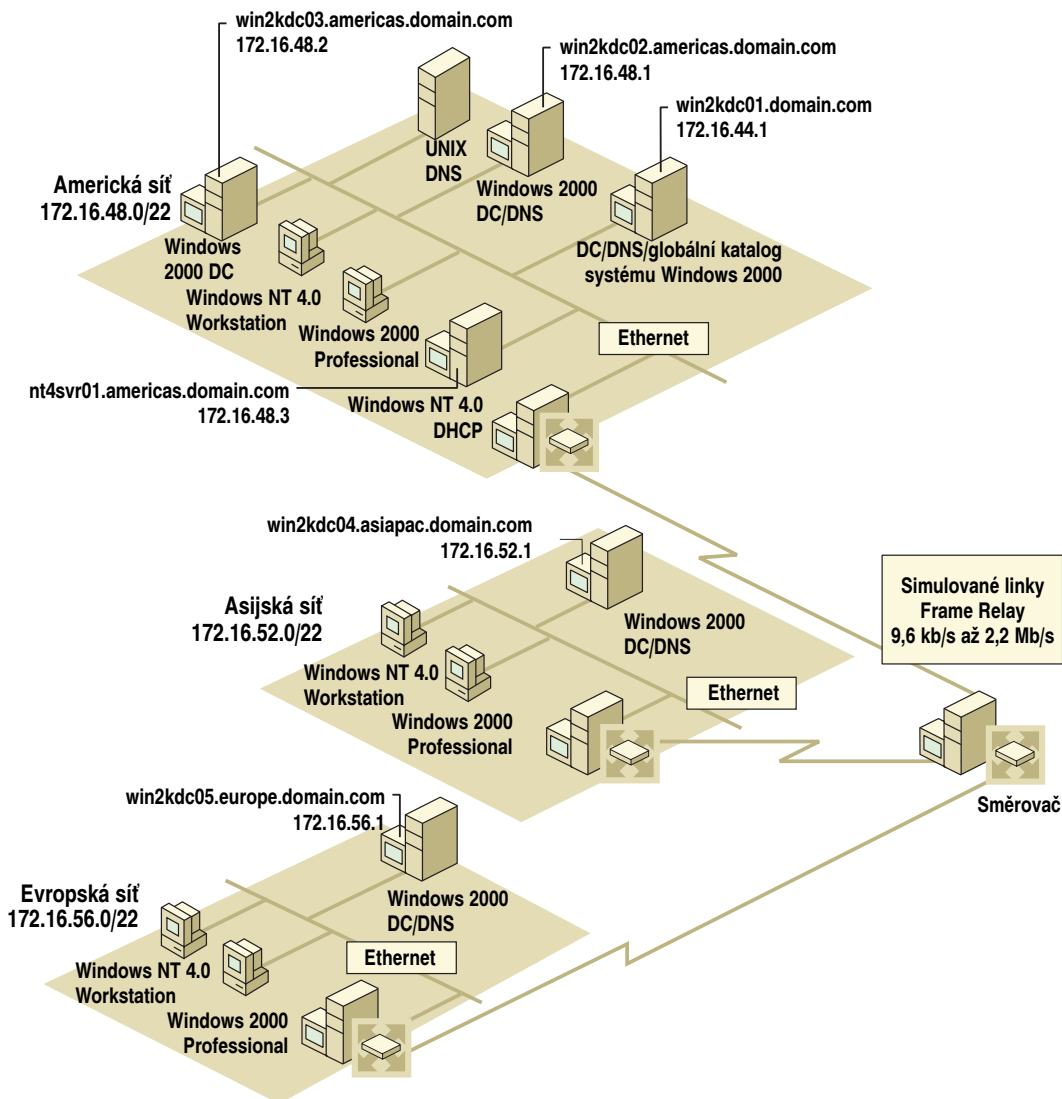
Fyzický diagram

Do fyzického diagramu uveďte následující informace:

- Síťové součásti, jako:
 - směrovače a mosty,
 - rozbočovače,
 - simulátory linek,
 - proxy-servery,
 - nástroje sledování a generátory provozu,
 - analogové linky a linky ISDN,
 - spojení a rychlosti LAN, WAN a na Internet.
- Servery včetně:
 - názvu domény,
 - názvu počítače,
 - adresy IP,
 - funkce serveru.

- Klientské počítače včetně:
 - názvu počítače,
 - adresy IP, pokud používáte statické adresování.

Obrázek 4.6 je příkladem fyzického diagramu. Tento fyzický diagram znázorňuje stejnou laboratoř jako logický diagram na obrázku 4.5. V tomto diagramu vidíte tři podsítě pro tři podřízené domény. Každá podsít má jak nějaký klientský počítač systému Windows 2000 Professional tak i jiný typ klientského počítače. Laboratoř používá simulované linky Frame Relay a obsahuje server systému UNIX.



Obrázek 4.6 Příklad fyzického diagramu testovací laboratoře

Vybudování laboratoře

Jakmile navrhnete a zdokumentujete laboratoř, musí se s plánem seznámit podtýmy projektu a potvrdit, že byly zajištěny všechny potřebné podmínky. Když je schválen plán laboratoře, můžete začít získávat a instalovat příslušný hardware a software.

Plánujete-li periodicky přebudovávat laboratoř při změnách zaměření testování, zvažte k řízení změn v laboratoři použití speciálních nástrojů nebo produktů, jako je například server SMS. Také se zamyslete nad použitím funkce vzdálené instalace operačního systému, což vám pomůže rychle měnit konfigurace klientských počítačů v laboratoři. Další informace o použití vzdálené instalace OS k automatizování instalací klientských počítačů najdete v kapitole „Automatizování instalace a inovace klientů“ v této knize. Rozhraní Active Directory Service Interfaces (ADSI) a nástroj Windows Script Host vám pomohou rychle vytvořit, odstranit nebo změnit uživatele, skupiny a organizační útvary (jednotky) v laboratorním prostředí.

Při budování a úpravách laboratoře dokumentujte chronologicky všechny změny serverů a klientských počítačů. Tato dokumentace vám pomůže vyřešit problémy a pochopit, proč se nějaký počítač chová právě tak, jak se chová. Pomůže vám také vrátit nedávno změny a vyřešit tak krátkodobé problémy.

Budování laboratoře zahrnuje následující kroky:

- Získání hardwaru a softwaru včetně nástrojů pro správu.

Vybavení můžete zakoupit nebo použít z jiných míst. To záleží na vašem rozpočtu a vybraném modelu laboratoře. V obou případech je však důležité získat vybavení, které odpovídajícím způsobem otestuje zavádění a které odráží stav vašeho produkčního prostředí.

Ujistěte se, že se použitý hardware nachází na seznamu Microsoft Hardware Compatibility List (HCL). Můžete také kontaktovat prodejce a zjistit, zda jsou vaše produkty připraveny na systém Windows 2000. Zjistěte, zda vaši prodejci aktivně podporují daným hardwarem systém Windows 2000.

Jako hardware a software použijte stejné modely od stejných výrobců, jaké budou použity také v produkčním prostředí. Tento princip platí pro:

- rozbočovače, přepínače, směrovače a mosty,
 - síťové adaptéry,
 - hardware a operační systém serverů,
 - hardware a operační systém klientských počítačů.
- Nainstalujte a nakonfigurujte síťové součásti. Označte síťové kabely.
 - Otestujte všechna síťová spojení.

Testování sítě před instalací serverů zajistí snazší vyhledávání a řešení problémů.

- Nainstalujte a nakonfigurujte servery.

Pokud používáte již někde jinde nasazené servery, může být zapotřebí je inovovat, aby mohly provozovat systém Windows 2000 Server. Použijte stejnou velikost paměti, kapacitu disku a rychlost procesoru, jaké se budou vyskytovat i v produkčním prostředí. Nezapomeňte na antivirovou kontrolu a defragmentaci pevných disků.

Nainstalujte příslušný operační systém, buď Windows 2000 Server nebo operační systém, jehož inovaci plánujete. Pevné disky rozdělte stejným způsobem, jak to plánujete učinit během zavádění.

Jestliže inovujete řadiče domén, tyto servery ještě před inovací zálohujte. Otestujte zálohy a uložte je na bezpečné místo. Vytvoříte-li si spolehlivé zálohy, vyhnete se tak zásahům do produkčního prostředí v případě změny nebo selhání procesu inovace. Navíc bude snadné obnovit původní stav serverů.

Jestliže kupujete nové vybavení, komponenty nejprve dva až tři dny zkoušejte. Jen tak se ujistíte, že pracují správně.

- Aplikční software nainstalujte, jakmile budete připraveni na jeho testování. Nainstalujte všechny serverové aplikace, jako je Microsoft BackOffice, a obchodní či výrobní aplikace, které se vyskytují ve vašem produkčním prostředí.

Vybudujte nebo nahrajte kopie příslušných databází. Nainstalujte nástroje správy, které používáte nebo plánujete používat.

- Nainstalujte nástroje pro testování a správu. Plánujete-li ověřit síťový provoz nebo otestovat výkon, použijte hardwarový nebo softwarový nástroj sledování.
- Jestliže implementujete terminálové služby, nainstalujte reprezentativní sadu aplikací, abyste mohli vyzkoušet současnou práci více uživatelů.
- Nainstalujte a nakonfigurujte všechny klientské počítače.
- Plánujete-li vytvořit zálohy pro obnovení základních konfigurací, vytvořte tyto základní konfigurace a zálohujte je.

Jestliže například plánujete inovovat systémy Windows 95 na systémy Windows 2000 Professional a nevykonávat tedy čisté instalace, zálohujte klientské počítače se systémem Windows 95, na kterých jsou nahrány standardní aplikace.

Základní konfigurace by měly obsahovat všechny servisní balíky, které jsou ve vašem prostředí podporovány. Nezapomeňte otestovat a zdokumentovat proces obnovení.

- Otestujte jednotlivé součásti v laboratoři, čímž se vám podaří izolovat problémy nespojující se systémem Windows 2000 Server a zaváděním.

Jakmile začnete testovat, bude vaším zájmem trávit čas nad odhalováním problémů zavádění a nikoli nad řešením problémů s laboratoří.

- Potřebujete-li zajistit konektivitu k produkční síti, nakonfigurujte a otestujte směrovače tak, aby laboratoř izolovaly od produkčního prostředí.

Řízení laboratoře

Bude-li vaše laboratoř trvalá nebo ji bude využívat mnoho skupin, bude asi zapotřebí určit někoho k jejímu řízení. To je důležité zejména v případě, bude-li laboratoř využívána k testování několika skupinami během procesu řízení změn. Menší laboratoře nebo laboratoře používané jediným týmem nemusejí mít svého řídicího pracovníka. I když se rozhodnete nezřizovat funkci řídicího pracovníka laboratoře, alespoň vyberte někoho, kdo bude za laboratoř zodpovídat.

Bez ohledu na rozhodnutí ohledně vedoucího laboratoře vytvořte dobrý komunikační systém, který bude šířit informace o dostupnosti a stavu laboratoře. Uživatelé laboratoře musejí vědět, kdy budou moci vykonat své vlastní testy, zda jejich testování naruší nějaké jiné testy a v jakém stavu se laboratoř nachází. Pokud se například nějaká doména v laboratoři používá pro testování procesu migrace i funkcí kombinovaného režimu, uživatelé laboratoře musejí vědět, zda jsou počítače připraveny na inovaci nebo již byly inovovány.

Rozhodnete-li se jmenovat vedoucího laboratoře, zvažte výhody a náklady na dalšího pracovníka s faktory svěřením této role nějakému členovi týmu projektu. Vaše rozhodnutí závisí na velikosti a složitosti laboratoře. Další povinnosti vedoucího laboratoře mohou být ve spojení s jinou odpovědností ohledně projektu již příliš náročné.

Zodpovědnost řízení laboratoře

Vedoucí laboratoře zodpovídá za následující typy úkolů:

- Zajištění hardwaru a softwaru.
- Řízení chodu sítě a kapacity a konfigurace serverů.
- Řízení hardwarových a softwarových konfigurací a inovací.
- Koordinace testů mezi podtýmy (kdo testuje a kdy).

Vyžadují-li testy změnu konfigurace serverů nebo klientů, tyto změny je zapotřebí časově naplánovat a oznámit dalším uživatelům laboratoře.

- Vývoj a sledování procesu řízení změn.

Proces řízení změn definuje, kdo je oprávněn měnit laboratorní prostředí.

- Udržování dokumentace laboratoře (jako je popis laboratoře, diagramy a procesy).
- Zajištění fyzického zabezpečení.

Vedoucí laboratoře zajišťuje, že není možné zařízení laboratoře neoprávněně používat, a přístup do laboratoře omezuje pomocí klíčů a elektronických zámek.

- Vytvoření systému kontroly inventáře.
- Vytvoření rozpočtu laboratoře.
- Označení hardwaru včetně kabelů.
- Vyřešení problémů prostředí.
- Implementace programu preventivní údržby vybavení.
- Ustanovení procesu souhlasu s odstraněním zařízení (například zapůjčení).
- Periodické zálohování serverů.
- Zajištění čistoty a pořádku v laboratoři.

Vedoucí laboratoře je také zodpovědný za zajištění co nejvyšší možné využitelnosti a pružnosti laboratoře. Všechny procesy navržené ke splnění uvedených úkolů musejí usnadnit a nikoli omezit využívání laboratoře.

Vývoj pravidel laboratoře

Doporučujeme vám vyvinout a implementovat pravidla stanovující, jak mohou členové týmů používat laboratoř. Vytvořte pravidla, která se snadno pamatují a plní, obecně spíše z hlediska vyjasňování a nikoli diktování. Identifikujte a zdokumentujte tyto oblasti:

Pravidla a zodpovědnost.

Určete, kdo zodpovídá za úkoly, jako je plánování časového využívání laboratoře a vykonávání záloh.

Prostředky a pravidla pro speciální typy testů.

Identifikujte například domény a konfigurace, které mají členové týmů používat pro testování procesu migrace.

Pravidla řízení změn laboratoře.

Identifikujte, kdo může zadávat změny konfigurací. Definujte proces schvalování požadavků na změny. Určete například, kdo může měnit schéma a kdo musí být na takovou změnu upozorněn. Definujte dokumentaci vyžadovanou při jakékoli změně v laboratoři.

Inicializace procedur pro servery.

Dokumentujte kroky instalování, konfigurování a zaplňování řadičů domén a členských serverů daty. Nebudete-li používat systém DNS zabudovaný do Windows 2000, nezapomeňte na nastavení DNS.

Procedury obnovení laboratoře pro testování postupného zavádění.

Dokumentujte kroky obnovení řadičů domén do původního stavu a obnovení dat uživatelských účtů. Dokumentujte všechny serverové konfigurace. Ještě před začátkem testování migrace vyzkoušejte proces obnovení.

Procedury obnovení klientských počítačů.

Plánujete-li často přebudovávat klientské počítače v zájmu testování různých konfigurací, dokumentujte nástroje používané k rychlému obnovení do známého počátečního stavu. Můžete například používat službu RIS.

Testování

Dobré testování omezuje rizika, kterým je vystaveno vaše obchodní či výrobní prostředí při zavádění změn do produkčního prostředí. Zevrubné testování však vyžaduje pečlivé plánování. Chcete-li, aby vaše testy přesně odrážely funkci představovaného návrhu, musíte je vytvořit tak, aby realisticky reprezentovaly podmínky a variace ve vašem prostředí. Ani dobře navržená laboratoř nezachrání špatně navržený test.

Jako klíčová součást řízení testování rizik:

- ověřuje, že váš návrh naplňuje obchodní či výrobní a technické požadavky určené pro projekt zavádění systému Windows 2000,
- odhaluje potenciální rizika pro produkční prostředí,
- odhaluje potenciální rizika pro časový plán projektu.

Při plánování testů pamatujte, že není možné vyzkoušet úplně všechno. Nepokoušejte se tedy otestovat každou kombinaci, ale soustředte se na limity. Otestujte například nejpomalejší klientský počítač, obchodní či výrobní server nebo nejméně spolehlivé síťové spojení. Navíc se zaměřte na oblasti s největším rizikem nebo nejvyšší pravděpodobností výskytu. Je důležité udržet sadu testů ve formě, která se dá řídit.

Testování probíhá během celého projektu a vyvíjí se od testování na úrovni součástí (neboli jednotek) k testování integrace takto:

Testy jednotek

Tyto testy ověřují řádné vykonávání jednotlivých funkcí, součástí nebo aplikací. Testování jednotek začíná v okamžiku začátku vytváření návrhu a pokračuje až do okamžiku, kdy je návrh stabilní. Ve spojení s návrhem je iterační – výsledky testů ověřují předkládaný návrh a vedou ke změnám. Testy jednotek obvykle vykonávají architekti a vývojáři.

Testy integrace

Tyto testy ověřují dobrou spolupráci funkcí a součástí. Zatímco testy jednotek se do hloubky zabývají jednotlivými součástmi, testy integrace se zabývají fungováním celého systému.

K testování integrace dochází až po testování jednotek, když je již návrh stabilní. Jakmile je návrh vytvořen, testy jsou stále složitější a integrovanější, až nakonec zahrnují plně spolupracující funkce a součásti. Testy integrace vyžadují plně vybavenou testovací laboratoř, kde mohou pracovníci testování dokonale řídit testovací konfigurace a podmínky.

Doporučujeme, aby testy integrace vykonávala jiná skupina než návrháři. Mnoho organizací má týmy testování, které plánují a vykonávají testování integrace. Kromě ověření správné funkce technologie se musí pracovníci testování integrace podívat na výsledky také z hlediska obchodního či výrobního. Musejí se zamyslet nad tím, jak budou s daným řešením pracovat koncoví uživatelé a jak se řešení v tomto použití osvědčí. Musejí také ověřit, že navrhované řešení naplňuje obchodní či výrobní a technické požadavky kladené na projekt Windows 2000.

Definice a eskalace plánů

Ještě než začnete testovat, definujte plán předávání problémů, který tým projektu použije, objeví-li se nějaké problémy. Tento plán se musí zabývat následujícími otázkami:

- Kam členové týmu oznámí selhání testů a další problémy? Zaznamenají tyto okolnosti do systému sledování událostí, nebo je zaznamenají jinak, například na nějaké webové adresy?
- Jak budou postupovat, ještě než problém předají k řešení? Je například zapotřebí tento problém reprodukovat? Kdo jej bude reprodukovat?
- Jaké informace musejí postoupit při předávání problému k řešení? Příklady jsou:
 - Kontaktní informace (telefonní číslo, číslo pageru a adresa elektronické pošty vedoucího podtýmu a externí podpory)
 - Stav problému (nový nebo již odhalený)
 - Priorita a obchodní či výrobní ospravedlnění problému
 - Pořadí událostí vedoucích k problému (včetně odpovídajících informací, jako je adresa IP a název domény)
 - Příčiny (známé nebo předpokládané)
 - Informace o řešení (stopy, diagnostika)
- Jakým způsobem upozorní skupinu návrhu na daný problém?
- Kdo problém prostuduje a vyřeší?
- Jaká je hierarchie upozorňování?

Vytvoření plánu testování

Již na počátku plánování systému Windows 2000 by měl každý podtým návrhu napsat testovací plán, který popisuje, jak se bude testovat jejich specifická technologie. Například tým práce v síti může vytvořit plán testování popisující, jak se budou testovat funkce práce v síti. Všichni členové podtýmu by si měli plán ještě před začátkem testování prostudovat a vyjádřit s ním souhlas. Z plánů testování se vyvinou testovací případy (neboli scénáře), které popisují, jak se budou jednotlivé funkce nebo prvky testovat.

vat. Testovací případy jsou podrobněji vysvětleny v oddílu „Návrh testovacích případů“ dále v této kapitole.

Plán testování platí jak pro testování jednotek, tak integrace. Poskytuje celkový rámec testování, a měli byste se zabývat dále uvedenými tématy.

Rozsah a cíle

V tomto oddílu plánu testování popište, čeho se vaše testování bude a nebude týkat. Své testování hardwaru klientských počítačů můžete například omezit na minimální podporované konfigurace nebo na standardní konfigurace.

Popište, čeho chcete svým testováním dosáhnout. Cílem jedné organizace byla například migrace prostředí Windows NT 4.0 do prostředí Windows 2000 postupně po součástech, přičemž seznamy řízení přístupu (Access Control List – ACL) a povolení Exchange měly zůstat nedotknuté. Cílem jiné organizace bylo změřit síťový provoz a sledovat výkon serverů během určitých úkolů adresářové služby.

Metodologie testování

Popište obecnou strategii použitou při testování. Vaší strategií testování změn schéma může být například nakonfigurovat izolovanou doménu v laboratoři, kde bude možné aplikovat změny schéma, aniž by to ovlivnilo jiné laboratorní testy. Tento oddíl plánu testování může obsahovat následující popisy:

- Architektura domén použitá pro test
- Nástroje a techniky použité k vykonání testů nebo měření výsledků
- Automatizované techniky použité pro testy

Vyžadované zdroje

Uvedte následující typy prostředků, které potřebujete k podpoře testování:

Hardware

Identifikujte například standardní konfigurace, které plánujete podporovat u klientských počítačů. Nezapomeňte na součásti, jako jsou grafické karty, modemy a externí jednotky.

Software

Do seznamu produktů, které potřebujete otestovat, zahrňte například Microsoft BackOffice nebo jiné serverové produkty.

Databáze

Určete také databáze, které pro testování aplikací potřebujete. Doporučujeme vám zahrnout také popis prostředků, jako jsou data o osobách a produkci, která potřebujete k zaplnění databáze.

Personál

Uvedte potřebný počet pracovníků testování a požadovanou úroveň znalostí. Nezapomeňte na konzultanty a další personál technické podpory.

Školení

Specifikujte školení v oblasti systému Windows 2000, jaké vaši testovací pracovníci potřebují, aby rozuměli testované technologii.

Nástroje

Zahrňte sem také například simulátory sloužící k testování spojení WAN, nemáte-li druhou laboratoř, kterou byste mohli pro tento účel využít. Uvedte všechny nástroje, které potřebujete k automatizování testování a sledování výsledků testů.

Funkce a prvky

Vytvořte seznam všech funkcí nebo aspektů funkcí, které se budou testovat. Jedná se o seznam testovaných položek, který nepopisuje, jak se bude testovat. Některé organizace uvádějí seznam testů do přílohy plánu testování. Jiné organizace vytvářejí samostatný dokument neboli specifikaci testů, který uvádí všechny testy a krátce popisuje, čeho se musejí jednotlivé testy týkat. Další organizace zase zahrnují seznam testů jako úkoly do časového plánu projektu.

Dále je uveden příklad specifikace testů jedné organizace:

Test 1 - Zachování vztahů důvěryhodnosti

Popis: Všechny vztahy důvěryhodnosti z domény a do ní je zapotřebí zachovat i po inovaci řadičů domény na systém Windows 2000. Ke zobrazení vztahů důvěryhodnosti použijte nástroj Domain Tree Manager. Pokud se tyto vztahy důvěryhodnosti neobjeví, test nebyl úspěšný.

Všimněte si, že popis neobsahuje instrukce, jak se má test vykonat.

V pozdějších fázích projektu vytvoří členové týmu podrobné procedury popisující, jak se vykonají jednotlivé testy uvedené v plánu testování. Oddíl „Návrh testovacích případů“ dále v této kapitole poskytuje více informací o vývoji procedur testování.

Váš plán testování by se měl zabývat následujícími typy testů:

- Funkčnost každého implementovaného prvku a služby.
- Spolupráce s existujícími součástmi a systémy v produkčním prostředí během postupného zavádění i po něm. Tyto testy zahrnují kombinované prostředí, které se bude vyskytovat během postupného zavádění systému, i prostředí systému Windows 2000, které se objeví po dokončení postupného zavádění.
- Kompatibilita hardwaru a ovladačů všech typů počítačů, na kterých poběží systém Windows 2000.
- Kompatibilita všech aplikací, které budou pracovat na systému Windows 2000.
- Testy základní linie a zátěže při plánování kapacity.
- Základní linie pro sledování výkonu.
- Optimalizace konfigurací jako jsou standardizované plochy na klientských počítačích.
- Procedury správy při zavádění systému a po jeho dokončení, jako je inovace klientského počítače a plány návratu k předchozí konfiguraci.
- Nástroje.

Další informace o plánování testování kompatibility aplikací najdete v kapitole „Testování kompatibility aplikací se systémem Windows 2000“ v této knize.

Rizika

Popište známá rizika, která mohou zamezit úspěšnému testování. Testovací laboratoř nemusí například plnit časový plán, hardware či software nemusí být k dispozici nebo mohou pracovníci testování pracovat na jiných projektech či vyžadovat další školení.

Časový plán

Náčrtněte časový plán zahrnující všechny testy uvedené v plánu testování. Časový plán vám pomůže koordinovat využití laboratoře s jinými podtýmy.

Návrh testovacích případů

Testovací případ je podrobná procedura, která plně testuje nějakou funkci nebo její aspekt. Zatímco plán testování popisuje, co se bude testovat, testovací případ popisuje, jak se konkrétní test vykoná. Testovací případ musíte vyvinout pro každý test uvedený v plánu testování nebo specifikaci testování.

Testovací případy musí napsat někdo, kdo rozumí testované funkci nebo technologii, a případy musejí projít další kontrolou.

Testovací případy obsahují například následující informace:

- Účel testu
- Speciální hardwarové požadavky, například modem
- Speciální softwarové požadavky, například nějaký nástroj
- Konkrétní požadavky na nastavení nebo konfiguraci
- Popis způsobu vykonání testu
- Očekávané výsledky nebo kritéria úspěchu testu

Návrh testovacích případů může být časově náročná fáze testování. Možná vás bude lákat této fázi se příliš nevěnovat, strávený čas se však z dlouhodobého hlediska vyplácí. Máte-li testy pečlivě naplánované, můžete je vykonat rychleji. Jinak testovací pracovníci stráví mnoho času laděním a opakovaným spouštěním testů.

Organizace používají k dokumentování testovacích případů mnoho různých přístupů, které sahají od vývoje podrobných kroků až po vytvoření obecných popisů. V podrobných testovacích případech jednotlivé kroky přesně popisují, jak se má test vykonat. V popisných testovacích případech se testovací pracovník rozhoduje až v okamžiku skutečného testování, jak se test vykoná a jaká data se použijí.

Výhodami podrobných testovacích případů je jejich reprodukovatelnost a snazší automatizace. Tento přístup je důležitý, zejména plánujete-li porovnávat výsledky v čase například při optimalizaci konfigurací. Nevýhodnou podrobných testovacích případů je, že jejich vývoj a údržba je časově náročnější. Na druhou stranu testovací případy s otevřenou interpretací nelze zopakovat a mohou vyžadovat další čas pro ladění, který se vztahuje spíše k samotnému testu a nikoli testované otázce.

Doporučujeme vám nalézt kompromis mezi těmito dvěma extrémami, který se bude spíše přiklánět více k podrobnostem. Při snaze dosáhnout integrity a spravovatelnosti testu vyrovnejte zevrubnost s praktičností.

Tabulka 4.1 poskytuje příklad několika prvních kroků podrobného testovacího případu.

Tabulka 4.1 Ukázkový testovací příklad

Krok	Procedura	Kritéria úspěchu	Výsledek
1	Odhlaste se za serveru a vraťte se k obrazovce přihlášení k síti.	Žádná.	
2	Otevřete si seznam domén.	Název místního serveru se nesmí objevit v seznamu.	
3	Otevřete si seznam domén.	Kořenová doména se musí objevit v seznamu.	
4	K serveru se přihlaste pomocí účtu s oprávněními správce.	Účet se bez problémů musí přihlásit k serveru.	

Řízení testů

Ještě než začnete s testováním, upravte nastavení laboratoře tak, aby splňovalo požadavky určené v testovacím případě. Při vykonávání testů postupujte pečlivě podle napsaného testovacího případu. Ke správnému vyhodnocení výsledků nebo k reprodukování testu musíte znát přesné kroky, které testovací pracovník vykonal.

Při vykonávání testů analyzujte výsledky ve vztahu ke kritériím v testovacím případě a určete, zda byl test úspěšný nebo neúspěšný. Pokud byl test neúspěšný, může problém spočívat v samotném testu, v nastavení laboratoře nebo v předkládaném návrhu. V případě neúspěšných testů zvažte tento postup:

Problém s testovacím případem.

Přepracujte testovací případ, test znovu spusťte a dokumentujte všechny vykonané změny.

Problém s nastavením laboratoře.

Postupujte podle procesu řízení změn v laboratoř, překonfigurujte ji a test znovu spusťte.

Problém s návrhem.

Postupujte podle procedury předávání problémů projektu a na situaci upozorněte příslušné osoby. Vytvořte priority mezi nevyřešenými problémy a sledujte je až do jejich úspěšného vyřešení a opakovaného otestování. Při vytváření priorit problémů uvažujte potenciální vliv a pravděpodobnost, že daná situace nastane.

Dokumentování výsledků testů

Problémy a chyby sice možná již zaznamenáváte do systému sledování událostí, potřebujete však ještě sledovací systém pro zaznamenávání výsledků testů. Sledovací systém vám pomáhá monitorovat postup a poměr úspěšnosti testování. Tyto informace jsou užitečné při vytváření zpráv pro management, zobrazování trendů a vyhodnocování úrovně personálu.

Některé organizace používají nějaký papírový systém a dokumentují výsledky testů na listy testovacích případů. Takový papírový systém však znesnadňuje sledování všech otestovaných případů a vytváření zpráv a sestav.

Jednou z alternativ je zakoupení komerčního produktu, který sleduje a vytváří sestavy testovacích případů. Jinou je vyvinout svou vlastní databázovou aplikaci a testy v ní or-

ganizovat a řídit. Pomocí těchto přístupů můžete automatizovat vytváření sestav sledujících výsledky testů a celkový postup. Ať už zvolíte jakoukoli metodu, je důležité, aby členové týmu projektu mohli k záznamu testů snadno přistupovat. Další informace o vytvoření systému sledování testů najdete v kapitole „Testování kompatibility aplikací se systémem Windows 2000“ v této knize.

Ať už se rozhodnete sledovat testy jakkoli, důležité je dokumentovat výsledky každého testu. Nezapomeňte na informace, jako jsou tyto:

- Jméno a oddělení testovacího pracovníka
- Datum a čas vykonání testu
- Název produktu systému Windows 2000 (Server nebo Professional)
- Úplný popis výsledků
- Vyřešení problémů
- Čísla problémů zadaná do systému sledování událostí

Testování po zavedení systému

Budete-li svou laboratoř využívat jako součást procesu řízení změn, může být cenná i dlouho po dokončení zavádění systému Windows 2000. Testování změn počítačového prostředí – ať už přidáváte nové součásti infrastruktury sítě, instalujete nové servery, měníte výrobce klientských počítačů, měníte konfigurace nebo implementujete servisní balíčky a opravy – je velmi důležité.

Nestačí však jen mít k dispozici laboratoř, třeba i dobře navrženou a vybavenou. Maximalizace efektivity laboratoře dosáhnete tak, že budete definovat její použití k implementování změn v produkčním prostředí. Nezapomeňte pravidelně vyhodnocovat součásti laboratoře a určovat vliv nahromaděných změn. Například počítač s mnoha aplikovanými změnami se již nemusí chovat stejně jako počítač se stejnou konfigurací, který byl nově instalován.

Použití laboratoře pro změnový management

Laboratoř řízení změn je místo, kde testujete navrhované změny ještě před jejich implementováním do produkčního prostředí a to včetně pilotního zavedení. Jakmile k řízení změn použijete laboratoř, stane se součástí většího procesu. Tento proces identifikuje tok informací a pořadí činností od okamžiku navržení změny až do okamžiku jejího implementování. Vyvinutý proces závisí na typu vykonávaných změn, využitých týmech a procesu fungování společnosti.

Se sestavením procesu řízení změn v prostředí IT vám pomůže mnoho prostředků. Prvním krokem je vytvoření plánu řízení změn. Než začnete tento plán psát, zamyslete se nad následujícími problémy:

- Kdo změny autorizuje?
- Jak se dokumentuje a předává návrh?
- Kdo návrh analyzuje a určuje jeho důležitost a dopady?
- Jakou roli tu hrají metody a procedury (včetně laboratoře)?
- Jak se dokumentuje a hlásí stav změny?

Testování v laboratoři je jedním krokem v procesu zavedení změn do produkčního prostředí. Mnoho organizací testuje každou opravu a servisní balíček, pak teprve umožňu-

je jeho zavedení do pilotního projektu nebo jiné omezené zavedení. Budete-li změny testovat v různých scénářích a situacích, výrazně tím omezíte možnost vzniku problémů během implementování.

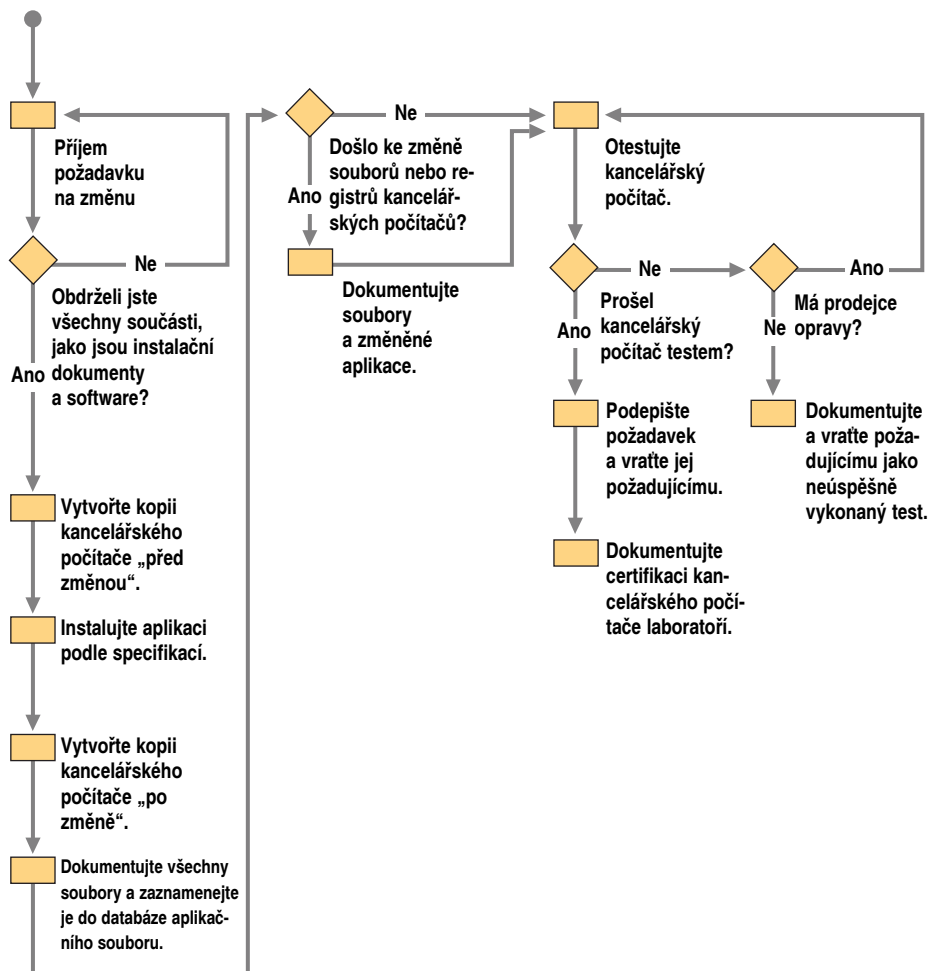
Definování role laboratoře v změnovém řízení

Je tedy důležité zahrnout do procesu implementování změn testování v laboratoři. Je také důležité definovat, jak se v tomto procesu používá laboratoř. Možnost přehlédnutí nějakého aspektu v laboratoři můžete omezit popisem kroků a požadavků obecně platících pro změny. Je například vhodné identifikovat tyto položky:

- Součásti vyžadované před implementováním změny v laboratoři.
- Kroky vyžadované k implementování změny.
- Dokumentace vytvářená v laboratoři.
- Akce vykonaná v případě neúspěchu laboratorního testu.
- Akce vykonaná v případě úspěchu laboratorního testu.

Obrázek 4.7 ilustruje, jak jedna významná organizace používá svou laboratoř klient-ských počítačů k testování změn standardních konfigurací kancelářských počítačů.

Začátek



Obrázek 4.7 Ukázkové použití laboratoře v procesu řízení změn

Seznam úkolů plánování laboratorního testování

Následující dva seznamy úkolů použijte při plánování testování zavádění systému Windows 2000. První tabulka vám pomůže s přípravou laboratoře a druhá s vytvořením, spuštěním a zdokumentováním testů.

Seznam úkolů přípravy laboratoře

Tabulka 4.2 shrnuje úkoly, které musíte vykonat při návrhu a budování testovací laboratoře.

Tabulka 4.2 Seznam úkolů přípravy laboratoře

Úkol	Umístění v kapitole
Vyberte model laboratoře.	Určení strategie laboratoře
Vyberte jedno nebo více umístění laboratoře.	Určení strategie laboratoře
Vytvořte předběžnou laboratoř (je-li zapotřebí).	Vytvoření předběžné laboratoře
Určete požadavky na prostor a prostředí laboratoře.	Návrh laboratoře
Určete požadavky na napájení a síťová připojení laboratoře.	Návrh laboratoře
Navrhněte a zdokumentujte logickou a fyzickou konfiguraci laboratoře.	Návrh laboratoře
Určete hardwarové požadavky.	Návrh laboratoře
Určete softwarové požadavky včetně obchodních či výrobních aplikací a nástrojů.	Návrh laboratoře
Určete, kdo potřebuje laboratoř používat.	Návrh laboratoře
Určete databázové požadavky.	Návrh laboratoře
Určete plány vedení kabelů a vytvoření sítě.	Návrh laboratoře
Získejte hardware včetně kabelů a software.	Vybudování laboratoře
Obstarejte vybavení pracovního prostoru, jako jsou stoly, židle, tabule, lampy, telefony a police.	Vybudování laboratoře
Vybudujte a nakonfigurujte síť.	Vybudování laboratoře
Otestujte konektivitu sítě.	Vybudování laboratoře
Vybudujte a nakonfigurujte servery.	Vybudování laboratoře
Nainstalujte aplikace a vybudujte databáze na serverech.	Vybudování laboratoře
Nainstalujte nástroje pro testování a správu.	Vybudování laboratoře
Vybudujte a nakonfigurujte klientské počítače.	Vybudování laboratoře
Nainstalujte aplikace na klientské počítače.	Vybudování laboratoře
Otestujte všechny součásti laboratoře.	Vybudování laboratoře
Jmenujte vedoucího laboratoře.	Řízení laboratoře
Definujte proces řízení změn pro laboratoř.	Vývoj pravidel laboratoře
Vytvořte, otestujte a zdokumentujte proces obnovení laboratoře.	Vývoj pravidel laboratoře

Seznam úkolů testování

Tabulka 4.3 shrnuje úkoly testování, které musíte vykonat.

Tabulka 4.3 Seznam úkolů testován

Úkol	Umístění v kapitole
Napište plán testování.	Vytvoření plánu testování
Vybudujte testovací případy.	Návrh testovacích případů
Vyvíjte proceduru předávání problémů k řešení.	Definování plánu předávání problémů
Vykonejte testy a vyhodnoťte výsledky.	Vykonání testů
Dokumentujte výsledky testů.	Dokumentování výsledků testů

KAPITOLA 5

Vykonání pilotního programu systému Windows 2000



Pilotní program je poslední důležitý krok před plnohodnotným zavedením systému Microsoft Windows 2000. Ještě před pilotním programem musíte dokončit testování integrace v laboratorním prostředí. Během pilotního programu testujete svůj návrh v řízeném prostředí skutečného světa, v němž uživatelé vykonávají své normální obchodní či výrobní činnosti pomocí nových funkcí.

Ještě dlouho před zavedením pilotního programu musí manažer projektu a návrháři systémů naplánovat, kde a jak se pilotní program uskuteční. Tato kapitola vám pomůže vytvořit pilotní plán, vybrat uživatele a sídla, a určit, jak se pilotní prostředí vytvoří a nastaví.

V této kapitole

Přehled vykonání pilotního programu 118

Vytvoření pilotního plánu 120

Příprava na pilotní program 124

Zavádění pilotního programu 126

Vyhodnocení pilotního programu 126

Seznam úkolů plánování vykonání pilotního programu 128

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Pilotní plán
- Procedura postupného pilotního zavádění

Související informace v sadě Resource Kit

- Další informace o testování před pilotním programem najdete v kapitole „Vytvoření testovací laboratoře systému Windows 2000“ v této knize.
- Další informace o migrování na systém Windows 2000 ze systému Microsoft Windows NT verze 3.51 či novějšího najdete v kapitole „Určení strategií migrace domén“ v této knize.
- Další informace o automatizování instalace systému Windows 2000 na servery najdete v kapitole „Automatizování instalace a inovace serveru“ v této knize.

- Další informace o automatizování instalace systému Windows 2000 na klientské počítače najdete v kapitole „Automatizování instalace a inovace klientů“ v této knize.

Přehled vykonání pilotního programu

Jakmile ověříte svůj návrh systému Windows 2000 v testovacím prostředí, musíte jej ještě ověřit s využitím omezeného počtu uživatelů v produkčním prostředí. Pilotní program snižuje rizika vzniku problémů během zavádění do celé struktury.

Hlavními cíli pilotního programu je demonstrovat, že váš návrh pracuje v produkčním prostředí podle očekávání a že naplňuje obchodní či výrobní potřeby vaší organizace. Druhotným důsledkem je skutečnost, že pilotní program dává týmu instalace šanci vyzkoušet si v praxi a doladit proces zavádění.

Pilotní program nabízí uživatelům možnost reagovat na funkce určitých prvků. Tuto zpětnou vazbu použijte k vyřešení problémů či k vytvoření kontingenčního plánu. Zpětná vazba vám také pomůže určit úroveň technické podpory, kterou budete pravděpodobně potřebovat po plném zavedení. V konečném důsledku vede pilotní program k rozhodnutí o následném plném zavedení nebo o jeho zpomalení, jež umožní vyřešit problémy, které mohou tento proces ohrozit.

Chcete-li minimalizovat rizika během zavádění, vytvořte několik pilotních projektů nebo jejich fází. Můžete mít například jeden pilotní projekt pro návrh oboru názvů, jiný pro standardní konfigurace kancelářských počítačů a model zabezpečení a třetí pilotní projekt pro vzdálené zavádění aplikací.

Pilotní proces

Proces pilotního zavádění je iterační. Zavedete omezený počet počítačů v řízeném prostředí, vyhodnotíte výsledky, opravíte problémy a zavedete další pilotní program. To vše budete provádět tak dlouho, dokud nedosáhnete plného rozsahu a kvality indikujících, že jste připraveni na plné zavedení. Obrázek 5.1 ilustruje základní kroky plánování a vykonání pilotního programu.

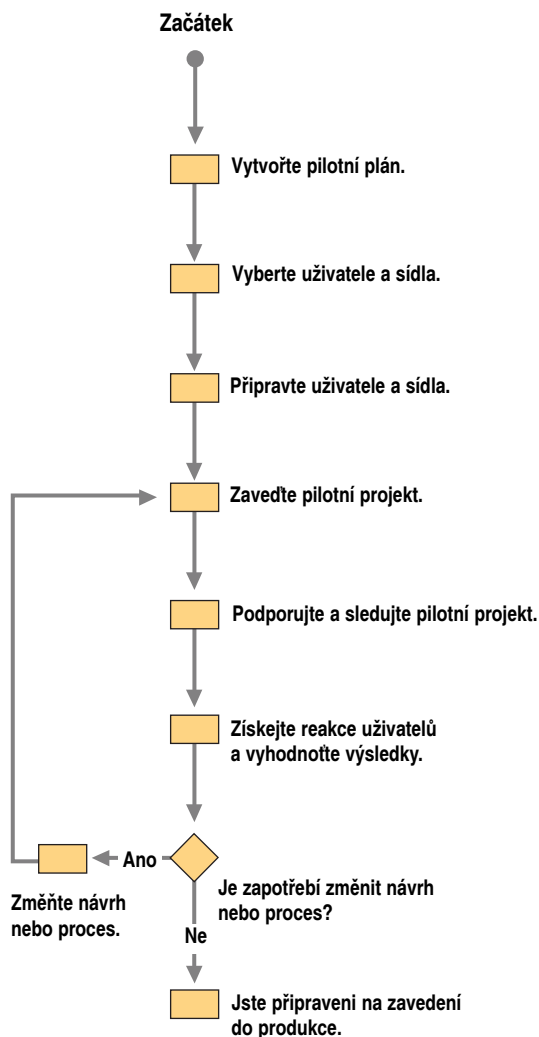
Začněte v oddělení informačních technologií

Plánujete-li více pilotních projektů, začněte s menším rozsahem a ten postupně rozšiřujte. Mnoho organizací používá k vykonání prvního pilotního programu svá oddělení informačních technologií (IT). Začnou zde budovat systém, který emuluje stav, jaký plánují zavést do produkčního prostředí; účastníci používají testovací počítače na testovací síti. Následně tyto organizace postupně přidávají do pilotního programu další personál.

Takový pilotní program v oddělení IT můžete využít také k vyřešení problémů škálovatelnosti a výkonu, protože do systému budete přidávat další a další uživatele. Jakmile vyřešíte všechny problémy, můžete začít s prvním pilotním projektem v produkčním prostředí. V tomto okamžiku zavádíte systém Windows 2000 na produkční počítače koncových uživatelů v obchodních či výrobních jednotkách.

Předpoklady pro vykonání pilotního programu v produkčním prostředí

Ještě než začnete s prvním pilotním projektem v produkčním prostředí, musí být vaše laboratoř stabilní a týmy testování musí dokončit testování integrace a aplikací. Současně návrhu musíte vyhodnotit ještě před jejich implementováním na síť společnosti. Ověř-

**Obrázek 5.1** Proces vykonání pilotního programu

te například protokoly, které plánujete použít, replikační provoz přes spojení rozlehlou sítí (WAN) a postupy zálohování a obnovování. Do pilotního programu nesmíte zavádět žádné nové technologie nebo postupy, které nebyly otestovány v laboratoři. Je-li jedním z cílů vašeho pilotního programu otestovat proces postupného zavádění, pak musí být celý proces důkladně vyvinutý, otestovaný a zdokumentovaný týmem instalace. Vyřešte všechny podstatné problémy návrhu nebo vyvíjte kontingenční plán.

Musíte také vyvinout a ověřit sérii testů, které může tým instalace spustit po inovaci počítačů. Těmito testy se ujistíte o správné funkci instalace, ještě než ji aplikujete na uživatele.

Než začnete se zaváděním pilotního projektu, musíte získat od managementu schválení pilotního plánu. Začněte pracovat na pilotním plánu brzy, abyste v okamžiku, kdy jste připraveni na zavedení pilotního programu, již měli zajištěny komunikační kanály a aby na tuto skutečnost byli připraveni také účastníci projektu.

Vytvoření pilotního plánu

Pilotní program udává tón celého zavádění, takže je důležité pečlivě jej naplánovat, dobře komunikovat s jeho účastníky a výsledky zevrubně vyhodnotit. Vytvoření plánu pro pilotní program vám pomáhá s promyšlením těchto otázek a informování účastníků, co mohou od programu očekávat.

Máte-li více pilotních programů, můžete vytvořit více pilotních plánů. Každý tým může mít například svůj vlastní pilotní program a může si napsat svůj vlastní plán. Váš pilotní program musí zahrnovat tyto položky:

- Rozsah a cíle
- Účastníci a místa
- Plán školení uživatelů pilotního programu
- Plán podpory pilotního programu
- Plán komunikací pilotního programu
- Známá rizika a kontingenční plány
- Plán návratu zpět
- Časový plán zavádění a vykonání pilotního programu

Jakmile máte pilotní plán připravený, požádejte o jeho prostudování a schválení management oddělení IT a management účastnících se obchodních či výrobních jednotek. Pak teprve můžete pokračovat.

Rozsah a cíle

Prvním krokem plánování pilotního programu je definovat, co do něj plánujete zahrnout a co naopak vyloučit (rozsah) a čeho chcete docílit (cíle). Rozsah a cíle definujte jasně, abyste věděli, co můžete od projektu očekávat a abyste mohli vytvořit kritéria úspěšnosti. Je-li to možné, použijte k vytvoření systému měření úspěšnosti pilotního programu své cíle. Měli byste také určit dobu trvání pilotního programu, buď z hlediska časového nebo z hlediska splnění kritérií.

Rozsah pilotního programu

Pilotní program rozšiřuje testování, takže zahrnuje i uživatele pracující na obchodních či výrobních úkolech. Neočekávejte, že budete moci během pilotního programu otestovat naprosto všechny funkce. Zaměřte se na funkce, které představují největší rizika, a události, ke kterým může nejpravděpodobněji dojít.

Rozsah pilotního programu definujte určením, co je a co není jeho součástí. Vytvořte seznam služeb a funkcí, které budou součástí pilotního programu, a uveďte, čeho chcete jejich zavedením docílit. Popište oblasti funkcí, které pilotní implementace ovlivní, do jakého rozsahu a v jakých situacích.

Vytvořte seznam služeb a funkcí, které nebudou součástí pilotního programu. Není-li možné pilotním programem pokrýt určité aspekty vašeho návrhu, popište je. Plánuje-

te-li například inovovat existující architekturu domén a později ji restrukturalizovat, první pilotní program asi nebude obsahovat proces restrukturalizace.

Popište, jaký stav očekáváte po zavedení pilotního programu. Plánujete-li zrušit některé funkce a zachovat jiné, vytvořte příslušné předpoklady. Jestliže si myslíte, že bude lepší později pilotní program zrušit a neponechávat jej v produkčním prostředí, zajistěte v pilotním plánu předpoklady pro návrat k původnímu stavu. Jestliže například měníte návrh oboru názvů, můžete jej po dokončení pilotního projektu zase vrátit zpět. Určení podobných informací v pilotním plánu připraví uživatele s předstihem na to, co mohou očekávat.

Cíle pilotního programu

Přesně určete cíle, které musí váš pilotní program naplnit. Tyto cíle použijte k určení kritérií měření úspěchu pilotního zavádění. Mnoho organizací má podobné základní cíle:

- Zajištění řádné funkce systému v podnikovém prostředí.
- Zajištění, že návrh naplňuje obchodní či výrobní požadavky.
- Zajištění podpory projektu zavádění systému Windows 2000 ze strany uživatelů.

Mnoho organizací má další cíle, jako jsou:

- Otestování procesu zavádění.
- Proškolení týmu instalace.
- Vytvoření dokumentace pro plné zavádění.
- Vyškolení týmů technické podpory.
- Sběr informací pro odhad budoucích potřeb podpory.
- Vyškolení týmů správy.
- Vývoj a otestování školicích materiálů pro koncové uživatele.

Uživatelé a sídla pilotního programu

Pečlivě vyberte uživatele a sídla, která se budou účastnit pilotního projektu. Nejprve stanovte kritéria výběru a pak zvolte metodu výběru kandidátů. Mezi použitelné metody patří rozhovory, dotazníky a výzvy k přihlášení dobrovolníků.

Máte-li více pilotních programů, může se typ vybraných uživatelů během postupu pilotních programů měnit. Nakonec byste měli využívat typické uživatele ve vaší organizaci. V počáteční fázi pilotního projektu musí však mít dobrá skupina uživatelů tyto vlastnosti:

- Musí být schopna viditelně využívat výhody systému Windows 2000.
- Nesmí hrát kritickou roli v každodenních operacích.
Skupina musí být schopna vyrovnat se s určitými výpadky nebo snížením výkonu, pokud se vyskytnou nějaké problémy.
- Musí být reprezentativním výběrem cílového prostředí.
Vyberte skupiny nebo sídla, které nemají zvláštní požadavky nebo operační prostředí, protože potřebujete pomocí pilotního programu zjistit, jak bude návrh a postupné zavádění fungovat v celkovém prostředí.
- Vykonává různé činnosti s různým počítačovým hardwarem.
- Podporuje projekt systému Windows 2000.

- Je znalá příslušných technologií.

Uživatelé, kteří nějaké technologii rozumějí, mají spíše pochopení pro problémy, které se objeví během pilotního projektu, a pravděpodobněji budou také systém naplno využívat. Tento typ uživatelů se však může smířit i s problémy, které je nutné vyřešit. Vyzývejte uživatele, aby hlásili každý problém, se kterým se setkají, jinak můžete zjistit, že křivka jejich učení nepředstavuje typické uživatele. Při plánování následujících pilotních programů a plného zavádění zvažte vliv takových rozdílů ve skupinách uživatelů.

- Ráda se na školení seznámí s novými technologiemi.

Pamatujte si, že uživatelé s menšími zkušenostmi s určitou technologií potřebují větší nápomoc při přípravě na jejich roli a větší podporu během pilotního projektu.

Určete počet sídel a uživatelů pilotního programu na základě těchto kritérií:

- Cíle pilotního programu
- Počet testovaných funkcí a prvků
- Velikost personálu technické podpory

Jakmile vyberete různé účastníky, určete jednoho z nich za zástupce uživatelů. Vyberte někoho s dobrými komunikačními schopnostmi a s dobrým vztahem jak se skupinou pilotního zavádění tak s týmem projektu. Při plánování pilotního programu s tímto uživatelem spolupracujte. Zástupce uživatelů vám může poskytnout informace o typu práce vykonávané pilotní skupinou a může skupinu připravit na její roli. Uživatele podněcujte k účasti a zpětné vazbě pomocí pobídkového programu. Můžete například předat nějaké ceny nebo pochvaly uživatelům, kteří se o pilotní program zvlášť zaslouží.

Plán školení pilotního programu

Ještě dlouho před zavedením pilotního programu musíte určit, jak a kdy jeho účastníky proškolíte. Určete prostředky, které pro školení použijete. Zvažte například najmutí externího konzultanta, uspořádání seminářů, vývoj programu školení nebo použití mediálních technologií k vysílání školení.

Mnoho organizací zjišťuje, že je nejlepší provést školení těsně před instalací. Určete, čeho se školení musí týkat, a odhadněte, jak dlouho bude trvat. Školení omezte na činnosti, které uživatelé potřebují pro svou práci. Nezapomeňte zahrnout školení do časového plánu pilotního programu.

Plán podpory pilotního programu

Plán technické podpory vytvoříte velmi brzy, protože bude možná nutné personál technické podpory proškolit. Váš plán podpory se musí zabývat tím, kdo bude poskytovat technickou podporu, jakou úroveň technické podpory je zapotřebí zajišťovat a jak mohou uživatelé hlásit problémy.

Určete, kdo bude podporovat pilotní uživatele: bude to tým projektu, oddělení technické podpory nebo externí zdroj? Bude-li podporu zajišťovat oddělení technické podpory, jak je proškolíte? Jaká bude role týmu projektu? Je-li jedním z cílů vašeho pilotního projektu vyškolit technickou podporu, budete potřebovat určité prostředky jak z týmu projektu, tak i z technické podpory.

Určete, jaké úrovně služeb můžete podporovat během pilotního programu. Musí být například kritické problémy vyřešeny do zadaného počtu hodin? V jakých časech musí být uživatelům k dispozici technická podpora?

Dokumentujte procesy řízení změn a řízení problémů pilotního programu. Váš proces se musí zabývat těmito otázkami:

- Jak se požadavky na změny předávají, schvalují, testují a implementují?
- Jak uživatelé oznamují své problémy?
- Mohou uživatelé hlásit problémy existujícímu systému nebo potřebujete nový mechanismus, jako je například webová adresa, kam budou moci zaznamenat své problémy a otázky?
- Jak budete zkoumat, řadit podle priority a řešit problémy?
- Jaký proces předávání problémů použijete k upozornění příslušných osob?

Komunikace

V pilotním plánu popište, jak budete komunikovat s účastníky během jejich přípravy ještě před pilotním programem a jak bude docházet k výměně hlášení o stavu během pilotního programu. Zaznamenejte typ informací, které budete rozšiřovat, komu je budete předávat, jakými prostředky a jak často. Popište například, jak a kdy upozorníte uživatele na postupné zavádění pilotního programu. Další informace o strategiích komunikace najdete v kapitole „Plánování zavedení“ v této knize.

Při určování způsobu komunikace během pilotního programu začněte vytvořením použitého mechanismu. Vytvořte například distribuční seznamy elektronické pošty pro různé skupiny, které potřebují určité typy informací. Bude vhodné, když si poznameneáte typy informací odesílané uživatelům uvedeným na jednotlivých distribučních seznamech. Zaveďte mechanismy předávání informací o pilotním programu, jako jsou webová sídla, často kladené otázky, postupy a hlášení stavu.

Plán návratu pilotního programu

Kritickou částí vašeho pilotního programu je procedura návratu k původnímu stavu, pokud pilotní program selže. Vyvíjte podrobnou proceduru vysvětlující, kdy a jak vytvářet zálohy a jak je obnovovat. Použijete bitové kopie obrazů nebo postupné zálohy? Zdokumentujte proces zálohování a obnovení a otestujte jej. K uložení médií vyberte bezpečné místo a uveďte je do svého plánu návratu zpět k původnímu stavu.

Specifikujte kritéria, kdy se má použít procedura návratu k původnímu stavu. Můžete například vytvořit systém klasifikace závažnosti problémů a popsat, jaké úrovně ospravedlňují zrušení pilotního programu. Pro různé typy problémů také můžete vytvořit různé plány návratu k původnímu stavu. Můžete například vyvinout jednu proceduru pro zrušení celého pilotního programu, je-li problém skutečně neřešitelný, a jiný postup pro zrušení specifických součástí, který se použije, když se podaří problém izolovat. Navíc můžete potřebovat proceduru obnovení v případě závažných poškození dat v adresářové službě.

Časový plán

Jednou z prvních činností plánování pilotního programu je vytvoření časového plánu. Sem zahrňte úkoly plánování pilotního programu, přípravy uživatelů a sídel, zavádění pilotního programu a testování během pilotního programu. Nezapomeňte naplánovat

čas na školení uživatelů, personálu technické podpory a týmu instalace. Nějakou dobu věnujte také inventarizování sídel, inovaci hardwaru a vyhodnocení pilotního programu. Může být rovněž zapotřebí naplánovat úkoly vývoje mechanismů technické podpory a komunikace, které určíte během plánování.

Abyste mohli vytvořit časový plán fáze zavádění, musíte znát počet inovovaných počítačů a odhadovaný čas potřebný pro jejich inovaci. Určete, kolik přístrojů plánujete inovovat za den a pořadí, v jakém je budete inovovat. Promyslete si, které denní hodiny nebo dny týdne jsou pro inovaci serverů a klientských počítačů nejvhodnější. Měli byste počítače inovovat v mimopracovní době, abyste nerušili uživatele? Měli byste počítače inovovat během pracovní doby, aby se uživatelé mohli zatím účastnit nějakého školení? Plánujete koncové uživatele nějak proškolit, ještě než na jejich počítače nainstalujete systém Microsoft Windows 2000 Professional? Je-li to váš případ, pak bude časový plán školení jedním ze závislých prvků zavádění pilotního programu.

Při zavádění pilotního programu můžete upřesnit časový plán pomocí nových odhadů vycházejících ze zkušeností s instalací, takže bude přesnější pro účely plného zavádění systému.

Příprava na pilotní program

Jak se bude přibližovat datum spuštění pilotního programu, začněte se připravovat na zavádění. Nechte si dostatek času na přípravu uživatelů i fyzických sídel. Během testování návrhu systému Windows 2000 uživateli musí tým instalace vyvinout, otestovat a doladit proceduru postupného zavádění.

Příprava pilotních sídel

Pilotní sídla připravte předem, aby mohl tým instalace při spuštění pilotního programu ihned začít s inovací operačního systému. Musíte již mít inventář počítačů a síťových součástí. Další informace o vytvoření inventáře síťového vybavení najdete v kapitole „Příprava infrastruktury sítě na systém Windows 2000“ v této knize.

Vyhodnoťte počítače a síťové vybavení použité na pilotním sídle a určete, jaké inovace hardwaru jsou zapotřebí. Přinejmenším identifikujte požadované úpravy a obstarajte potřebné součásti. Je-li to možné, již předem nainstalujte nové součásti a otestujte je. Provéřte následující typy inovací:

- Inovace klientských počítačů v zájmu naplnění minimální podporované hardwarové konfigurace (paměť, kapacita pevného disku, rychlost a typ procesoru, síťové adaptéry).
- Inovace serverů na optimální hardwarové konfigurace.
- Inovace sítě v zájmu naplnění požadavků návrhu.
- Inovace klientů a serverů v zájmu zajištění kompatibility se systémem Windows 2000 (hardware, aplikace, ovladače).

Musíte také určit tyto položky:

- Aplikace používané v sídle.
- Speciální požadavky na zabezpečení.
- Speciální požadavky na konektivitu

Musíte otestovat kompatibilitu veškerého hardwaru a softwaru a tým instalace musí být připraven na všechny zvláštní požadavky.

Příprava pilotních uživatelů

Je důležité včas zajistit komunikaci v pilotní skupině. Váš prvotní kontakt by měl otevřít komunikační kanál a sdělit uživatelům, co lze očekávat. Jakmile se datum spuštění pilotního projektu přiblíží, uživatele proškolete a informujte je o specifických plánech zavádění a cílových datech.

Vytvoření včasné komunikace

Jakmile vyberete účastníky, sejděte se s nimi a zajistěte toto:

- Získejte jejich souhlas s pilotním programem.
- Vyberte zástupce uživatelů.
- Vyjasněte zodpovědnost.
- Projednejte plány podpory a návratu k původnímu stavu.

Účastníci pilotního programu musejí pochopit, co s sebou tento program přináší. Musejí porozumět tomu, jak pilotní program ovlivní jejich práci a jakou zodpovědnost budou mít. Prodiskutujte trvání pilotního projektu, úroveň poskytované technické podpory a jaké testování se bude vykonávat. Účastníci pilotního programu sice budou nadále vykonávat svou každodenní práci, můžete je však požádat, aby se zaměřili na nějaké určité oblasti. Vyřešte všechny pochybnosti o pilotním programu a jejich roli.

Informování účastníků

Jak budou vaše plány pilotního programu postupovat, může vás zástupce uživatelů informovat o pochybnostech uživatelů a uživatelé může informovat o nových událostech. Při vývoji plánů podpory informujte uživatele, jak a kdy mohou požadovat technickou podporu a jak mají hlásit problémy a klást otázky.

Informujte uživatele o typu školení, kterým projdou, a kdy je mohou očekávat. Některé organizace zajišťují jedno- až dvouhodinové školení těsně před zaváděním systému.

Na začátku zavádění pilotního programu připomeňte účastníkům tyto oblasti:

- Cílová data školení a inovace počítačů.
- Postupy, kterými musejí projít před inovací počítačů.
- Kontaktní jména a čísla technické podpory.

Vývoj procesu postupného zavádění

Je-li jedním z cílů vašeho pilotního programu otestovat proces zavádění, tým instalace musí vyvinout, dokumentovat a otestovat tyto postupy během testovací fáze projektu. Testovací laboratoř je sice vhodné místo k vyřešení problémů, pilotní program však představuje test ve skutečném světě, v němž lze vyladit přesnost a výkonnost procedur. Ujistěte se, že jsou skripty a nástroje automatizování inovací vhodné pro počítače v pilotním prostředí.

Při vývoji procedur zavádění systému Windows 2000 na různé typy počítačů vytvořte dokumentaci, která bude pro pracovníky, kteří instalaci zajišťují, užitečná. Dokumentace postupného zavádění může obsahovat tyto položky:

- Seznam nástrojů a dodávek, které pracovník vykonávající instalaci potřebuje.
- Seznam skriptů a jejich umístění.
- Zálohy, které musí pracovník vykonávající instalaci provést před zavedením a během něj.
Zahrňte zálohy uživatelských dat na klientských počítačích.
- Kroky migrace na novou strukturu domén.
Další informace o strategiích migrace na novou strukturu domén a používaných nástrojích najdete v kapitole „Určení strategií migrace domén“ v této knize.
- Kroky vykonání automatizované i ruční inovace počítačů.
Ruční metodu lze použít, pokud automatizovaná metoda nefunguje správně. Další informace o automatizování instalací najdete v kapitolách „Automatizování instalace a inovace serveru“ a „Automatizování instalace a inovace klientů“ v této knize.
- Testy přijatelnosti, které musí pracovníci vykonávající instalaci provést během zavádění a ihned po něm, aby ověřili, že zavádění pracuje podle předpokladů.
- Operační procedury, které budou provádět pracovníci vykonávající instalaci a správcí (změna oprávnění, změna hesel, obnovení uživatelských dat).
- Kroky návratu k původnímu stavu, pokud pilotní program selže.

Zavádění pilotního programu

Ještě před zavedením pilotního programu si celý proces vyzkoušejte. Tato zkouška zahrnuje naplánování nějaké mimopracovní doby, vykonání celého procesu inovace, důkladné otestování nové instalace a následné zrušení všech změn.

Během zavádění pilotního programu nezapomeňte ověřovat všechny zálohy. Jasně je označte a uložte na bezpečné místo. Každý krok při jeho vykonání ověřujte. Jak budete postupovat, zaznamenávejte si, jak dlouho instalace trvá, abyste mohli upřesnit časový plán. Během zavádění systému musíte mít k dispozici správce systému, který bude mít plná bezpečnostní oprávnění včetně práv spravovat hesla pošty a databázového serveru.

Zaznamenávejte si všechny úpravy postupů zavádění. Úpravy zadávejte postupně a otestujte je při další inovaci. Identifikujte a dokumentujte všechny nevýhodné kroky a metody, a tyto informace použijte k doladění procesu zavádění.

Vyhodnocení pilotního programu

Váš tým musí sledovat vývoj v rámci celého pilotního programu, opravovat a opakovaně testovat vzniklé problémy. Systém sledování systémů musíte mít vytvořený hned na začátku pilotního projektu a pilotní uživatele musíte vyzývat, aby do něj zaznamenávali své problémy. Uživatelé často zanedbávají hlášení problémů, buď protože si myslí, že je daný problém nevýznamný, nebo protože najdou nějaký způsob, jak jej obejít. Abyste však mohli pilotní program přesně vyhodnotit, potřebujete, aby uživatelé hlásili skutečně všechny problémy.

Na konci pilotního programu potřebujete k vyhodnocení jeho úspěšnosti vstupy z mnoha zdrojů. Čím více informací během pilotního programu nashromáždíte, tím přesněji jej budete moci na konci vyhodnotit.

Sledování pilotního programu

Váš tým musí trvale sledovat pilotní síť a vyhledávat úzká místa systému a oblasti, které je zapotřebí doladit. Sledujte jak tok provozu, tak i výkon aplikací. Nástroje sledování sice poskytují mnoho informací, je však vhodné pilotní sídlo také pravidelně navštěvovat. Časté rozhovory s uživateli odhalí problémy, které můžete jinak přejít bez povšimnutí. Často kontrolujte hlášení problémů a sledujte celkové trendy.

Během pilotního programu vyhodnocujte rizika pro projekt. Zabývejte se například těmito tématy:

- Změny rozsahu
- Vzrůst nákladů
- Problémy spolupráce (interoperability)
- Neočekávané výpadky

Zajištění zpětné vazby

Na konci pilotního programu vyhodnoťte jeho úspěšnost a doporučte managementu další postupný krok. Management se pak musí rozhodnout, zda bude celý projekt pokračovat. S tímto vyhodnocením a doporučením vám pomůže analýza informací z různých zdrojů. Můžete například získat informace z:

- formulářů zpětné vazby na webovém sídle,
- jednání s obchodními či výrobními manažery,
- hlášení problémů,
- přehledů koncových uživatelů,
- pozorování týmu projektu oddělení IT.

Pokuste se získat informace jak o návrhu, tak i o procesu zavádění. Vytvořte přehled prvků, které fungovaly a které nefungovaly, abyste mohli svůj plán revidovat a doladit. Sbírejte informace o problémech, jako jsou:

- školení,
- proces zavádění,
- technické podpora,
- komunikace,
- zjištěné problémy,
- návrhy na vylepšení.

Pomocí zpětné vazby ověřte, že celkový vytvořený návrh odpovídá původním specifikacím i obchodním či výrobním požadavkům. Splnil pilotní program kritéria úspěchu definovaná ještě před jeho spuštěním? Jestliže jste vytvořili nějaký systém měření úspěšnosti, jak pilotní program dopadl?

Seznam úkolů plánování vykonání pilotního programu

Tabulka 5.1 shrnuje úkoly, které musíte vykonat při plánování pilotního programu.

Tabulka 5.1 Seznam úkolů plánování vykonání pilotního programu

Úkol	Umístění v kapitole
Vytvořte plán pilotního projektu, který zahrnuje <ul style="list-style-type: none">■ Rozsah a cíle.■ Uživatele a sídla.■ Plán školení, podpory, komunikace a návratu k původnímu stavu.■ Časový plán.	Vytvoření pilotního plánu
Připravte své uživatele a sídla.	Příprava na pilotní program
Vyviňte proces zavádění.	Příprava na pilotní program
Pilotní program zaveďte.	Zavádění pilotního programu
Pilotní program podporujte a sledujte.	Vyhodnocení pilotního programu
Zajistěte zpětnou vazbu pilotního programu.	Vyhodnocení pilotního programu
Vyhodnoťte výsledky pilotního programu.	Vyhodnocení pilotního programu

Předpoklady infrastruktury sítě



Příprava infrastruktury sítě je zásadní první krok směrem k zavedení systému. Část 2 vám pomůže s dokumentováním současného síťového prostředí a s přípravou sítě na systém Microsoft Windows 2000.

V této části

Příprava infrastruktury sítě na systém Windows 2000 131

Určení strategií konektivity sítě 151

Analýza infrastruktury sítě pomocí serveru Systems Management Server 178

KAPITOLA 6

Příprava infrastruktury sítě na systém Windows 2000



Ještě před zavedením systému Microsoft Windows 2000 do organizace musíte připravit svou síť. Tato kapitola pomůže vám, správci sítě, identifikovat oblasti infrastruktury sítě, jako jsou servery, směrovače a síťové služby, které může být zapotřebí před zavedením systému Windows 2000 inovovat nebo upravit. Tato kapitola také popisuje dokumentování současné infrastruktury sítě.

Než začnete číst tuto kapitolu, prohlédněte si materiál uvedený v kapitolách „Vytvoření cesty postupného zavádění“ a „Plánování zavedení“ v této knize.

V této kapitole

Dokumentování současného prostředí 131

Příprava architektury sítě 140

Seznam úkolů přípravy infrastruktury sítě 149

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Inventáře, diagramy a dokumentace současného síťového prostředí
- Plán přípravy infrastruktury na zavedení systému Windows 2000

Související informace v sadě Resource Kit

- Další informace o protokolu TCP/IP systému Windows 2000 najdete v knize *Microsoft Windows 2000 Server Sítě TCP/IP*.
- Další informace o vyhodnocení existující sítě, infrastruktury a protokolů najdete v kapitole „Určení strategií konektivity sítě“ v této knize.
- Další informace o vytvoření plánu migrace domén najdete v kapitole „Určení strategií migrace domén“ v této knize.

Dokumentování současného prostředí

Dokumentování fyzické a logické topologie existující sítě a vytvoření úplného a přesného inventáře hardwaru a softwaru používaného ve vaší organizaci jsou velmi důležité předběžné kroky plánování infrastruktury sítě systému Windows 2000.

Oblastmi současného síťového prostředí, které musíte zdokumentovat a připravit tak síť na zavedení systému Windows 2000, jsou:

- Hardware and software
- Infrastruktura sítě
- Souborové, tiskové a webové servery
- Obchodní či výrobní aplikace
- Architektura adresářových služeb
- Zabezpečení

Aplikace diagnostiky sítě systému Microsoft Windows NT, jako je například Sledování sítě (Network Monitor), jsou k dokumentování sítě užitečné. Výrobci originálních zařízení také často nabízejí software řešení problémů a konfigurací, který je pro dokumentování konfigurace vybavení a ovladačů ideální.

Během přípravy infrastruktury sítě na systém Windows 2000 budete vykonávat značné množství plánování. V kapitole „Vytvoření cesty postupného zavádění“ uvedené dříve v této knize jste definovali rozsah svého projektu zavádění a vybrali jste funkce systému Windows 2000, které chcete zavést. Také jste identifikovali technické závislosti systému Windows 2000, které mohou ovlivnit vaše plánování, a vytvořili jste projektový plán zavádění.

Tato kapitola se zaměřuje na přípravu infrastruktury vaší sítě na systém Windows 2000; tato příprava však nemůže stát stranou od plánování popsaného v jiných kapitolách této knihy. Ať už připravujete novou síť nebo migrujete systém Windows 2000 do existující síťové struktury, konkrétní úkoly přípravy infrastruktury určí plánování v oblastech restrukturalizace domén, inovací serverů a požadavků na infrastrukturu.

Inventář hardwaru a softwaru

Pokud jste tak ještě neučinili, vytvořte inventáře hardwaru a softwaru všech serverů a klientských počítačů používaných na síti. Dokumentujte veškeré směrovače, tiskárny, modely a další hardware, jako jsou redundantní pole nezávislých disků (RAID) a hardware serveru služby vzdáleného přístupu (Remote Access Service – RAS). Nezapomeňte na podrobnosti o nastavení systému BIOS a konfiguraci všech periferních zařízení, jako jsou tiskárny, skenery a vstupní zařízení. Poznamenejte si verze ovladačů a další informace o softwaru a firmwaru.

Inventář softwaru musí uvádět všechny aplikace nalezené na všech počítačích a musí obsahovat také čísla verzí (nebo data a časy vytvoření) dynamicky připojitelných knihoven souvisejících s aplikacemi na vašem systému. Nezapomeňte zdokumentovat všechny servisní balíčky, které jste na operační systém nebo programy aplikovali. K získání těchto informací ze sítí systémů Windows a Windows NT, které používají Windows Management Instrumentation (WMI), můžete použít skripty a různé aplikace nezávislých výrobců.

Server Systems Management Server je také užitečný k získávání informací o síti systému Windows NT a dokáže vytvářet podrobné sestavy hardwaru, softwaru a aplikací používaných ve vaší společnosti. Další informace o analyzování sítě pomocí serveru Systems Management Server najdete v kapitole „Analýza infrastruktury sítě pomocí serveru Systems Management Server“ v této knize.

Dokumentujte síťové konfigurace serverů a klientských počítačů. Na počítačích se systémem Windows NT lze nastavení sítě získat snadno.

▼ **Chcete-li zjistit síťová nastavení v systému Windows NT, postupujte takto:**

1. Stiskněte tlačítko **Start**, vyberte příkaz **Nastavení** (Settings) a pak klepněte na položku **Ovládací panely** (Control Panel).
2. Poklepejte na ikonu **Síť** (Network).
3. Poznamenejte si informace uvedené na kartách **Identifikace** (Identification), **Služby** (Services), **Protokoly** (Protocols), **Adaptéry** (Adapters) a **Vazby** (Bindings).

Na každém počítači s přiřazenou statickou adresou protokolu Internet Protocol (IP) si otevřete okno příkazového řádku, zadejte příkaz **ipconfig /all** a poznamenejte si výsledky. Nezávislí prodejci hardwaru často poskytují diagnostický software a software pro správu, který sbírá podrobné informace o hardwaru a konfiguračních nastavení.

Tyto inventáře můžete využít k těmto účelům:

- Potvrdit, že jsou současná infrastruktura, hardware serverů, BIOS počítačů a softwarové konfigurace kompatibilní se systémem Windows 2000 Server – stačí inventář porovnat se seznamem Hardware Compatibility List (HCL). Další informace o seznamu HCL najdete v odkazu Microsoft Windows Hardware Compatibility List stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/res-kit/webresources>.
- Určit konkrétní cesty inovace pro jednotlivé serverové a klientské počítače a vytvořit specifikace pro získání nového vybavení.

Infrastruktura sítě

Při dokumentování současného síťového prostředí si všimněte zejména oblastí, kde se v současné době potýkáte s problémy. Pokud se vám podaří stabilizovat síť před zaváděním nového operačního systému, zavádění a řešení problémů bude jednodušší a v inovovanou síť budete mít větší důvěru. Dobrým způsobem vyhodnocení vlivu zavádění systému Windows 2000 s danou sadou protokolů, hardwarových ovladačů a konfigurací klient/server je vytvoření testovací laboratoře a duplikování problémů. Další informace o vytvoření testovací laboratoře najdete v kapitole „Vytvoření testovací laboratoře systému Windows 2000“ v této knize.

Při dokumentování infrastruktury sítě získáváte jak hardwarová data sloužící ke zdokumentování fyzické struktury infrastruktury, tak i softwarová data sloužící ke zdokumentování existence a konfigurace protokolů používaných na síti. Také musíte zdokumentovat logické uspořádání sítě, metody překladu názvů a adres a existenci a konfiguraci použitých služeb. Také zdokumentování umístění síťových sídel a dostupné šířky pásma mezi nim vám pomůže při určování, zda při inovaci nebo migraci na systém Windows 2000 používat nevyžádané nebo vyžádané instalace. Další informace o instalování, inovování a migrování na operační systém Windows 2000 najdete v kapitolách „Automatizování instalace a inovace klientů“ a „Automatizování instalace a inovace serverů“ v této knize.

Vývoj fyzického a logického diagramu sítě vám pomůže uspořádat získané informace pochopitelným a intuitivním způsobem.

Fyzický diagram sítě

Fyzický diagram představuje následující informace o existující síti:

- Podrobnosti o fyzických komunikačních linkách, jako je délka kabelů, úroveň linky a přiblížení fyzických cest kabelů a analogových linek a linek ISDN.
- Popis serverů s názvem počítače, adresou IP (je-li statická), rolí serveru a členství v doméně. Server může mít mnoho rolí, mezi které patří primární nebo záložní řadič domény, server služby Dynamic Host Configuration Protocol (DHCP), server systému Domain Name System (DNS) server, server služby Windows Internet Name Service (WINS), tiskový server, směrovač a aplikační nebo souborový server.
- Umístění zařízení, jako jsou tiskárny, rozbočovače, přepínače, modemy, směrovače, mosty a proxy-servery, které se nacházejí na síti.
- Komunikační linky (analogové a ISDN) rozlehlou síť (WAN) a dostupná šířka pásma mezi sídly. Může jít o nějaké přiblížení nebo skutečně změřenou kapacitu.
- Počet uživatelů na jednotlivých sídlech včetně mobilních uživatelů.

Obrázek 6.1 je příkladem fyzického diagramu sítě.

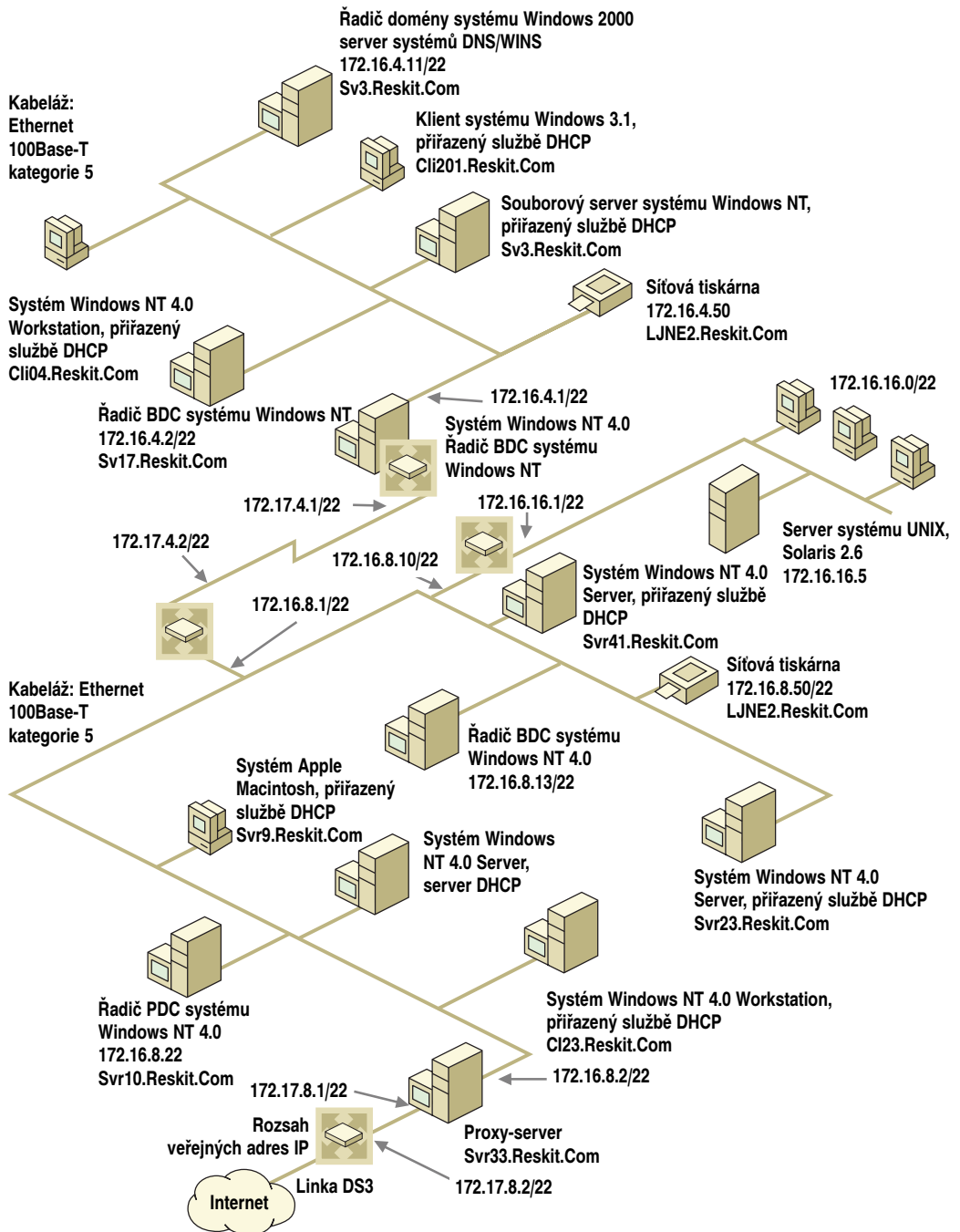
Dokumentujte verze firmwaru, průchodnost a všechny speciální konfigurační požadavky všech zařízení na síti. Pokud nějakým zařízením přiřazujete statické adresy IP, zaznamenejte je. Další informace o konektivitě sítě a systému Windows 2000 najdete v kapitole „Určení strategií konektivity sítě“ v této knize.

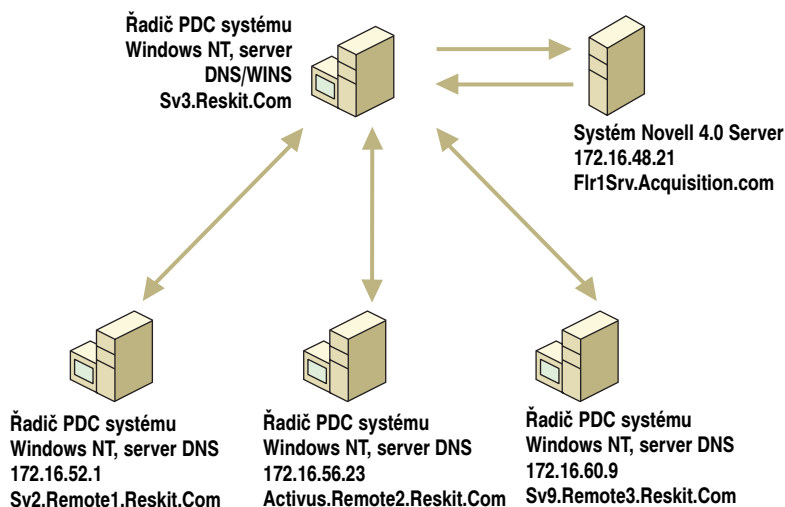
Logický diagram sítě

Logický diagram zobrazuje architekturu sítě včetně následujících informací:

- Architektura domén včetně existující hierarchie domén, názvů a schéma adresování.
- Role serverů včetně hlavních a záložních řadičů domén, serverů služby DHCP a serverů WINS.
- Vztahy důvěryhodnosti včetně reprezentace přenosných, jednosměrných a obousměrných vztahů důvěryhodnosti.

Obrázek 6.2 je příkladem logického diagramu sítě.


Obrázek 6.1 Fyzický diagram sítě



Obrázek 6.2 Logický diagram sítě

Konfigurace sítě

Oblasti konfigurace sítě, které musíte zdokumentovat, jsou obecně uvedeny v následujících oddílech.

Služby překladu názvů

Nezapomeňte zdokumentovat všechny servery DNS a WINS na síti a poznamenat si informace o konfiguracích a verzích i podrobnosti o hardwaru. Poznamenejte si, zda některý ze serverů DNS na síti, na kterém není systém Windows NT, podporuje dynamickou registraci a záznamy o prostředcích služeb (SRV), nebo zda jsou od jeho výrobce k dispozici inovace nabízející tyto schopnosti.

Máte-li na síti hostitele, na nichž nepracuje systém Windows NT, zdokumentujte jimi poskytované služby, například UNIX BIND. Měli byste také zaznamenat verze jednotlivých používaných služeb. Je-li například na síti použita služba BIND, uvědomte si, že její verze dřívější než 4.9.4 nejsou se systémem Windows 2000 kompatibilní. Zdokumentujte služby Service Advertising Protocol (SAP) a Routing Information Protocol (RIP), pokud je některá z nich na síti použita.

Metody adresování IP a konfigurace služeb

Ujistěte se, že jste zdokumentovali všechny servery služby DHCP na síti včetně:

- všech adres IP, které jste přiřadili serverům nebo klientským počítačům,
- nastavení DHCP, jako je výchozí brána,
- podrobností o podsítích a jejich vztahu v celkové struktuře domén,
- počtu podsítí a hostitelů na síti a záznamu adres IP a masek podsítí používaných na síti,
- toho, jak dlouho může mít klient na síti propůjčenu nějakou adresu IP.

Vzdálené a telefonické připojování k síti

Máte-li nějaké vzdálené nebo mobilní uživatele, poznamenejte si konfigurace vzdáleného a telefonického přístupu. Používáte-li k podpoře mobilních uživatelů software jiných společností, zobrazte si a zaznamenejte konfigurace těchto produktů. Používáte-li virtuální privátní síť (Virtual Private Network – VPN), dokumentujte konfigurace sítě VPN s cílem vyhodnotit, zda je možné nahradit ji sítí VPN systému Windows 2000 VPN.

Problémy s šířkou pásma

Zdokumentujte současné využití šířky pásma sítě. Tyto údaje použijete jako základní linii, podle které se budou měřit změny. K změření parametrů šířky pásma, jako jsou přijaté či odeslané bajty nebo pakety, chyby vysílání nebo příjmu a přenos paketů za sekundu, můžete použít různé nástroje nezávislých výrobců i společnosti Microsoft. Dokumentujte rychlost síťových linek mezi síťovými segmenty a geografickými místy vaší organizace.

Podívejte se na logické a geografické rozčlenění vaší organizace z hlediska problémů se šířkou pásma. Má organizace nějaké pobočky nebo mobilní či vzdálené uživatele? Zvažte množství a typ provozu přes komunikační linky organizace. Dochází například k pravidelnému zpomalování linek WAN při replikaci mezi řadiči domén na různých sídlech? Zdokumentujte čistou dostupnou šířku pásma všech linek WAN a síťových segmentů. Pokuste se zaznamenat dostupnou šířku pásma během nízkého, středního a vysokého využívání sítě.

Souborové, tiskové a webové servery

Dokumentujte konfigurační podrobnosti o členských serverech, přičemž se věnujte zejména všem zvláštním konfiguracím, jako je server hostící banku modemů nebo server oddělení s více síťovými kartami. Poznamenejte si, zda se jedná o podnikový server nebo o server oddělení. Všimněte si všech zvláštních provozních požadavků serverů a určete, zda se některé z těchto serverů spoléhají na určité speciální protokoly nebo ovladače. Pokud se například nějaký produkt musí nacházet na záložním řadiči domény, může po inovaci příslušného řadiče na systém Windows 2000 dojít k ovlivnění funkce daného produktu. Stejně jako u všech ostatních počítačů vyhodnoťte na těchto počítačích pomocí seznamu HCL kompatibilitu hardwaru a souvisejících ovladačů se systémem Windows 2000.

Vyhledejte tiskárny v organizaci a zaznamenejte jejich konfigurace. Věnujte se zejména webovým serverům a proxy-serverům – při plánování zavádění musíte zvážit bezpečnostní dopady v této třídě serverů a šířku pásma, jakou každý server vyžaduje zejména pro službu Active Directory. Další informace o plánování souborových, tiskových a webových serverech najdete v kapitole „Inovace a instalace členských serverů“ v této knize.

Obchodní či výrobní aplikace

Identifikujte všechny aplikace, které váš podnik potřebuje k vykonávání svých základních činností. Obvykle objevíte základní sadu aplikací, jako jsou databázové aplikace, systém elektronické pošty a finanční sadu, přičemž každá z těchto aplikací musí v zájmu dosažení obchodních či výrobních cílů správně fungovat. Prověřte kompatibilitu těchto aplikací se systémem Windows 2000. Chcete-li například svůj program elektronické pošty integrovat se službou Active Directory, musíte kontaktovat jeho výrobce a dotázat se, zda nabízí, nebo plánuje vytvoření nějaké cesty inovace zajišťující kompa-

tibilitu se systémem Windows 2000 a službou Active Directory. Mnoho výrobců softwaru se spojilo se společností Microsoft a snaží se zajistit, aby jejich produkty pracovaly v systému Windows 2000 správně. Logo „Certified for Windows“ je nejlepší zárukou kompatibility. Další informace o určením, zda jsou vaše aplikace kompatibilní se systémem Windows 2000, najdete v kapitole „Testování kompatibility aplikací se systémem Windows 2000“ v této knize. Informace o aplikacích kompatibilních se systémem Windows 2000 najdete v odkazu Directory of Windows 2000 Applications stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Architektura adresářových služeb

Jako součást plánu přechodu na službu Active Directory zdokumentujte existující strukturu domén. Identifikujte architektury domén, uživatele a skupiny uživatelů v organizaci a jejich geografické umístění a domény prostředků a správy. Zdokumentujte jedno- a obousměrné vztahy důvěryhodnosti existující mezi doménami. Určete, zda máte nespojitý obor názvů, který je zřejmě důsledkem nákupů, sloučení nebo jiných rozsáhlých akcí. Tyto informace vám pomohou při plánování doménové struktury systému Windows 2000 a určení typů vztahů důvěryhodnosti vytvořenými mezi doménami.

Určete všechny adresářové služby pracující na vaší síti, které nejsou zajišťovány systémem Windows NT, jako jsou rozšíření adresářových služeb systému Microsoft Exchange Server nebo UNIX BIND. Identifikujte všechny uživatelské účty existující pro jednotlivé uživatele. Tyto informace se vám budou hodit jak během migrace na službu Active Directory, tak i při zajišťování správné funkce mezi službou Active Directory a dalšími adresářovými službami, protože již budete mít informace o všech účtech jednotlivých uživatelů.

Model správy domén

Určete hlavní model (neboli standard) správy domén sloužící ke správě domén. Máte centralizovaný, hierarchický model správy, nebo vaše organizace používá distribuovaný model správy? Co mohou vykonat místní správci v porovnání s podnikovými správci? Překrývají se nějak modely správy ve vaší organizaci? Tyto informace vám pomohou určit, zda lze v systému Windows 2000 restrukturalizovat povinnosti správy a učinit správu domén levnější a výkonnější. Systém Windows 2000 nabízí výrazné zlepšení schopností spravovat jak nejširší tak i nejmenší podrobnosti sítě.

Při zkoumání existující struktury domén zdokumentujte následující informace o síti:

Typ struktury domén

Většina sítí má více hlavních domén uživatelských účtů s mnohem větším počtem domén prostředků. Při migraci nebo inovaci existujících domén na systém Windows 2000 ovlivní existující struktura domén návrh struktury domén systému Windows 2000. Další informace najdete v kapitole „Určení strategií migrace domén“ v této knize.

Existující vztahy důvěryhodnosti

Poznamenejte si existující jedno- a obousměrné vztahy důvěryhodnosti v síti. Identifikujte všechny domény a vztahy důvěryhodnosti, které nechcete přenést do doménové struktury systému Windows 2000. Domény inovované na domény systému Windows 2000 a přiřazené jako součást jedné doménové struktury se připojí k ostatním doménám systému Windows 2000 pomocí přenosných (tranzitivních) vztahů důvěryhodnosti. Po inovování domén na systém Windows 2000 musíte vytvořit explicitní vztahy dů-

věryhodnosti mezi doménami systému Windows 2000 a všemi doménami, které nechcete přesunout do nové doménové struktury.

Počet a umístění řadičů domén na síti

To vám umožní naplánovat inovaci jednotlivých domén. Hlavní a záložní řadiče domén byste měli mít zaznamenané na fyzickém a logickém diagramu sítě. Poznamenejte si jejich fyzická umístění a konfigurační podrobnosti. Další informace o určení pořadí a načasování inovací řadičů domén najdete v kapitole „Určení strategií migrace domén“ v této knize.

Obory názvů DNS existující ve vaší organizaci

Když budete vědět, jaké obory názvů existují ve vaší organizaci, pomůže vám to vytvořit jednoznačný obor názvů doménové struktury systému Windows 2000. Určení oboru názvů DNS za kořen hierarchie služby Active Directory je důležitou součástí plánování, protože po vytvoření návrhu hierarchie je velmi komplikované změnit kořenový obor názvů. Další informace o plánování struktury domén pro službu Active Directory najdete v kapitole „Návrh struktury služby Active Directory“ v této knize.

Zabezpečení

Vytvoření přehledu standardů zabezpečení ve vaší organizaci a jejich implementace je užitečné, i když nepřecházíte na nový operační systém; v takové situaci se však jeho důležitost znásobuje. Vytvořte přehled standardů a procedur zabezpečení pro mobilní uživatele a uživatele kancelářských počítačů, interní a externí sítě a účty vzdáleného a telefonického přístupu.

Jsou úkoly správy, jako je vytváření uživatelů, skupin, míst sdílení souborů, změna hesel a konfigurování zařízení a atributů objektů, vykonávány centralizovanou skupinou, nebo několika skupinami? Jaká jsou specifická práva a seznamy členství těchto skupin?

Dokumentujte typy vztahů, které v současné době existují mezi místy kanceláří, obchodními či výrobními jednotkami a odděleními ve vaší organizaci. Jsou úkoly správy v těchto jednotkách sdíleny, nebo každá jednotka zodpovídá za svou správu? Přesahuje vaše skupiny uživatelů hranice oddělení společnosti či jednotlivá místa, nebo je konstruuje podle organizačních útvarů? Zaznamenejte tyto informace a všechny existující zásady zabezpečení platící pro uživatele i podnik. Zdokumentujte, jaké typy informací jsou dostupné jednotlivým skupinám, a také všechna významná omezení vyžadovaná pro konkrétní typy informací, jako jsou například účetní data.

Zdokumentujte všechna existující pravidla související se správným používáním sítě, jako například zda může personál přistupovat k Webu a za jakým účelem a jaký přístup je považován za zakázaný nebo nežádoucí.

Vztahy vaší organizace s externími prodejci, zákazníky a obchodními partnery ovlivňují strategii zabezpečení. Zodpovězte si následující otázky o vztazích společnosti:

- Zavázali jste se svým partnerům k plnění nějakých služeb nebo jim umožňujete přístup na síť na úrovni rozpoznávaných uživatelů?
- Jaké jsou zásady související s jejich přístupem k vašim datům a prostředkům na síti?
- Mohou si data pouze zobrazovat nebo mohou data na vaší síti měnit a přidávat je sem?
- Jak omezujete přístup k aplikacím?

Zdokumentujte v současné době existující nebo plánované standardy zabezpečení a šifrování pomocí těchto informací:

- Dokumentujte oprávnění zabezpečení na síti podle uživatelů a skupin uživatelů.
- Vytvořte seznam domén a existujících vztahů důvěryhodnosti mezi řadiči domén.
- Zdokumentujte standardy hesel – jak dlouhé musí heslo být, jaké jsou povolené kombinace znaků, jak dlouho si může uživatel heslo ponechat atd.
- Vytvořte seznam protokolů zabezpečení používaných v síti.
- Uveďte, jak ověřujete externí uživatele z Internetu, telefonického připojení nebo z linek rozlehlé sítě (WAN) na síti.
- Zdokumentujte podrobnosti o všech vícenásobných účtech existujících pro jediného uživatele. Mají například někteří vaši uživatelé účet v systému Windows NT a jiný účet v systému UNIX? Popište oprávnění, uživatele a členství uživatelů ve skupinách a další podrobnosti o těchto vícenásobných účtech.

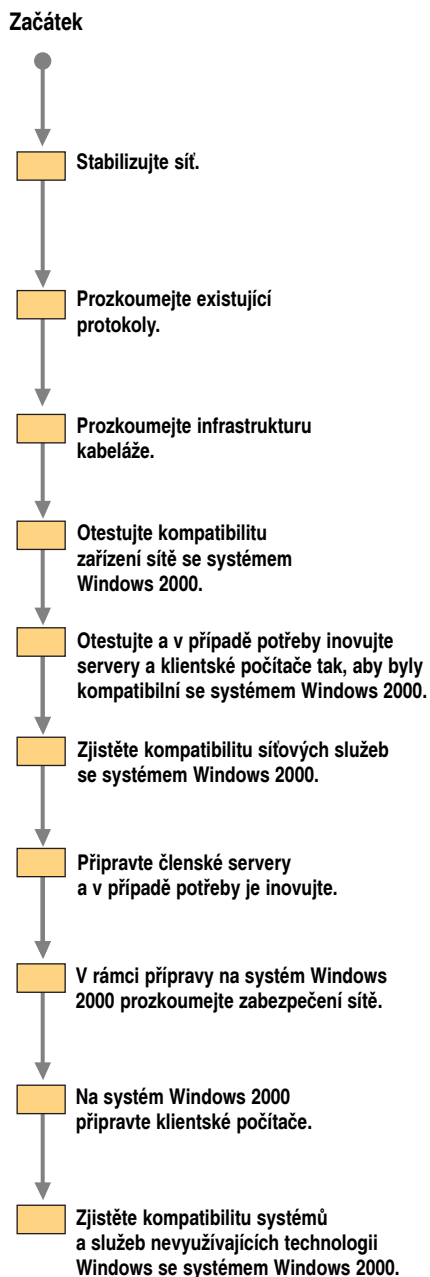
Další informace o problémech souvisejících s vytvářením plánu zabezpečení sítě najdete v kapitole „Plánování distribuovaného zabezpečení“ v této knize. Mezi tyto problémy patří rozpoznání typů bezpečnostních rizik, kterým může vaše organizace čelit, a plánování způsobů omezení těchto rizik. Jako součást tohoto procesu naplánujete a vyvinete zásady související s infrastrukturou veřejných klíčů a ověřování uživatelů, a vyvinete také možnosti zabezpečení elektronické pošty a webových serverů.

Při zkoumání existujících bezpečnostních uspořádání se podívejte také na schémata zálohování včetně toho, zda můžete bezpečnostní rizika omezit ukládáním záloh mimo sídlo a zda je váš plán zotavení po havárii aktuální a vyhovuje současným požadavkům sítě a její velikosti. Další informace o vývoji zásad konfigurace úložišť a plánu zotavení po havárii najdete v kapitole „Určení strategií správy úložišť systému Windows 2000“ v této knize.

Další informace o problémech a plánování zabezpečení pomocí funkcí systému Windows 2000 najdete v kapitole „Internet Protocol Security“ v knize *Microsoft Windows 2000 Server Sítě TCP/IP* a v kapitole „Plánování distribuovaného zabezpečení“ v této knize.

Příprava architektury sítě

Následující oddíly popisují, jak je zapotřebí připravit infrastrukturu sítě na systém Windows 2000. Přestože je každá síť jiná a vaše priority budou určeny mnoha technickými a organizačními faktory, můžete použít obecnou cestu přípravy uvedenou na obrázku 6.3.



Obrázek 6.3 Vývojový diagram přípravy sítě

Všechna tato témata jsou podrobně prodiskutována v kapitolách uvedených dále v této knize. Tato kapitola vysvětluje otázky a problémy, kterých si musíte být vědomi v jednotlivých uvedených oblastech při přípravě infrastruktury sítě na systém Windows

2000. Také vás naviguje do příslušných kapitol této knihy, kde o daném tématu najdete více informací.

Předběžné kroky

Na začátku přípravy infrastruktury sítě na systém Windows 2000 stabilizujte existující síť a seznámte se s jejími síťovými protokoly.

Stabilizace existující sítě

Ještě před implementováním projektu inovace sítě nebo migrace musíte identifikovat a odstranit všechna úzká místa přenosů v síti, špatně fungující hardware, nestabilní nebo nejisté konfigurační a další problematické oblasti. V projektu migrace nebo inovace mohou nedostatečné šířky pásma a nestabilní síťové součásti dosažení cílů značně zkomplikovat.

Během plánování inovace hardwaru se zaměřte na nestabilní počítače, periferní zařízení a síťová zařízení. Ještě před inovací se snažte změnit úpravu časového plánu údržby sítě tak, aby odpovídal nové situaci. Nahrazovaná síťová zařízení, jako jsou síťové adaptéry, zaměňujte zařízeními kompatibilními se systémem Windows 2000, jež jsou uvedené v seznamu HCL.

Zjištění síťových protokolů

Každá síť používá podle potřeby různé protokoly. Organizace udržující síť Ethernet mohou používat kombinaci protokolů TCP/IP, NetBEUI, SPX/IPX a dalších podle potřeb práce v síti, ověřování a zabezpečení a podle schopností zavedeného operačního systému. Identifikujte protokoly používané na vaší síti. Přitom zvažte, zda je možné některé z těchto protokolů nahradit jejich verzemi v systému Windows 2000, nebo zda je lze odstranit, protože je inovovaní klienti již nebudou potřebovat. Pokud například jako součást migrace nahradíte všechny klienty používající protokol SPX/IPX klienty systému Windows 98 nebo Windows 2000 Professional, můžete na síti úplně přestat používat protokol IPX/SPX a uvolnit tak určitou šířku pásma. Zvažte zjednodušení sítě tím, že použijete výhradně protokoly ze sady TCP/IP.

Systém Windows 2000 nabízí sadu protokolů TCP/IP, která poskytuje více funkcí než předchozí verze, jako je podpora velkých rámců a selektivního potvrzování. V zájmu získání specifických funkcí, jako je například podpora služby Active Directory, a plného využití pokročilých prvků systému Windows 2000 musíte použít protokol Microsoft TCP/IP. Například předchozí verze systému Windows NT používaly k zabezpečení komunikačních linek protokol Point-to-Point Tunneling Protocol (PPTP). Systém Windows 2000 také podporuje protokol PPTP, nabízí však lepší funkce a zabezpečení komunikační linky pomocí protokolu Layer 2 Tunneling Protocol (L2TP). Další informace o funkcích a vylepšeních výkonu v sadě TCP/IP systému Windows 2000 najdete v kapitole „Protokol TCP/IP systému Windows 2000“ v knize *Microsoft Windows 2000 Server Sítě TCP/IP*.

Posudek fyzické infrastruktury

Zvažte kvalitu a šířku pásma existující síťové kabeláže a zařízení, a určete, jestli budou podporovat vaše plány inovace nebo migrace. Existují tu nějaká síťová zařízení, například rozbočovače a kabeláž, která jsou pro vaše účely dostatečně rychlá? Jak rychlá jsou spojení ke geograficky rozptýleným sídlům? Jaké množství provozu je vytvářeno na vaší síti interně a přes další linky? Například vzdálená pobočka, která používá jako hlav-

ní kancelářské aplikace textový procesor a tabulkový kalkulátor, nevytváří směrem k serveru pobočky velký síťový provoz, takže síťová kabeláž kategorie 3 schopná přenosů na úrovni 10 Mb/s s odpovídajícími rozbočovači může být přijatelná. V hlavní kanceláři jsou základními aplikacemi kancelářských počítačů sdílené aplikace se sdílenými daty, jako jsou databázové a účetní systémy. Tyto aplikace vytvářejí značně větší síťový provoz a vyžadují rychlejší síťová zařízení a kabeláž.

Rostoucí potřeba přístupu k Internetu a multimédiím dostupným na kancelářských počítačích dále zvyšuje požadavky kladené na šířku přenosového pásma. Síť Ethernet provozující sdílené aplikace pak mohou vyžadovat kabely kategorie 5 schopné přenosů o rychlosti 100 Mb/s.

V testovací laboratoři vyhodnoťte požadavky určitých konfigurací na šířku pásma. Jestliže například vaše organizace plánuje přenášet přes datovou síť audio a video, vaše kabeláž a přepínače musejí být schopny naplnit požadavky těchto služeb.

S určením požadavků na šířku pásma například pro odesílání komprimovaného video-signálu přes spojení WAN vám pomohou nástroje jiných společností i nástroje zabudované do systému Windows NT. V testovací laboratoři můžete také vyzkoušet několik možných konfigurací zařízení a operačních parametrů a určit nejmenší požadavky.

Váš plán zavádění bude ovlivněn konfiguračními požadavky funkcí systému Windows 2000, které plánujete použít. Jestliže se například svazek DFS v pobočkové kanceláři replikuje přes pomalé spojení do alternativního svazku DFS, bude asi v zájmu omezení síťového provozu přes dané pomalé spojení zapotřebí buď linku inovovat a zvýšit její šířku pásma, nebo umístit alternativní svazek přímo do pobočkové kanceláře.

Některé funkce systému Windows 2000 vyžadují specifickou konfiguraci, například umístění serveru VPN na jeden konec spojení WAN jako součást zajištění zabezpečeného spojení VPN. Ve svém plánu musíte počítat s různými konfiguračními úvahami, například jak plánujete integrovat server VPN s proxy-servery. Podívejte se na existující infrastrukturu sítě a očekávané přínosy a funkce, jako jsou zabezpečené linky WAN prostřednictvím VPN, jejichž zavedení lze očekávat se systémem Windows 2000. Další informace o konfigurování strategie zabezpečení systému Windows 2000 najdete v kapitole „Určení strategií zabezpečení sítě systému Windows 2000“ v této knize. Další informace související se zabezpečením najdete v kapitole „Plánování distribuovaného zabezpečení“ v této knize.

Proveďte kompatibilitu síťových zařízení se systémem Windows 2000. Na seznamu Hardware Compatibility List vyhledejte příslušné síťové karty, modemy a konkrétní typy rozbočovačů. Systém Windows 2000 může například zatížení výpočtů kontrolních součtů protokolu TCP přenést na síťové adaptéry, které tuto funkci systému Windows 2000 podporují, a zlepšit tak výkon sítě. Další informace o schválených systémech a zařízeních na seznamu HCL najdete v odkazu Microsoft Windows Hardware Compatibility List stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Systém Windows 2000 podporuje technologii Asynchronous Transfer Mode (ATM) a poskytuje tak další cestu migrace z tradičních sítí se sdílenými médii na síť ATM, protože nabízí služby emulace LAN (LANE). Systém Windows 2000 také podporuje přenos IP přes ATM. Plánujete-li používat ATM systému Windows 2000, nebo používáte-li v současné době ATM systému Windows NT 4.0, zajistěte, aby vám dodavatel ATM obstaral aktualizované ovladače pro systém Windows 2000. Ujistěte se, že jsou vaše adaptéry ATM uvedeny na seznamu HCL.

Příprava serverů

Možná zavádíte systém Windows 2000 do kombinovaného prostředí nebo nakonec přejdete na nativní síť systému Windows 2000. Například plánování uskutečněné v kapitolách „Návrh struktury služby Active Directory“ a „Určení strategií migrace domén“ dále v této knize vám pomůže s implementací nebo inovací plánu adresování IP ve spojení s plánováním služby Active Directory.

Již jste identifikovali své servery infrastruktury – hlavní a záložní řadiče domén, servery DNS, DHCP, WINS a další servery, které tvoří vaši infrastrukturu. Ověřte, že ovladače vašeho hardwaru jsou dostupné i pro systém Windows 2000. Nejsou-li ovladače nebo vybavení, které používáte, na seznamu HCL, obstarajte si od výrobce nové ovladače nebo sami otestujte jejich kompatibilitu se systémem Windows 2000.

Předchozí verze systému Windows NT a mnoho serverů DNS nezávislých společností se nedokáží dynamicky synchronizovat s DHCP, a proto nedokáží udržovat aktualizovanou přiřazení mezi názvy a adresami IP. Z toho důvodu zvažte inovování služeb DNS na systém DNS kompatibilní se systémem Windows 2000. Systém DNS Windows 2000 automaticky aktualizuje pole záznamů DNS a omezuje tak potřebu ručních aktualizací, které byly vyžadovány dříve.

Zvažujete-li inovování sítě, zamyslete se také nad umístěním serverů DHCP podle počtu a velikosti geografických sídel na síti a rychlosti a spolehlivosti jejich linek WAN. Provoz DHCP mezi vzdálenými sídly vyžaduje zlepšení šířky pásma i spolehlivosti linek mezi sídly. Další informace o tomto tématu najdete v kapitole „Určení strategií konektivity sítě“ v této knize.

Plánujete-li podporovat klienty, kteří překládají adresy IP pomocí požadavků systému NetBIOS, budete i nadále potřebovat k překladu názvů počítačů na adresy IP systém WINS. Obecně platí, že NetBIOS používají k překladu adres IP systémy MS-DOS, Windows verze 3.2x a dřívější, Windows 95, Windows 98 a Windows NT. Nyní je vhodná doba začít eliminovat používání systému WINS na vaší síti.

Protokol DHCP systému Windows 2000 zajišťuje podporu multimédií pomocí zlepšeného sledování, modul snap-in správu a podporu vícesměrového vysílání. Protokol DHCP systému Windows 2000 je také dynamicky integrován se systémem DNS Windows 2000 v rámci podpory služby Active Directory. Starší verze systému DNS nenabízejí tuto podporu a plánujete-li používat službu Active Directory nebo chcete-li vyrovnávat zatížení serverů DHCP pomocí služby vyrovnávání zatížení, zvažte inovaci tohoto systému.

Instalování služby Směrování a vzdálený přístup (Routing and Remote Access) systému Windows 2000 je nezbytné pro linky mezi sítěmi LAN a zabezpečenými linkami VPN a pro zajištění vzdáleného přístupu. Služba Směrování ze vzdáleného přístupu je integrovaná do systému Windows 2000 a podporuje různé další protokoly, jako jsou IPX/SPX a AppleTalk.

Jestliže zavádíte systém Windows 2000 do kombinovaného prostředí se systémem UNIX, poznamenejte si verzi služby BIND existující na systému. Systém Windows 2000 je sice plně kompatibilní s dřívějšími verzemi BIND, s verzemi služby BIND 4.9.4 a novějším však nabízí zlepšenou funkčnost DNS.

Příprava řadičů domén

Některé společnosti plánují postupné zavádění systému Windows 2000 do svých produkčních prostředí, jiné zase plánují úplnou migraci na nový systém. Když systém Windows 2000 nainstalujete jen na několik serverů v organizaci, můžete zachovat existující

cí domény systému Windows NT 4.0 a vztahy důvěryhodnosti v rámci domén systému Windows 2000 a poskytnout společnosti čas na seznámení s koncepty a operacemi systému Windows 2000. Další informace o strategiích migrace najdete v kapitole „Určení strategií migrace domén“ v této knize.

Systém Windows 2000 je vytvořen tak, aby mohl pracovat v síti systému Windows NT 4.0. Pracovní stanice Windows NT 4.0 používající protokol NTLM mohou odesílat požadavky na síťové ověření libovolnému řadiči domény se systémem Windows 2000, který funguje jako řadič domény v doméně systému Windows NT. Vztahy důvěryhodnosti se mezi doménami systému Windows 2000 a doménami systému Windows NT 4.0 vytvářejí snadno a podporují ověřování mezi doménami. Při zavádění systému Windows 2000 nemusíte migrovat všechny své domény systému Windows NT 4.0 na domény systému Windows 2000 najednou.

Během inovace domény na systém Windows 2000 musíte nejprve v dané doméně inovovat hlavní řadič domény. Následně můžete libovolným tempem inovovat záložní řadiče dané domény na řadiče domény systému Windows 2000. Pak přidáte doménu do stromu služby Active Directory. Členské servery a klientské počítače můžete inovovat nezávisle na své strategii inovace domén, nenainstalujete-li však žádný řadič domény se systémem Windows 2000, tyto počítače nebudou mít přístup ke službě Active Directory a k dalším pokročilým funkcím.

Když inovujete řadič domén, pak musíte mít (stejně jako v případě většiny operací souvisejících se sítí) plán návratu k původnímu stavu, pokud se něco pokazí. Jedním z úkolů, který musíte vykonat v rámci přípravy na inovaci řadiče domény, je aktualizovat nějaký záložní řadič domény a následně jej izolovat, aby mohl fungovat jako řadič domény pro obnovení. Další informace o přípravě řadiče domény pro obnovení najdete v kapitole „Určení strategií migrace domén“ v této knize.

Jestliže řadič domény se systémem Windows 2000 stále funguje v doméně obsahující záložní řadiče se systémem Windows NT, celkový počet objektů (uživatelů, skupin uživatelů a počítačů) v dané doméně nesmí překročit doporučený limit pro domény systému Windows NT, který má hodnotu 40 000.

Příprava členských serverů

Členský server je libovolný server, který funguje jako člen domény Windows NT nebo Windows 2000, který však není řadičem domény. Mezi role členských serverů patří:

- Souborové, aplikační a tiskové servery
- Webové a proxy-servery a servery vzdáleného přístupu
- Databázové servery
- Certifikační servery

Když na své členské servery nainstalujete systém Windows 2000, zlepší se funkce rolí jednotlivých členských serverů.

Nezapomeňte při vyhodnocování kompatibility hardwaru počítače zvážit jeho roli po inovaci. Neexistují žádné přesné specifikace pro odhad hardwarových součástí potřebných k určité funkci. Budete muset otestovat počítač v jeho roli (nejlépe v testovací laboratoři a nikoli v produkční síti) – jen tak zjistíte, zda je dostatečný z hlediska rychlosti procesoru, paměti RAM a místa na pevném disku a zda je při provozování ovladačů, aplikací a protokolů jeho zamýšlené role dostatečně výkonný.

Další informace o přípravě členských serverů najdete v kapitolách „Inovace a instalace členských serverů“ and „Automatizování instalace a inovace serverů“ v této knize.

Příprava infrastruktury zabezpečení

Systém Microsoft Windows 2000 byl vytvořen tak, aby zajistil velmi vysokou úroveň zabezpečení dat a zároveň umožnil správcům její jednoduchou implementaci a správu. Nové funkce, jako jsou protokol IPSec, ověřování protokolem Kerberos a veřejné klíče, nabízejí vyšší úroveň zabezpečení než předchozí verze systému Windows NT.

Protože je systém Windows 2000 navržen tak, aby mohl pracovat v existující struktuře domén systému Windows NT, můžete snadno do své existující struktury zabezpečení sítě zavést servery se systémem Windows 2000. Při migrování či inovaci existující sítě systému Windows NT na systém Windows 2000 však vaši strategii zabezpečení ovlivní bezpečnostní funkce systému Windows 2000, které plánujete zavést. Jestliže například v současné době používáte ve své síti program Microsoft Proxy Server, budete jej muset inovovat pro systém Windows 2000 a nainstalovat příslušný klientský software, abyste jej mohli nadále používat.

Systém Windows 2000 podporuje infrastrukturu veřejných klíčů (Public Key Infrastructure – PKI), metodu ověřování používající digitální certifikáty, certifikační úřady a software správy certifikátů. Ověřování pomocí certifikátů můžete použít k zabezpečení klientů elektronické pošty a internetových komunikací, k podpoře technologie karet Smart Card a k zabezpečení komunikace (pomocí protokolu IPSec) klientů, kteří nepodporují protokol Kerberos. Další informace o plánování a zavádění PKI najdete v kapitole „Plánování infrastruktury veřejných klíčů“ v této knize. Podrobnosti zavádění PKI jsou určeny specifickými certifikačními službami, které používáte – můžete používat službu Microsoft Certificate Services nebo certifikační služby nezávislých společností.

Definujte požadavky na certifikáty, postupy a strategie. Přemýšlejte-li o implementování PKI jiné společnosti, ujistěte se, že je tato struktura kompatibilní se systémem Windows 2000. V takovém případě znamená kompatibilita podporu certifikačních hierarchií s kořeny, jaké jsou implementovány v systému Windows 2000. Uvědomte si, že PKI systému Windows 2000 nenahradí existující vztahy důvěryhodnosti mezi doménami systému Windows ani mechanismy autorizování, jako je protokol Kerberos. Funkce PKI systému Windows 2000 jsou integrovány s řadiči domény a ověřovacími službami protokolu Kerberos.

Strukturu PKI můžete implementovat ve fázích v zájmu podpory určitých cílů, jako je podpora elektronické pošty nebo podpora ověřování pro existující systémy, podle svých priorit.

▼ Chcete-li implementovat PKI ve fázích, postupujte takto:

1. Instalujte kořenové certifikační úřady v nadřazených doménách v jednotlivých strozech systému Windows 2000 v doménové struktuře.
2. Instalujte prostřednické certifikační úřady v doménách jednotlivých organizačních jednotek (útvárů).
3. Instalujte a konfiguruje vystavující certifikační úřady a služby v doménách pro jednotlivé skupiny uživatelů na jednotlivých sídlech podle potřeby.

Příprava klientů

Protože je systém Windows 2000 navržen tak, aby umožňovat spolupráci s jinými systémy (interoperabilitu), klientské počítače s předchozími verzemi systému Windows mohou spolupracovat se systémem Windows 2000 v kombinovaném prostředí. Inovace klientských počítačů na systém Windows 2000 Professional vám však poskytne zlepšení zabezpečení klientských počítačů a uživatelů, vyšší spolehlivost a vyšší funkčnost.

Na systém Windows 2000 Professional nelze inovovat všechny předchozí verze systému Windows. Na systém Windows 2000 Professional lze inovovat následující verze systému Windows a Windows NT:

Windows 95

Lze inovovat všechny verze včetně OSR2.x. Pokud však vaši klienti provozují systém Windows 95 ze serveru, musíte systém instalovat přímo na daný počítač, nebo vykonat čistou instalaci systému Windows 2000 Professional.

Windows 98

Lze inovovat všechny verze. Viz oddíl „Úvahy o inovaci na systém Windows 2000 Professional“ uvedený dále.

Windows NT 4.0 Workstation

Lze inovovat všechny verze. Viz oddíl „Úvahy o inovaci na systém Windows 2000 Professional“ uvedený dále.

Windows NT 3.51 Workstation

Lze inovovat všechny verze.

Důležitým požadavkem kladeným na klientské počítače je kompatibilita jejich hardwaru a ovladačů se systémem Windows 2000.

Úvahy o inovaci na systém Windows 2000 Professional

Některé aplikace a ovladače, které v předchozím operačním systému fungovaly, budou mít s řádnou funkcí v prostředí systému Windows 2000 Professional problémy. Následující oddíly popisují problémy, s nimiž se můžete setkat při inovování klientů systémů Windows NT, Windows 95 a Windows 98.

Poznámka Systémy Windows verze 3.1 a dřívější nelze přímo inovovat.

Inovování klientů systému Windows NT

Klienty systému Windows NT lze obvykle na systém Windows 2000 Professional inovovat jednoduše. Platí tu následující úvahy:

- Žádné aplikace na úrovni klientů, které závisejí na filtrech systému souborů, jako je antivirový software a programy diskových kvót, nebudou řádně fungovat. To je dáno změnami v modelu systému souborů Windows 2000.
- Jestliže vaši klienti provozují síťové protokoly, které nemají aktualizované verze ve složce I386\Winntupg, jež se nachází na CD operačního systému Windows 2000, znovu zvažte používání těchto protokolů, nebo si pro inovaci zajistěte jejich aktualizované verze kompatibilní se systémem Windows 2000.
- Jestliže vaši klienti používají nástroje řízení spotřeby od jiných společností, zvažte použití rozhraní Advanced Configuration and Power Interface (ACPI) a Advanced

Power Management (APM) systému Windows 2000, kterými nahradíte předchozí řešení.

- Před inovováním na systém Windows 2000 odstraňte všechny ovladače Plug-and-Play od jiných společností.

Inovování klientů systémů Windows 95 a Windows 98

Cesta inovování klientů systémů Windows 95 a Windows 98 je obvykle jednoduchá. Při zvažování inovace těchto klientů však pamatujte na následující problémy:

- Jak již bylo řečeno, žádné aplikace na klientské úrovni, které závisejí na předchozím systému souborů, nebudou správně fungovat. Nebudou například fungovat žádné nástroje pro kompresi disku ani třeba defragmentátory disku. Antivirové aplikace musí být kompatibilní se systémem Windows 2000, aby správně pracovaly.
- Aplikace a nástroje používající ovladače virtuálních zařízení (VxD) a ovladače .386 také nebudou správně fungovat. Kontaktujte výrobce daných aplikací a zjistěte, zda existují aktualizované ovladače.
- Mnoho klientských počítačů má instalováno ovladače zařízení od jiných společností. Při instalaci těchto ovladačů se někdy také nainstaluje nějaká aplikace ovládacích panelů, které nabídnou určité další funkce (například nástroj pro řízení konfigurace). Tyto aplikace ovládacích panelů otestujte v prostředí systému Windows 2000 a jejich výrobce se zeptejte na kompatibilitu se systémem Windows 2000.
- Upozornění uvedená v předchozím oddílu ohledně síťových protokolů, nástrojů řízení spotřeby od nezávislých společností a ovladačů Plug-and-Play od jiných výrobců platí také pro klienty systémů Windows 98 a Windows 95.

Příprava na spolupráci s jinými systémy

Mnoho organizací pracuje v heterogenním prostředí, kde se nachází kombinace různých operačních systémů. Systém Windows 2000 Server nabízí služby bran k jiným operačním systémům a umožňuje tak klientům Windows získávat přístup k jiným operačním systémům a prostředkům. Například po nainstalování součásti Gateway Services for NetWare budou moci vaši klienti Windows těžit z výhod své existence v síti Windows 2000 a zároveň budou moci procházet hierarchiemi služby Novell Directory Services (NDS), používat přihlašovací skripty systému Novell verze 4.x a novějšího a ověřovat se serveru Novell.

Seznam úkolů přípravy infrastruktury sítě

Tabulka 6.1 uvádí doporučené úkoly, které byste měli vykonat v rámci přípravy existující infrastruktury sítě na systém Windows 2000.

Tabulka 6.1 Seznam úkolů plánování přípravy infrastruktury

Úkol	Umístění v kapitole
Vytvořte inventář hardwaru a softwaru.	Inventář hardwaru a softwaru
Ujistěte se, že se veškerý používaný hardware nachází na seznamu HCL a že odpovídá vašim plánům zavádění, a určete specifický plán inovace hardwaru pro jednotlivé počítače.	Inventář hardwaru a softwaru
Dokumentujte serverové a klientské síťové konfigurace. Dokumentujte servery infrastruktury.	Infrastruktura sítě
Dokumentujte podrobnosti o konfiguraci sítě – služby překladu názvů, adresování IP, podrobnosti o linkách WAN a fyzické rozmístění.	Infrastruktura sítě
Vytvořte fyzický a logický diagram sítě.	Infrastruktura sítě
Dokumentujte konfiguraci členských serverů.	Souborové, tiskové a webové servery
Identifikujte všechny kritické aplikace a prověřte jejich kompatibilitu se systémem Windows 2000.	Obchodní či výrobní aplikace
Dokumentujte strukturu domén a model správy včetně vztahů důvěryhodnosti, umístění hlavních a záložních řadičů domén a oborů názvů DNS.	Architektura adresářových služeb
Dokumentujte podrobnosti o zabezpečení sítě.	Zabezpečení
Stabilizujte síť.	Předběžné kroky
Zajistěte síťové protokoly.	Předběžné kroky
Připravte fyzickou infrastrukturu.	Příprava fyzické infrastruktury
Zjistěte kompatibilitu síťových služeb se systémem Windows 2000.	Příprava fyzické infrastruktury
Připravte servery infrastruktury.	Příprava serverů
Inovujte řadiče domén.	Příprava řadičů domén

KAPITOLA 7

Určení strategií konektivity sítě



Systém Microsoft Windows 2000 Server obsahuje několik funkcí, které mohou správci sítě využít ke zlepšení nových nebo existujících infrastruktur sítě. Tato kapitola obsahuje informace o problémech konektivity sítě, přidělování adres, protokolu TCP/IP další úvahy o protokolech. Tyto informace vám pomohou určit nejlepší strategii konektivity sítě vaší organizace.

Chcete-li ze čtení této kapitoly získat maximum, budou se vám hodit určité znalosti o systému Microsoft Windows NT a jeho práci v síti. Také byste měli být seznámeni se základními i pokročilými koncepty práce v síti, jako jsou adresování protokolu TCP/IP, protokoly směrování a vzdálený přístup.

V této kapitole

Přehled konektivity sítě 152

Externí konektivita v organizaci 155

Protokol TCP/IP systému Windows 2000 157

Infrastruktura směrování protokolu IP 169

Protokol DHCP systému Windows 2000 177

Technologie Asynchronous Transfer Mode v systému Windows 2000 180

Služba Quality of Service 185

Seznam úkolů plánování strategií práce v síti 186

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Vyhodnocení infrastruktury současné sítě, protokolů a směrování
- Strategie konektivity sítě
- Diagram fyzického návrhu sítě
- Návrh infrastruktury síťových protokolů a směrování

Související informace v sadě Resource Kit

- Další informace o protokolu TCP/IP systému Windows 2000 najdete v knize *Microsoft Windows 2000 Server Sítě TCP/IP*.
- Další informace o službě Směrování a vzdálený přístup (Routing And Remote Access) systému Windows 2000 najdete v knize *Microsoft Windows 2000 Server Internetworking*.

- Další informace o zavádění zabezpečení v infrastruktuře systému Windows 2000 najdete v kapitole „Určení strategií zabezpečení sítě systému Windows 2000“ v této knize.

Přehled konektivity sítě

Při určování implementace nebo inovace sítě na systém Windows 2000 musíte zvážit několik věcí. Existuje-li nějaký síťový diagram vaší současné sítě, pak s jeho pomocí určete, kde se strategicky budou implementovat nové funkce systému Windows 2000. Například se musíte podívat na klienty, servery, přepínače a směrovače a zjistit, zda právě používají nebo nepoužívají služby, jako jsou Quality of Service (QoS), Asynchronous Transfer Mode (ATM) nebo protokoly směrování. V případě potřeby také prostudujte a upravte schémata adresování protokolu TCP/IP, abyste mohli plně využít nové funkce protokolu Dynamic Host Configuration Protocol (DHCP) systému Windows 2000.

Pokud jste tak zatím neučinili, vytvořte fyzické a logické diagramy odrážející vaše síťové potřeby. To je velmi důležité, protože tyto diagramy vám dávají celkový přehled infrastruktury ještě před jejím skutečným sestavováním. To umožňuje spolupráci návrháře a správce při umísťování síťových systémů a zařízení. Následující oddíly popisují, co můžete do tohoto diagramu zahrnout.

Síťové pozice

V diagramu graficky znázorníte, kde jsou umístěna síťové pozice. To vám pomůže při určování metod konektivity rozlehlé sítě a vzdálených sídel. Sídla musíte implementovat podle geografických hranic, hranic správy, nebo obou prvků.

Metody vzdálené konektivity

Do svého diagramu zahrňte média připojení vzdálených sídel k centrálnímu sídlu. Může jít o linky T1, E1, Frame Relay, Integrated Services Digital Network (ISDN) nebo obyčejné telefonní linky (plain old telephone service – POTS). Pomocí diagramu můžete také zobrazit typy směrovačů používaných k připojení sídel k páteřnímu spojení rozlehlé oblasti. Může jít o směrovače systému Windows 2000 nebo o směrovače od různých nezávislých výrobců. Zobraďte metody připojení vzdálených uživatelů k sídlům pomocí technologií, jako je přímé telefonické spojení nebo virtuální soukromá síť (virtual private network – VPN).

Interní konektivita sítí LAN uvnitř pozic

Vytvořte grafický popis interních sítí sídel, abyste mohli využít nové funkce systému Windows 2000 co nejvýhodněji. Zahrňte sem následující informace:

Síťové médium

Uveďte plánovaný typ použité infrastruktury, jako je konektivita 10 nebo 100BaseT, ATM nebo gigabitový Ethernet. Plánujete-li použít ATM, určete, které sekce sítě budou přímo připojeny k ATM s využitím přenosu IP přes ATM nebo emulace místní sítě (local area network emulation – LANE).

Infrastruktura směrování a přepínání

Určete, kde budou směrovače a přepínače. To je důležité k zachování šířky pásma sítě a minimalizaci vzniku úzkých míst. Také se přesvědčte, že hardware směrová-

ní a přepínání, který chcete používat, podporuje takové technologie, jako je například QoS.

Protokoly

Plánujete-li používat protokol TCP/IP, pro každou podsít v sídle vytvořte schéma adresování IP. Plánujete-li používat jiné protokoly, jako je IPX, AppleTalk nebo NetBIOS Enhanced User Interface (NetBEUI), také je zobrazte. Také zvažte použití směrovacích protokolů, jako jsou OSPF nebo RIP, které lze použít k propojení sítí. Další informace použití protokolu TCP/IP najdete v kapitole „Protokol TCP/IP systému Windows 2000“ v knize *Microsoft Windows 2000 Server Sítě TCP/IP*. Také si přečtěte kapitoly „Unicast IP Routing“, „IPX Routing“ a „Services for Macintosh“ v knize *Microsoft Windows 2000 Server Internetworking*.

Struktura systému DNS a služby Active Directory

Navrhněte strukturu systému DNS a služby Active Directory ve vaší síti. Do diagramu sítě uveďte také logický diagram domén, který zobrazuje domény a doménové struktury ve vaší společnosti. Další informace o adresářové službě Active Directory najdete v kapitole „Návrh struktury služby Active Directory“ v této knize.

Infrastruktura serverů

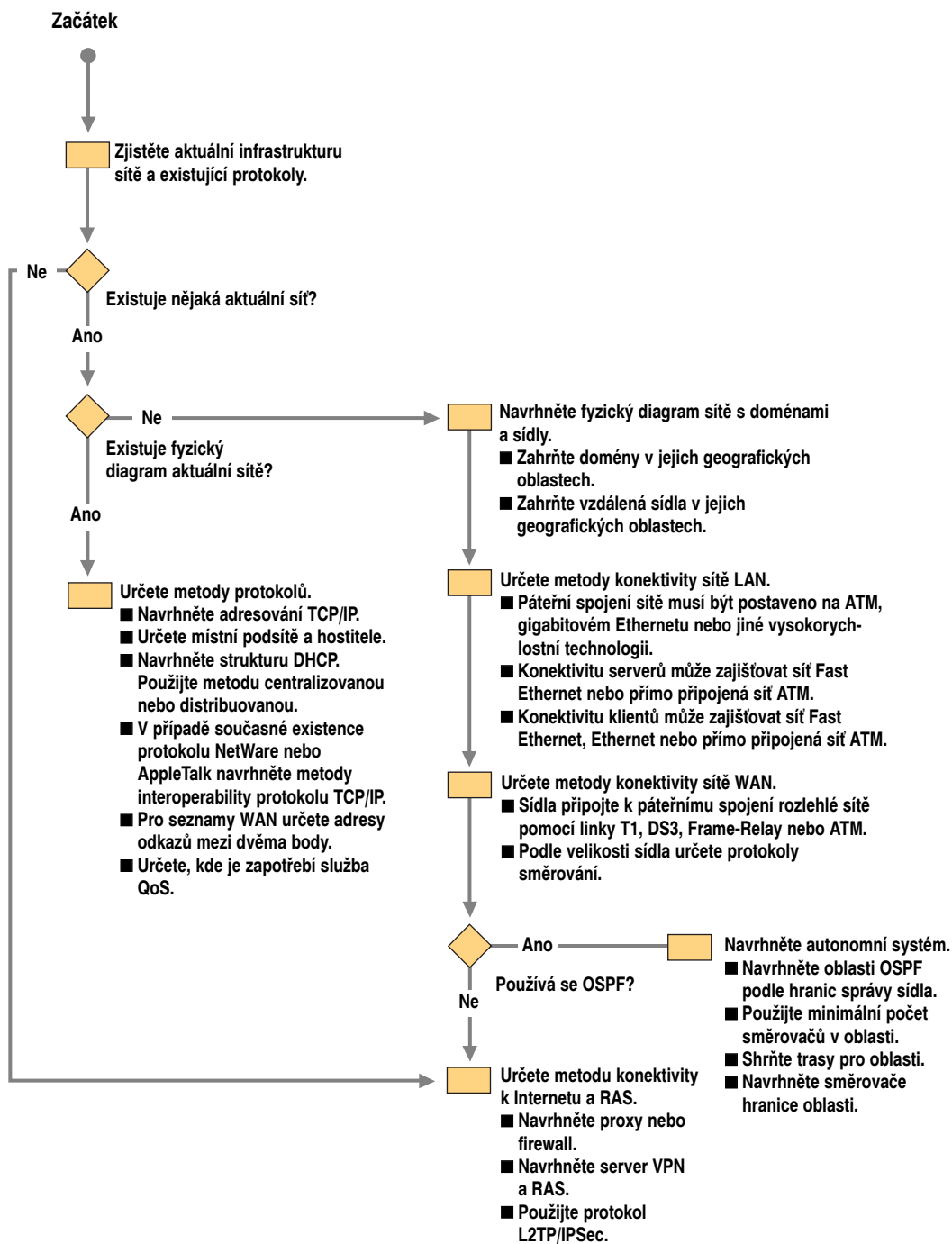
V diagramu znázorněte umístění serverů DNS, DHCP a WINS.

Metody vzdáleného připojení

Ve svém diagramu zobrazte, jak se k podnikové síti budou připojovat vzdálení klienti a vzdálené sítě.

Následující oddíly pojednávají o návrhu takové sítě, která do vaší organizace nejlépe začlení funkce systému Windows 2000 Server, a uvádějí kroky určování strategie konektivity sítě.

Obrázek 7.1 ilustruje základní kroky určování strategie konektivity sítě.



Obrázek 7.1

Proces určení strategií konektivity sítě

Při návrhu sítě systému Windows 2000 je nejprve zapotřebí navrhnout mnoho menších částí sítě, které formují celkovou infrastrukturu. Následující oddíly popisují různé aspekty rozlehlé sítě (WAN) a jednotlivé postupu a úvahy. Jsou zde popsány aspekty externí, rozsáhlé sítě vzhledem k infrastruktuře podnikové sítě, jako jsou demilitarizované zóny (DMZ), implementace sídel a konektivita vzdáleným přístupem. Oddíly se zabývají také interními aspekty sítě, jako jsou protokoly, zabezpečení a metody konektivity místních sítí (LAN).

Externí konektivita v organizaci

Aby mohli vzdálení uživatelé získat přístup ke vzdálenému sídlu, musíte zavést takovou metodu konektivity, která umožní propojení mezi sídly a konektivitu vzdálených klientů. Centrální sídlo vaší organizace musí mít síť, která umožní jiným sídlům a vzdáleným klientům získat přístup k interní síťové struktuře centrálního sídla. Následující oddíly popisují, co musíte zahrnout do strategie externí konektivity.

Návrh demilitarizované zóny

Důležitou součástí každé velké podnikové sítě je zóna DMZ. Tento oddíl popisuje, k čemu se DMZ používá, a oddíly uvedené dále v této kapitole uvádějí příklady použití DMZ.

Demilitarizovaná zóna (DMZ) je síť umožňující rozšíření Internetu do soukromé sítě a současné zajištění zabezpečení dané sítě. DMZ dává podniku možnost používat Internet jako médium šetřící náklady a zároveň se na Internetu prezentovat. DMZ šetří peníze, protože využívá existující infrastrukturu Internetu ve spojení se sítěmi VPN, a tedy šetří náklady na propojení rozlehlých sítí pronajatými komunikačními linkami. DMZ je v zásadě síť, která se nachází mezi soukromou sítí a Internetem.

DMZ obsahuje zařízení, jako jsou servery, směrovače a přepínače, které udržují zabezpečení tím, že zabráňují vystavení interní sítě Internetu. Servery, které se nacházejí uvnitř DMZ, se obvykle skládají z polí proxy-serverů, jež síť používá k zajištění přístupu na síť WWW pro interní uživatele, externí služby Internet Information Services (IIS), kterou může organizace využívat pro své prezentování na Internetu, a dalších serverů VPN, jež se používají k zajištění zabezpečených připojení vzdálených klientů. Další informace o sítích VPN najdete v oddílech „Zabezpečení sítí VPN“ a „Sítě VPN využívající protokol L2TP ve spojení s protokolem IPSec“ dále v této kapitole.

Příklad DMZ je uveden na obrázku 7.2. Zařízení na okraji DMZ je směrovač. Pro větší organizaci by měla být rychlost připojení na Internet alespoň na úrovni DS3 neboli 45 Megabitů za sekundu (Mb/s). Propojení mezi směrovačem a servery v DMZ může být libovolnou vysokorychlostní technologií LAN, očekáváte-li však značný internetový provoz, mělo by se jednat o gigabitový Ethernet nebo síť ATM.

V případě menších a středně velkých sítí můžete na rozhraní DMZ používat jako směrovač službu Směrování a vzdálený přístup (Routing and Remote Access) systému Windows 2000. Před nežádoucím provozem se ochráníte a bezpečnost zajistíte pomocí filtrování paketů na internetových rozhraních.

Konektivita sídel organizace

Mnoho velkých korporací má kanceláře, které se nacházejí na různých geografických místech. Tyto kanceláře potřebují nějakou možnost připojit se a zůstat připojeny k hlav-

nímu neboli centrálnímu sídlu. V různých částech světa se používají odlišná média připojení rozlehlých sítí. Tabulka 7.1 popisuje různé technologie rozsáhlých sítí a jejich využití.

Tabulka 7.1 Technologie rozlehlých sítí

Technologie rozlehlých sítí	Definice
T1	Přenáší data rychlostí 1,544 Mb/s a skládá se z 23 B-kanálů, které se používají pro data, a jednoho D-kanálu, který se používá pro časování. T1 lze také rozdělit na samostatné segmenty 64 kilobitů za sekundu (Kb/s).
E1	Používá se především v Evropě. Přenáší data rychlostí 2,048 Mb/s.
T3	Přenáší data DS3 rychlostí 44,736 Mb/s.
Frame Relay	Technologie přepínání paketů, která je považována za náhradu X.25. Obecně pracuje na rychlostech až do úrovně T1.
Digital Subscriber Line (DSL)	Technologie DSL zahrnuje asymetrickou digitální linku (asymmetric digital subscriber line – ADSL), vysokorychlostní digitální linku (high-data-rate digital subscriber line – HDSL), jednolinkovou digitální linku (single-line digital subscriber line – SDSL) a digitální linku s velmi vysokou rychlostí (very-high-data-rate digital subscriber line – VDSL).

V případě linek s nízkým zatížením nebo pro účely zálohování spojení se může konektivita sídla také opírat o využití telefonických médií, jako jsou Integrated Services Digital Network (ISDN) nebo analogové telefonické linky (POTS). Organizace může mít například malé sídlo, k němuž se obvykle připojuje částečnou linkou T1, když však jejich poskytovatel rozsáhlé sítě selže, mohou jako zálohu použít linku POTS.

Jednotlivá sídla v organizaci jsou obvykle propojena přes směrovače. Služba Směrování a vzdálený přístup (Routing and Remote Access) systému Windows 2000 nabízí směrovací služby umožňující organizacím z hlediska nákladů výhodně připojovat vzdálená sídla k centrálnímu sídlu společnosti. Sídla mohou být připojena přes Internet pomocí sítí VPN, čímž organizace šetří peníze. Máte-li sídlo, které nevyžaduje stálé připojení k centrálnímu sídlu, pak můžete implementovat vytáčené připojení mezi směrovači na požádání, čímž se dále snižují náklady na připojení přes rozsáhlou síť.

Konektivita vzdálených klientů

Jednou z věcí, které zaručují větší efektivitu organizace, je schopnost jejích uživatelů přistupovat k prostředkům společnosti, ať už jsou doma nebo na cestách. Mnoho společností začíná využívat strategii práce doma. Tato strategie umožňuje zaměstnancům ušetřit náklady na dojíždění do práce a společnosti zároveň dovolí nákladově efektivně spravovat prostor v kancelářích při růstu počtu zaměstnanců. Další výhodou implementace konektivity vzdálených klientů je možnost povolit cestujícím prodejcům a technikům telefonicky se připojit a převzít si soubory a zprávy elektronické pošty.

V každém případě se uživatelé, kteří nejsou v kanceláři, potřebují připojovat k souborovým serverům a serverům elektronické pošty, jež se nacházejí v infrastruktuře sítě společnosti. Služba Směrování a vzdálený přístup systému Windows 2000 to zajišťuje

tím, že dokáže přijímat příchozí připojení vzdáleného přístupu a data pak směřovat do jejich cílových míst. Službu Směrování a vzdálený přístup lze používat také k příjmu příchozích připojení VPN a zajistit tak zabezpečený způsob přenosu dat přes Internet. Další informace o sítích VPN najdete v oddílech „Zabezpečení sítí VPN“ a „Sítě VPN využívající protokol L2TP ve spojení s protokolem IPSec“ dále v této kapitole.

Vzdálený přístup klientů k infrastruktuře společnosti se neomezuje výhradně na klienty protokolu Internet Protocol (IP). Služba Směrování a vzdálený přístup systému Windows 2000 umožňuje také dalším klientům prostřednictvím svých funkcí podpory více protokolů používat vzdálený přístup – sem patří klienti systémů Macintosh, UNIX nebo NetWare. Protokoly VPN podporované v systému Windows 2000, Point-to-Point Tunneling Protocol (PPTP) a Layer 2 Tunneling Protocol (L2TP), také podporují více-protokolová připojení přes Internet.

Protokol TCP/IP systému Windows 2000

Sítě v dnešních organizacích vyžadují protokol, který je na výši z hlediska výkonu a škálovatelnosti a který kladе vysoký důraz na spolupráci s Internetem. Protokol TCP/IP je standardní sadou protokolů, tvoří základnu propojených sítí s velkým rozsahem zasahujícím přes síť LAN i WAN a rychle se stává hlavním protokolem jak pro intranety tak i pro Internet.

Protokol TCP/IP systému Windows 2000 je:

- síťový protokol vycházející z průmyslových standardů,
- směrovatelný síťový protokol, který podporuje připojení serverů a klientů se systémem Windows k sítím LAN i WAN,
- škálovatelný protokol pro integraci serverů a pracovních stanic se systémem Windows s heterogenními systémy,
- základnou pro získání přístupu ke globálním internetovým službám.

Protokol Microsoft TCP/IP poskytuje základní a pokročilé funkce umožňující počítači se systémem Windows 2000 připojit se k počítačům s jinými spuštěnými systémy, například se systémem UNIX, a sdílet s nimi informace.

Nové funkce v sadě TCP/IP systému Windows 2000

Nová sada Microsoft TCP/IP je navržena tak, aby se sama přizpůsobovala z hlediska spolehlivosti a výkonu. Následující čtyři oddíly popisují nové funkce v sadě TCP/IP.

Konfigurace automatického privátního adresování IP

Konfigurace automatického privátního adresování IP (Automatic Private IP Addressing – APIPA) spočívá v tom, že není-li přítomen server DHCP, automaticky se alokují jedinečné adresy z rozsahu 169.254.0.1 až 169.254.255.254 s maskou podsítě 255.255.0.0. Technologie APIPA se používá v sítích s jedinou podsítí, jako jsou síť SOHO, které svou malou velikostí neospravedlňují provozování samostatného serveru DHCP.

Máte-li například domácí kancelář a potřebujete mít nějakou možnost distribuce adres IP interním serverům a klientům systému Windows 2000, stačí vám jen spojit systém dohromady nějakým síťovým médiem – každý počítač se systémem Windows 2000 si pak sám přiřadí adresu z oblasti adres APIPA.

Podpora velkých datových rámců

Podpora velkých datových rámců příjmu zvyšuje množství dat, které lze najednou v rámci jednoho připojení uložit do zásobníku, čímž se snižuje provoz v síti a zrychluje přenos dat.

Poznámka Podpora velkých datových rámců není standardně aktivní. Výchozí velikost datových rámců má hodnotu přibližně 16 kilobajtů (KB), což je dvojnásobek velikosti datových rámců v systému Windows NT 4.0.

Výběrové potvrzení

Výběrová potvrzení umožňují příjemci informovat odesílatele o nutnosti opakovaného zaslání pouze těch dat, která nebyla přijata, a nikoli tedy celých bloků dat. To zajišťuje lepší využití šířky pásma sítě.

Zlepšený odhad času od odeslání požadavku do příchodu ozvěny

Protokol TCP používá k odhadu doby potřebné pro komunikaci mezi odesílatelem a příjemcem čas od odeslání požadavku do příchodu ozvěny (RTT). Protokol TCP systému Windows 2000 lépe odhaduje RTT pro nastavení časovačů přenosů, čímž se zlepšuje celková výkonnost protokolu TCP. Toto zlepšení protokolu TCP pomáhá zejména v sítích WAN zasahujících na velmi dlouhé vzdálenosti nebo přes pomalá připojení, jako je satelitní komunikace.

Úvahy o plánování protokolu Microsoft TCP/IP

Jestliže vaše síť zatím nepoužívá protokol TCP/IP, pak musíte vyvinout zevrubný plán adresování IP ve vaší síti. Při plánování infrastruktury IP nezapomeňte na identifikátory sítí IP a masky podsítí. Pracovní plán vytvořte s využitím informací uvedených v následujících oddílech.

Třídy adres IP

Volba použitých tříd adres závisí na tom, zda je vaše síť soukromá nebo připojená k Internetu. Adresování v síti je také určeno velikostí vaší infrastruktury, která má přímý vztah k použitému rozsahu adres. Při plánování adres IP pro svou síť se zamyslete nad následujícími tématy:

Inventář fyzických podsítí a hostitelů

Spočítejte podsítě a hostitele, které máte v současné síti, a následně pomocí rozdělení adresového prostoru IP do podsítí určete, kolik jich budete potřebovat pro novou síť. Přitom počítejte přinejmenším s plánovaným růstem na příštích pět let, aby vám příliš brzy nedošly adresy nebo podsítě. Je-li vaše síť přímo připojena na Internet, budete potřebovat oblast adres IP, kterou vám přiřadil váš poskytovatel připojení k Internetu. Další informace o rozdělení adresových prostorů IP do podsítí nejdete v kapitole „Internet Protocol Security“ v knize *Microsoft Windows 2000 Server Sítě TCP/IP*.

Poznámka Je důležité, aby ve vaší síti existovalo jen velmi málo systémů TCP/IP, které jsou přímo připojeny k Internetu, jako je zóna DMZ. Čím méně systémů je přístupných z Internetu, tím bezpečnější je vaše síť před útokem.

Soukromé sítě s připojením proxy k Internetu a bez tohoto připojení

V případě sítí TCP/IP, které nejsou připojeny k Internetu, nebo jsou k Internetu připojeny přes proxy-server, můžete použít libovolný rozsah platných adres IP ze tříd adres A, B a C. Doporučujeme vám však používat soukromé adresy, abyste nemuseli své připojení sítí přechíslovávat, až se jednou připojíte k Internetu. Soukromý prostor adres IP je definován jako sada tří adres IP vyhrazených organizací Internet Assigned Numbers Authority (IANA). Vyhrazené rozsahy adres IP jsou:

- 10.0.0.1/8 až 10.255.255.254/8
- 172.16.0.1/12 až 172.31.255.254/12
- 192.168.0.1/16 až 192.168.255.254/16

Poznámka Další informace o soukromém adresování najdete v dokumentu RFC 1918. Zde uvedený rozsah soukromých síťových adres používá k definování masek podsítí zápis předpony sítě, který se také označuje za zápis Classless Interdomain Routing (CIDR).

Masky podsítí a používání podsítí

Protože veřejných adres IP je nedostatek, můžete používání podsítí IP implementovat pomocí svých vlastních masek podsítí. Používání vlastních podsítí je definováno jako používání podsítí, směrování Classless Interdomain Routing (CIDR) nebo maska podsítě s proměnnou délkou (variable length subnet mask – VLSM). Pomocí používání vlastních podsítí IP překonáváte omezení výchozích masek podsítí a využíváte svou oblast adres IP výhodněji.

Když si upravíte délku masky podsítě, můžete tím omezit počet bitů používaných pro vlastní identifikátor hostitele. V některých případech můžete použít výchozí masky podsítí pro sítě standardní velikosti třídy A, B a C. Výchozí masky podsítí jsou desítkové hodnoty oddělené tečkami, které v adrese IP oddělují identifikátor sítě od identifikátoru hostitele. Máte-li například síťový segment a používáte-li rozsah adres IP třídy A se začátkem v hodnotě 10.0.0.0, bude vaší použitou výchozí maskou podsítě hodnota 255.0.0.0. Výchozí hodnoty masek podsítí jsou obvykle přijatelné v sítích bez speciálních požadavků, kde každý segment sítě IP odpovídá jedné fyzické síti.

Poznámka Chcete-li se vyhnout problémům s adresováním a směrováním, zajistěte, aby všechny počítače TCP/IP na všech síťových segmentech používaly stejnou masku podsítě.

Masky podsítí můžete také zobrazovat v adresách IP tak, že použijete zápis předpony sítě. Tato možnost vám dovoluje zobrazit zkrácenou verzi masky podsítě, přitom však zachovat její hodnotu. Tabulka 7.2 popisuje tento proces. Podtržené bity v tabulce 7.2 tvoří předpony sítě.

Tabulka 7.2 Masky podsítí využívající předponu sítě

Třída adresy	Maska podsítě dvojkově	Předpona sítě s desítkovým ekvivalentem
Třída A	11111111 00000000 00000000 00000000	/8 = 255.0.0.0
Třída B	11111111 11111111 00000000 00000000	/16 = 255.255.0.0
Třída C	11111111 11111111 11111111 00000000	/24 = 255.255.255.0

Protokol TCP/IP a služba Windows Internet Name Service

Windows Internet Name Service (WINS) je služba, která připojuje (mapuje) názvy základního systému vstupu a výstupu (NetBIOS) k adresám IP. V dřívějších verzích systému Windows se používala služba WINS ve spojení se službou DHCP k registraci názvů systému NetBIOS a dynamicky přiřazovaných adres IP v databázi WINS. V takovém případě požaduje hostitel podporující protokol DHCP po serveru DHCP nějakou adresu IP a daný server DHCP pak přiřadí klientovi DHCP nějaký server WINS. Po dokončení procesu propůjčení DHCP zaregistruje klient DHCP název systému NetBIOS a jemu přiřazenou adresu IP v databázi WINS.

Systém Windows 2000 zajišťuje integraci mezi službami DNS a WINS. Nemůže-li server DNS systému Windows 2000 přeložit plně kvalifikovaný název domény (fully qualified domain name – FQDN), převede daný FQDN na název systému NetBIOS a dotazuje se nakonfigurovaného serveru WINS. Adresa IP vrácená serverem WINS se odešle klientovi DNS.

Používáte-li pouze servery a klienty systému Windows 2000, nepotřebujete mít v systému Windows 2000 nad protokolem TCP/IP službu WINS a systém NetBIOS. Používáte-li operační systémy Windows NT verze 3.5x, Windows NT 4.0, Windows 95, Windows 98 nebo Windows 3.x, služba WINS je nadále vyžadována. Tyto systémy totiž používají k vytvoření připojení k místům sdílení souborů a tiskáren překlad názvů systému NetBIOS a relace NetBIOS.

Úvahy o návrhu systému WINS

Je-li vyžadován překlad názvů systému NetBIOS, každé sídlo v doméně musí mít alespoň jeden server WINS. Server WINS můžete nainstalovat na stejný systém jako server DNS, nebo jej můžete nainstalovat odděleně. Na jiné místo sítě musíte také nainstalovat záložní server WINS. Záložní server WINS můžete nainstalovat na stejný systém jako řadič domény Windows 2000, nebo jej můžete nainstalovat odděleně.

Služba Směrování a vzdálený přístup

Směrování je proces využití adresovacích informací, které se nacházejí v síťovém paketu, k určení cesty, jíž paket dosáhne svého cílového místa. Směrování je zapotřebí, když se zdrojový hostitel a cílový hostitel nacházejí na různých logických sítích. Směrování je vyžadováno ve větších síťových infrastrukturách, protože je nepraktické používat jednu sadu adres pro celou síť. Během růstu sítě totiž narůstá také složitost adresování. Navíc je nevhodné umístit všechny systémy ve velké síti na stejnou logickou síť, protože to má za následek velké množství síťového provozu.

Síť TCP/IP můžete rozdělit do segmentů tak, že rozdělíte rozsah adres IP do podsítí. Jakmile dojde k rozkladu adres IP, nově zformované *podsítě* používají k předávání dat

z jedné podsítě do druhé směrovače. Směrovače lze použít také ke spojení odlišných sítí, jako jsou Ethernet, ATM a Token Ring.

Ke sledování cest z hostitelů nacházejících se v jedné podsíti k hostitelům z jiné podsítě se používají směrovací (trasovací) tabulky. Jak roste velikost sítí, zvyšuje se také počet směrovačů v infrastruktuře a zvětšují se směrovací tabulky. Pokud by se měli správci starat o tyto směrovače, museli by neustále sledovat směrovače v síti, které přejdou do režimu offline, a spojení, která dočasně selžou, a následně ručně zadávat tyto informace do směrovacích tabulek. Směrovače však používají k dynamické aktualizaci směrovacích tabulek při změnách sítě standardní směrovací protokoly.

Systém Windows 2000 Server poskytuje řešení pro podniky vyžadující směrování mezi sítěmi LAN a nabízí tak alternativu k zakoupení vyhrazeného hardwarového směrovače – integrovanou součástí systému Windows 2000 je služba Směrování a vzdálený přístup (Routing and Remote Access). Tato služba podporuje možnost dynamicky směrovat provoz protokolů TCP/IP, Internetwork Packet Exchange (IPX) a AppleTalk, přičemž využívá zabudované směrovací protokoly. Služba Směrování a vzdálený přístup může také zajistit konektivitu vzdálené kanceláře, protože podporuje připojení přes rozlehlé sítě.

Nové funkce služby Směrování a vzdálený přístup systému Windows 2000

Tento oddíl popisuje nové funkce služby Směrování a vzdálený přístup systému Windows 2000, které umožňují podnikům a jejich vzdáleným klientům zabezpečeněji odesílat a přijímat data, přičemž jako přenosové médium se využívá Internet. Klienti v rámci síťové struktury systému Windows 2000 budou těžit z výhod přístupu k datům vícesměrového vysílání z Internetu.

Tabulka 7.3 popisuje nové funkce služby Směrování a vzdálený přístup systému Windows 2000.

Tabulka 7.3 Nové funkce služby Směrování a vzdálený přístup systému Windows 2000

Funkce	Popis
Integrace služby Active Directory systému Windows 2000	Umožňuje procházení a správu serverů vzdáleného přístupu pomocí nástrojů využívajících službu Active Directory, jako je nástroj správy služby Směrování a vzdálený přístup.
Verze 2 protokolu Challenge Handshake Authentication Protocol (CHAP) společnosti Microsoft	Silně zabezpečené předávání informací o totožnosti a generování šifrovacích klíčů. Tento protokol je vytvořen specificky pro ověřování připojení VPN pomocí protokolu PPTP.
Protokol Extensible Authentication Protocol (EAP)	Umožňuje zapojit metody ověřování nezávislých výrobců do implementace protokolu Point-to-Point Protocol (PPP) systému Windows 2000. Zabudovaná metoda EAP/Transport Layer Security (TLS) podporuje zavádění karet Smart Card sloužících pro zabezpečené ověřování a silné generování šifrovacích klíčů.

Protokol Bandwidth Allocation Protocol (BAP)	Dynamickým přidáváním a odpojováním linek podle změn v provozu umožňuje výkonnější vícelinkové připojení PPP. To je užitečné pro sítě, které jsou zpoplatňovány na základě využití šířky pásma. Užitečné u kanálů ISDN a podobných komunikačních technologiích.
Zásady vzdáleného přístupu	Dává správci možnost řídit připojení podle denní hodiny, členství ve skupinách, typu připojení a dalších kritérií.
Protokol Layer 2 Tunneling Protocol (L2TP)	Zajišťuje spojení VPN mezi klientem a branou a mezi dvěma branami, které je zabezpečeno protokolem IPSec.
Podpora vícesměrového vysílání IP	Podporuje protokol Internet Group Membership Protocol IGMP verze 2 a funguje jako směrovač předávající vícesměrové vysílání, který umožňuje předávání provozu IP vícesměrového vysílání mezi připojenými klienty a Internetem nebo podnikovou sítí.
Network Address Translation (NAT)	Pro menší až střední sítě zajišťuje jediné rozhraní, které je připojeno k Internetu a poskytuje služby překladu adres IP mezi veřejnými a soukromými adresami IP. Interním síťovým klientům také zajišťuje služby přiřazování adres IP a překlad názvů proxy systému.
Internet Connection Sharing (ICS)	Pro malou síť zajišťuje jednoduše konfigurovatelné avšak omezené rozhraní připojující klienty SOHO k Internetu. ICS zajišťuje překlad názvů DNS, automatické přiřazování adres a jediný rozsah adres IP určený pro distribuci IP.

Zásady vzdáleného přístupu

V systému Windows NT verze 3.5x a 4.0 vycházelo ověření vzdáleného přístupu z jednoduchého povolení vzdáleného připojení uživatele ve Správci uživatelů (User Manager) nebo v nástroji pro správu vzdáleného přístupu. Volby zpětného volání se také konfigurovaly podle jednotlivých uživatelů. V systému Windows 2000 vychází ověření z vlastností telefonického připojení účtu uživatele a ze zásad vzdáleného přístupu. Zásady vzdáleného přístupu je sada podmínek a nastavení připojení, které dává správci sítě při autorizování pokusů o připojení větší flexibilitu. Služby Směrování a vzdálený přístup (Routing and Remote Access) a Internet Authentication Service (IAS) systému Windows 2000 používají zásady vzdáleného přístupu k určení, zda se mají dané pokusy o připojení přijmout nebo odmítnout. V obou případech jsou zásady vzdáleného přístupu uloženy místně. Zásady tedy nyní vycházejí z jednotlivých volání.

Pomocí zásad vzdáleného přístupu můžete ověření potvrdit nebo zamítnout podle denní hodiny nebo dne týdne, podle skupiny systému Windows 2000, do níž uživatel vzdáleného přístupu patří, podle typu požadovaného připojení (telefonické připojení sítě nebo připojení VPN) atd. Můžete nakonfigurovat nastavení, která omezí maximální dobu relace, určit sílu ověřování a šifrování, zadat zásady protokolu Bandwidth Allocation Protocol (BAP) atd.

Je důležité zapamatovat si, že při využití zásad vzdáleného přístupu je připojení autorizováno pouze v případě, kdy nastavení pokusu o připojení odpovídají alespoň jedné ze zásad vzdáleného přístupu (které odpovídají podmínkám vlastností telefonického připojení účtu uživatele a vlastnostem profilu dané zásady vzdáleného přístupu). Neodpovídají-li nastavení pokusu o připojení alespoň jedné ze zásad vzdáleného přístupu, dojde k odmítnutí pokusu o připojení bez ohledu na vlastnosti telefonického připojení účtu uživatele.

Úvahy o návrhu vzdáleného přístupu

Dále jsou uvedeny některé úvahy související s návrhem schémat vzdáleného přístupu:

- Pokud jste nainstalovali server DHCP, nakonfigurujte server služby Směrování a vzdálený přístup tak, aby používal k získávání adres IP pro klienty vzdáleného přístupu daný server DHCP.
- Nemáte-li instalovaný server DHCP, nakonfigurujte server služby Směrování a vzdálený přístup fondem statických adres IP, což je podmnožina adres z podsítě, k níž je server vzdáleného přístupu připojen.
- Konfigurujete-li IPX, nakonfigurujte server vzdáleného přístupu tak, aby automaticky přiřadil všem klientům vzdáleného přístupu stejný identifikátor sítě IPX.

Zabezpečení sítí VPN

Zabezpečení sítě je problém ve většině organizací. Dvěma protokoly, které sítě systému Windows 2000 používají k zajištění zabezpečených komunikací přes Internet, jsou Point-to-Point Tunneling Protocol (PPTP) a L2TP, který se používá ve spojení se zabezpečeným protokolem Internet Protocol (IPSec). Protokoly TCP/IP, PPTP a L2TP/IPSec společnosti Microsoft poskytují nejvyšší úroveň zabezpečení a chrání cesty mezi hostiteli a branami.

Výhody použití virtuálních soukromých sítí

Následující seznam obsahuje důvody výhodnosti využívání připojení VPN místo přímých telefonických připojení na velké vzdálenosti.

Snížené dodatečné náklady

Jedním z důležitých problémů větší organizace jsou dodatečné náklady – náklady na telefony jsou přitom jedním z největších výdajů společnosti. Použije-li místo meziměstských či mezistátních telefonních služeb jako připojovací médium Internet, společnost ušetří náklady za telefony a navíc potřebuje méně hardwaru. Klientovi například stačí dovolat se jenom k místnímu poskytovateli připojení k Internetu (ISP) a protokoly L2TP a IPSec následně uživateli umožní získat zabezpečené připojení k serverům VPN systému Windows 2000 také připojeným k Internetu, na kterých běží služba Směrování a vzdálený přístup.

Snížená dodatečná správa

Protože o telefonní linky podporující vaše připojení VPN se stará místní telefonní společnost, která je také vlastní, pro správce sítí to znamená méně úkolů správy.

Přidané zabezpečení

Systém Windows 2000 používá standardní, interoperabilní protokoly ověřování a šifrování, které umožňují skrýt data v nezabezpečeném prostředí Internetu, ale zachovat je dostupná uživatelům společnosti přes VPN. Také platí, že je-li tunel VPN zašifrovaný

pomocí IPSec, Internet vidí pouze externí adresy IP, zatímco interní adresy jsou chráněny. Jinými slovy, pro hackera (počítačového piráta) je nesmírně obtížné interpretovat data odeslaná přes tunel VPN.

Sítě VPN využívající protokol Point-to-Point Tunneling Protocol

PPTP je vynikající řešení tunelových potřeb klientů. V porovnání s kombinací L2TP/IPSec se relativně jednoduše nastavuje a poskytuje dobré zabezpečení při použití metody uživatelské jméno/silné heslo. PPTP je standardní protokol, který byl prvně podporován v systému Windows NT 4.0. Tento protokol používá ověřování, kompresi a šifrování protokolu PPP. PPTP se na dnešních sítích ještě široce používá. Jelikož však protokol L2TP společně s protokolem IPSec zajišťují lepší zabezpečení, tato kapitola se podrobněji zabývá šifrováním L2TP a IPSec.

Sítě VPN využívající protokol L2TP ve spojení s protokolem IPSec

Sítě VPN využívající protokol L2TP ve spojení s protokolem IPSec umožňují podnikům přenášet data přes Internet a přitom zajistit jejich ochranu na vysoké úrovni. Tento typ zabezpečeného připojení můžete použít u malých klientů nebo vzdálených kanceláří, které potřebují přístup k podnikové síti. Sítě VPN využívající protokol L2TP ve spojení s protokolem IPSec můžete také použít pro směrovače na vzdálených sídlech – stačí použít místního poskytovatele ISP a vytvořit telefonické připojení na požádání do hlavní kanceláře společnosti.

Když se rozhodujete, kde a jak navrhnout připojení protokolem L2TP/IPSec, pamatujte si, že server VPN bude umístěn v bodu přístupu k Internetu neboli v zóně DMZ sítě. Server VPN zodpovídá za aplikování rozhodnutí zásad přístupu uživatelů, které lze nakonfigurovat na účtu uživatele na řadiči domény systému Windows 2000, v zásadách vzdáleného přístupu a profilech telefonických připojení uživatelů na serveru VPN nebo v systému IAS.

Protokol L2TP vytvoří nezbytné zásady zabezpečení protokolu IPSec zajišťující provoz v tunelu. Na žádném počítači nemusíte přiřazovat nebo aktivovat své vlastní zásady IPSec. Jsou-li na daném počítači již zásady protokolu IPSec aktivní, protokol L2TP jednoduše přidá k existujícím zásadám bezpečnostní pravidlo chránící provoz v tunelu L2TP.

Úvahy o zavedení protokolu L2TP

Aby došlo k připojení protokolem L2TP/IPSec, musíte na počítače klienta VPN a serveru VPN instalovat certifikáty počítačů. Jakmile klient požaduje připojení VPN, přístup VPN je zajištěn pomocí kombinace vlastností telefonického připojení v účtu uživatele a zásad vzdáleného připojení. V systému Windows NT 4.0 stačilo správci jen vybrat položku umožnění telefonického připojení uživatele ve Správci uživatelů (User Manager) nebo ve Správci uživatelů pro domény (User Manager for Domains) a vzdálený přístup bylo možné používat.

V systému Windows 2000 může správce povolit nebo zakázat vzdálený přístup k síti společnosti pomocí zásad vzdáleného přístupu na serveru VPN a v systému IAS, což vám umožňuje lépe definovat nastavení zabezpečení. V případě využití zásad vzdáleného připojení je připojení přijato, pouze pokud jeho nastavení odpovídají alespoň jedné zásadě vzdáleného přístupu. Neodpovídají-li, připojení je zamítnuto.

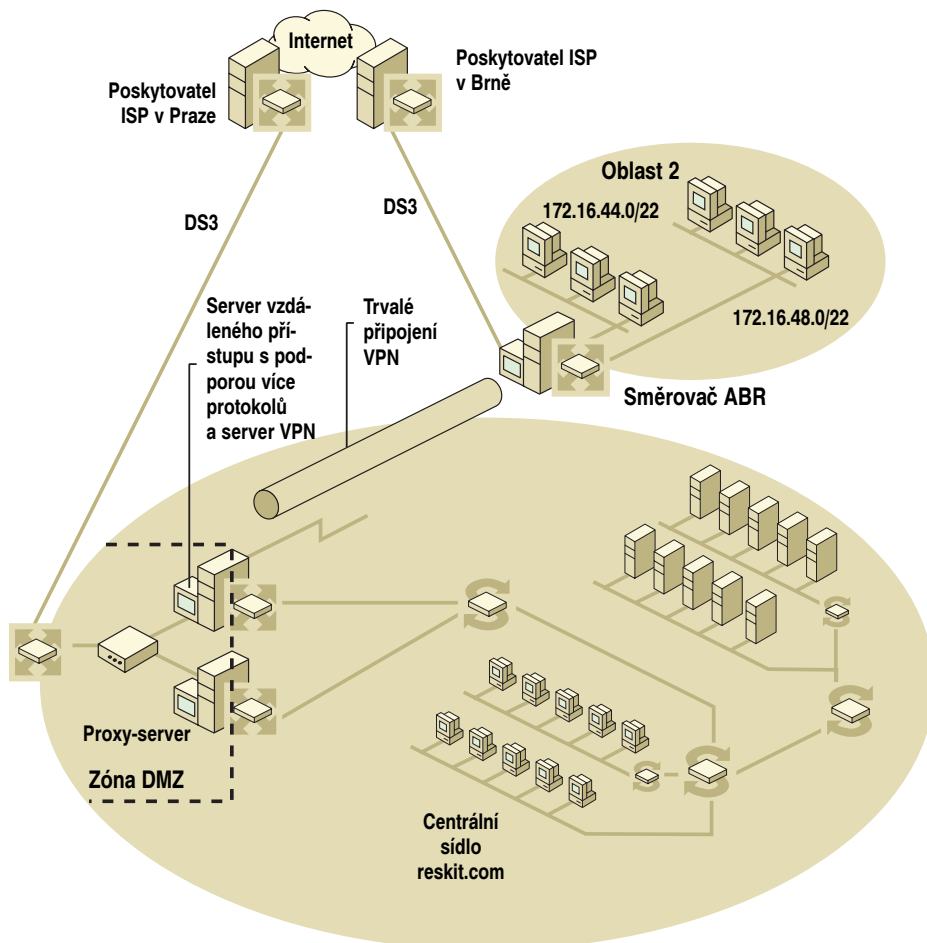
Při zavádění rozsáhlých sítí VPN vzdáleného přístupu můžete použít Správce připojení (Connection Manager) a sadu Connection Manager Administration Kit, kterými všem klientům vzdáleného přístupu v celé vaší organizaci zajistíte předkonfigurovanou součást připojení k síti VPN. Tyto nástroje dovolují uživatelům telefonicky se připojit do sítě VPN jediným klepnutím myši a dva či tři obvyklé kroky tak spojují do jediného.

Příklady protokolu L2TP

Protokol L2TP můžete využít v následujících situacích:

Síť VPN s trvalým připojením mezi směrovači

Síť VPN s připojením mezi směrovači se obvykle používá pro připojení vzdálených kanceláří v případech, kdy jsou oba směrovače připojeny k Internetu pomocí trvalých připojení WAN, jako jsou linky T1, T3, Frame-Relay a kabelové modemy. V tomto typu konfigurace musíte na každém směrovači nakonfigurovat jen jedno rozhraní vyžádaného telefonického připojení. Trvalá připojení lze inicializovat a ponechat aktivní 24 hodin denně. Obrázek 7.2 znázorňuje síť VPN s připojením mezi směrovači.



Obrázek 7.2

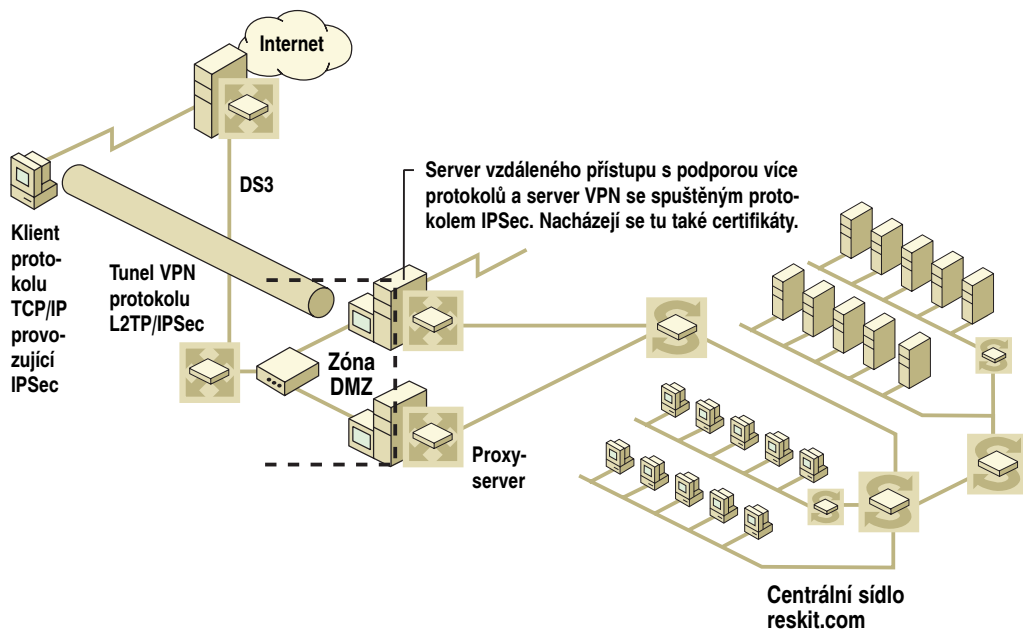
Síť VPN mezi směrovači

Síť VPN s připojením mezi směrovači na požádání

Není-li trvalé připojení WAN možné nebo praktické z důvodu umístění nebo nákladů, můžete nakonfigurovat síť VPN s připojením mezi směrovači na požádání. Odpovídající směrovač pak musíte trvale připojit k Internetu. Volající směrovač se připojuje k Internetu pomocí telefonní linky, jako je analogová linka nebo ISDN. Pak stačí konfigurovat jediné rozhraní telefonického spojení na požádání na odpovídajícím směrovači.

Zabezpečení sítě VPN protokolem IPSec

Na serveru VPN umístěném v zóně DMZ společnosti musí být zaveden protokol IPSec. Návrh na obrázku 7.3 ukazuje server VPN zkombinovaný se serverem vzdáleného přístupu podporujícím více protokolů. Tato kombinace představuje efektivní způsob udržení části sítě zajišťující vzdálený přístup pohromadě, což zjednodušuje možnosti správy a zlepšuje zabezpečení. Když se klient telefonicky připojí k síti společnosti pomocí VPN s protokolem IPSec, určuje klient použitý typ zásad zabezpečení protokolu IPSec a server vzdáleného přístupu, na němž je protokol IPSec instalovaný. Pak automaticky vytváří tunel podle definice klienta.



Obrázek 7.3 Připojení klienta služby Směrování a vzdálený přístup přes tunel L2TP/IPSec

V tomto příkladu má server VPN tři rozhraní. Jedno je v zóně DMZ, druhé rozhraní je v interní síti připojené na směrovač a třetí je rozhraní vzdáleného přístupu. Nejméně zabezpečené rozhraní se nachází v zóně DMZ. Jak bylo řečeno již dříve, DMZ je oblast, kde se Internet rozšiřuje do interní, soukromé sítě, a musí obsahovat všechny servery, které se prezentují na Internetu.

Implementace protokolu IPSec v systému Windows 2000 vychází z průmyslových standardů vyvinutých pracovní skupinou IPSec organizace Internet Engineering Task Force. Šifrování dat umožňuje podnikům využívat Internet jako zabezpečený a z hlediska nákladů výhodný způsob přenášení informací ze vzdáleného sídla nebo od uživatele do infrastruktury společnosti. Tato strategie je z hlediska nákladů výhodná, protože využívá již existující médium Internetu. Zabezpečení je zajištěno protokolem IPSec.

Na Internetu vkládá data do tunelu protokol L2TP a protokol IPSec zajišťuje ochranu dat zabezpečením samotného tunelu. Jak je to však s tím přímo vystaveným rozhraním? Rozhraní vystavené Internetu na serveru VPN můžete před hackery chránit těmito způsoby:

- Při počátečním nastavování serveru VPN se ujistěte, že na rozhraní neexistuje žádný směrovací protokol, který se nachází v zóně DMZ. Rozhraní musí ukazovat do soukromé sítě společnosti sadou shrnutých statických tras.
- Na rozhraní provozujte směrovací protokol, který je na soukromé síti.
- Na internetovém rozhraní použijte filtry služby Směrování a vzdálený přístup (nikoli filtrování IPSec) a nastavte filtry povolení vstupu a výstupu pro protokol L2TP, které používají port „Any“ protokolu User Datagram Protocol (UDP) a cílový port 1701. Také nastavte filtry povolení vstupu a výstupu směrování a vzdáleného přístupu pro protokol Internet Key Exchange (IKE), které používají zdrojový port „Any“ UDP a cílový port 500 a zabráňují tak veškerému provozu s výjimkou provozu L2TP/IPSec. Pak nakonfigurujte filtrování paketů v profilu zásad vzdáleného přístupu skupin uživatelů a umožněte, nebo zakažte určité typy provozu IP. Aby se situace uživatelů zjednodušila, tyto filtry se nakonfigurují při použití průvodce nastavením služby Směrování a vzdálený přístup (Routing and Remote Access) – není tedy vyžadována žádná konfigurace ze strany uživatele.

Pro připojení L2TP/IPSec používá vyjednávání zabezpečení protokolu IPSec (IKE) ověřování samotných počítačů vycházející z certifikátů. L2TP vykoná ověření uživatele pomocí konstrukce doména\identifikátor uživatele a heslo, nebo použitím karty Smart Card, certifikátu nebo karty tokenu protokolem Extensible Authentication Protocol (EAP). Další informace o změně tohoto výchozího chování a použití ověřování pomocí předem sdíleného klíče najdete v kapitole „Virtual Private Networking“ v knize *Microsoft Windows 2000 Server Internetworking*.

Protokol IPSec vyžaduje, abyste vytvořili vztahy důvěryhodnosti pomocí certifikátů vystavených jednotlivým počítačům. Například prodejce z domény domain.com má pravidelné prodejní transakce v doméně reskit.com. V zájmu urychlení procesu objednávání se daný prodejce každý týden telefonicky připojuje a z oddělení dodávek společnosti Reskit si nahrává formulář objednávky produktů.

Aby bylo zajištěno zabezpečení všech transakcí před konkurencí domény domain.com, prodejce se telefonicky připojuje k doméně reskit.com s využitím ISP pomocí sítě VPN, kde pracuje protokol L2TP/IPSec. Jak vzdálený klient tak i server VPN musí mít vystavené certifikáty a musí být schopny vzájemně svým certifikátům důvěřovat. Na počítači prodejce musí být instalován certifikát počítače, který vyjedná vztah důvěryhodnosti se serverem VPN domény reskit.com. Počítač prodejce nejčastěji získává certifikát od certifikačního serveru systému Windows 2000 v okamžiku připojení daného počítače do domény domain.com. Počítač obdržel nastavení zásad skupiny obsahující instrukce zápisu na certifikační server domény domain.com označovaný za zásady automatického zápisu certifikátů. Zásady certifikátů infrastruktury veřejných klíčů (PKI) také určují

jí, že klient může důvěřovat certifikačnímu serveru, který vystavil certifikát serveru VPN, což je pravděpodobně certifikační server domény reskit.com. Server VPN je nakonfigurován tak, aby důvěřoval certifikačnímu serveru domény domain.com, takže přijme certifikáty poskytnuté klientem.

Jakmile je vytvořeno přiřazení zabezpečení IPSec protokolu L2TP, zkontrolují se zásady vzdáleného přístupu prodejce. Jedná se o vlastnost umožňující vzdálený přístup pro účet uživatele v doméně. Podrobněji můžete řídit přístup uživatelů pomocí služby Internet Authentication Service (IAS), serveru, který předává zásady přístupu pomocí protokolu Remote Access Dial-In User Service (RADIUS).

Prostřednictvím protokolu IPSec můžete také zajistit, aby se k jiným počítačům mohly připojovat pouze určité počítače s řádnými certifikáty a identifikačními informacemi. Identifikátory uživatelů a skupiny systému Windows 2000 zadané v seznamech řízení přístupu (access control list – ACL) určují, kdo může k danému sdílenému místu přistupovat.

Poznámka Protokol IPSec můžete také použít v rámci podnikové sítě k šifrování dat přenášejících mezi klienty nebo od klienta k serveru.

Další informace o protokolu IPSec najdete v kapitole „Internet Protocol Security“ v knize *Microsoft Windows 2000 Server Sítě TCP/IP*.

Služba Internet Authentication Service a centralizovaná správa

V sítích větších společností může být správa zásad na více serverech vzdáleného přístupu velmi náročná. Služba IAS může pomoci správcům sítí ve správě geograficky rozptýlených serverů vzdáleného přístupu z centrálního místa.

Služba IAS nabízí:

Centralizované ověřování uživatelů

Služba IAS podporuje schopnost centrálně spravovat zásady uživatelů ověřováním uživatelů, kteří se nacházejí v doménách systémů Windows NT 4.0 a Windows 2000. V zájmu ověřování uživatelů podporuje služba IAS různé ověřovací protokoly. Patří mezi ně:

- Protokol Password Authentication Protocol (PAP)
- Protokol Challenge Handshake Protocol (CHAP)
- Protokol Microsoft Challenge Handshake Protocol (MS-CHAP)
- Protokol Extensible Authentication Protocol (EAP)

Vzdálený přístup s využitím nezávislých společností

To vám umožňuje připojovat zaměstnance k podnikové síti přes tunel VPN pomocí sítě místního ISP. Služba IAS vám umožňuje sledovat výdaje a uživatele, kteří se připojují k ISP, což vám následně dovoluje platit poskytovateli za použité služby. Takové pojetí má za následek úsporu peněz v organizaci.

Centralizovaná správa serverů vzdáleného přístupu

Služba IAS umožňuje správcům sítě nakonfigurovat zásady vzdáleného přístupu jen na jednom serveru vzdáleného přístupu – ostatní severy vzdáleného přístupu mohou fungovat jako klienti protokolu RADIUS a přejímat zásady ze serveru IAS.

škálovatelnost

Službu IAS mohou používat malé a střední sítě ve větších společnostech a poskytovatelé připojení k Internetu (ISP).

Vzdálené monitorování

Správce sítě může sledovat servery IAS z libovolného místa na síti pomocí Prohlížeče událostí (Event Viewer) nebo Sledování sítě (Network Monitor). Může si také nainstalovat protokol Simple Network Management Protocol.

Import/export konfigurace IAS

Správce sítě může importovat a exportovat konfiguraci IAS pomocí určitého nástroje příkazového řádku. Další informace o službě IAS najdete v kapitole „Internet Authentication Service“ v knize *Microsoft Windows 2000 Server Internetworking*.

Systémy s více adresami

Počítač nakonfigurovaný s více než jednou adresou IP se označuje za systém s více adresami (multihome). Systém s více adresami můžete implementovat několika způsoby podle svých potřeb. Můžete vytvořit servery DHCP s více adresami a poskytovat tak služby více podsítím. Také systém DNS může využít výhody více adres, protože službu DNS lze povolit na jednotlivých rozhraních a lze ji svázat pouze se zadanými adresami IP. Služba DNS se standardně váže ke všem jednotlivým rozhraním nakonfigurovaným na počítači.

Systémy s více adresami jsou podporovány několika různými způsoby:

- Více adres IP pro každý síťový adaptér
- Více síťových adaptérů

Infrastruktura směrování protokolu IP

Aby mohli uživatelé a správci plně využít funkce systému Windows 2000 Server pracujícího jako směrovač, musíte analyzovat strukturu sítě a rozhodnout se, jaký typ infrastruktury směrování nejlépe vyhovuje potřebám vaší organizace. Tabulka 7.4 popisuje různé typy konfigurací směrování a jejich použití.

Tabulka 7.4 Konfigurace směrování

Konfigurace směrování	Popis
Staticky směrované propojení mezi sítěmi	Ke směrování síťového provozu používá ručně přidávané trasy.
Protokol Routing Information Protocol (RIP) pro IP propojení mezi sítěmi	K dynamickému předávání směrovacích informací mezi směrovači se používá protokol RIP pro IP.
Protokol Open Shortest Path First (OSPF) propojení mezi sítěmi	K dynamickému předávání směrovacích informací mezi směrovači se používá směrovací protokol OSPF.

Staticky směrované sítě

Staticky směrované propojení IP mezi sítěmi nepoužívá pro přenos směrovacích informací mezi směrovači protokoly jako RIP pro IP nebo OSPF. Všechny směrovací infor-

mace jsou uloženy ve směrovací tabulce na každém směrovači. Rozhodnete-li se implementovat statické směrování, zajistěte, aby měl každý směrovač ve své směrovací tabulce potřebné trasy umožňující předávání provozu mezi libovolnými dvěma koncovými body na propojení sítí IP.

Ke zdokumentování všech statických tras v infrastruktuře sítě můžete použít síťový diagram popsaný na začátku této kapitoly, který je také ideálním prostředkem záznamu organizace tras. Statické trasy lze zadat do směrovací tabulky směrovače systému Windows 2000 pomocí konzoly pro správu služby Směrování a vzdálený přístup (Routing and Remote Access). Další informace o přidávání statických tras najdete v kapitole „Unicast IP Routing“ v knize *Microsoft Windows 2000 Server Internetworking*.

Ještě než budete moci použít tuto směrovací službu, musíte ji nakonfigurovat a povolit z uvedené konzoly pro správu. Další informace o spuštění a konfiguraci služby Směrování a vzdálený přístup (Routing and Remote Access) systému Windows 2000 najdete v online nápovědě systému Windows 2000 Server. Další informace o instalaci a inovaci členských serverů systému Windows 2000 najdete v kapitole „Inovace a instalace členských serverů“ v této knize.

Statické trasy můžete implementovat v malých sítích, které vyžadují jen malou správu a které v čase příliš nerostou, jaké se nacházejí v malých podnicích s méně než deseti síťovými segmenty. Protože však statické trasy vyžadují určitou správu, můžete je považovat za nepraktické, zejména vezmete-li v úvahu také schopnost služby Směrování a vzdálený přístup systému Windows 2000 dynamicky vytvářet tabulky směrovacích informací pro malé i velké sítě pomocí protokolů Open Shortest Path First (OSPF) nebo RIP pro IP.

Návrh sítě s protokolem RIP pro IP

RIP pro IP je směrovací protokol využívající vektor vzdálenosti, který dynamicky předává směrovací informace mezi sousedními směrovači a automaticky přidává a odstraňuje trasy podle potřeby. Protokol RIP je omezen na úroveň 16 směrovačů. Všechny úrovně vzdálené 16 a více směrování se považují za nedosažitelné. Síť RIP se nejlépe implementují v menších až středních infrastrukturách, jaké se nacházejí ve středně velkých podnicích nebo pobočkách.

Mezi další problémy použití protokolu RIP pro IP v síti patří:

- Protokol RIP pro IP používá k měření nejlepší trasy počet skoků. Má-li například sídlo s linkou T1 nějakou záložní satelitní linku a náklady spojené s oběma linkami jsou stejné, pak může protokol RIP pro IP vybrat libovolnou linku. Chcete-li se tomuto problému vyhnout, můžete nakonfigurovat pomalejší linku (satelitní) s náklady o hodnotě dvě – směrovač pak bude jako primární linku využívat T1.
- Dalším problémem je spotřeba šířky pásma, protože směrovače RIP oznamují své seznamy dosažitelných sítí každých 30 sekund. V závislosti na velikosti sítě mohou tato oznámení využívat značnou šířku pásma WAN. S růstem velikosti sítě také narůstá pravděpodobnost vzniku úzkých míst. K omezení šířky pásma využívané směrovacím protokolem RIP můžete použít autostatické aktualizace tohoto protokolu.

Služba Směrování a vzdálený přístup systému Windows 2000 podporuje verze 1 a 2 protokolu RIP pro IP. RIP verze 1 je určen pro prostředí se třídami a neoznamuje masku podsítě pro každou trasu. Existují-li ve vaší síti směrovače podporující pouze protokol RIP verze 1 a chcete-li používat směrování bez tříd mezi doménami (classless interdomain routing – CIDR) nebo masky podsítí s proměnnou délkou (Variable Length

Subnet Mask – VLSM), pak inovujte směrovače tak, aby podporovaly protokol RIP verze 2, nebo se protokolu RIP úplně vyhněte a používejte protokol OSPF.

Protokol RIP pro IP můžete implementovat pomocí následujících kroků:

1. Podívejte se na diagram sítě a zjistěte, kam budou umístěny směrovače RIP. Nemáte-li aktuální diagram, raději jej ihned vytvořte. Chcete-li dosáhnout minimálního počtu úzkých míst v systému, umístěte směrovače na síť s dostatečnou šířkou pásma.
2. Určete použité schéma adres IP. Zapište si, které adresy se použijí pro směrovače, které pro servery a které pro klienty. Používáte-li například rozsah soukromých adres 172.16 0.0/22, můžete zvolit formát uvedený v tabulce 7.5.

Tabulka 7.5 Schémata adres IP

Směrovač	Adresa
Rozhraní směrovače Router1 na síti 172.16.4.0/22	172.16.4.1
Rozhraní směrovače Router2 na síti 172.16.8.0/22	172.16.8.1
Řadič domény na síti 172.16.4.0/22	172.16.4.10
Řadič domény na síti 172.16.8.0/22	172.16.8.10
Klient na síti 172.16.4.0/22	172.16.4.20
Klient na síti 172.16.8.0/22	172.16.8.20

3. Dále rozhodněte, jaká verze protokolu RIP se bude na jednotlivých rozhraních používat. Vytváříte-li novou síť, dejte přednost výhradnímu použití protokolu RIP verze 2, protože tato verze podporuje CIDR a VLSM. Máte-li existující síť využívající protokol RIP verze 1, zamyslete se nad její inovací na protokol RIP verze 2.

Návrh sítě s protokolem OSPF

Protokol RIP pro IP představuje jednoduchou možnost integrace směrovacího protokolu do malých až středně velkých síťových prostředí. Máte-li však implementovánu větší síť, nemusí vám protokol RIP pro IP dostačovat. Další směrovací protokol podporovaný službou Směrování a vzdálený přístup systému Windows 2000 se nazývá Open Shortest Path First (OSPF). Síť OSPF se nejlépe hodí pro velké infrastruktury s více než 50 sítěmi.

OSPF je směrovací protokol zaznamenávající stav linky, který vypočítává položky směrovacích tabulek pomocí konstrukce stromu nejkratší cesty. Je to výkonnější protokol než RIP a nevyskytuje se v něm problém s omezením 16 přeskoků, který způsobuje ztrátu dat po 16. přeskoku. Síť OSPF může mít akumulované náklady na cestu až do hodnoty 65 535, což vám umožňuje konstruovat velmi rozsáhlé sítě (s maximální hodnotou TTL na úrovni 255) a přiřazovat široký rozsah nákladů. OSPF také podporuje vyhrazená spojení mezi dvěma body, síť s vysíláním, jako je Ethernet, a síť bez vysílání, jako je Frame Relay. Nevýhodnou použití protokolu OSPF je to, že jeho konfigurace je složitější než jiných směrovacích protokolů, jako je třeba RIP.

Tyto sítě můžete strukturovat hierarchicky. Následující oddíly popisují protokol OSPF podrobněji.

Autonomní systémy

Autonomní systém (AS) je kolekce sítí, které sdílejí společný úřad správy. Při návrhu AS protokolu OSPF byste se měli držet dále uvedených pokynů:

- Rozdělte AS do oblastí OSPF.

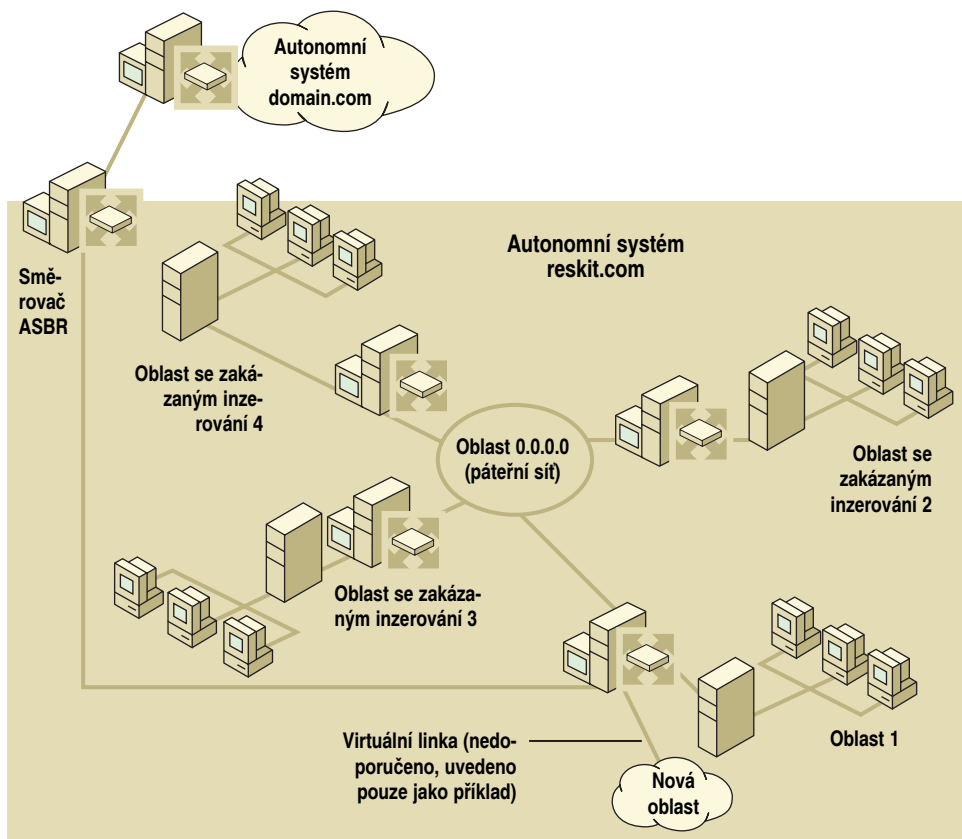
Rozčleňte AS do oblastí tak, aby mohl protokol OSPF řídit provoz a maximalizovat svou schopnost přenášet pouze provoz v rámci dané oblasti a komunikaci s jinými oblastmi AS udržovat na minimu.

- Páteční oblast vyhraďte jako síť s vysokou propustností.

Vytvořte páteční spojení, které je schopno poskytovat velkou kapacitu a napomoci tak minimalizaci úzkých míst v jednotlivých oblastech.

- Zajistěte, aby veškerý provoz mezi oblastmi probíhal přes páteční spojení. Vyhýbejte se vytváření virtuálních linek připojujících k páteční síti nové nebo měněné oblasti.

Zobrazení AS najdete na obrázku 7.4.



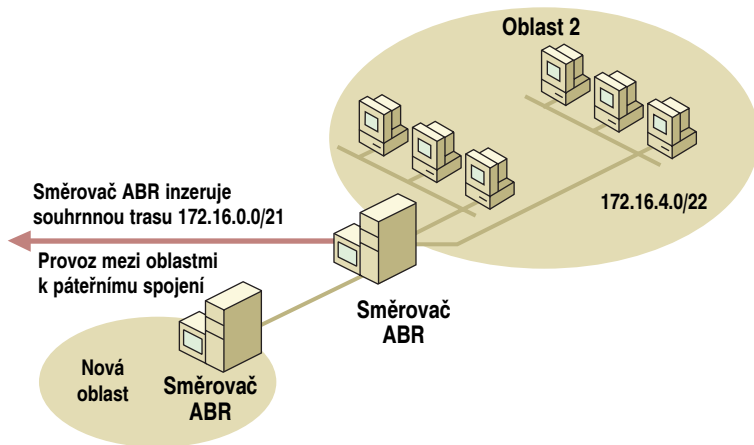
Obrázek 7.4 Autonomní systém

Návrh oblasti OSPF

Oblasti OSPF jsou pododdíly AS OSPF, které obsahují spojitou kolekci podsítí. Oblasti jsou hranice správy, které lze použít k oddělení sídel, domén nebo skupin. V těchto oblastech jsou sítě, které po vzájemném propojení přes páteční spojení tvoří AS.

V interní síti nakonfigurujte tyto oblasti tak, aby byla minimalizována komunikace mezi oblastmi. Sem patří provoz překladu názvů systému DNS a provoz replikace služby Active Directory.

Jednou z cest, kterou provoz opouští oblast OSPF a vstupuje do ní, je směrovač označovaný za směrovač hranice oblasti (area border router – ABR). Tento směrovač je připojen k páteřnímu spojení nazvanému Oblast 0.0.0.0, které následně spojuje dohromady oblasti OSPF. Směrovače ABR mají obvykle rozhraní na síti páteřní oblasti. Nastává však také situace, kdy není možné fyzicky připojit směrovač ABR k segmentu páteřního spojení. Dojde-li k tomu, můžete nové oblasti OSPF připojit k páteřnímu spojení prostřednictvím virtuální linky. Tato metoda sice bude fungovat, její použití vám však nedoporučujeme, protože její vytvoření je komplikované a také je náchylná k chybám. Obrázek 7.5 ukazuje páteřní spojení, oblasti a virtuální linku.



Obrázek 7.5 Návrh oblasti OSPF

Chcete-li navrhnout oblast OSPF, postupujte podle následujících pokynů:

- Adresy IP přiřadte spojitě, aby je bylo možné shrnout. Shrnutí trasy je akt kondenzování rozsahů adres IP. V ideálním případě bude směrovač ABR oblasti shrnovat všechny své síťové adresy IP do jediné. Toto pojetí kondenzuje směrovací informace a omezuje tak zatížení směrovačů ABR a počet položek směrovacích tabulek OSPF.
- Kdykoli je to možné, vytvářejte oblasti se zakázaným inzerováním. Pamatujte na následující:
 - Oblasti se zakázaným inzerováním lze nakonfigurovat tak, že se všechny externí trasy a trasy k cílům mimo daný AS OSPF shrnují jedinou statickou výchozí trasou.
 - Žádné trasy externí danému systému AS (externí trasy) nelze přenášet oblastí se zakázaným inzerováním; sem patří také trasy využívající jiné směrovací protokoly. To znamená, že oblasti se zakázaným inzerováním nemohou používat směrovače hranice AS (ASBR).
- Vyhněte se vytváření virtuálních linek. Virtuální linky se používají pro připojení nových oblastí v AS do páteřního spojení. Virtuální linky mohou způsobovat problémy

se směrováním a další problémy, a obtížně se konfiguruje. Vždy se snažte připojit nové oblasti v systému AS přímo k páteřnímu spojení. Počítejte s tím při svém plánování ještě před implementací AS.

Struktura směrování protokolu IPX

Servery systému NetWare a systémy Windows 2000 mohou spolupracovat na jedné síti pomocí nástrojů NWLink, Client Services for NetWare a Gateway Services for NetWare. Systém Windows 2000 Server poskytuje služby, které mohou fungovat současně se sítěmi a servery systému Novell NetWare a mohou s nimi také spolupracovat. Součástí systému Windows 2000 je protokol IPX/SPX/NetBIOS Compatible Transport Protocol (NWLink). Tento protokol zajišťuje konektivitu mezi systémy Windows 2000 a Novell NetWare. Důvody pro použití protokolů IPX/SPX v kombinovaném prostředí a povolení směrování IPX jsou:

- Ke směrování provozu mezi klienty a servery NetWare mohou být zapotřebí směrovače Windows 2000.
- Klienti systému Windows 2000 mohou potřebovat přistupovat ke službám na serverech NetWare.

Směrování systému Windows 2000 podporuje protokol RIP pro IPX, který se svou funkcí velmi podobá protokolu RIP pro IP a protokolu Service Advertising Protocol (SAP) pro IPX. Je to protokol umožňující uzlům, jako jsou souborové servery a tiskové servery, inzerovat své názvy služeb a adresy IPX. Servery hostící služby odesílají periodická vysílání SAP a směrovače IPX a servery SAP tato vysílání přijímají a šíří informace o službách prostřednictvím oznámení SAP, která se odesílají každých 60 sekund.

Návrh sítě s protokolem IPX

Identifikátor sítě IPX je čtyřbajtová hodnota vyjádřená jako osmičíselné šestnáctkové číslo. Tento identifikátor sítě musí být jedinečný, jinak mohou mít klienti systému NetWare problémy s připojením. Čtyřbajtový identifikátor sítě IPX je adresový prostor, který můžete využít k seskupení sítí IPX na základě těchto prvků:

Interní versus externí sítě

Interní sítě jsou virtuální sítě v rámci serverů systému Novell NetWare, směrovačů Windows 2000 a dalších směrovačů IPX, které také hostí služby. Určení interní sítě zajišťuje správné směrování k těmto službám.

Sítě pro různé typy rámců Ethernet

V případě prostředí IPX, které musí podporovat více typů rámců Ethernet, musíte nakonfigurovat pro každý typ rámce Ethernet vlastní identifikátor sítě IPX.

Sítě vzdáleného přístupu

Používáte-li počítač se systémem Windows 2000 jako server vzdáleného přístupu, klientům vzdáleného přístupu se přiřazuje identifikátor sítě IPX. Server vzdáleného přístupu standardně volí jedinečný identifikátor sítě IPX. Identifikátor sítě IPX můžete zadat nebo zvolit nějaký rozsah identifikátorů sítí IPX, aby bylo možné provoz IPX vzdáleného přístupu identifikovat podle síťové adresy IPX jeho zdroje.

Oddělení nebo geografické umístění

Části adresového prostoru IPX můžete alokovat na základě geografie (podle budovy nebo sídla) nebo oddělení (jako je prodej či výzkum). Například v prostředí rozsáhlé-

ho areálu mohou všechny sítě IPX v budově 5 používat jako první číslo svých adres právě hodnotu 5.

Maximální průměr

Maximální průměr protokolů RIP a SAP pro IPX je 16 přeskoků, stejně jako v případě protokolu RIP pro IP. Průměr je mírou velikosti propojení sítí z hlediska počtu směrovačů, které musí paket překonat, aby dosáhl svého cíle. Sítě a služby, které jsou dále než 16 přeskoků, jsou považovány za nedosažitelné.

Omezení a ovládání provozu NetBIOS/IPX

Provoz systému NetBIOS/IPX můžete řídit zákazem šíření vysílání NetBIOS/IPX na specifických rozhraních a nakonfigurováním statických názvů systému NetBIOS. Jestliže například určitá síť IPX neobsahuje žádné uzly využívající NetBIOS/IPX, pak můžete zakázat šíření vysílání NetBIOS/IPX na všech rozhraních směrovačů připojených k dané síti.

Zabránění šíření vysílání protokolu SAP

Protokol Service Advertising Protocol (SAP) se používá na sítích IPX k tomu, aby informoval síťové klienty o dostupných síťových prostředcích a službách. Existují-li nějaká vysílání SAP, které není zapotřebí šířit ve všech propojených sítích, můžete inzerování služeb IPX mimo určitou skupinu sítí IPX zabránit pomocí filtrování protokolu SAP. Chcete-li například skrýt souborové servery v oddělení lidských zdrojů, nakonfigurujte směrovače připojené k síti lidských zdrojů tak, aby filtrovaly vysílání SAP odpovídající službám sdílení souborů souborových serverů oddělení lidských zdrojů. Dalším důvodem je omezení provozu odesílaného podsítím, které nevyžadují služby SAP.

Struktura směrování protokolu AppleTalk

Práce v sítích na platformě systému Macintosh se spoléhá na sadu protokolů AppleTalk. Tyto protokoly obsahují zabudované schopnosti směrování, které lze povolit a s jejichž pomocí lze vytvořit směrovače v propojení sítí AppleTalk.

Podpora vícesměrového vysílání

Služby podpory multimédií se na Internetu a v soukromých sítích objevují stále častěji. Protokol TCP/IP systému Windows 2000 podporuje předávání provozu vícesměrového vysílání a služba Směrování a vzdálený přístup systému Windows 2000 podporuje protokol Internet Group Management Protocol (IGMP) pracující jako směrovač. IGMP používají hostitelé pro připojení ke skupině vícesměrového vysílání. Rozhraní služby Směrování a vzdálený přístup (Routing and Remote Access Service) podporující protokol IGMP mohou fungovat v jednom ze dvou režimů:

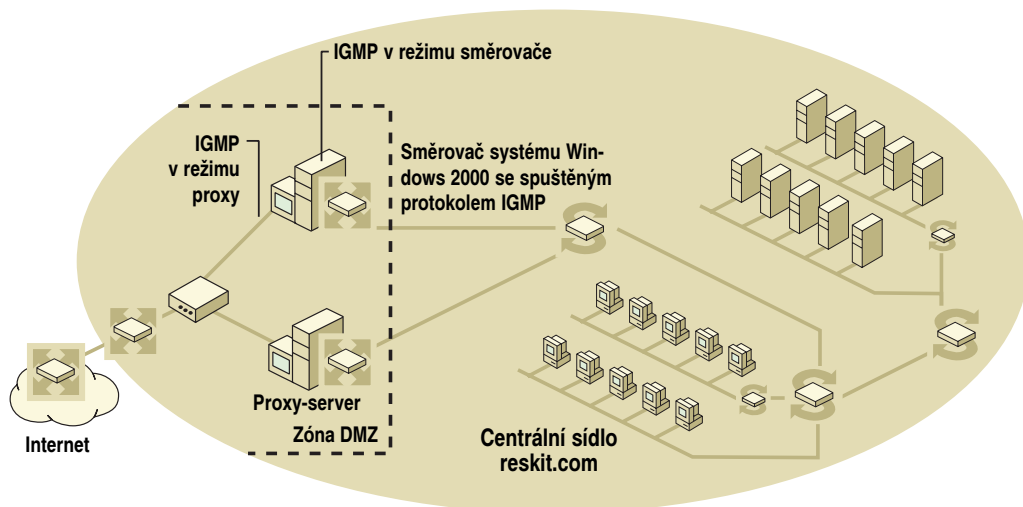
- Rozhraní pracující v režimu proxy IGMP předávají dále zprávy IGMP a provoz vícesměrového vysílání z ostatních rozhraní, která pracují v režimu směrovače IGMP.
- Rozhraní pracující v režimu směrovače IGMP naslouchají provozu IGMP od hostitelů a podle potřeby aktualizují tabulku předávání vícesměrového vysílání protokolu TCP/IP a zároveň odesílají dotazy IGMP.

Proxy IGMP, který je součástí systému Windows 2000 Server, je vytvořen tak, aby předával pakety zpráv o členství IGMP z jednoho síťového intranetu na část Internetu schopnou vícesměrového vysílání.

Proxy směrovač IGMP můžete umístit do zóny DMZ infrastruktury společnosti, čímž zajistíte pro hostitele interní sítě video a audio provoz z Internetu. Zajistíte umístění smě-

rovače IGMP na síti se širokým pásmem a rychlými přepínači, aby se omezila úzká místa v systému. Server VPN, který se nachází v zóně DMZ, lze používat zároveň jako směrovač IGMP, ale pouze v menších síťových strukturách, kde nebude daný server přetížen provozem vzdáleného přístupu a vícesměrového vysílání.

Při konfigurování rozhraní IGMP směruje rozhraní v režimu proxy k síti Internet umožňující vícesměrové vysílání a rozhraní v režimu směrovače směruje k interní síti. Příklad je uveden na obrázku 7.6.



Obrázek 7.6 Rozhraní IGMP v režimu proxy

Poznámka Příklad na obrázku 7.6 bude fungovat, pouze pokud hardwarový směrovač propojující směrovač IGMP systému Windows 2000 s Internetem podporuje vícesměrové vysílání a je-li ISP na páteřním spojení vícesměrového vysílání.

Překlad síťových adres

Překlad síťových adres (network address translation – NAT) systému Windows 2000 umožňuje počítačům na malé síti, jaké jsou v malých nebo domácích kancelářích (small office/home office – SOHO), sdílet jediné připojení k Internetu. Počítač, na němž je služba NAT instalována, může fungovat jako překladač síťových adres, zjednodušený server DHCP, proxy systému DNS a proxy služby WINS. NAT umožňuje hostitelským počítačům sdílet jednu nebo více veřejně registrovaných adres IP, což pomáhá šetřit veřejný adresový prostor.

Existují dva typy připojení k Internetu: směrované a překládané. Při plánování směrovaného připojení budete od svého poskytovatele připojení k Internetu (ISP) potřebovat nějaký rozsah adres IP, které budete používat na interní části vaší sítě. ISP vám také dá adresu IP serveru DNS, kterou musíte použít. Můžete buď nakonfigurovat statickou adresu IP na každém počítači SOHO, nebo použít server DHCP.

Na směrovači systému Windows 2000 musí být nakonfigurován síťový adaptér pro interní síť (například Ethernet 10BaseT nebo 100BaseT). Musí tu také být nakonfigurované internetové připojení využívající například analogový modem či modem ISDN, modem xDSL, kabelový modem nebo částečnou linku T1.

Metoda překladu neboli NAT vám poskytuje zabezpečenější síť, protože adresy vaší soukromé sítě jsou před Internetem úplně skryty. Počítač sdílený připojením, který používá službu NAT, zajišťuje veškerý překlad internetových adres na vaši soukromou síť a naopak. Uvědomte si však, že počítač NAT nemá schopnost překládat všechna přenášovaná data. Je tomu tak proto, že některé aplikace používají kromě standardních polí hlavičky TCP/IP adresy IP také v dalších polích.

Se systémem NAT nefungují následující protokoly:

- Kerberos
- IPSec

Funkce přidělování DHCP systému NAT umožňuje všem klientům DHCP v síti SOHO automaticky získat adresu IP, masku podsítě, výchozí bránu a adresu serveru DNS od počítače NAT. Máte-li na síti nějaké počítače nepodporující DHCP, pak zadejte jejich konfiguraci adres IP staticky.

Aby bylo v sítích SOHO dosaženo minimálních nákladů na prostředky, je zapotřebí jen jeden server systému Windows 2000. Podle toho, zda provozujete překládané nebo směrované připojení, může tento jediný server zastávat funkce služeb NAT, APIPA, Směrování a vzdálený přístup a DHCP.

Další informace o systému NAT a jeho konfiguraci najdete v online nápovědě systému Windows 2000 Server.

Protokol DHCP systému Windows 2000

Každý počítač na síti TCP/IP musí mít jedinečný název a adresu IP. Protokol Dynamic Host Control Protocol (DHCP) systému Windows 2000 vám nabízí možnost zjednodušení a zautomatizování tohoto procesu a zajištění dynamického přiřazování adres IP klientům na síti bez ohledu na to, kde se nacházejí, nebo jak často se přesunují. To snižuje zatížení správce.

Výhody používání protokolu DHCP

Protokol DHCP zajišťuje spolehlivé přiřazování adres IP v síti tím, že omezuje potřebu ručně přiřazovat adresy jednotlivým hostitelům. Tak se zabraňuje konfliktům IP, které mohou narušit funkci sítě.

Také mobilní uživatelé mohou protokol DHCP velmi dobře využívat, protože jim umožňuje libovolně se přesunovat v rámci propojených sítí a automaticky získávat adresy IP po připojení k síti.

Spolupráce se servery DNS zajišťuje překlad názvů pro síťové prostředky, což umožňuje serverům DHCP a klientům DHCP registrovat se v systému DNS.

Nové funkce protokolu DHCP systému Windows 2000

Nové funkce protokolu DHCP systému Windows 2000 umožňují zavedení flexibilnějších a rozšiřitelných způsobů přiřazování adres IP hostitelům. Tyto nové funkce jsou popsány v následujících oddílech.

Vylepšené zprávy serveru

Obecný stav serverů DHCP, oborů a klientů neboli „členských položek“ lze graficky sledovat pomocí ikon zobrazených v nástroji Správce služby DHCP (DHCP Manager). Další informace o tomto tématu najdete v online nápovědě nástroje Správce služby DHCP.

Podpora dalších oborů

Rozšíření standardního protokolu DHCP systému Windows 2000 podporuje přiřazování adres IP vícesměrového vysílání, které se distribuují stejným způsobem jako adresy jednosměrového vysílání. V protokolu Multicast DHCP se obory vícesměrového vysílání konfiguruji stejně jako normální obory DHCP, místo adres tříd A, B nebo C se však používá obor D s rozsahem 224.0.0.0 až 239.255.255.255.

Typickými aplikacemi vícesměrového vysílání jsou video a audio konference, které obvykle vyžadují, aby uživatelé speciálně nakonfigurovali adresy vícesměrového vysílání. Na rozdíl od všesměrového vysílání IP, které musí být čitelné všemi počítači na síti, je adresa vícesměrového vysílání skupina počítačů, která k určení příjemce zprávy používá členství ve skupině.

Funkce přiřazení adresy vícesměrového vysílání má dvě části: stranu serveru, která předává adresy vícesměrového vysílání, a programovací rozhraní aplikací (API) klientské strany, které požaduje, obnovuje a uvolňuje adresy vícesměrového vysílání. Chcete-li použít tuto funkci, musíte nejprve na serveru prostřednictvím modulu snap-in DHCP nakonfigurovat obory vícesměrového vysílání a odpovídající rozsahy IP vícesměrového vysílání. Adresy vícesměrového vysílání se pak spravují jako normální adresy IP a klient může voláním API požadovat nějakou adresu vícesměrového vysílání z daného oboru.

Integrace DHCP a DNS

Servery systému DNS zajišťují překlad názvů pro síťové prostředky a úzce souvisejí se službami DHCP. V systému Windows 2000 se mohou servery a klienti DHCP registrovat pomocí protokolu dynamické aktualizace DNS. Integrace DHCP a DNS umožňuje registraci jak záznamů typu A (název na adresu), tak i ukazatelů (PTR) neboli převodu adresy na název. To umožňuje serveru DHCP fungovat jako proxy místo klientů systému Windows 95 a Windows NT 4.0 Workstation za účelem registrace dynamickou aktualizací ve službě Active Directory.

Úvahy o návrhu integrace DHCP a DNS

Při společném používání DHCP a DNS na síti zvažte, zda používáte nebo nepoužíváte starší, statické servery DNS. Statické servery DNS nemohou dynamicky spolupracovat s DHCP a udržovat synchronizované informace přiřazení názvů k adresám v případech, kdy se změní klientská konfigurace DHCP, jako je tomu u mobilního uživatele, který se neustále přesunuje mezi podsítěmi v rámci propojení sítí. V takové situaci pro vás bude nejlepší inovovat všechny statické servery DNS na DNS systému Windows 2000.

Detekce neautorizovaných serverů DHCP

Služba DHCP systému Windows 2000 je vytvořena tak, aby zabránila neautorizovaným serverům DHCP ve vytváření konfliktů přiřazovaných adres. Tak se řeší problém, který by se jinak mohl vyskytnout v případě, kdyby uživatelé vytvořili neautorizované servery DHCP, jež by mohly přiřazovat neplatné adresy IP klientům na jiných místech sítě. Uživatel mohl třeba zamýšlet vytvoření místního serveru DHCP, ale použil nejedno-

značné adresy, což může způsobit propůjčování adres nechtěným klientům požadujícím adresy z jiných míst sítě.

Server DHCP systému Windows 2000 má funkce správy, které zabraňují neautorizovanému zavádění a detekují existující neautorizované servery DHCP. V minulosti mohl na síti vytvořit server DHCP kdokoli, nyní je však nutný krok autorizování. Mezi autorizované osoby obvykle patří správce domény, do níž patří daná platforma systému Windows 2000 Server, nebo ten, komu byl delegován úkol správy serverů DHCP.

Dynamická podpora klientů protokolu Bootstrap Protocol

Servery DHCP reagují jak na požadavky protokolu Bootstrap Protocol (BOOTP) tak na požadavky DHCP. BOOTP je zavedený standard TCP/IP [RFC 951] konfigurace hostitele, který předcházel DHCP. BOOTP byl původně vytvořen tak, aby umožňoval konfiguraci spouštění bezdiskových pracovních stanic. Takové stanice mají omezené možnosti ukládat si a místně přejímat adresy IP a další konfigurovatelné informace, které jsou zapotřebí v procesu spouštění pro připojení sítě vycházející z protokolu TCP/IP.

Pomocí nové podpory dynamického protokolu BOOTP lze klientům BOOTP přiřadit fond adres stejným způsobem, jakým se u klientů DHCP používá nějaký obor adres. To umožňuje dynamicky spravovat adresy IP určené k distribuci klientům protokolu BOOTP. Také to umožňuje službě DHCP opakovaně používat adresy IP použité v dynamickém fondu adres BOOTP, ovšem až po ověření, že vypršel daný čas propůjčení adresy a že jednotlivé adresy jsou nadále používány klienty BOOTP.

Přístup pouze pro čtení ke Správci služby DHCP prostřednictvím konzole

Tato funkce nabízí místní skupinu uživatelů se speciálním účelem, skupinu DHCP Users, která se objeví po instalaci služby DHCP. Když pomocí konzoly Správce služby DHCP (DHCP Manager) přidáte nějaké členy do této skupiny, poskytnete tak jiným uživatelům než správcům přístup k informacím souvisejícím se službami DHCP na serverovém počítači, ovšem na úrovni pouze pro čtení. Uživatel, který je členem této místní skupiny, to umožní zobrazovat si, nikoli však upravovat informace a vlastnosti uložené na zadaném serveru DHCP. Tato funkce je užitečná pro personál technické podpory, když potřebuje získat hlášení o stavu DHCP. Přístup pro čtení a zápis lze zajistit prostřednictvím členství ve skupině DHCP Administrators.

Návrh protokolu DHCP ve vaší síti

Při návrhu či inovaci sítě můžete implementovat protokol DHCP s využitím centralizovaného nebo distribuovaného pojetí (viz obrázky 7.7 a 7.8). V centralizovaném prostředí se adresy IP distribuují centrálně danému serveru DHCP jedním serverem DHCP zodpovědným za distribuci adres v jemu přidělené podsíti nebo sídlo. V distribuovaném prostředí může být server DHCP zodpovědný za sídlo, v němž se nachází, a libovolně jiné sídlo, místní či vzdálené, které je součástí určené struktury společnosti.

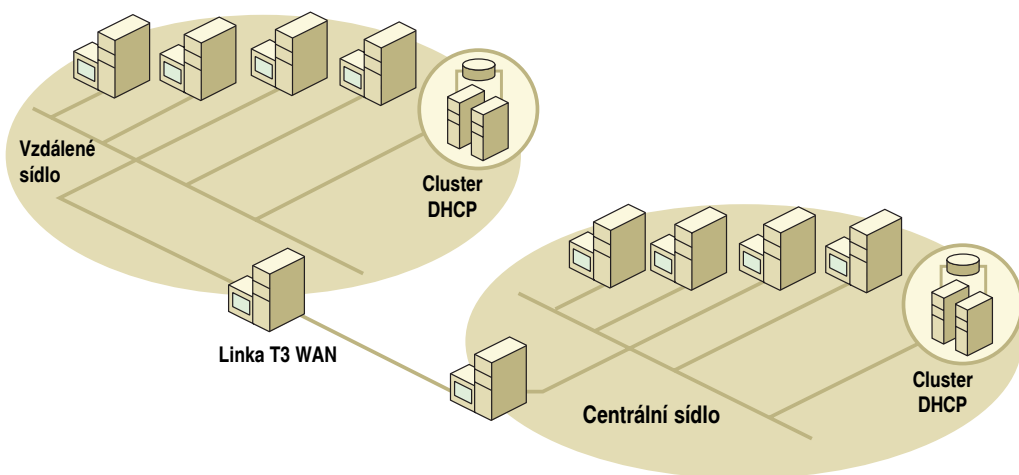
Chcete-li efektivně naplánovat použité schéma distribuce adres, zamyslete se nad tématy uvedenými v následujících oddílech.

Velikost infrastruktury sítě

Kolik sídel máte ve struktuře domén? Máte-li jen jedno centrální sídlo a dvě vzdálená sídla, pak je implementace distribuované struktury protokolu DHCP ideální. Struktura domén se třemi či více sídly vyžaduje centralizovanou strukturu DHCP, v níž servery DHCP přiřazují adresy IP svým určeným sídlům.

Obrázky 7.7 a 7.8 jsou příklady distribuovaného a centralizovaného prostředí DHCP. Distribuované prostředí se používá k distribuci adres IP na vzdálená síťová sídla. Centralizované prostředí se používá k distribuci adres IP v rámci určitého sídla. Protože služba Windows Clustering spolupracuje se všemi službami systému Windows, které podporují clustering, mohou na serveru, na němž pracují klastrové služby DHCP, fungovat i další služby podporující clustering.

Na obrázku 7.7 jsou dvě sídla, jedno hlavní neboli centrální sídlo a jedno vzdálené sídlo. Obě sídla obsahují klastry DHCP, které přiřazují adresy IP ve svých sídlech, takže přes linku rozlehlé oblasti neprochází žádný provoz DHCP.



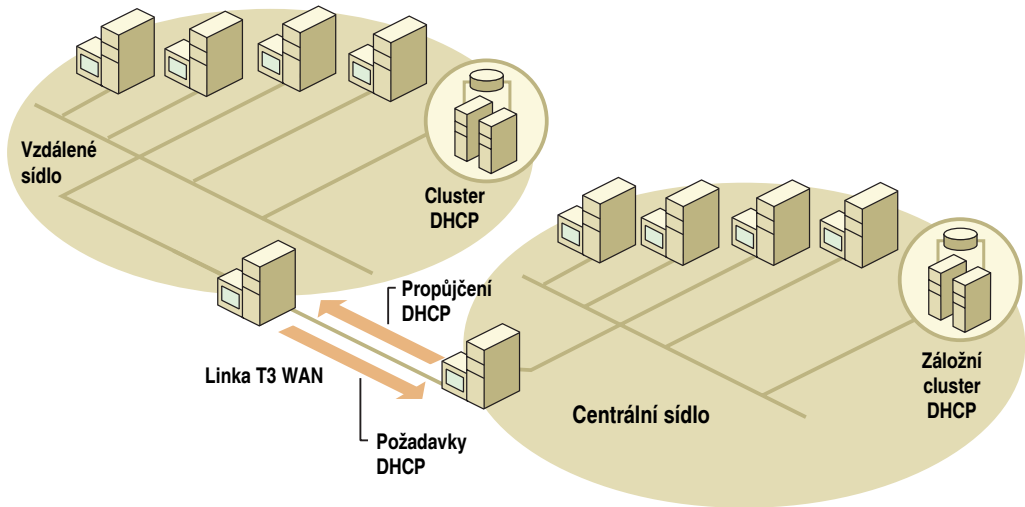
Obrázek 7.7 Centralizovaná struktura protokolu DHCP

Na obrázku 7.8 jsou opět dvě sídla, centrální a vzdálené, tentokrát je však centrální sídlo zodpovědné za distribuci adres IP jak pro sebe, tak i pro vzdálené sídlo. Všimněte si, že vzdálené sídlo má záložní klastrový server DHCP, který se stará o provoz DHCP v případě výpadku linky rozlehlé oblasti nebo jiného problému.

Další informace o DHCP najdete v nápovědě systému Windows 2000 a v knize *Microsoft Windows 2000 Server Síť TCP/IP*.

Technologie Asynchronous Transfer Mode v systému Windows 2000

Technologie Asynchronous Transfer Mode (ATM) systému Windows 2000 zajišťuje flexibilní, škálovatelné, vysokorychlostní řešení zvyšujících se potřeb zajištění kvality služeb v sítích, kde je podporováno více typů informací, jako jsou data, hlas nebo video a audio v reálném čase. S využitím ATM mohou všechny typy informací procházet jediným síťovým připojením. Služby ATM systému Windows 2000 umožňují dokonalou migraci existujících páteřních spojení sítí na technologii ATM a jejich propojení s tradičními sítěmi LAN pomocí služeb emulace LAN (LANE) systému Windows 2000. Další informace o LANE najdete v oddílu „Funkce ATM systému Windows 2000“ dále v této kapitole.



Obrázek 7.8 Distribuovaná struktura protokolu DHCP

Výhody používání ATM systému Windows 2000

ATM systému Windows 2000 přináší následující výhody:

- Vysokorychlostní komunikace
- Služba orientovaná na spojení, podobně jako tradiční telefonie
- Rychlé hardwarové přepínání
- Jediný, univerzální, interoperabilní síťový přenos
- Jediné síťové připojení, které může spolehlivě slučovat hlas, video a data
- Flexibilní a výkonné přiřazování šířky pásma sítě
- Podpora služby Quality of Service (QoS), která dává správcům možnost vyhrazovat šířku pásma sítě na základě několika parametrů, mezi které patří (nejsou však jedinámi): kdo požadavek inicioval, typ odesílaných dat (jako jsou datové proudy videa) nebo cílové místo. Další informace o QoS najdete v knize *Microsoft Windows 2000 Server Sítě TCP/IP*.

Funkce ATM systému Windows 2000

Nové funkce systému Windows 2000 umožňují zavedení rozšiřitelného, škálovatelného rámce, v němž lze vybudovat různé síťové struktury, jako je například ATM. Následující oddíly popisují nové funkce, které jsou součástí ATM systému Windows 2000.

Správce volání uživatelského síťového rozhraní ATM

Systém Windows 2000 nyní obsahuje Správce volání (Call Manager), který podporuje a spravuje volání na síti ATM. Odpovídá signalizačním specifikacím ATM Forum UNI verze 3.1 a podporuje vytváření přepínaných virtuálních obvodů (switched virtual circuit – SVC) a trvalých virtuálních obvodů (permanent virtual circuit – PVC).

Aktualizovaná podpora NDIS a hardwaru ATM

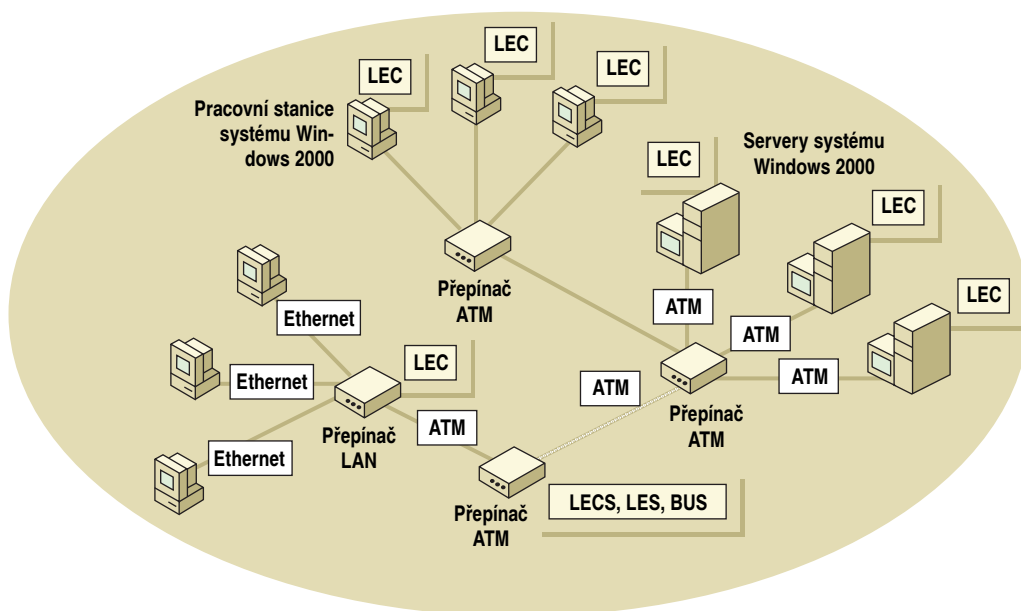
NDIS verze 5 nyní přímo podporuje síťové adaptéry ATM. To umožňuje prodejcům adaptérů ATM výhodněji využívat svůj hardware tím, že vytvoří ovladače zařízení miniportu ATM, které budou spolupracovat se systémem Windows 2000. Ovladače výrobců většiny síťových adaptérů ATM jsou nyní součástí Windows 2000.

Emulace LAN na síti ATM

Služby emulace LAN sítě ATM (LANE) jsou zapotřebí k zajištění spolupráce mezi ATM a tradičními prostředím LAN. LANE umožňuje jednodušší migraci a integraci s tradičními síťovými technologiemi LAN, jako je Ethernet nebo Token Ring, protože tyto sítě LAN emuluje na sítích ATM. Systém Windows 2000 obsahuje podporu emulace LAN na síti ATM a emulované sítě LAN (Emulated LAN – ELAN) se může účastnit jako klient emulace LAN (LAN Emulation Client – LEC). Klient emulace LAN systému Windows 2000 může využívat služby emulace LAN, které výrobci ATM dodávají se svými síťovými přepínači. Systém Windows 2000 standardně nainstaluje klienta emulace LAN v případě, kdy detekuje instalovaný síťový adaptér ATM. LEC se také bude standardně pokoušet účastnit se ve výchozí nespecifikované síti ELAN. Ve službách emulace LAN musí být nakonfigurována tato výchozí síť ELAN.

Obrázek 7.9 ukazuje síť LANE.

Obrázek 7.9 Síť LANE



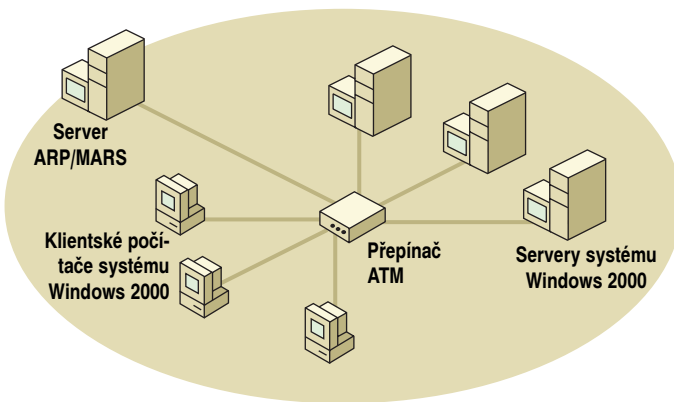
IP/ATM

IP/ATM umožňuje protokolu TCP/IP přímo používat funkce sítě ATM. Systém Windows 2000 nyní zahrnuje podporu IP/ATM. S touto podporou mohou aplikace používající protokol TCP/IP přímo využívat síť ATM. Také aplikace vytvořené tak, aby využívaly službu Generic Quality of Service (QoS) pod Windows Sockets, budou přímo těžit ze zabudovaných schopností QoS poskytovaných sítí ATM.

IP/ATM je skupina služeb pro komunikaci přes síť ATM, kterou lze využít jako alternativu emulace LAN na síti ATM. Služby IP/ATM jsou řízeny dvěma hlavními součástmi: klientem IP/ATM a serverem IP/ATM. Server IP/ATM zahrnuje server ARP sítě ATM a server překladu adres vícesměrového vysílání (multicast address resolution server – MARS). Součásti serveru IP/ATM mohou být umístěny na serveru se systémem Windows 2000 nebo na přepínači ATM.

Hlavní výhodnou použití IP/ATM je větší rychlost, než nabízí LANE, protože v případě použití IP/ATM se do paketů procházejících zásobníkem protokolu nepřidávají žádné dodatečné informace hlaviček. Jakmile vytvoří klient IP/ATM požadované spojení, data lze přenášet bez úprav.

V případě IP/ATM můžete používat statickou adresu IP nebo nakonfigurovat profil TCP/IP tak, aby používal server DHCP. Obrázek 7.10 znázorňuje síť IP/ATM.



Obrázek 7.10 Síť IP/ATM

Služba vícesměrového vysílání a překladu adres (MARS)

Systém Windows 2000 obsahuje službu vícesměrového vysílání a překladu adres (Multicast and Address Resolution Service), která podporuje používání IP/ATM. Tato služba podporuje protokol překladu adres (Address Resolution Protocol – ARP) IP/ATM a umožňuje výhodné používání vícesměrového vysílání na sítích ATM.

PPP/ATM

S nástupem technologií digitálních odebíraných linek (xDSL) bude vysokorychlostní přístup k síti z domova a z prostředí malých kanceláří stále častější. V těchto oblastech existuje několik standardů, které zahrnují také Asymmetric DSL (ADSL) a Universal ADSL (UADSL neboli DSL Lite). Tyto technologie fungují přes místní smyčku (poslední úsek měděného drátu mezi telefonní sítí a domovem). V mnoha oblastech Spojených států se tato místní smyčka následně připojuje k základní síti ATM.

ATM přes službu xDSL zachovává vysokorychlostní charakteristiky a služba QoS zaručuje dostupnost v základní vrstvě sítě, aniž by bylo nutné měnit protokoly. Nabízí se tak možnost vytvoření sítě ATM mezi dvěma koncovými body do místa bydliště nebo malé kanceláře. Taková síť poskytuje několik výhod, mezi které patří:

- Transparentnost protokolů
- Podpora více tříd QoS se zárukami
- Škálovatelnost šířky pásma
- Evoluční cesta k novějším technologiím DSL

Když se k této architektuře koncových bodů přidá protokol Point-to-Point Protocol (PPP), nabízejí se nové funkce a dále se zvyšuje její užitečnost. PPP nabízí následující dodatečné výhody:

- Ověřování připojení na úrovni uživatelů
- Přiřazování adres vrstvy 3
- Více současných relací k různým cílovým místům
- Transparentnost protokolů vrstvy 3
- Šifrování a komprese

Pokud každý virtuální obvod (virtual circuit – VC) nese jen jednu relaci protokolu Point-to-Point Protocol (PPP), každé cílové místo bude mít svou vlastní ověřenou relaci PPP, čímž bude zajištěno ověření jednotlivých obvodů VC. To zajišťuje dodatečné zabezpečení a zaručuje šířku pásma, jako byste měli pevnou linku. Náklady na další prostředky může také omezit použití technologie Null Encapsulation přes AAL5 (protože PPP zajišťuje multiplexing protokolů).

Úvahy o návrhu sítě ATM

Sítě ATM jsou tvořeny třemi součástmi: koncovými prvky (uživateli), přepínači ATM a rozhraními. Při návrhu sítě ATM vezměte v úvahu pokyny uvedené v následujících oddílech.

Použijte výchozí síť ELAN

Systém ATM Windows 2000 je zpočátku nakonfigurován s výchozím nespecifikovaným názvem sítě ELAN. Plánujete-li implementovat emulaci malé sítě LAN, doporučujeme vám použít předkonfigurovanou výchozí nespecifikovanou síť ELAN. Implementujete-li velkou síť ATM, pak vám umožní více vytvořených sítí ELAN lepší správu a zabezpečení.

Při koupi přepínače ATM vám doporučujeme prověřit specifikace výrobku a ujistit se, že je předkonfigurován na síť ELAN využívající výchozí nezadaný název sítě ELAN. Přepínače předkonfigurované výchozí sítí ELAN zaručí v malých prostředích ATM prakticky bezproblémové nastavení.

Použijte podporované adaptéry ATM

Ještě než si koupíte adaptér ATM, který budete používat v systému Windows 2000, ujistěte se, že je na seznamu Hardware Compatibility List. Další informace najdete v odkazu Hardware Compatibility List stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Před inovací si poznamenejte konfigurace

Ještě před inovací systému Windows NT 4.0 na systém Windows 2000 si u každého klienta emulace LAN, kterého plánujete inovovat, poznamenejte následující konfigurační informace:

- Název sítě ELAN
- Typ média emulovaného na síti LAN
- Adresy ATM serveru emulace LAN (LAN Emulation Server – LES) a serveru Broadcast and Unknown Server (BUS) přidruženého síti ELAN

Nakonfigurujte síť ELAN

Když si poznamenáte tyto konfigurační parametry, použijte ke konfiguraci služeb LAN Emulation Configuration Service (LECS), LAN Emulation Service (LES) a Broadcast and Unknown Service (BUS) tak, aby podporovaly síť ELAN a jejich přiřazené parametry, konfigurační rozhraní přepínače ATM. Dále nainstalujte systém Windows 2000 a nakonfigurujte název sítě ELAN každé služby LEC.

Pro každou logickou podsít' IP použijte jen jeden server ARP/MARS ATM

Používá-li vaše síť IP/ATM, doporučujeme vám pro každou logickou podsít' IP vaší sítě nakonfigurovat jen jeden server ARP/MARS ATM. Máte-li více serverů ARP na jednom segmentu sítě a váš klient ARP je nakonfigurován na adresy těchto serverů, může dojít k narušení synchronizace mezí pamětí ARP. Části vaší sítě pak mohou být nedosažitelné.

Služba Quality of Service

Služba Quality of Service (QoS) systému Windows 2000 je sada součástí a technologií, které dovolují správci sítě přidělovat a spravovat síťové prostředky mezi dvěma koncovými body. QoS umožňuje zavedení konzistentních šířek pásma síťového provozu například pro video a audio aplikace a aplikace ERP, které obvykle spotřebovávají velké množství šířky pásma sítě. QoS je metoda umožňující sítím efektivně řídit svůj provoz a ve svém důsledku tak snižovat náklady na nové hardwarové prostředky. Správu zjednodušuje služba Admission Control Service, což je administrativní rozhraní QoS, které umožňuje centralizovanou správu zásad QoS. Tyto zásady, které si můžete nakonfigurovat tak, aby naplňovaly potřeby uživatelů, programů a fyzických lokací, určují, jak si můžete rezervovat a přidělovat prioritní šířky pásma. V minulosti byla služba QoS zakomponována do hardwaru směrovačů a přepínačů. Protože je nyní dostupná jako součást systému Windows 2000, lze dosáhnout nové úrovně řízení v rámci celého podniku až na úroveň jednotlivých kancelářských počítačů.

Služba QoS systému Windows 2000 vám nabízí tyto výhody:

- Centralizované zásady a konfigurace podsítí pomocí nástroje QoS Admission Control Services Manager.
- Používá identity podniku, podsítě a uživatele jako kritéria rezervování síťových prostředků a nastavení priorit.
- Zajišťuje rezervování prioritní šířky pásma, které je pro uživatele transparentní a nevyžaduje žádné školení.
- Umožňuje správci sítě přidělovat síťové prostředky prioritnímu provozu.
- Zajišťuje služby předávání dat mezi koncovými body a zaručuje malá zpoždění.
- Možnost spolupráce s konfiguracemi LAN, WAN, ATM, Ethernet a Token Ring.

- Podpora vícesměrových přenosů zpráv rezervování šířky pásma.
- Služba QoS Admission Control systému Windows 2000 zjednodušuje správu prioritní šířky pásma při zachování nízkých nákladů na vlastnictví. V tomto případě nízké náklady na vlastnictví znamenají, že v zájmu získání větší šířky pásma nemusíte vyměňovat síťová média.

Další informace o DHCP najdete v nápovědě systému Windows 2000 a v knize *Microsoft Windows 2000 Server Sítě TCP/IP*.

Seznam úkolů plánování strategií práce v síti

Tabulka 7.6 shrnuje úkoly, které musíte vykonat v rámci určování strategií konektivity sítě.

Tabulka 7.6 Seznam úkolů plánování strategií práce v síti

Úkol	Umístění v kapitole
Pomocí diagramu současné sítě zjistěte strukturu konektivity. Nemáte-li žádný diagram, vytvořte jej.	Přehled konektivity sítě
Prozkoumejte strukturu protokolu TCP/IP. 2000	Protokol TCP/IP systému Windows
Určete metody konektivity Internetu a služby Směrování a vzdálený přístup.	Služba Směrování a vzdálený přístup
Určete potřeby služby WINS.	Protokol TCP/IP a služba Windows Internet Name Service
Seznamte se s úvahami o službě Směrování a vzdálený přístup.	Služba Směrování a vzdálený přístup
Seznamte se s úvahami o zabezpečení dat.	Zabezpečení sítí VPN
Seznamte se se strukturou směrování protokolu IP.	Infrastruktura směrování protokolu IP
Určete potřeby vícesměrového vysílání.	Podpora vícesměrového vysílání
Určete požadavky protokolu DHCP.	Protokol DHCP systému Windows 2000
Seznamte se s problematikou služby Quality of Service.	Služba Quality of Service

KAPITOLA 8

Analýza infrastruktury sítě pomocí serveru Systems Management Server



Správci sítí mohou použít server Microsoft Systems Management Server (SMS) k vykonání různých úkolů zavedení systému Microsoft Windows 2000, mezi něž patří sběr informací o plánování, příprava počítačů, zavádění systému Windows 2000 a sledování procesu zavádění. Tato kapitola se zaměřuje na ty funkce SMS, které lze využít k analýze infrastruktury sítě. Výsledky této analýzy vám pomohou určit změny infrastruktury sítě, které musíte učinit v rámci přípravy na zavedení systému Windows 2000. Pomocí SMS můžete ušetřit náklady související s uskutečněním zavádění na podnikové úrovni.

Pro pochopení konceptů a postupů uvedených v této kapitole nepotřebujete žádné předchozí zkušenosti se serverem SMS. Kapitola však neobsahuje postupy zavádění a používání serveru SMS. Tyto podrobnosti najdete v dokumentaci SMS. K řádnému zavedení serveru SMS a jeho používání dobře naplánovaným způsobem budete potřebovat personál vyškolený v oblasti serveru SMS. Zdroje, které vám mohou poskytnout další informace o SMS, najdete v oddílu „Další zdroje“ na konci této kapitoly.

V této kapitole

Analýza infrastruktury sítě 188

Vytvoření inventáře 192

Použití inventáře k přípravě infrastruktury sítě 186

Sledování sítě 201

Zajištění kompatibility aplikací 201

Seznam úkolů plánování analýzy sítě 203

Další zdroje 203

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Proces analýzy infrastruktury sítě využívající server SMS
- Sestavy podrobně popisující existující infrastrukturu sítě včetně veškerého hardwaru a softwaru

Související informace v sadě Resource Kit

- Další informace o zavádění systému Windows 2000 serverem SMS najdete v kapitole „Zavádění systému Windows 2000 pomocí serveru Systems Management Server“ v této knize.
- Další informace o testování kompatibility aplikací se systémem Windows 2000 najdete v kapitole „Testování kompatibility aplikací se systémem Windows 2000“ v této knize.

Analýza infrastruktury sítě

Kritickým krokem zavádění systému Windows 2000 je příprava infrastruktury sítě. Chcete-li připravit síť na zavádění nového systému, musíte vykonat řadu úkolů, které začínají právě analýzou současného stavu infrastruktury sítě.

Mezi hlavní úkoly vykonávané při analýze a přípravě sítě na zavedení systému Windows 2000 patří tyto:

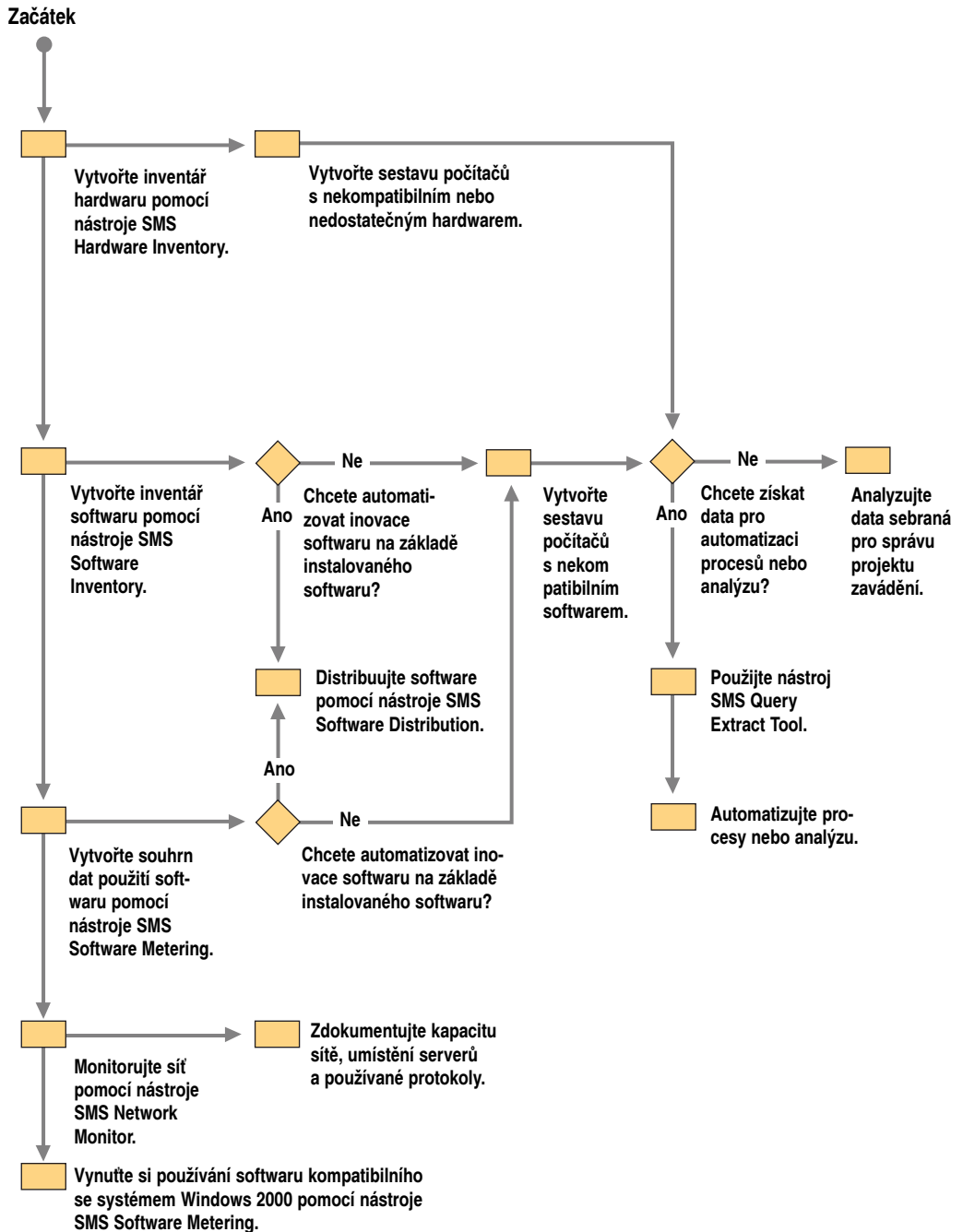
- Určení počítačů, které nemají dostatečný nebo kompatibilní hardware.
- Inovace hardwaru.
- Určení počítačů se softwarem, který není kompatibilní nebo nebude řádně fungovat v systému Windows 2000.
- Určení nejčastěji používaných aplikací, aby bylo možné prioritně a důkladně otestovat kompatibilitu právě těch nejdůležitějších aplikací.
- Analýzování použití sítě, jehož výsledkem bude zjištění dostupnosti kapacity sítě, používané protokoly a počítače, které pracují jako servery.
- Inovace nekompatibilních aplikací.
- Vyloučení nekompatibilních aplikací.

Server Systems Management Server (SMS) vám poskytuje nástroje, které potřebujete k nejefektivnějšímu vykonání těchto úkolů v podnikovém prostředí.

Práce se serverem Systems Management Server

SMS je extrémně škálovatelný systém, který lze používat k vykonávání různých úkolů správy počítačů. Během zavádění systému Windows 2000 můžete použít SMS k urychlení mnoha opakujících se úkonů. Úkoly plánování zavádění související s analýzou a přípravou sítě jsou uvedeny na obrázku 8.1.

Poznámka V rámci této kapitoly je infrastruktura sítě definována jako souhrn všech počítačů kompatibilních se systémem SMS, které se nacházejí ve vaší síti. To zahrnuje počítače se systémy Windows 2000, Windows NT Server, Windows NT Workstation, Windows 95, Windows 98, Windows 3.1 a Windows for Workgroups.



Obrázek 8.1 Vývojový diagram analýzy infrastruktury sítě pomocí serveru SMS

Použití SMS v rámci procesů plánování a zavádění systému Windows 2000 vyžaduje do-datečné prostředky. Náklady vydané na plánování a používání serveru SMS se však velmi rychle vrátí, protože budete schopni zautomatizovat úkoly zavádění systému Windows 2000.

SMS můžete použít k automatizaci úkolů zavádění systému Windows 2000 mnoha koncovým uživatelům najednou. Tyto úkoly a dokonce i v první řadě začlenění počítačů do SMS lze všechny vykonat, aniž by technici museli navštěvovat jednotlivé počítače. Automatizované úkoly nabízejí tyto výhody:

- Výrazně omezují manuální práci a návštěvy sídel.
- Distribuce v rozsáhlé geografické oblasti.
- V případě nějakých chyb je zotavení velmi jednoduché.
- Flexibilní časové plánování.
- Denní (nebo ještě častější) aktualizace stavu.

Poznámka Systém SMS závisí na softwarových součástech, které běží na klientovi a které se (přínejmenším občas) připojují k infrastruktuře SMS přes síť. Proto nelze použít SMS k instalaci systému Windows 2000 na nové počítače, které ještě nemají operační systém a síťového klienta. Kapitola „Automatizování instalace a inovace klientů“ v této knize nabízí metody, které lze využít k nastavení nových počítačů se systémem Windows 2000.

Jak může server Systems Management Server urychlit zavádění systému Windows 2000

SMS vám pomůže s plánováním zavádění systému Windows 2000 tím, že vám zodpoví různé důležité otázky. Se zaváděním systému Windows 2000 vám pomůže:

- přípravou počítačů,
- distribucí zdrojových souborů systému Windows 2000 do blízkosti počítačů uživatelů,
- inicializací inovací na systém Windows 2000 řízeným a zabezpečeným způsobem,
- hlášením stavu zavádění.

Systém SMS vám také může pomoci vyřešit problémy související se zaváděním a poskytnout ihned po dokončení zavádění použitelnou strukturu správy infrastruktury systému Windows 2000.

Tato kapitola se zaměřuje na to, jak můžete použít server SMS ke sběru podrobností o infrastruktuře sítě, které potřebujete pro zavádění systému Windows 2000. K naformátování dat do snadno použitelných sestav můžete použít různé nástroje. Informace můžete také extrahovat do jiných programů, například do programu Microsoft Excel, kde je lze dále analyzovat. Sebrané informace můžete použít také k automatizování úkolů zavádění.

Sebrané informace vám umožní zodpovědět různé důležité otázky plánování zavádění, jako jsou tyto:

- Kolik počítačů máte? Kde jsou? Mají hardware s dostatečnou kapacitou pro systém Windows 2000? Které počítače mají hardware nekompatibilní se systémem Windows 2000?

- Jaký software je instalován na počítačích vašich uživatelů? Jaký software skutečně používají? Které počítače mají software nekompatibilní se systémem Windows 2000?
- Jaká kapacita je k dispozici na síťových linkách? Jaké protokoly se na vaší síti používají?

Také se dozvíte, jak vám může server SMS pomoci s problémy kompatibility aplikací.

Poznámka Další důležitou výhodou použití serveru SMS při zavádění systému Windows 2000 je jeho schopnost distribuovat systém Windows 2000 na počítače, které budou migrovat, a následně inicializovat inovaci a hlásit její stav. Tato témata jsou podrobně probírána v kapitole „Zavádění systému Windows 2000 pomocí serveru Systems Management Server“ v této knize.

Rozdíly oproti serveru Systems Management Server 1.2

Systems Management Server 2.0 se od svého předchůdce, serveru Systems Management Server 1.2, výrazně liší. Obě verze mají podobnou sadu funkcí, ale každá verze dosahuje těchto funkcí zásadně odlišnými technikami. Plánujete-li k analýze sítě a k zavedení systému Windows 2000 použít SMS 1.2, musíte si být vědomi následujících odlišností od SMS 2.0:

- Inventář softwaru vychází z předem zadaných definic aplikací. Proto musíte nejprve zjistit, jaké aplikace se mohou ve vaší organizaci nacházet, a následně zajistit jejich definování v SMS. Server SMS sice obsahuje velké množství předdefinovaných aplikací, většina organizací jich však bude muset nadefinovat ještě celou řadu, než bude kolekce inventáře softwaru SMS 1.2 sloužit jejich potřebám. Tyto definice lze získat také u konzultantů, na Internetu a od nezávislých výrobců softwaru.
- Inventář hardwaru není tak rozsáhlý, a proto může být obtížné získat všechny požadované podrobnosti o hardwaru. Výrobci počítačů mají agenty správy počítačů rozhraní Desktop Management Interface (DMI) poskytující rozsáhlé informace o inventáři hardwaru, které může SMS 1.2 využít. Každý výrobce však má jiné řešení, takže jejich zavedení v kombinovaném prostředí může být obtížné. Nezávislí výrobci softwaru poskytují řešení, která mohou těmito způsoby zlepšit inventář hardwaru.
- Distribuce softwaru není tak flexibilní, jak z hlediska možností zacílení, tak i vykonání.
- Inventář hardwaru je vyžadován u všech klientů. Není tu žádná obdoba procesů objevování klientů serveru SMS 2.0. Proto nemůže SMS 1.2 pracovat s klienty, dokud nebyli hlášeni prostřednictvím inventáře hardwaru.
- Není tu žádný nástroj měření softwaru. Proto SMS 1.2 nedokáže zabránit uživatelům ve spouštění nekompatibilních aplikací. K dispozici jsou však aplikace měření softwaru od nezávislých výrobců, z nichž mnoho se různými způsoby integruje se systémem SMS 1.2.
- Není tu žádná databáze kompatibilních produktů. Definováním porovnatelné databázové tabulky však je možné vytvořit ekvivalentní systém.
- Není tu nástroj Network Monitor Control Tool ani Network Monitor Experts, což jsou vylepšené nástroje Network Monitor (popsané dále v této kapitole).
- Server SMS 1.2 se při šíření přihlašovacích skriptů SMS a jejich součástí, pokud se používají, spoléhá na replikaci mezi řadiči domén systému Windows NT.

Vytvoření inventáře

Analýza infrastruktury sítě začíná sběrem inventáře hardwaru a softwaru. Tato data budou zásadní pro zavádění systému Windows 2000.

Vyhodnocení současného stavu hardwaru

Systém Windows 2000 je vytvořen tak, aby mohl pracovat na mnoha různých počítačích. V posledních letech se však objevilo tolik různých modelů počítačů a součástí, že je jen přirozené předpokládat, že některé počítače nebudou na systém Windows 2000 připraveny. Server SMS vám pomůže tyto počítače identifikovat.

Kapacita hardwaru

Počítače zakoupené v nedávné době pravděpodobně mají dostatečnou kapacitu pro systém Windows 2000, starším počítačům však mohou chybět požadované prostředky. Mezi chybějící prostředky patří nejčastěji nedostatečná paměť počítače, nedostatek diskového prostoru, příliš pomalý procesor, chybějící jednotka CD-ROM nebo velmi zastaralý procesor.

Budete muset nalézt počítače s nedostatečnými prostředky, abyste je mohli inovovat nebo nahradit. Proces inovování počítačů bude také výkonnější, když si distribuci předem naplánujete a budete přesně vědět, kde se nacházejí počítače vyžadující inovaci. Jakmile se dostavíte na nějaké sídlo, budete s sebou mít správné součásti a můžete přímo přejít k počítačům vyžadujícím úpravy.

Kompatibilita hardwaru

Pro plánování inovace může být důležitá řada podrobností o hardwaru. Kromě obvyklého diskového prostoru, paměti počítače a rychlosti procesoru musíte ještě zvážit následující položky:

- Systém BIOS
- Grafická karta
- Síťová karta
- Řadič disku
- Správa napájení
- Další hardware, jako je čipová sada procesoru

Tyto součásti jsou sice obvykle kompatibilní se systémem Windows 2000, nemusí tomu tak však být naprosto vždy. Jestliže jste nakoupili počítače certifikované jejich prodejci jako kompatibilní se systémem Windows 2000 nebo jestliže se nacházejí na seznamu Hardware Compatibility List systému Windows 2000, pak nebudete mít žádné problémy. Seznam Hardware Compatibility List najdete na adrese <http://www.microsoft.com> pomocí klíčového slova „HCL“. Jinak musíte všechny problémy odhalit během pilotního testování. Pilotní testování zahrnuje testování rozumného počtu jednotlivých modelů počítačů používaných vaší společností ještě před jejich inovací.

Jakmile určíte nekompatibilní modely nebo součásti, můžete pak pomocí funkce inventáře serveru SMS vyhledat všechny další počítače ve vaší společnosti, které mají stejný problém.

Prozkoumáním podrobností o součástech z inventáře hardwaru serveru SMS způsobují problémy v systému Windows 2000 můžete vybrat charakteristiky, které dané součásti přesně identifikují a následně také počítače s těmito součástmi, které při inovaci selžou. Pak můžete upravit sestavy hardwaru a vyhledat další počítače se stejnými problémy. Doporučujeme vám dále otestovat a prověřit, že všechny tímto způsobem identifikované počítače skutečně mají problémy a že se vám podařilo odhalit každý problém. Jakmile získáte větší důvěru v testování a jeho výsledky, budete také věřit, že inovace uskutečněné na základě těchto sestav budou úspěšné.

Práce s inventářem hardwaru serveru Systems Management Server

Jakmile máte ve své organizaci zavedený systém SMS, je povolení funkce Hardware Inventory serveru SMS relativně přímočaré. Klientský software SMS, který sbírá podrobnosti o inventáři hardwaru, pracuje se součástími Windows Management Instrumentation (WMI), s jejichž pomocí zjišťuje podrobnosti o hardwaru daného počítače. WMI je součástí serveru SMS a je také dostupné z dalších zdrojů. Klientské počítače automaticky hlásí podrobnosti o inventáři hardwaru serverům SMS a data se předávají hierarchicky směrem vzhůru. Ke všem datům pak můžete přistupovat z centrálního místa. Data se standardně aktualizují jednou týdně, tuto frekvenci však můžete změnit.

Poznámka SMS vyhledává počítače pomocí procesů označovaných za metody objevování. Samo objevování již poskytuje určité základní informace o počítačích včetně skutečnosti, že existují, jejich názvů, jejich síťových adres a jejich umístění. To již může dostačovat pro určité typy dotazů a sestav inventářů hardwaru. Objevování má výhodu v tom, že vyžaduje méně prostředků než inventář hardwaru. Tyto rozdíly v prostředcích jsou však často nevýznamné.

SMS sbírá velmi bohatou sestavu podrobností o inventáři hardwaru, což zahrnuje většinu vámi požadovaných informací. Inventář hardwaru SMS lze snadno rozšířit, potřebujete-li dodatečné podrobnosti. Typickým rozšířením je zeptat se uživatele, na jakém podlaží se nacházejí, v jaké kanceláři atd. Dalším obvyklým rozšířením je získávání informací specifických jednotlivým výrobcům, které mohou být obsaženy v systému BIOS, jako je sériové číslo nebo číslo modelu. Tyto typy dat se často jen obtížně sbírají elektronicky, nelze je získat pomocí standardních technik, nebo závisí na subjektivních preferencích, a proto je zapotřebí použít rozšíření specifická pro jednotlivé zákazníky. Taková rozšíření se však implementují snadno, jak je popsáno v dokumentaci SMS.

Tabulka 8.1 nabízí hypotetické příklady hardwarových součástí, které mohou mít problémy s kapacitou nebo kompatibilitou se systémem Windows 2000. Obsahuje také třídy a vlastnosti SMS, které se používají k jejich kontrole. Použití tříd a hodnot je popsáno v následujícím oddílu o vytváření sestav, analyzování a použití sebraných dat.

Tabulka 8.1 Příklad hardwarových požadavků systému Windows 2000

Prostředek	Professional	Server	Třída SMS	Vlastnost SMS
Paměť	90 MB	128 MB	SMS_G_System_X86_PC_MEMORY	TotalPhysicalMemory
Diskový prostor	1 GB	1 GB	SMS_G_System_Logical_Disk	FreeSpace
Procesor	Pentium	Pentium II	SMS_G_System_PROCESSOR	Name
Grafická karta	neidentifikována	neidentifikována	MS_G_System_VIDEO	AdapterChipType

Hodnoty uvedené v tabulce jako požadavky jsou pouze hypotetické, lze je však v některých společnostech použít. Požadavky se budou měnit v závislosti na různých typech uživatelů a různých cestách inovace a podobné konfigurace počítačů se budou chovat jinak. Proto je důležité, abyste sami odhadli minimální požadavky systému Windows 2000. Také platí, že grafické karty obvykle nemají s kompatibilitou se systémem Windows 2000 problémy. Výběr systémů k inovaci na základě toho, zda se systému SMS podařilo identifikovat jejich grafické karty, slouží jako příklad jednoho kritéria hardwarové kompatibility – můžete zjistit, že musíte vyřadit počítače s určitým grafickým čipem nebo na základě mnoha jiných podrobností o hardwaru, jejichž data vám systém SMS poskytuje.

Vyhodnocení současného stavu softwaru

Systém Windows 2000 obsahuje stejná programovací rozhraní a funkce, které byly dostupné také v předchozích verzích systému Windows, vylepšené funkce se však nechovaly vždy stejným způsobem. Problémy s kompatibilitou se obvykle minimalizují různými programovacími standardy, avšak ne všechny aplikace byly vyvinuty přesně podle těchto standardů. Z těchto a podobných důvodů nemusí být určitý software vytvořený pro různé verze systému Windows kompatibilní se systémem Windows 2000.

Kapitola „Testování kompatibility aplikací se systémem Windows 2000“ zevrubně popisuje problémy s kompatibilitou softwaru a poskytuje podrobnosti o tom, jak určit kompatibilitu aplikací se systémem Windows 2000. Přesto však budete muset zodpovědět dvě velmi obsáhlé otázky: „Jaké softwarové aplikace vaše společnost používá?“ a „Na kterých počítačích jsou instalovány nebo používány?“. SMS nabízí odpovědi na tyto otázky.

Inventář softwaru SMS se povoluje a používá velmi podobně jako inventář hardwaru SMS. Metoda, kterou SMS používá k získání informací, je však výrazně odlišná, protože spočívá v prohledávání pevného disku každého klienta a hledání souborů s příponou názvu .exe. Dále se zjistí další podrobnosti, pokud jsou k dispozici, o nalezených souborech a tyto informace se hlásí serverům sídla SMS. Inventář softwaru SMS můžete rozšířit nakonfigurováním SMS na vyhledávání také souborů s jinými příponami než jen .exe, jako jsou .dll nebo .com.

Protože inventář softwaru SMS sbírá podrobnosti o všech spustitelných programech na všech počítačích, můžete si být jisti, že takto identifikujete veškerý software instalovaný na počítačích vaší společnosti. Inventář softwaru SMS se také pokouší získat z každého programu data hlaviček. Data hlaviček jsou informace o softwaru a jsou součástí

spustitelných souborů. Data hlaviček existují ve většině nově vyvinutých programech, každý počítač však bude obsahovat také nějaké starší programy. Informace hlaviček programu poskytují například popisné názvy – nemusíte vycházet z často kryptických názvů programových souborů.

Tabulka 8.2 uvádí několik vlastností, které budete potřebovat k práci s daty z inventáře softwaru SMS. Vlastnosti softwaru s daty hlaviček jsou ze třídy SMS_G_System_SoftwareProduct. Vlastnosti softwaru bez dat hlaviček jsou ze třídy SMS_G_System_UnknownFile.

Tabulka 8.2 Softwarová data

Data	Software s daty hlaviček	Software bez dat hlaviček
Název souboru	FileName	FileName
Velikost souboru	FileSize	FileSize
Název produktu	ProductName	Neexistuje
Verze produktu	ProductVersion	Neexistuje
Jazyk produktu	ProductLanguage	Neexistuje

Inventář softwaru SMS dokáže identifikovat veškerý software instalovaný na počítačích, neříká vám však, který software se skutečně používá. Když se již nějaký software nepoužívá, je zbytečné vynakládat peníze na jeho inovaci.

Inventář softwaru SMS dokáže sbírat soubory z klientských počítačů. Máte-li mnoho klientských počítačů s velkými soubory, může to výrazně zatěžovat síť a diskový prostor na serverech síťového sídla. Budete-li však inventář softwaru používat rozumně, získáte mocný nástroj. Můžete například spustit inovaci na systém Windows 2000 na počítačích se systémy Windows 95 a Windows 98 takovým způsobem, že se vytvoří pouze hlášení o inovaci (soubor Upgrade.txt v adresáři Windows).

Chcete-li pouze vytvořit hlášení o inovaci, použijte příkaz **Winnt32 /checkupgradeonly** nebo příslušný soubor odpovědí a postupy popsané v kapitole „Zavádění systému Windows 2000 pomocí serveru Systems Management Server“ v této knize. Inventář softwaru SMS pak může převzít tyto soubory od všech počítačů a uložit je centrálně na místo, kde si je můžete snadno zobrazit. Hlášení o inovaci mohou obsahovat popisy problémů s hardwarem a softwarem, které je zapotřebí vyřešit ještě před pokusem o inovaci daných počítačů.

Systém SMS obsahuje funkci označovanou za měření softwaru, která hlásí skutečné využívání softwaru. Měření softwaru hlásí vyvolání každého programu a tato data následně zaznamenává do databáze sídla SMS. Programy, které jsou součástí operačního systému, jako je například Poznámkový blok (Notepad), jsou z této kolekce dat často vyloučeny.

Kapitola „Metering Software“ v knize *Microsoft Systems Management Server Administrator's Guide* popisuje, jak se používá měření softwaru SMS včetně tvorby sestav na základě dat této funkce. Zvažte zejména použití režimu offline, který získává stejné informace, nehlásí je však příliš často. Tím se výrazně snižuje zatížení sítě, klientů a serverů.

Použití inventáře k přípravě infrastruktury sítě

Jakmile získáte všechna data, můžete je použít k zodpovězení otázek vznikajících během plánování zavádění systému Windows 2000. Data lze použít také k urychlení procesů zavádění.

Vytváření sestav získaných dat

Základním způsobem použití dat inventáře SMS je vytvářet sestavy zodpovídající konkrétní otázky. Další informace o vytváření sestav SMS najdete v odkazu Microsoft Systems Management Server Technical Details stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Pro účely zavádění systému Windows 2000 můžete vytvořit následující sestavy:

- Počítače s dostatečnou kapacitou pro systém Windows 2000
- Počítače kompatibilní se systémem Windows 2000

Technici vykonávající inovace na systém Windows 2000 mohou použít tyto dvě sestavy k určení počítačů, které vyžadují inovaci hardwaru.

Musíte-li se zabývat oběma uvedenými problémy, budete pravděpodobně používat kombinaci těchto dvou sestav.

- Počítače vyžadující inovaci hardwaru

Tuto sestavu mohou používat technici starající se o hardwarové inovace. Mohou si tak objednat potřebný hardware a určit, které počítače inovaci vyžadují.

- Počítače vyžadující inovaci softwaru

Tuto sestavu mohou používat technici starající se o softwarové inovace. Mohou si tak objednat potřebný software a určit, které počítače inovaci vyžadují.

Každou z uvedených sestav lze dále rozdělit podle sídel nebo jiných podrobností podle toho, jak může vaše organizace tyto informace využít.

Ukázková sestava serveru Systems Management Server připravenosti na systém Windows 2000

Následující dotaz používá třídy SMS uvedené v tabulce 8.1 k vyhledání počítačů, které jsou připraveny na inovaci na systém Windows 2000. Kritérii použitými v tomto případě jsou 1 gigabajt volného diskového prostoru na jednotce C:, alespoň 90 megabajtů paměti, procesor třídy Pentium a skutečnost, že grafická karta není neidentifikovaná (tedy není rovna prázdnému řetězci). Tato kritéria předpokládají, že jednotka C: je systémový oddíl uživatele. Sestava vytvořená z tohoto ukázkového dotazu je uvedena na obrázku 8.2.

Windows 2000-Ready PCs

Site	Computer	Disk Free	CPU	Memory	Video
ORA	ORANGE2	1505	Intel Pentium II processor	67	ATI3D RAGE PRO AGP (GT
	RED1	2242	Intel Pentium II processor	130	ATI3D RAGE PRO AGP (GT
	RED2	1504	Intel Pentium II processor	130	ATI3D RAGE PRO AGP (GT
PUR	PURPLE1	1331	Intel Pentium II processor	67	ATI3D RAGE PRO AGP (GT
RED	ORANGE2	1505	Intel Pentium II processor	67	ATI3D RAGE PRO AGP (GT
	RED1	2242	Intel Pentium II processor	130	ATI3D RAGE PRO AGP (GT
	RED2	1504	Intel Pentium II processor	130	ATI3D RAGE PRO AGP (GT

Obrázek 8.2 Ukázková sestava SMS počítačů s dostatečnou kapacitou pro systém Windows 2000

Mnoho organizací bude chtít inovovat také počítače s méně než 90 MB paměti a 1 GB volného diskového prostoru. Není také důvod předpokládat, že grafická karta, kterou systém SMS neidentifikoval, bude nekompatibilní se systémem Windows 2000. Máte-li nějaké grafické karty, u nichž máte podezření, že nemusí být kompatibilní se systémem Windows 2000, můžete nahradit prázdné řetězce hodnotami typu jejich čipů. V případě potřeby je možné přidat další kritéria.

Ukázkový dotaz vypadá takto:

```
SELECT DISTINCT SMS_G_System_LOGICAL_DISK.FreeSpace, SMS_G_System_PROCESSOR.Name, SMS_G_System_X86_PC_MEMORY.TotalPhysicalMemory, SMS_G_System_VIDEO.AdapterChipType, SMS_R_System.Name, SMS_R_System.SMSAssignedSites
FROM (((SMS_R_System LEFT JOIN SMS_G_System_PROCESSOR ON
SMS_R_System.ResourceId = SMS_G_System_PROCESSOR.ResourceID) LEFT JOIN
SMS_G_System_VIDEO ON SMS_R_System.ResourceId =
SMS_G_System_VIDEO.ResourceID) LEFT JOIN
SMS_G_System_X86_PC_MEMORY ON SMS_R_System.ResourceId =
SMS_G_System_X86_PC_MEMORY.ResourceID) LEFT JOIN
SMS_G_System_LOGICAL_DISK ON SMS_R_System.ResourceId = SMS_G_Sys-
tem_LOGICAL_DISK.ResourceID
WHERE (((SMS_G_System_LOGICAL_DISK.FreeSpace)>1000) AND ((SMS_G_Sys-
tem_X86_PC_MEMORY.TotalPhysicalMemory)>90000) AND ((SMS_G_System_VIDEO.AdapterChipType)<>'') AND ((SMS_G_System_LOGICAL_DISK.DeviceID)='C:') AND
((InStr(1,[SMS_G_System_PROCESSOR].[Name],"Pentium")>0))
ORDER BY SMS_R_System.SMSAssignedSites;
```

Tento dotaz můžete použít v programu Microsoft Access. Použijete-li uvedený dotaz v konzole SMS Administrator, můžete jej použít přímo v programu Microsoft Access prostřednictvím nástroje SMS Query Extract Tool. Tento nástroj se nachází v adresáři Support disku CD-ROM SMS 2.0 a je také součástí sady *Microsoft BackOffice Resource Kit 4.5*. Podrobný popis vytváření sestav SMS pomocí programu Microsoft Access nástrojem SMS Query Extract Tool najdete na výše uvedené adrese stránky webových prostředků.

Použití podsystému kompatibility produktů

SMS má databázi kompatibility produktů, která se často používá k porovnání softwaru na jednotlivých počítačích, jak je hlásí podsystém inventáře softwaru SMS, se seznamem softwaru se známými problémy kompatibility s rokem 2000. Tento podsystém můžete také použít k porovnání softwaru se seznamem softwaru se známými problémy kompatibility s měnou Euro. Totéž platí pro kompatibilitu se systémem Windows 2000 – můžete použít databázi kompatibility produktů v sestavách SMS k určení počítačů s problémy kompatibility aplikací se systémem Windows 2000.

SMS neobsahuje seznam softwarových produktů se známými problémy kompatibility se systémem Windows 2000. Kapitola „Testování kompatibility aplikací se systémem Windows 2000“ v této knize vám pomůže zjistit, kde se ve vaší organizaci nacházejí nějaké aplikace s problémy kompatibility.

Rozšíření podsystému kompatibility produktů informace o kompatibilitě hardwaru a softwaru se systémem Windows 2000

Kapitola „Determining Product Compliance“ v knize *Microsoft Systems Management Server Administrator's Guide* popisuje podsystém kompatibility produktů SMS. Zahrnuje také procedury přidávání nových produktů a vytváření sestav na základě polí třídy kompatibility produktů.

Jen stručně řekněme, že nová položka se do databáze kompatibility aplikací přidává pomocí konzole SMS Administrator. Vyberte položku **Product Compliance** (kompatibilita produktu) a z nabídky **Akce** (Action) zadejte příkaz **Nový** (New) a dále **Product Compliance**. Zobrazí se dialogové okno vlastností kompatibility produktů. Jednotlivá pole popisuje online nápověda.

Upozornění Pole kompatibility produktů musí přesně odpovídat polím nalezeným procesem inventáře softwaru SMS. Pomocí tlačítka **Procházet** (Browse) můžete vyhledat konkrétní soubor a zajistit tak, že název a velikost budou zadány naprosto přesně. Pole názvu produktu, verze a jazyka nabízejí rozevírací seznamy, které vám umožní vybrat přesné hodnoty, jež inventář softwaru SMS nalezl.

Věnujte se zejména polím **Compliance Type** (typ kompatibility) a **Compliance Level** (úroveň kompatibility). Obě pole obsahují rozevírací seznam uvádějící všechny dříve použité hodnoty v daném poli. Standardně nabízí pole **Compliance Type** pouze hodnotu „Year 2000 Compliance“ (kompatibilita s rokem 2000), můžete sem však zapsat libovolnou hodnotu. Lze tak například použít zadání „Windows 2000 Compat.“ (kompatibilita se systémem Windows 2000), přičemž hodnota je omezena na 20 znaků.

Seznam **Compliance Level** bude prázdný, dokud nevyberete typ kompatibility. Jakmile vyberete nějaký typ kompatibility, bude seznam **Compliance Level** obsahovat všechny hodnoty dříve použité jako typ kompatibility. Zpočátku platí, že zatím nebyly použity žádné hodnoty, a proto tedy bude tento seznam prázdný. Můžete sem zapsat libovolnou hodnotu, například „Compatible“ (kompatibilní), „Incompatible“ (nekompatibilní), „Compatible with minor issues“ (kompatibilní s menšími problémy) nebo „Compatible with major issues“ (kompatibilní se zásadními problémy).

Tip Chcete-li pro systém Windows 2000 použít stejné úrovně kompatibility, jaké jsou poskytnuty pro kompatibilitu s rokem 2000, pak dočasně vyberte jako typ kompatibility položku „Year 2000 Compliance“, vyberte úroveň kompatibility, kterou chcete použít, a zkopírujte ji do schránky. Změňte typ kompatibility na systém Windows 2000 a do pole **Compliance Level** vložte zkopírovanou hodnotu.

Vytváření sestav podsystémem kompatibility produktů

Databázi sídla SMS můžete použít k vytváření sestav kompatibility se systémem Windows 2000. Třída SMS_G_System_SoftwareProduct má vlastnosti pro všechny softwarové produkty, které proces inventáře softwaru SMS objevil. SoftwareProductCompliance má vlastnosti z databáze kompatibility. Porovnání souvisejících vlastností z obou tabulek vám umožní zjistit, zda jsou známy nějaké problémy kompatibility s jednotlivými produkty. Tabulka 8.3 uvádí vlastnosti, které potřebujete.

Tabulka 8.3 Data kompatibility produktů

Data	Vlastnost inventáře softwaru SMS	Vlastnost kompatibility produktu SMS
Název souboru	FileName	FileName
Velikost souboru	FileSize	FileSize
Název produktu	ProductName	ResProdName
Verze produktu	ProductVersion	ResProdVer
Jazyk produktu	ProductLanguage	ResProdLangID
Typ kompatibility	N/A	Type
Úroveň kompatibility	N/A	Category

Nejjednodušší možností, jak začít používat podsystém kompatibility SMS k vytváření sestav kompatibility se systémem Windows 2000, je zkopírovat příkaz dotazu z jednoho z existujících dotazů kompatibility s rokem 2000. Pak vytvořte nový prázdný dotaz a vložte do něj daný příkaz dotazu. Změňte hodnotu typu kompatibility a zadejte další údaje dotazu. Například následující dotaz vychází ze standardního dotazu „Y2K All Compliant Software by System in This Site and Its Subsites“ (veškerý software kompatibilní s rokem 2000 v tomto sídle a jeho podsídlech). Dotaz byl upraven jen na dvou místech – text „Year 2000 Compliance“ byl nahrazen textem „Windows 2000 Compat.“ Ukázkový dotaz vypadá takto:

```
SELECT DISTINCT sys.Name, compl.Category, compl.ProdName, compl.ProdVer, compl.ProdCompany, compl.ProdLang, compl.URL, compl.Comment FROM SMS_SoftwareProductCompliance as compl INNER JOIN SMS_G_System_UnknownFile as unknownfile ON UPPER(unknownfile.FileName) = UPPER(compl.FileName) AND unknownfile.FileSize = compl.FileSize AND unknownfile.ProductID = 0 INNER JOIN SMS_R_System as sys ON unknownfile.ResourceID = sys.ResourceID WHERE compl.Category != „Compliant“ AND compl.Type = „Windows 2000 Compat.“ UNION SELECT DISTINCT sys.Name, compl.Category, compl.ProdName, compl.ProdVer, compl.ProdCompany, compl.ProdLang, compl.URL, compl.Comment FROM SMS_SoftwareProductCompliance as compl INNER JOIN SMS_G_System_SoftwareProduct as prod ON compl.ResProdName = prod.ProductName AND compl.ResProdVer = prod.ProductVersion INNER JOIN SMS_G_System_SoftwareFile as prodfile ON UPPER(prodfile.FileName) = UPPER(compl.FileName) AND prodfile.FileSize = compl.FileSize INNER JOIN SMS_R_System as sys ON prod.ResourceID = sys.ResourceID WHERE compl.Category != „Compliant“ AND compl.Type = „Windows 2000 Compat.“ AND (compl.ResProdLangID = prod.ProductLanguage OR compl.ResProdLangID = 65535) AND prod.ProductID = prodfile.ProductID
```

Tento dotaz vrací data uvádějící nekompatibilní software podle sídel. Pomocí těchto dat můžete vytvořit sestavu programu Microsoft Access, jak ukazuje obrázek 8.3.

Site	Vendor	Product
RBD1	Microsoft Corporation	Windows 95 Starts Here
RBD3	Microsoft Corporation	Windows 95 Starts Here

Obrázek 8.3 Ukázková sestava kompatibility softwaru

Správci na příslušných sídlech pak mohou být upozorněni, že musejí na svých sídlech vyřešit uvedené problémy kompatibility aplikací. V případě potřeby lze do sestavy snadno zakomponovat názvy počítačů a další podrobnosti. Výsledky dotazu lze také použít jako základ nějaké kolekce SMS, pro kterou může být inzerován určitý balíček SMS inovující či odstraňující danou aplikaci.

Analyzování a použití získaných dat

Lidé často analyzují data sestav v zájmu nalezení odpovědí na takové otázky jako: „Kolik bude stát inovace klientských počítačů na systém Windows 2000?“ nebo „Kolik mám naučtovat tomuto středisku nákladů?“. Taková ruční analýza však může být nemožná nebo velmi náročná, pokud se týká mnoha sídel a počítačů. Proto může být vhodnější přenést data do nástroje, který k analýze používáte nejraději.

Ke snadné extrakci dat SMS, která mohou být užitečná pro zavádění systému Windows 2000, do programů jako je Microsoft Excel nebo Microsoft Access, můžete použít nástroj SMS Query Extract Tool. To je podrobně popsáno v kapitole „Reporting Options for SMS 2.0“ v knize *Microsoft Systems Management Server Resource Guide*, která je součástí sady *Microsoft BackOffice Resource Kit 4.5*.

Vášim konečným cílem je zavést systém Windows 2000 a k automatizaci tohoto procesu můžete použít právě data získaná serverem SMS. Stejné dotazy poskytující data sestav, jako je „Naše počítače připravené na systém Windows 2000“, lze použít také jako základ pro kolekce počítačů v databázi SMS, jimž se systém Windows 2000 inzeruje.

Podobně, jak bylo ukázáno v případě podsystému kompatibility produktů SMS, platí, aby byly určité počítače připraveny na systém Windows 2000, může být zapotřebí inovovat jejich software. Získaná data inventáře softwaru lze také použít k zacílení příslušných inovací na těchto počítačích, které lze uskutečnit pomocí SMS.

K instalaci systému Windows 2000 a inovaci aplikací můžete použít také jiné nástroje než systém SMS. Takové nástroje ovšem také potřebují seznam cílových počítačů, k jehož vytvoření lze využít právě data SMS. Data lze extrahovat výše popsanými technikami a lze je pak importovat do jiných nástrojů metodami, které tyto nástroje samy poskytují.

Další informace o zavádění systému Windows 2000 pomocí serveru SMS najdete v kapitole „Zavádění systému Windows 2000 pomocí serveru Systems Management Server“ v této knize. Zavádění aplikací kompatibilních se systémem Windows 2000 se uskutečňuje velmi podobně.

Sledování sítě

Důležitým aspektem přípravy na zavedení systému Windows 2000 je porozumění vlastní síti. Musíte zodpovědět otázky, jako:

- Které síťové linky a segmenty mají omezenou kapacitu?
- Jaké protokoly se používají?
- Kde se nacházejí servery služeb Dynamic Host Configuration Protocol (DHCP), Windows Internet Name Service (WINS) a podobné?

Přenos zdrojových souborů systému Windows 2000 na vzdálená sídla spotřebovává značnou část kapacity sítě. Instalace systému Windows 2000 ze sdílených míst vyžaduje ještě větší kapacitu, ta však musí být k dispozici na místních sítích. Když si ověříte, jaké protokoly se používají a kde jsou umístěny síťové servery, budete pak moci do svého plánu zahrnout všechny potřebné podrobnosti.

SMS vám pomáhá s analýzou sítě a zodpovězením uvedených a podobných otázek svým nástrojem Sledování sítě (Network Monitor) a souvisejícími funkcemi. Nástroj Network Monitor můžete použít k zobrazení úrovně aktivity na jednotlivých síťových segmentech, jak je uvedeno na obrázku 8.4. Network Monitor můžete také použít k zachytávání síťových paketů. Pak je můžete zkoumat a zjišťovat, jaké protokoly se používají a jaké počítače poskytují určité služby. Nástroj Network Monitor obsahuje funkci nazvanou Poradci programu sledování sítě (Network Monitor Experts), která dokonce vytváří tabulku protokolů a procentuální hodnoty rámců a bajtů použitých jednotlivými protokoly.

Nástroj Network Monitor Control Tool můžete nakonfigurovat tak, aby neustále sledoval síťovou aktivitu a odhaloval neautorizované servery DHCP a WINS. Nástroji předáte adresy serverů DHCP a WINS, o kterých víte, a on pak zobrazí adresy všech dalších serverů DHCP a WINS, jejichž pakety zachytí.

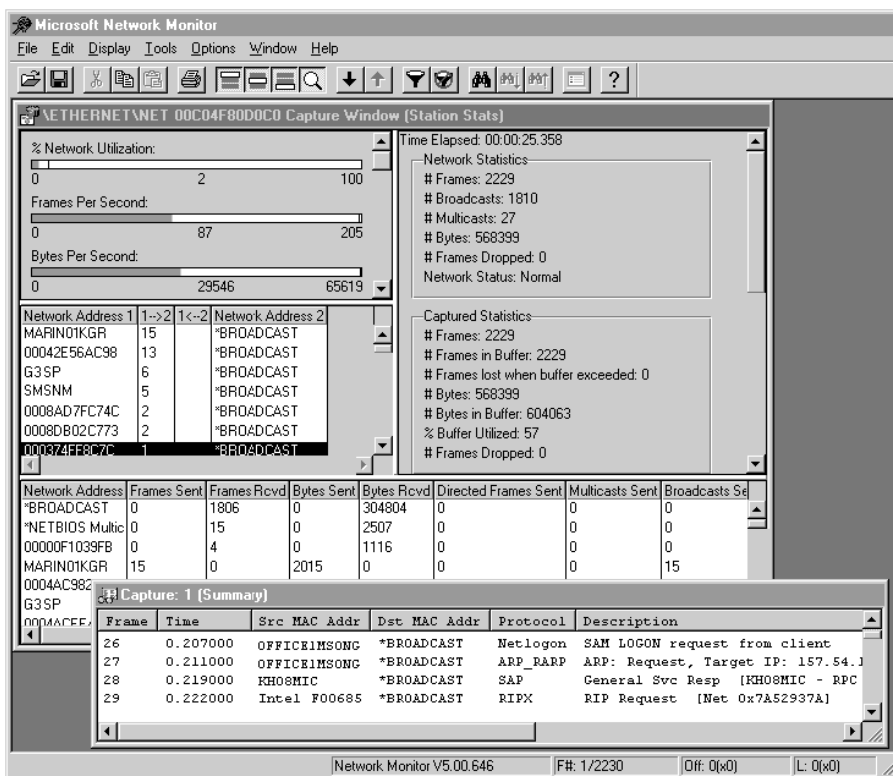
Podrobný popis nástroje Network Monitor najdete v kapitole „Údržba sítě pomocí serveru SMS“ v knize *Systems Management Server Administrator's Guide*.

Poznámka Systém Windows 2000 také obsahuje jednu verzi nástroje Sledování sítě (Network Monitor). Tato verze však pouze sleduje provoz k počítači, na němž je instalována, a z něj, včetně všesměrových vysílání. Verze SMS nástroje Network Monitor sleduje veškerý síťový provoz na segmentech, jejichž sledování jste nakonfigurovali. Nástroj Network Monitor v systému SMS 2.0 také obsahuje další vylepšení, jako je funkce Poradci programu sledování sítě (Network Monitor Experts).

Zajištění kompatibility aplikací

Systém SMS vám může se zaváděním systému Windows 2000 pomáhat různými způsoby. Jednou z důležitých funkcí SMS je vynucení používání aplikací kompatibilních se systémem Windows 2000.

SMS můžete použít k zacílení příslušných počítačů, na nichž je nutná inovace softwaru, a k dodání potřebného softwaru na tyto počítače. Inovaci lze vykonat automaticky nebo pomocí zadání uživatele. Načasování inovace lze zadat ve správci SMS a uživatelé si mohou časový plán upravit tak, aby k inovaci došlo v době, kdy se účastní nějakého jednání, nebo v jinou příhodnou dobu.



Obrázek 8.4 SMS Network Monitor

Inovaci lze také uskutečnit se speciálními bezpečnostními právy udělenými serveru SMS, takže uživatelé nemusí mít ani dočasně nějaká pokročilá práva na počítačích, které používají. Jednou z nejdůležitějších výhod používání distribuce softwaru pomocí SMS je skutečnost, že inovace vracejí stavové zprávy. Proto lze velmi snadno hlásit postup inovací.

SMS vám pomůže zajistit kompatibilitu aplikací se systémem Windows 2000 tím, že zneumožní uživatelům spouštět nekompatibilní aplikace. Uživatelé někdy chtějí používat určité aplikace nebo jejich verze, které již dobře znají, a to i přes výhody dodržování standardů společnosti nebo nových funkcí dostupných v inovovaných aplikacích. Proto může být nutné vynutit si kompatibilitu s aplikačními standardy. K určení aplikací, které nejsou kompatibilní se systémem Windows 2000, použijte techniky uvedené v kapitole „Testování kompatibility aplikací se systémem Windows 2000“ v této knize.

Jakmile je určena kompatibilita, dané aplikace lze definovat pro měření softwaru SMS a počet dostupných licencí lze nastavit na hodnotu 0. To zabráni uživatelům v používání starých verzí softwaru. Samozřejmě je zapotřebí toto pojetí doplnit efektivní komunikací a plánem školení, aby uživatelé pochopili potřebu používat výhradně schválené aplikace a aby pro ně byl přechod na nový software co nejjednodušší.

Poznámka Měření softwaru SMS může pracovat ve dvou režimech: online nebo offline. V režimu online se klienti spojují se servery při každém vyvolání nějakého programu. Tento režim je nutný pro sdílení licencí. V režimu offline klienti zaznamenávají všechna vyvolání programů, tato data však předávají serveru jen občas. Tím se výrazně snižuje zatížení sítě, klientů a serverů. V režimu offline nelze vynutit sdílení licencí, lze však znemožnit používání programů nastavením počtu dostupných licencí na hodnotu 0 a nedostupného naplánování na 24 hodin denně. Vynucení licencí nesmí být založeno na členství uživatelů ve skupinách systému Windows NT.

Další informace o distribuci softwaru včetně procesu vytvoření, distribuování, inzerování a sledování softwarového distribučního balíčku SMS najdete v kapitole „Zavádění systému Windows 2000 pomocí serveru Systems Management Server“ v této knize. Obecné pojednání o distribuci softwaru systému SMS a měření softwaru SMS najdete v knize *Systems Management Server Administrator's Guide*.

Seznam úkolů plánování analýzy sítě

Ke kontrole vykonání všech kroků potřebných pro přípravu infrastruktury sítě použijte tabulku 8.4.

Tabulka 8.4 Seznam úkolů plánování analýzy sítě

Úkol	Umístění v kapitole
Získejte inventář hardwaru.	Vyhodnocení současného stavu hardwaru
Získejte inventář softwaru.	Vyhodnocení současného stavu softwaru
Získejte data používání softwaru.	Vyhodnocení současného stavu softwaru
Vytvořte sestavy získaných dat.	Vytváření sestav získaných dat
Analyzujte získaná data.	Analyzování a použití získaných dat
Analyzujte získaná data ve spojení s databází kompatibility.	Vytváření sestav získaných dat
Sledujte síť.	Sledování sítě

Další zdroje

- Další informace o plánování a používání systému SMS najdete v knize *Microsoft Systems Management Server Administrator's Guide*, která je součástí SMS.
- Informace o produktu SMS najdete v odkazu Microsoft Systems Management Server stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>
- Informace o zápisu sestav vycházejících z dat získaných systémem SMS najdete v odkazu Microsoft Systems Management Server Technical Details stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.
- Pokročilé informace o systému SMS najdete v knize *Microsoft Systems Management Server Resource Guide* sady *Microsoft BackOffice Resource Kit 4.5*.

Infrastruktura služby Active Directory



Plánování služby Microsoft Active Directory vyžaduje znalosti mnoha funkcí systému Microsoft Windows 2000 i pochopení vzájemných souvislostí těchto funkcí. Část 3 vám poskytuje informace o vývoji plánů služby Active Directory, zabezpečení a migrace domén vhodných pro vaši organizaci.

V této části

Návrh struktury služby Active Directory 207

Určení strategií migrace domén 259

Plánování distribuovaného zabezpečení 309

Plánování infrastruktury veřejných klíčů 353

KAPITOLA 9

Návrh struktury služby Active Directory



System Windows 2000 Server obsahuje adresářovou službu nazvanou *Active Directory*. Koncepty, součásti architektury a funkce služby Active Directory uvedené v této kapitole pomohou architektovi a strategickému plánovači IT ve vaší organizaci vytvořit dokumenty návrhu velmi důležité pro úspěšné zavedení služby Active Directory systému Microsoft Windows 2000.

Ještě než začnete číst tuto kapitolu, musíte mít podrobné znalosti o skupinách správy IT, hierarchii správy a topologii sítě ve vaší organizaci. Tyto znalosti vám pomohou aplikovat pokyny plánování uvedené v této kapitole na vaše konkrétní prostředí.

V této kapitole

Přehled služby Active Directory 206

Plánování služby Active Directory 210

Vytvoření plánu doménových struktur 212

Vytvoření plánu domén 218

Vytvoření plánu organizačních jednotek 239

Vytvoření plánu topologie sídel 249

Seznam úkolů plánování návrhu struktury služby Active Directory 257

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Plán doménových struktur
- Plán domén jednotlivých doménových struktur
- Plán organizačních jednotek (Organizational Unit – OU) jednotlivých domén
- Plán topologie sídel jednotlivých doménových struktur

Související informace v sadě Resource Kit

- Další informace o migraci domén na systém Windows 2000 najdete v kapitole „Určení strategií migrace domén“ v této knize.
- Další informace o standardech zabezpečení systému Windows 2000, jako je protokol Kerberos, najdete v kapitole „Plánování distribuovaného zabezpečení“ v této knize.
- Další informace o pokročilé práci v síti najdete v kapitole „Určení strategií konektivity sítě“ v této knize.

- Další informace o funkci Microsoft IntelliMirror a zásadách skupiny najdete v kapitole „Aplikování správy změn a konfigurací“ v této knize.
- Další technické informace o službě Active Directory najdete v knize *Microsoft Windows 2000 Server Distribuované systémy*.
- Další informace o systému Domain Name System (DNS) najdete v kapitolách „Introduction to DNS“ a „Windows 2000 DNS“ v knize *Microsoft Windows 2000 Server Síť TCP/IP*.

Přehled služby Active Directory

Služba Active Directory hraje mnoho rolí, od páteře distribuovaného zabezpečení až po rámec publikování služeb. Služba Active Directory představuje pro správce centrální službu umožňující uspořádávat síťové prostředky, spravovat uživatele, počítače a aplikace a zabezpečovat intranetový a internetový síťový přístup.

Protože službu Active Directory využívá stále větší počet distribuovaných aplikací, nemusíte již implementovat a spravovat adresářové služby specifické pro jednotlivé aplikace. Výsledkem je úspora nákladů na správu a hardware.

Poznámka Systémy Microsoft Windows 2000 Server a Windows 2000 Professional můžete zavádět před službou Active Directory, současně s ní, nebo až po jejím zavedení. Není tedy nutné zavádět službu Active Directory jako první. Mnoho nových funkcí systému Windows 2000 můžete začít využívat okamžitě po inovaci členských serverů a klientských počítačů. Další informace o inovaci členských serverů najdete v kapitole „Inovace a instalace členských serverů“ v této knize.

Hlavní funkce služby Active Directory

Služba Active Directory systému Windows 2000 nabízí vaší síti mnoho výhod, mezi něž patří také tyto:

Zabezpečení

Služba Active Directory dodává infrastruktuře různé nové možnosti zabezpečení. Prostřednictvím vzájemného ověřování si mohou nyní klienti ověřit identitu serveru, ještě než mu odešlou citlivá data. S využitím podpory zabezpečení veřejnými klíči se mohou uživatelé přihlašovat pomocí karet Smart Card a nikoli hesly.

Zjednodušená a flexibilní správa

Přístup k objektům ve službě Directory lze řídit podle jednotlivých atributů, což umožňuje velmi podrobné delegování správy. Delegování správy vám dovoluje výhodněji distribuovat zodpovědnosti správy ve vaší organizaci a omezit tak počet uživatelů, kteří musí disponovat řízením na úrovni domény.

Škálovatelnost

Služba Active Directory používá jako mechanismus lokátoru systém *Domain Name System* (DNS). DNS je hierarchický, distribuovaný, vysoce škálovatelný obor názvů používaný na Internetu k překladu názvů počítačů a služeb na adresy protokolu Transmission Control Protocol/Internet Protocol (TCP/IP).

Adresář ukládá informace prostřednictvím *domén*, což jsou oddíly umožňující vám distribuovat daný adresář v rozsáhlé síti s různými rychlostmi a spolehlivostí. Adresář po-

užívá databázovou technologii, která může (jak bylo potvrzeno testy) obsahovat miliony objektů (uživatelů, skupin, počítačů, sdílených složek souborů, tiskáren a dalších). Tato kombinace škálovatelného lokátoru, rozdělení do oddílů a škálovatelného úložiště zajišťuje možnost pohodlného rozšiřování adresáře podle růstu vaší organizace.

Vysoká dostupnost

Tradiční adresáře replikace s jediným hlavním počítačem nabízejí vysokou dostupnost operacím dotazů, nikoli však operacím aktualizace. Pomocí replikace s více hlavními počítači poskytuje služba Active Directory vysokou dostupnost jak pro operace dotazů tak aktualizace.

Rozšiřitelnost

Schéma, které obsahuje definici každé třídy objektů existující v adresářové službě, je rozšiřitelné. To umožňuje jak správcům tak i vývojářům softwaru přizpůsobit si adresář svým potřebám.

Podpora otevřených standardů

Služba Active Directory je postavena na standardních protokolech, jako jsou:

- DNS pro vyhledávání serverů provozujících službu Active Directory,
- protokol *Lightweight Directory Access Protocol* (LDAP) jako protokol dotazů a aktualizací,
- protokol Kerberos pro přihlašování a ověřování.

Tato podpora otevřených standardů umožňuje používat ve spojení se službou Active Directory velké množství softwaru, jako jsou klienti adresářů využívající protokol LDAP.

Jednoduchý programový přístup

Rozhraní Active Directory Service Interfaces (ADSI) jsou přístupná z různých programovacích platform včetně skriptových jazyků, jako je například Visual Basic Script. Použitím ADSI mohou správci a vývojáři softwaru rychle vyvíjet mocné aplikace podporující adresáře. Příkladem aplikace využívající adresář je aplikace, která čte z adresáře nějaká data nebo konfigurační informace.

Zajištění základů nových technologií

Kromě výše popsaných základních výhod hraje služba Active Directory také důležitou roli v zavádění systému Windows 2000, protože poskytuje infrastrukturu dalším novým technologiím a schopnostem, mezi které patří:

Funkce IntelliMirror

Systém Windows 2000 nabízí mnoho technologií správy změn a konfigurací. Funkce IntelliMirror a správy vzdálené instalace operačního systému (Remote Operating System Installation Management) vám mohou pomoci omezit množství práce a náklady související se správou a technickou podporou klientů. Další informace o implementování těchto technologií najdete v kapitolách „Aplikování správy změn a konfigurací“ a „Definování standardů správy a konfigurace klientů“ v této knize.

Konsolidace adresářů

Škálovatelnost a rozšiřitelnost činí ze služby Active Directory ideální bod konsolidace aplikací na vaší síti, které používají oddělené, interní adresáře. Můžete například:

- Zajistit úplnou konsolidaci adresářů, kdy produkty jako Microsoft Exchange Server sdílejí součásti adresáře a při správě a provozu se spoléhají výhradně na službu Active Directory.
- Zajistit konsolidaci správy, kdy spravujete adresářové informace ve službě Active Directory a pomocí synchronizování adresářů zaručujete aktualizaci vzdálených adresářů.
- Konsolidovat existující domény systému Microsoft Windows NT, což může snížit celkový počet objektů a množství hardwaru, které je zapotřebí na síti spravovat.

Pokročilá práce v síti

Příklady pokročilých funkcí práce v síti podporovaných službou Active Directory jsou protokol Internet Protocol Security (IPSec), síťové funkce služby Quality of Service a nové možnosti vzdáleného přístupu.

Plánování služby Active Directory

Při plánování a zavádění služby Active Directory na úrovni celého podniku definujete významnou část infrastruktury sítě vaší organizace. V tomto plánu vytváříte sadu struktury, které nejlépe odrážejí vaši organizaci. Vytvořené struktury určí:

- Dostupnost adresáře a jeho odolnost proti chybám
- Charakteristiky používání klientů a serverů adresáře v síti
- Jak výkonně můžete spravovat obsah adresáře
- Způsob, jakým si uživatelé adresář zobrazují a pracují s ním
- Schopnost struktur vašeho adresáře vyvíjet se s vaší společností

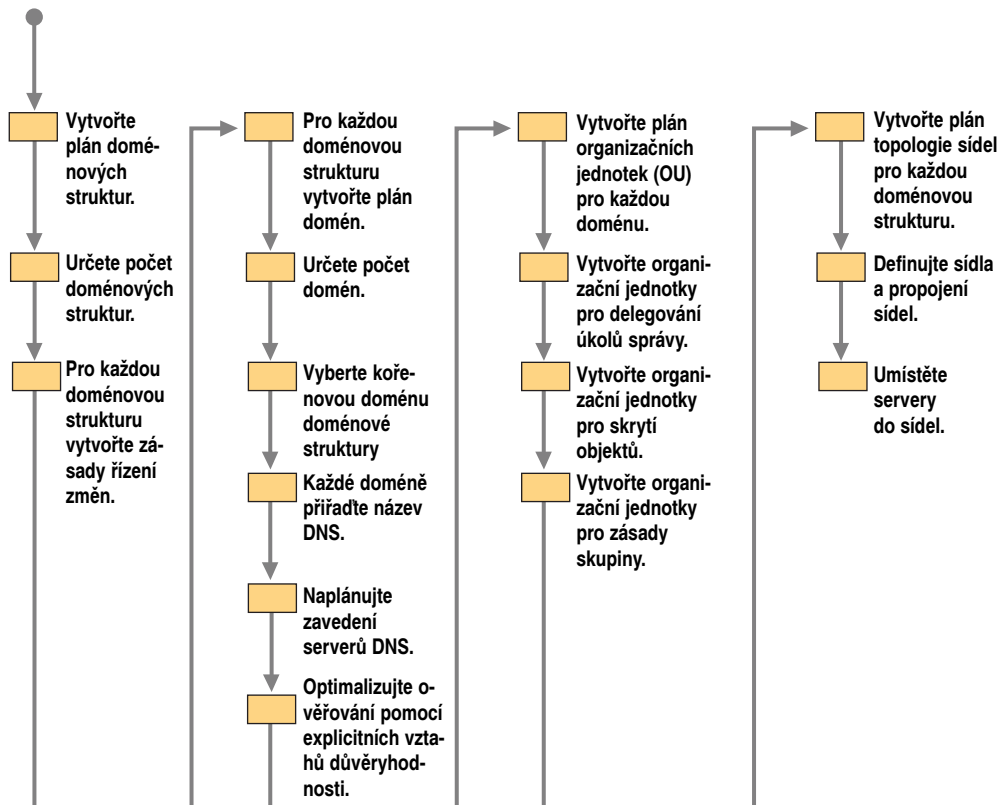
Chcete-li zajistit zavádění výhodné z hlediska nákladů, musíte si plán služby Active Directory velmi dobře promyslet. Jestliže ve fázi plánování investujete dostatečné množství času, pomůže vám to vyhnout se časovým ztrátám i dodatečným nákladům vyplývajícím z nutnosti přepracovat již zavedené struktury.

Při vytváření plánů struktury adresářů postupujte podle kroků plánování uvedených v této kapitole. Během vytváření plánů:

- se seznámte s klíčovými koncepty služby Active Directory, které ovlivňují plánování struktur, a podle potřeby upravte navrhované kroky plánování tak, aby nejlépe vyhovovaly vaší organizaci,
- identifikujte ve své organizaci osoby, které by se měly účastnit plánování struktur,
- snažte se zjistit, jak může být zapotřebí změnit či vyvinout existující obchodní či výrobní postupy, aby bylo možné využít všechny výhody služby Active Directory,
- seznámte se s možnostmi flexibility vytvářených struktur a uvědomte si, které z vašich voleb bude možné později snadno změnit a u kterých to bude obtížné.

Obrázek 9.1 ilustruje základní kroky návrhu struktury služby Active Directory. Tato kapitola podrobně zkoumá všechny uvedené kroky.

Začátek



Obrázek 9.1 Proces návrhu struktury Active Directory

Obecné principy návrhu

Při práci na plánu služby Active Directory použijte následující principy návrhu, které vám pomohou v procesu rozhodování:

Jednoduchost je nejlepší investice.

Jednoduché struktury se snáze vysvětlují, snáze se udržují a snáze se v nich vyhledávají a odstraňují problémy. Zavedením určité složitosti sice můžete získat nějakou hodnotu, tu však musíte porovnávat s možnými budoucími náklady na údržbu. Například maximální optimalizace provozu dotazů a replikací může vyžadovat vytvoření složité topologie sídel. Složitá topologie sídel se však spravuje obtížněji než jednoduchá topologie. Před zavedením složité struktury vždy vyhodnoťte poměr mezi dodatečnými schopnostmi a zvýšenou složitostí.

Vše, co vytvoříte, bude během své existence vyžadovat určitou údržbu. Vytvoříte-li nějakou strukturu, aniž byste pro ni měli dobře definované důvody, bude vás to časem stát více než jakákoli hodnota, kterou tato struktura mohla představovat. Musíte proto důkladně ospravedlnit existenci všech struktur, které vytváříte.

Vaše obchodní či výrobní činnost a vaše organizace se budou vždy měnit.

Vaši strukturu služby Active Directory budou ovlivňovat obvyklé změny, k nimž dochází v každé organizaci, od přesunů zaměstnanců až po reorganizace na úrovni podniků či nákup jiných podniků. Při návrhu vaší struktury se zamyslete nad tím, jak tyto možné změny ovlivní interakci koncových uživatelů a správců s adresářem. Zvažte například dopad, jaký by měla poslední velká reorganizace podniku na vámi navržené struktury. Jaké změny budou zapotřebí, když přidáte novou lokaci nebo kancelář pobočky? Vyžadovaly by tyto změny významné a nákladné úpravy struktury služby Active Directory? Vytvořte takový návrh, který je dostatečně obecný a dostatečně flexibilní, aby se dokázal vyrovnat s neustálými i významnými změnami.

Vaším cílem musí být ideální návrh.

Během prvního vytváření návrhu navrhnete takovou strukturu, kterou považujete za ideální, i když zatím neodráží vaši současnou infrastrukturu domén či adresářů. Je užitečné a praktické ujasnit si, jaký stav by byl ideální, i když zatím není dosažitelný. Další informace o nákladech souvisejících s migrací sítě na ideální plán najdete v kapitole „Určení strategií migrace domén“ v této knize. Tyto náklady porovnejte s dlouhodobými úsporami zajištěnými zavedením ideálního plánu a návrh podle získaných údajů upravte.

Prozkoumejte alternativní návrhy.

Každému návrhu se věnujte několikrát. Hodnota určitého návrhu je zřejmější, když jej porovnáte s dalšími návrhy. Do plánu, který budete implementovat, zkombinujte to nejlepší z jednotlivých plánů.

Složení plánu struktury služby Active Directory

Existují čtyři základní součásti, které společně vytvářejí strukturu služby Active Directory: doménové struktury, domény, organizační jednotky (útvary) a sídla (sítě). Cílem plánu struktury služby Active Directory je vytvořit dokument plánování pro jednotlivé součásti struktury, přičemž se budou činit důležitá rozhodnutí a zdůvodnění. Tyto dokumenty plánování pak slouží jako počáteční bod vašeho dalšího úkolu plánování, migrace. Čtyřmi dokumenty, které dohromady tvoří plán struktury Active Directory, jsou:

- Plán doménových struktur
- Plán domén pro každou doménovou strukturu
- Plán organizačních jednotek (Organizational Unit – OU) pro každou doménu
- Plán topologie sídel pro každou doménovou strukturu

Vytvoření plánu doménových struktur

Doménová struktura je kolekce domén služby Active Directory. Doménové struktury slouží dvěma hlavním účelům: zjednodušují interakci uživatelů s adresářem a zjednodušují správu více domén. Doménové struktury mají následující klíčové charakteristiky:

Jediné schéma

Schéma služby Active Directory definuje *třídy objektů* a atributy tříd objektů, které lze v adresáři vytvořit. Třídy objektů definují typy objektů, které lze vytvořit v adresáři. Toto schéma existuje jako kontext vytváření názvů, který se replikuje na každý řadič do-

mény v doménové struktuře. Skupina se zabezpečením správců schéma má k dispozici plné řízení schéma.

Jediný kontejner konfigurace

Kontejner konfigurace služby Active Directory je kontext vytváření názvů, který se replikuje na každý řadič domény v doménové struktuře. Aplikace podporující adresáře ukládají do kontejneru konfigurace informace, které platí pro celou doménovou strukturu. Například služba Active Directory ukládá do kontejneru konfigurace informace o fyzické síti a používá je k vytvoření replikačních spojení mezi řadiči domén. Skupina se zabezpečením správců podniku má k dispozici plné řízení kontejneru konfigurace.

Sdílení jediné, konzistentní konfigurace ve všech doménách doménové struktury eliminuje potřebu konfigurovat domény samostatně.

Úplná důvěryhodnost

Služba Active Directory automaticky vytváří mezi doménami v doménové struktuře přenosné (tranzitivní), obousměrné vztahy důvěryhodnosti. Uživatelé a skupiny z libovolné domény může rozpoznat jakýkoli členský počítač v doménové struktuře a lze je také vkládat do skupin nebo na seznamy řízení přístupu (Access Control List – ACL).

Úplná důvěryhodnost zjednodušuje v systému Windows 2000 správu více domén. V předchozích verzích systému Windows NT se nejčastěji k zavádění domén používal model domény s více hlavními počítači. V tomto modelu se doména obsahující především účty uživatelů označovala za hlavní doménu uživatelských účtů a doména obsahující především účty počítačů a prostředků se označovala za doménu prostředků. V obvyklém zavedení se vyskytoval menší počet hlavních domén účtů, každé z nichž důvěřoval velký počet domén prostředků. Přidání nové domény do zavedené implementace vyžadovalo vytvoření několika vztahů důvěryhodnosti. Když přidáte nějakou doménu do doménové struktury pomocí služby Active Directory systému Windows 2000, automaticky se nakonfiguruje na obousměrnou přenosnou důvěryhodnost. Tím se odstraňuje potřeba vytvářet další vztahy důvěryhodnosti mezi doménami v jedné doménové struktuře.

Jediný globální katalog

Globální katalog obsahuje kopie všech objektů ze všech domén v doménové struktuře, avšak jen vybranou sadu atributů jednotlivých objektů. Globální katalog umožňuje rychlé a výkonné vyhledávání v rámci celé doménové struktury.

Globální katalog činí adresářové struktury v doménové struktuře pro koncové uživatele transparentní. Hledání objektů v adresáři na úrovni globálního katalogu je velmi jednoduché. Přihlašování je zjednodušeno pomocí globálního katalogu a hlavních uživatelských jmen, jak je popsáno dále:

Uživatelé prohledávají globální katalog

V uživatelském rozhraní prohledávání adresáře se po výběru hledání na úrovni **Celý adresář** (Entire Directory) pracuje s globálním adresářem. Uživatelé mohou prohledávat doménovou strukturu, aniž by měli nějaké předchozí znalosti o její struktuře. Toto jednoduché, konzistentní rozhraní vyhledávání omezuje potřebu školit uživatele v oblasti struktury adresářů a umožňuje správcům změnit strukturu v rámci doménové struktury, aniž by to mělo vliv na způsob, jakým uživatelé pracují s adresářem.

Uživatelé se přihlašují pomocí hlavních uživatelských jmen

Hlavní uživatelské jméno (User Principal Name – UPN) se podobá adrese elektronické pošty a jednoznačně představuje určitého uživatele. Jméno UPN se skládá ze dvou částí, části identifikace uživatele a doménové části. Tyto dvě části jsou odděleny symbolem „@“ a tvoří tak zápis `<uživatel>@<název-domény-DNS>`, například `jana@noam.reskit.com`. Každému uživateli se automaticky přiřadí výchozí jméno UPN, kde část `<uživatel>` je stejná jako přihlašovací jméno uživatele a část `<název-domény-DNS>` názvu je názvem systému DNS domény služby Active Directory, kde se daný uživatelský účet nachází. Při přihlašování pomocí UPN již nemusejí uživatelé vybírat doménu ze seznamu v dialogovém okně přihlášení.

Jména UPN můžete nastavit na libovolné hodnoty. I když se třeba účet Jany nachází v doméně `noam.reskit.com`, její jméno UPN lze nastavit na hodnotu `jana@reskit.com`. Když se uživatel přihlašuje, příslušný účet s odpovídající hodnotou UPN se vyhledá v globálním katalogu. Protože jsou hodnoty UPN nezávislé na názvech domén, správci mohou přesunovat uživatelské účty mezi doménami, přičemž hodnoty UPN se nemění a přesuny v rámci domény jsou pro uživatele transparentnější.

Proces plánování doménových struktur

Hlavními kroky vytvoření plánu doménových struktur vaší organizace jsou:

- Určit počet doménových struktur ve vaší síti.
- Vytvořit zásady řízení změn doménových struktur.
- Zjistit vliv změn na plán doménových struktur po zavedení.

Při vytváření plánu doménových struktur budete muset pravděpodobně spolupracovat se:

- současnými správci domén, kteří zodpovídají za účty uživatelů, skupiny a počítače,
- týmem zabezpečení sítě.

Určení počtu doménových struktur v síti

Plánování modelu doménových struktur začněte jedinou doménovou strukturou. V mnoha situacích je jediná z doménových struktur dostačující, rozhodnete-li se však vytvořit další doménové struktury, ujistěte se, že k tomu máte dobré technické zdůvodnění.

Vytvoření prostředí s jedinou doménovou strukturou

Prostředí s jedinou doménovou strukturou se jednoduše vytváří i spravuje. Všichni uživatelé vidí přes globální katalog jediný adresář a nemusí o struktuře adresářů vůbec nic vědět. Ani při přidání nové domény do doménové struktury není zapotřebí dodatečná konfigurace vztahů důvěryhodnosti. Změny konfigurace ovlivňující všechny domény lze aplikovat jen jednou.

Vytvoření prostředí s více doménovými strukturami

Je-li správa sítě rozdělena do mnoha nezávislých oddělení, může být nezbytné vytvořit více doménových struktur.

Jelikož doménové struktury mají určité sdílené prvky, jako je například schéma, je nezbytné, aby se všichni účastníci v doménové struktuře dohodli na obsahu a správě těchto sdílených prvků. Organizace, jako jsou partnerství nebo konglomeráty, nemusí mít centrální orgán, který by mohl tento proces řídit. V krátkodobých organizacích, jako jsou joint ventures, asi nebude realistické očekávat od správců jednotlivých organizací spolupráci na správě doménové struktury.

Více doménových struktur může být zapotřebí vytvořit, pokud platí tyto podmínky:

Jednotlivé organizace vzájemně nedůvěřují svým správcům.

V globálním katalogu se nachází reprezentace každého objektu v doménové struktuře. Správce, kterému byla delegována možnost vytvářet objekty, může úmyslně nebo neúmyslně zapříčinit vznik stavu „odmítnutí služby“. Tento stav lze vytvořit rychlým vytvářením nebo odstraňováním objektů a následným velkým rozsahem replikací globálního katalogu. Rozsáhlé replikace mohou spotřebovávat značnou část šířky pásma sítě a zpomalovat servery globálního katalogu, které věnují svůj čas zpracování replikací.

Jednotlivé organizace se nemohou dohodnout na zásadách změn doménové struktury.

Změny schématu, změny konfigurace a přidání nových domén do doménové struktury mají vliv na úrovni celé doménové struktury. Všechny organizace v doménové struktuře musí souhlasit s určitým procesem implementování těchto změn a musí se shodnout na členství ve skupinách správců schéma a správců podniku. Nedokážou-li se organizace dohodnout na jednotných zásadách, nemohou sdílet jednu doménovou strukturu. Vytvoření zásad změn doménové struktury je popsáno dále v této kapitole.

Jednotlivé organizace chtějí omezit rozsah vztahů důvěryhodnosti.

Každá doména v doménové struktuře důvěřuje všem ostatním doménám v doménové struktuře. Každý uživatel může být zahrnut do nějaké skupiny nebo se může objevit na seznamu řízení přístupu na libovolném počítači v doménové struktuře. Chcete-li zabránit určitým uživatelům v získání oprávnění k některým prostředkům, pak se tito uživatelé musejí nacházet v jiné doménové struktuře, než jsou dané prostředky. Je-li to nutné, můžete takovým uživatelům zajistit přístup k prostředkům ve specifických doménách pomocí vztahů explicitní, přímo zadané důvěryhodnosti.

Nárůst nákladů na další doménové struktury

Každá vytvořená doménová struktura znamená určité pevné další náklady na správu:

- Každá další doménová struktura musí obsahovat alespoň jednu doménu. Můžete se tak dostat k většímu počtu domén, než jste původně plánovali. S vytvořením a správou domény se váží určité pevné náklady. Tyto náklady jsou podrobně specifikovány dále v této kapitole.
- Součástí na úrovni doménové struktury musíte spravovat v každé doménové struktuře samostatně (například součástí kontejneru schéma a konfigurace a členství ve skupinách správy s nimi souvisejících), i když jsou v zásadě stejné.

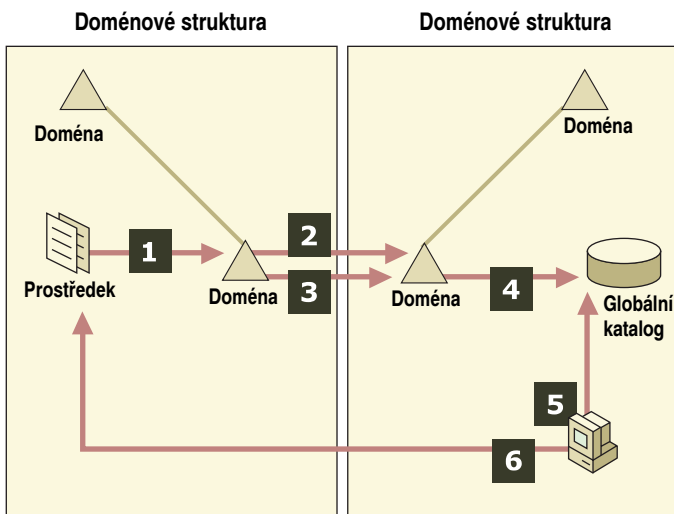
Aby mohl uživatel v jedné doménové struktuře použít nějaký prostředek v jiné doménové struktuře, musíte vykonat následující dodatečnou konfiguraci:

- Aby mohli uživatelé z jedné doménové struktury přistupovat k prostředkům v jiné doménové struktuře, musíte mezi oběma doménovými strukturami vytvořit a udržovat explicitní vztah důvěryhodnosti. Explicitní vztah důvěryhodnosti mezi doménami v různých doménových strukturách je jednosměrný a nepřenosný. Bez vytvořeného vztahu důvěryhodnosti nelze uživatelům z jedné doménové struktury zajistit přístup k objektům v jiné doménové struktuře.
- Uživatelům v jedné doménové struktuře se standardně zobrazují pouze objekty v globálním katalogu jejich doménové struktury. Chtějí-li uživatelé objevit objekty v jiné doménové struktuře, musí se explicitně dotazovat domén, které se nacházejí mimo jejich doménovou strukturu. Alternativně mohou správci importovat data z ji-

ných domén do doménové struktury, kde se daný uživatel nachází. To však může představovat další náklady, protože:

- Uživatelé je nutné proškolit v oblasti adresářové struktury, aby věděli, kam mají směřovat své dotazy, když selže globální katalog.
- Když importujete data z nějaké domény do samostatné doménové struktury, musíte ještě vytvořit nějaký proces, který bude importovaná data aktualizovat, když dojde k jejich změně ve zdrojové doméně.

Obrázek 9.2 je příkladem konfigurace spojení mezi doménovými strukturami, kde uživatel v jedné doménové struktuře potřebuje přistupovat k prostředku publikovanému v jiné doménové struktuře. Byl vytvořen explicitní, jednosměrný vztah důvěryhodnosti, aby bylo možné zajistit uživateli přístup k danému prostředku. Reprezentace tohoto prostředku v adresáři se importuje do doménové struktury uživatele, kde se objevuje v globálním katalogu.



1. Prostředek je publikován v adresářové službě.
2. Správce nakonfiguruje explicitní jednosměrný vztah důvěryhodnosti.
3. Správce importuje daný objekt do doménové struktury.
4. Objekt se replikuje do globálního katalogu.
5. Uživatel objekt najde dotazováním globálního katalogu.
6. Uživatel k prostředku přistupuje.

Obrázek 9.2 Dodatečná konfigurace pro zajištění přístupu k prostředkům mezi doménovými strukturami

Některé funkce dostupné v rámci doménové struktury nejsou dostupné mezi doménovými strukturami. Patří sem tyto situace:

- Nachází-li se účet uživatele v jiné doménové struktuře než počítač používaný pro přihlašování, lze používat pouze výchozí jména UPN. To je nutné, protože řadič domény v doménové struktuře počítače nenajde v globálním katalogu žádný účet uživatele s odpovídajícím jménem UPN. Účet uživatele se totiž nachází v globálním katalogu jiné doménové struktury. Řadič domény zpracovávající přihlášení musí k vy-

hledání jiného řadiče domény, který dokáže ověřit identitu uživatele, použít část <název-domény-DNS> jména UPN.

- Přihlašování pomocí karet Smart Card se spoléhá na hlavní uživatelské jméno. Aby proces přihlašování probíhající mezi doménovými strukturami využívající karty Smart Card fungoval, musí být použita výchozí jména UPN.
- Komitenty zabezpečení můžete přesunovat mezi doménami jedné doménové struktury, při přesunu mezi doménami v různých doménových strukturách je však zapotřebí je klonovat. Klonování není pro koncové uživatele tak transparentní jako přesun mezi doménami. Další informace o klonování najdete v kapitole „Určení strategií migrace domén“ v této knize.

Při určování počtu doménových struktur, které budete potřebovat, pamatujte, že věci užitečné pro uživatele nemusí být zároveň záležitostmi důležitými pro správce. Uživatelé však ve scénáři více doménových struktur ztrácejí nejvíce. Některé organizace například předávají zodpovědnost za správu své sítě několika různým externím nezávislým kontraktorům. Kontraktori jsou obvykle placeni za výkon sítě a jejich prvořadou odpovědností je zajistit stabilitu sítě. Určitý kontraktor asi nebude chtít, aby jiný kontraktor mohl ovlivňovat jím řízené počítače – tento problém vyřeší zavedení samostatných doménových struktur. Oddělené doménové struktury však mohou být nevýhodné pro uživatele, kteří tak již nemají k dispozici jediné, konzistentní zobrazení adresáře. V takových situacích se pokuste nevytvářet samostatné doménové struktury jen kvůli řešení hranic problému správy.

V případech, kdy není důležité, aby měli všichni uživatelé k dispozici konzistentní zobrazení adresáře, může být zavedení více doménových struktur vhodné. Představme si například společnost poskytovatele připojení k Internetu (ISP), který hostí služby Active Directory několika společností. Uživatelé v různých klientských společnostech nemají žádný důvod sdílet nějaké konzistentní zobrazení adresáře. Navíc neexistuje žádný důvod vytvářet mezi společnostmi přenosné vztahy důvěryhodnosti. V takovém případě je vytvoření samostatných doménových struktur užitečné a vhodné.

Vytvoření zásad řízení změn doménové struktury

Každá doménová struktura, kterou vytvoříte, musí mít v plánu doménových struktur určené zásady řízení změn doménové struktury. Tyto zásady vás budou provádět změnami s dopady na celou doménovou strukturu. Než budete pokračovat, nemusíte sice určit jednotlivé postupy, musíte však porozumět jejich vlastnictví. Zásady musí obsahovat informace o každém ze sdílených prvků v doménové struktuře.

Zásady změny schématu

Skupina správců schématu má k dispozici úplné řízení schéma doménové struktury. Zásady změny schéma musí zahrnovat:

- Název týmu ve vaší organizaci, který řídí skupinu správců schématu.
- Počáteční členství ve skupině správců schématu.
- Pokyny a postup požadování a vyhodnocení změn schématu.

Další informace o schématu služby Active Directory najdete v knize *Microsoft Windows 2000 Server Distribuované systémy*.

Zásady změny konfigurace

Skupina správců podniku má k dispozici úplné řízení kontejneru konfigurace, který se replikuje v celé doménové struktuře. Zásady změny konfigurace musí zahrnovat:

- Název týmu ve vaší organizaci, který řídí skupinu správců podniku.
- Počáteční členství ve skupině správců podniku.
- Pokyny a postup vytváření nových domén v doménové struktuře.
- Pokyny a proces úpravy topologie sídel doménové struktury. (Topologie sídel je popsána v oddílu „Vytvoření plánu topologie sídel“ dále v této kapitole.)

Změna plánu doménových struktur po zavedení

Jakmile je vytvořena nějaká doména, lze ji připojit k existující doménové struktuře. Doménu vytvoříte tak, že nějaký server se systémem Windows 2000 povýšíte do role řadiče domény služby Active Directory, nebo že inovujete primární řadič domény se systémem Microsoft Windows NT verze 3.51 či Microsoft Windows NT verze 4.0 na systém Windows 2000.



Důležité rozhodnutí Dvě doménové struktury nelze sloučit v jediném kroku. Jediným krokem nelze ani přesunout nějakou doménu mezi doménovými strukturami. Je důležité navrhnout plán doménových struktur tak, aby během vývoje vaší organizace vyžadoval minimální restrukturalizace.

Jednotlivé objekty lze mezi doménovými strukturami přesunovat. Typ přesunovaného objektu určuje konkrétní nástroj, který k jeho přesunutí použijete. Většinu dávkových importů a exportů lze vykonat nástrojem příkazového řádku LDAP Data Interchange Format (LDIFDE.EXE). Komitenty zabezpečení lze klonovat nástrojem ClonePrincipal. Další informace o těchto nástrojích najdete v oblasti Tools Help na doprovodném CD sady *Windows 2000 Resource Kit*.

Vytvoření plánu domén

Dále jsou uvedeny určité klíčové charakteristiky domén systému Windows 2000, které budete muset zvážit na začátku vytváření plánu struktury domén.

Rozdělení doménové struktury

Doménová struktura služby Active Directory je distribuovaná databáze, jejíž jednotlivé části jsou definované doménami. *Distribuovaná databáze* je taková databáze, která se skládá z mnoha částečných databází nacházejících se na mnoha počítačích; nejedná se tedy o jedinou databázi na jediném počítači. Rozdělení databáze na menší části a jejich umístění na nejvhodnější místa umožňuje výhodně distribuovat rozsáhlou databázi na velké síti.

Obsluha serverů řadičů domén

Stejně jako v systému Windows NT 4.0 se servery systému Windows 2000, které hostí databázi domény, označují za řadiče domény. *Řadič domény* může hostit právě jednu doménu. Můžete zadávat změny objektů v určité doméně na libovolném řadiči dané domény. Všechny řadiče domén v určité doménové struktuře také hostí kopii kontejnerů konfigurace a schéma doménové struktury.

Ověřovací jednotka

Každá databáze domény obsahuje objekty komitentů zabezpečení, jako jsou uživatelé, skupiny a počítače. Objekty komitentů zabezpečení jsou zvláštní v tom, že jim lze povolit nebo odpírat přístup k prostředkům na síti. Objekty komitentů zabezpečení musí být ověřeny řadičem domény, v níž jsou dané objekty komitentů zabezpečení umístěny. Ověření slouží k potvrzení identity objektů ještě před jejich přístupem k nějakému prostředku.

Hranice správy a zásad skupiny

Každá doména má skupinu správců domény. Správci domény mají k dispozici plnou kontrolu nad všemi objekty v doméně. Tato oprávnění správy jsou platná pouze v dané doméně a nešíří se do jiných domén.

Zásady skupiny svázané s jednou doménou se také automaticky nešíří do dalších domén v doménové struktuře. Aby se zásady skupiny jedné domény přiřadily také jiné doméně, musí být tyto domény explicitně propojeny.

Zásady zabezpečení pro jedinečné uživatelské účty domény

Některé zásady zabezpečení platící pro uživatelské účty domény lze zadat pouze na úrovni jednotlivých domén:

- Zásady hesel. Určují pravidla, která musí být splněna, jako je délka hesel, když uživatel zadává nové heslo.
- Zásady uzamčení účtů. Definují pravidla detekování narušitelů a deaktivace účtů.
- Zásady lístků protokolu Kerberos. Určují životnost lístku protokolu Kerberos. Lístek protokolu Kerberos se získá během procesu přihlašování a používá se k síťovému ověření. Konkrétní lístek je platný pouze po dobu zadanou těmito zásadami. Dojde-li k vypršení platnosti lístku, systém se automaticky pokusí obdržet nový lístek.

Další informace o zásadách zabezpečení pro uživatelské účty domény najdete v kapitole „Ověřování“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.

Názvy domén systému DNS

Doména je určena názvem DNS. Systém DNS se používá k vyhledání serverů řadičů dané domény. Názvy DNS jsou hierarchické a název DNS domény služby Active Directory indikuje její umístění v hierarchii doménové struktury. Příkladem názvu domény může být reskit.com. Doména nazvaná eu.reskit.com může být v hierarchii doménové struktury podřízenou doménou domény reskit.com.

Proces plánování domén

Váš plán domén určí dostupnost adresáře na síti, charakteristiky provozu dotazů klientů a charakteristiky provozu replikací řadičů domén.

Každá doménová struktura, kterou vytvoříte, bude obsahovat jednu nebo více domén. Kroky vytvoření plánu domén vypadají takto:

- Určíte počet domén v jednotlivých doménových strukturách.
- Vyberte kořenovou doménu doménové struktury.
- Každé doméně přiřadíte název DNS, čímž vytvoříte hierarchii domén.
- Naplánujete zavádění serverů DNS.
- Optimalizujete ověřování pomocí explicitních vztahů důvěryhodnosti.
- Snažte se porozumět vlivu změn na plán domén po jeho zavedení.

Při vytváření plánu domén pro jednotlivé doménové struktury budete muset pravděpodobně spolupracovat se:

- současnými správci domén, kteří zodpovídají za účty uživatelů, skupiny a počítače,
- týmy, které řídí a sledují vaši fyzickou síť,
- týmy, které řídí službu DNS na vaší síti,
- týmy zabezpečení.

Určení počtu domén v jednotlivých doménových strukturách

Při určování počtu domén v jednotlivých doménových strukturách začněte zvážením možnosti vytvořit jedinou doménu, i když máte v současné době více domén systému Windows NT 4.0. Pak zajistěte podrobné zdůvodnění vzniku všech dalších domén. Každá vytvořená doména bude znamenat částečné zvýšení nákladů na dodatečnou správu. Proto vždy zajistěte, aby domény přidávané do doménové struktury sloužily nějakému užitečnému cíli.

Jak se změnilo vytváření domén

Některé z faktorů, které vedly k vytváření prostředí s více doménami v předchozích verzích systému Windows NT Server, již pro službu Active Directory a systém Windows 2000 neplatí. Tyto faktory následují:

Omezení velikosti Správce zabezpečení účtů (Security Accounts Manager – SAM)

V předchozích verzích systému Microsoft Windows NT Server byla z praktických důvodů velikost databáze SAM omezena na asi 40 000 objektů v doméně. Služba Active Directory může snadno pojmout miliony objektů v doméně. Proto by již nikdy nemělo být zapotřebí vytvářet nové domény jen kvůli možnosti zpracování většího počtu objektů.

Požadavky dostupnosti primárního řadiče domény (Primary Domain Controller – PDC)

V předchozích verzích systému Windows NT Server mohl přijímat aktualizace databáze domény jen jediný řadič domény, PDC. V organizacích s velkými sítěmi toto omezení znesnadňovalo zajištění vysoké dostupnosti řadiče PDC, protože výpadek sítě mohl zabránit správcům v jedné části sítě v aktualizaci domény. V zájmu naplnění požadavku dostupnosti jste tedy vytvářeli další domény, aby bylo možné servery PDC distribuovat v celé síti. To již v systému Windows 2000 není zapotřebí, protože aktualizace mohou nyní přijímat všechny řadiče domén služby Active Directory.

Omezené delegování správy v doméně

V předchozích verzích systému Windows NT Server jste delegovali správu pomocí zabudovaných místních skupin, jako byla skupina Account Operators, nebo vytvořením více domén a přesných sad správců domén. Například abyste mohli delegovat správu nějaké množiny uživatelů, vytvořili jste novou doménu uživatelů. Pro delegování správy serverů prostředků, jako jsou tiskové a souborové servery, jste vytvořili doménu prostředků. V systému Windows 2000 je možné delegovat správu v doméně pomocí *organizačních útvarů* (OU). OU je kontejner, který se používá k uspořádání objektů v doméně do logických podskupin správy. Útvary (jednotky) OU se snáze vytvářejí, odstraňují, přesunují a upravují než domény a lépe slouží roli delegování.

Další informace o použití jednotek OU k delegování správy najdete v oddílu „Vytvoření plánu organizačních jednotek“ dále v této kapitole.

Kdy vytvořit více domén

Existují tři možné důvody vytvoření dalších domén:

- Zachování existujících domén systému Windows NT
- Rozdělení správy
- Fyzické rozdělení

Zachování existujících domén systému Windows NT

Máte-li již vytvořeny domény systému Windows NT, můžete upřednostňovat jejich zachování a nikoli konsolidaci do menšího počtu domén Active Directory. Ať už se rozhodnete nějakou doménu zachovat nebo konsolidovat, vždy musíte porovnat příslušné náklady s dlouhodobými výhodami používání menšího počtu domén. Náklady spojené s konsolidací domén jsou popsány v kapitole „Určení strategií migrace domén“ v této knize. Pokud navrhuje domény poprvé, doporučujeme vám snažit se dosáhnout co nejnižšího počtu domén a tento plán znovu vyhodnotit po přečtení uvedené kapitoly.

Rozdělení správy

V závislosti na dále popsaných požadavcích ohledně správy a zásad vaší organizace může být zapotřebí použít další domény.

Požadavky na zvláštní zásady zabezpečení uživatelů domény

Můžete požadovat, aby na vaší síti existovali určití uživatelé, řízení zásadami zabezpečení uživatelů domény, které se liší od zásad zabezpečení aplikovaných na zbývající část uživatelů. Můžete například vyžadovat, aby pro vaše správce platily přísnější zásady hesel, jako je například kratší doba obměny hesel, než pro obvyčejné uživatele sítě. Chcete-li toho dosáhnout, musíte dané uživatele umístit do samostatné domény.

Oddělení organizace vyžaduje autonomní správu domén

Členové skupiny správců domény v určité doméně mají plnou kontrolu nad všemi objekty v dané doméně. Máte-li ve své organizaci oddělení, které nechce umožnit řízení svých objektů vnějším správcům, dané objekty musíte umístit do samostatné domény. Například z právních důvodů nebude neobvyklé, když bude oddělení organizace pracující s vysoce citlivými projekty odmítat řízení své domény skupinou IT na vyšší úrovni. Pamatujte si, že všechny domény v doménové struktuře musejí sdílet kontejnery konfigurace a schéma.

Fyzické rozdělení

Fyzické rozdělení zahrnuje převzetí domén v doménové struktuře a jejich rozdělení na větší počet menších domén. Budete-li mít větší počet menších domén, umožní vám to optimalizovat replikační provoz – stačí zadat pouze replikace objektů na taková místa, která jim nejvíce přísluší. Například v doménové struktuře obsahující jedinou doménu se každý objekt v doménové struktuře replikuje na všechny řadiče domény v doménové struktuře. To může vést k replikaci objektů na místa, kde se používají jen zřídka, což znamená nevýhodné využívání šířky pásma. Například uživatel, který se vždy přihlašuje v místě ústředí, nemusí mít svůj uživatelský účet replikovaný na pobočkách. Replikačnímu provozu se lze vyhnout vytvořením samostatné domény pro ústředí a ne-replikováním této domény do poboček.

Poznámka Jestliže jste již zavedli domény systému Windows NT 4.0, možná jste se svým fyzickým rozdělením spokojeni. Když se však na toto rozdělení podíváte znovu s „čistou hlavou“, můžete objevit oblasti možné konsolidace domén. Pokud jste se již rozhodli inovovat své domény systému Windows NT 4.0 tak, jak jsou a nevykonávat žádnou konsolidaci, můžete přeskočit pojednání o rozdělování.

Chcete-li určit zda a jak se bude doménová struktura dělit, musíte:

- nakreslit topologii sítě,
- umístit do sítě řadiče domén podle požadavků dostupnosti,
- rozdělit doménovou strukturu na základě replikačního provozu mezi řadiči domén.

Nakreslení topologie sítě

Začněte nakreslením diagramu základní topologie sítě. Později v procesu plánování budete na tento diagram přidávat další podrobnosti, jakmile bude plánovat topologii sídel. Chcete-li vytvořit diagram topologie, postupujte takto:

- Nakreslete kolekce sídel.

Síťové sídlo je síť s rychlou a spolehlivou konektivitou. Za síťové sídlo lze považovat místní síť (Local Area Network – LAN) nebo sadu sítí LAN propojených vysokorychlostním páteřním spojením. Do svého síťového diagramu zakreslete všechna sídla a zaznamenejte přibližný počet jejich uživatelů.

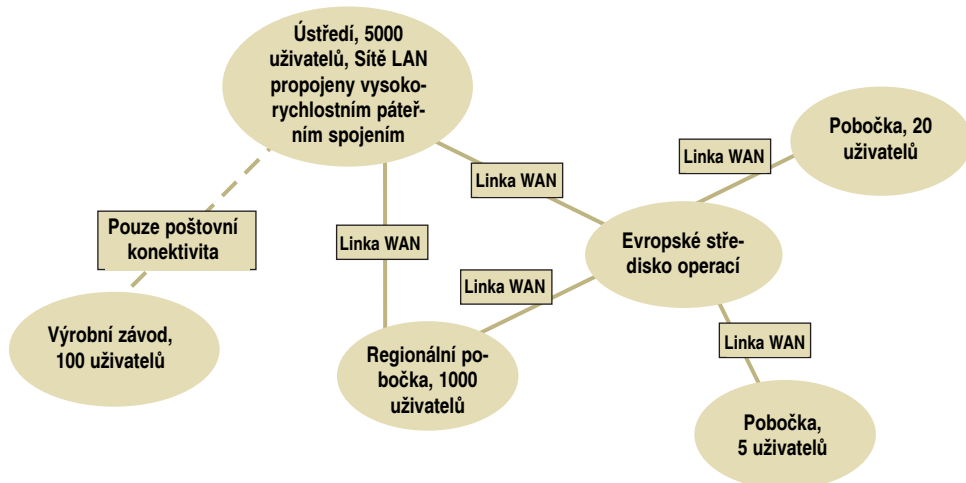
- Propojte sídla linkami.

Spojení sítí (linka či spojení mezi sídly) je pomalé nebo nespolehlivé spojení propojující dvě sídla. Příkladem spojení sítí je rozlehlá síť (Wide Area Network – WAN) propojující dvě rychlé sítě. Doporučujeme vám považovat všechny linky pomalejší než rychlost sítě LAN za pomalé linky. V diagramu topologie vyznačte, jak jsou sídla vzájemně propojena spojením sítí.

U každé linky mezi sídly poznamenejte:

- Rychlost linky a současné úrovně využívání
 - Zda je linka placena podle používání
 - Zda je ze zkušeností patrné, že je linka nespolehlivá
- Vyznačte sídla pouze s konektivitou SMTP.
- Máte-li sídlo bez fyzického připojení ke zbytku sítě, které je však dosažitelné pomocí protokolu elektronické pošty Simple Mail Transfer Protocol (SMTP), označte dané sídlo v tom smyslu, že má pouze poštovní konektivitu.

Obrázek 9.3 ukazuje topologii sítě fiktivní společnosti Reskit.



Obrázek 9.3 Topologie sítě společnosti Reskit

Umístěte řadiče domén

Dostupnost služby Active Directory je určena dostupností řadičů domén. Řadiče domén musí být dostupné, aby bylo možné ověřovat uživatele. V tomto kroku určíte, kam musíte umístit řadiče domén, abyste dosáhli dostupnosti i v případě možných výpadků sítě.

K umístění řadičů domén použijte následující postup:

- Vyberte „domovské“ sídlo a označením v diagramu topologie do tohoto sídla umístěte řadič domény.

Domovské sídlo můžete vybrat libovolně. Použijte třeba ústředí společnosti, sídlo s nejvyšším počtem uživatelů nebo sídlo s nejlepší celkovou konektivitou ke zbytku sítě. Všichni uživatelé v domovském sídle budou ověřováni tímto řadičem domény. Zatím ignorujte otázky, jakou doménu daný řadič domény vlastně obsluhuje a kolik replik dané domény bude v sídle zapotřebí.

- U každého sídla přímo připojeného k domovskému sídlo určete, zda do něj musíte umístit řadič domény.

Nebo namísto vložení řadiče domény do daného sídla určete, zda lze uživatele v tomto sídle ověřovat přes spojení sítí řadičem domény v domovském sídle. Je-li pro vás přijatelné, aby ověřování selhalo v případě výpadku tohoto propojení sítí, pak do uvažovaného sídla nemusíte umísťovat řadič domény.

U malých poboček, které mají klientské počítače nikoli však servery, není řadič domény zapotřebí. Pokud selže spojení k centrálnímu sídlu, uživatelé v pobočce se stále budou moci přihlásit ke svým počítačům pomocí identifikačních informací uložených v mezipaměti. Další ověřování je zbytečné, protože v pobočce neexistují žádné serverové prostředky, ke kterým by bylo možné přistupovat – všechny takové prostředky jsou na centrálním sídle.

Řadič domény byste měli do sídla umístit, pokud:

- V sídle je velký počet uživatelů a propojení sítí je pomalé nebo na maximu své kapacity. V takovém případě nechcete, aby klientský provoz služby Active Directory zabíral kapacitu spojení. Další informace o plánování kapacity sítě a provozu vytvářeném klientem služby Active Directory najdete v odkazu Microsoft Windows 2000 Server stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.
 - Máte zkušenosti s nespolehlivostí linky. Nechcete, aby selhalo ověřování, pokud vypadne toto spojení sítí.
 - Linka je občas nedostupná. Nechcete, aby v určitých denních hodinách selhalo ověřování, ani se nechcete spoléhat na linku vytáčenou na požádání.
 - Sídlo je dostupné pouze prostřednictvím pošty SMTP. Je-li sídlo dostupné pouze prostřednictvím pošty SMTP, uživatelé musí mít zajištěno ověřování místním řadičem domény.
 - Předchozí proces zopakujte a určete, kam je zapotřebí umístit řadiče domén.
- Stejný postup aplikujte postupně u sousedních sídel, dokud nenavštívíte každé sídlo a neurčíte, zda je v něm potřebný místní řadič domény.

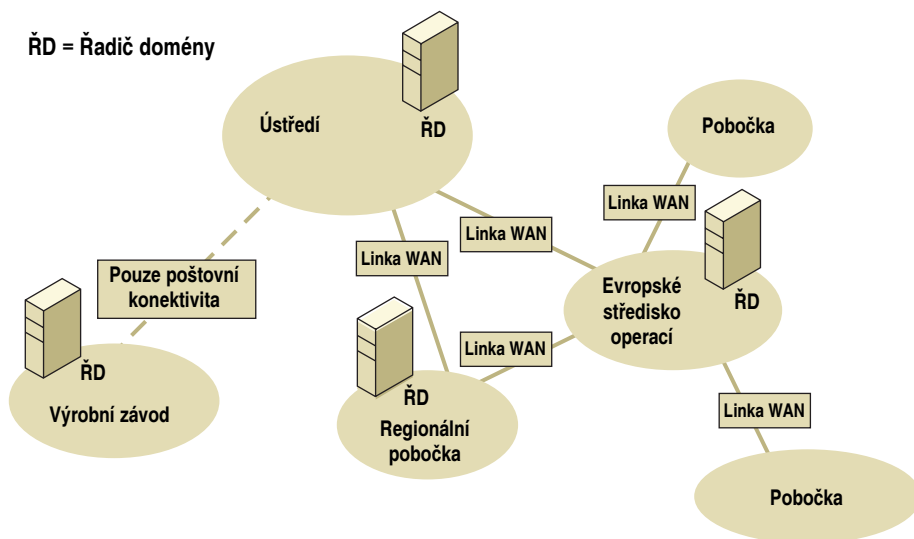
Poznámka

Řadiče domén obsahují citlivé bezpečnostní informace, jako jsou kopie tajných klíčů uživatelů používaných pro ověřování v doméně. Méně kopií těchto informací pochopitelně snižuje příležitost získání neautorizovaného přístupu. Řadiče domén musí být před neautorizovaným přístupem fyzicky chráněny. Doporučuje se například umístit řadiče domén do nepřístupných místností s omezenými možnostmi vstupu. Fyzický přístup může narušiteli umožnit získat kopie zašifrovaných dat hesel, které pak může použít pro offline útok na heslo. Silnější možnosti zabezpečení nabízí nástroj Syskey. Další informace o nástroji Syskey najdete v kapitole „Encrypting File System“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.

Když se uživatel přihlašuje, musí být řadič domény obsluhující požadavek na ověření schopen komunikovat se serverem globálního katalogu. Rozhodnete-li se do nějakého sídla umístit řadič domény, musíte zvážit také funkci daného řadiče jako serveru globálního katalogu. Při dalším čtení si uvědomte, že servery globálního katalogu vytvářejí větší replikační provoz než normální řadiče domén. Obsahují jak úplnou kopii jedné domény, tak i částečnou kopii určenou pouze pro čtení všech dalších domén v doménové struktuře.

Obrázek 9.4 ukazuje umístění řadičů domén ve společnosti Reskit.

- První řadič domény je umístěn v domovském místě ústředí.
- Další řadič domény je umístěn v evropském středisku operací, protože transoceánská linka WAN již pracuje na hranici své kapacity.
- Řadič domény je také umístěn v regionální pobočce, protože je tu příliš mnoho uživatelů, takže linka WAN nedokáže zvládnout ověřovací provoz.
- Řadiče domén nejsou v jiných pobočkách, protože se tu nenacházejí žádné místní servery.
- Řadič domény musí být také ve výrobním závodě, protože ten je dosažitelný jen prostřednictvím elektronické pošty SMTP.



Obrázek 9.4 Umístění řadičů domén ve společnosti Reskit

Rozdělte doménovou strukturu

Nyní každému řadiči domény přiřadíte doménu, určíte, zda vaše síť dokáže zvládnout replikační provoz, a v případě potřeby rozdělíte svou doménovou strukturu na menší domény. Přitom si pamatujte, že cílem rozdělení je přesunout fyzické kopie objektů adresáře blíže uživatelům, kteří tyto objekty potřebují. Například objekt uživatelského účtu uživatele musí být umístěn na řadiči domény, který se nachází ve stejném sídle jako daný uživatel.

Doménovou strukturu rozdělíte vykonáním následujících kroků v doménách, které se právě nacházejí v plánu domén:

- U každého sídla obsahujícího řadič domény určete, zda uživatelům v sídle odpovídá daná doména. Je-li to vhodné, vložte do sídla řadič dané domény.
- Vysledujte trasu, kterou bude probíhat replikace mezi řadiči pro danou doménu. Předpokládejte, že každý řadič domény zvolí jako replikačního partnera další nejbližší řadič domény pro stejnou doménu, kde pojem „nejbližší“ je určen z hlediska nákladů nejefektivnější cestou sítě.
- Množství replikačního provozu mezi libovolnými dvěma řadiči dané domény je faktorem toho, jak často se objekty v doméně mění, kolik z nich se mění a jak často se objekty přidávají nebo odstraňují. Rozdělením domény na dvě nebo více menších domén můžete snížit množství replikačního provozu, který bude procházet určitou linkou. Prozkoumejte všechny aspekty replikační cesty a rozhodněte, zda daný replikační provoz povolíte, nebo zda doménu rozdělíte.

Tyto faktory zvažte při určování, zda bude či nebude probíhat replikace domény mezi sídly, a při rozhodování, zda bude doména rozdělena na dvě nebo více menších domén.

- Rozdělení domény zvažte, pokud nějaké propojení sítí v replikační cestě nedokáže zvládnout očekávaný replikační provoz.

Skutečná kapacita propojení sítí je funkcí rychlosti linky, charakteristik každodenního používání, spolehlivosti a dostupnosti. Při určování vytvoření další domény zjistěte následující informace o daném spojení:

- Linka pracující na hranici své kapacity nemusí být schopna replikaci zvládnout. Pamatujte, že replikaci adresářové služby Active Directory lze naplánovat, takže pokud není v některých časech linka využívána, může poskytovat dostatečnou šířku pásma pro vykonání replikace.
- Linka může být dostupná jen v některou denní dobu, čímž se dále snižuje její skutečná šířka pásma. Replikaci služby Active Directory lze naplánovat na dobu, kdy je linka opravdu dostupná, vlastní šířka pásma však musí replikaci dostát.

Další informace o plánování kapacity sítě a replikačním provozu služby Active Directory najdete v odkazu Microsoft Windows 2000 Server stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

- Rozdělení domény zvažte také v případě, kdy nechcete, aby replikační provoz bojoval s jiným, důležitějším provozem na lince.

Přerušení nebo zdržení provozu kritického pro fungování podniku může být mnohem dražší než přidání další domény.

- Rozdělení domény zvažte, když bude replikační provoz přenášen linkou placenou za využití.

Jedná-li se o linku placenou za množství přenesených dat, pak se minimalizováním jejího využívání sníží náklady.

- Vytvořte domény pro sídla, která jsou připojena pouze prostřednictvím elektronické pošty SMTP.

K replikaci služby Active Directory elektronickou poštou může dojít pouze mezi doménami. Replikaci elektronickou poštou nelze použít mezi řadiči jedné domény.

Rozhodnete-li se rozdělit nějakou velkou doménu do několika menších domén, pak je vhodné pro vytváření menších domén využívat geografické nebo geopolitické hranice. Vytvořte například domény odpovídající zemím nebo kontinentům. Geografické rozdělování domén lze doporučit, protože topologie sítě má tendenci využívat geografická místa a geografie obecně má menší tendenci ke změnám než jiné výchozí prvky pro rozdělení.

Vyšší počet menších domén můžete chtít na své síti vytvořit čistě kvůli optimalizaci replikačního provozu. Pamatujte však, že tato optimalizace musí být vyvážená s dalšími faktory, jakými jsou:

- Složitost

Jak již bylo řečeno, každá další doména představuje určité pevné dodatečné náklady na správu.

- Provoz dotazů versus replikační provoz

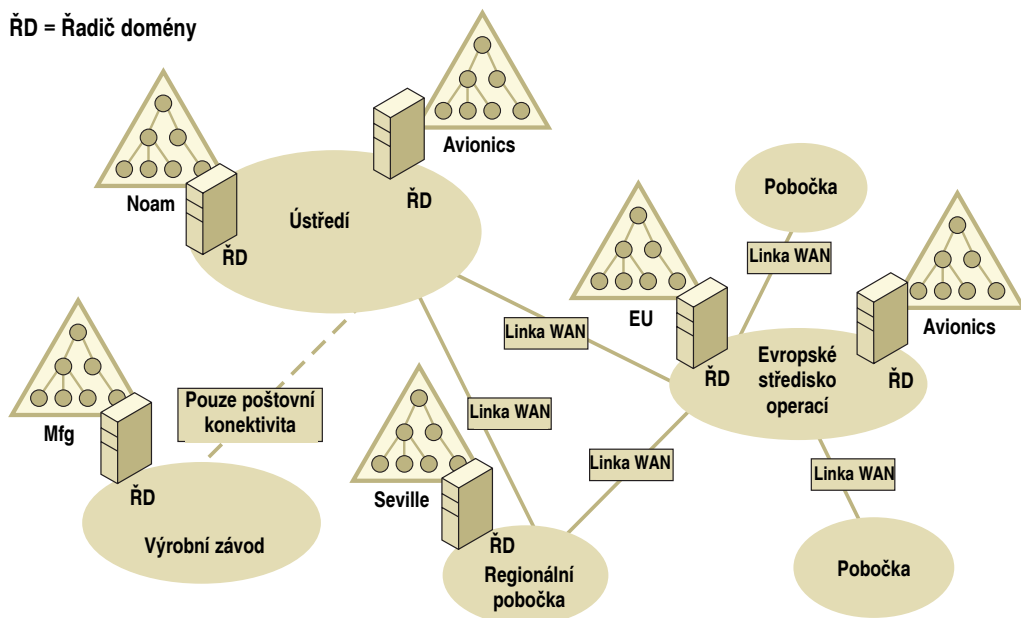
Čím méně je objektů v doméně, tím spíše bude uživatel v dané doméně chtít přistupovat k objektům v nějaké jiné doméně. Neexistuje-li žádný místní řadič této druhé domény, dotazování bude způsobovat provoz opouštějící sídlo.

Poznámka Model s jedinou velkou doménou nejlépe funguje u rozsáhlého množství cestujících uživatelů, protože každý uživatelský účet bude dostupný na každém sídle, které má řadič domény. V takovém případě cestující uživatel nikdy nepřijde o možnost přihlásit se k síti, pokud dojde k výpadku sítě mezi aktuálním místem uživatele a jeho domovským místem.

Obrázek 9.5 zobrazuje fyzické rozdělení společnosti Reskit. Přiřazení domén vypadá takto:

- Doména Noam uživatelů v Severní Americe je přiřazena řadiči domény v domovském sídle.
- Doména Letectví, která byla vytvořena z důvodů správy, je přiřazena jinému řadiči domény v domovském sídle, protože v ústředí se nacházejí uživatelé domény Letectví.
- Řadiči domény v evropském středisku operací je přiřazena nová doména Eu, protože transoceanická linka WAN pracuje již na hranici své kapacity. Tato linka nedokáže zpracovat replikační provoz pro kombinované severoamerické a evropské domény.
- Doména Letectví je také reprezentována v evropském středisku operací, protože uživatelé domény Letectví se nacházejí i v Evropě.
- Řadiči domény v regionální pobočce v Seville je přiřazena nová doména Seville, jelikož linka WAN do evropského střediska operací přenáší provoz důležitý pro podnik.
- Řadiči domény ve výrobním závodě je přiřazena nová doména Mfg, protože k němu lze přistupovat pouze prostřednictvím elektronické pošty SMTP.

ŘD = Řadič domény



Obrázek 9.5 Přiřazení domén společnosti Reskit

Nárůst nákladů na další domény

Každá doména v doménové struktuře bude představovat určité dodatečné výdaje na správu. Při určování, zda se má nebo nemá přidat nějaká doména do plánu domén, porovnejte následující náklady s výhodami zjištěnými dříve v této kapitole.

Více správců domén

Protože správci domén mají k dispozici úplné řízení domény, je zapotřebí pečlivě sledovat členství ve skupině správců dané domény. Každá přidaná doména do doménové struktury představuje tuto nutnost dodatečné správy.

Více hardwaru řadičů domén

V systému může řadič domény hostit jen jednu doménu. Každá nově vytvořená doména bude vyžadovat přinejmenším jeden počítač; ve většině případů však půjde o dva počítače, protože jen pak bude možné naplnit požadavky na spolehlivost a dostupnost. Jelikož všechny řadiče domén systému Windows 2000 mohou přijímat a zadávat změny, musíte je fyzicky chránit pečlivěji než záložní řadiče domén (Backup Domain Controller – BDC) systému Windows NT 4.0, což byly počítače určené pouze pro čtení. Uvědomte si, že delegování správy v doménách služby Active Directory omezuje potřebu domén prostředků. Některé vzdálené lokace musí nyní hostit dva řadiče domény (hlavní doménu uživatelských účtů a místní doménu prostředků), zvolíte-li však konsolidaci na menší počet domén služby Active Directory, budou již potřebovat jen jeden řadič domény.

Více vztahů důvěryhodnosti

Aby mohl řadič domény v jedné doméně ověřit uživatele v jiné doméně, musí být schopen kontaktovat řadič domény v dané druhé doméně. Tato komunikace představuje další možný bod selhání, pokud je například v takovém okamžiku síť mezi oběma doménami nefunkční. Čím více uživatelů a prostředků se nachází v jedné doméně, tím méně se musí jednotlivý řadič domény spoléhat na možnost komunikace s jinými řadiči domén.

Větší pravděpodobnost nutnosti přesunu komitentů zabezpečení mezi doménami

Čím více máte domén, tím větší je pravděpodobnost, že budete mezi doménami muset přesunovat komitenty zabezpečení, jako jsou uživatelé a skupiny. Například reorganizace podniku nebo změna pracovního zařazení může zapříčinit nutnost přesunu uživatele mezi doménami. Pro koncové uživatele a správce je přesun komitenta zabezpečení mezi organizačními útvary v doméně triviální a transparentní operací. Přesun komitenta zabezpečení mezi doménami je však mnohem složitější a může mít dopady i na koncového uživatele.

Další informace o přesunu komitentů zabezpečení mezi doménami najdete v kapitole „Určení strategií migrace domén“ v této knize.

Zásady skupiny a řízení přístupu se nepřenášejí mezi doménami

Zásady skupiny a řízení přístupu aplikované v rámci jedné domény se nepřenášejí automaticky do jiných domén. Máte-li zásady nebo delegované úkoly správy prostřednictvím řízení přístupu, které jsou v mnoha doménách stejné, musíte je aplikovat na každou doménu samostatně.

Volba kořenové domény doménové struktury

Jakmile máte určeno, kolik domén umístíte do své doménové struktury, musíte rozhodnout, která doména bude kořenovou doménou doménové struktury. *Kořenová domé-*

na doménové struktury je první doména, kterou v doménové struktuře vytvoříte. V této doméně se budou nacházet dvě skupiny s rozsahem na úrovni celé doménové struktury, správci podniku a správci schématu.

Poznámka Dojde-li při nějaké katastrofické události ke ztrátě všech řadičů kořenové domény doménové struktury a ze zálohy nelze obnovit žádný řadič domény, budou trvale ztraceny skupiny správců podniku a správců schéma. Neexistuje žádná možnost opakovaně instalovat kořenovou doménu doménové struktury.

Obsahuje-li vaše doménová struktura pouze jednu doménu, pak bude tato doména kořenovou doménou doménové struktury. Obsahuje-li vaše doménová struktura dvě nebo více domén, pak při výběru kořenové domény doménové struktury zvažte následující dvě pojetí:

Použití existující domény

Ze seznamu svých domén vyberte doménu, která je pro fungování vaší organizace nejdůležitější, a učíte ji kořenovou doménou doménové struktury. Protože si nemůžete dovolit přijít o tuto doménu, bude ihned vyžadovat takovou odolnost proti chybám a možnost obnovení či zotavení, jaká je vyžadována pro kořenovou doménu doménové struktury.

Použití vyhrazené domény

Vytvoření další, vyhrazené domény, která bude sloužit výhradně jako kořenová doména doménové struktury, sebou sice nese veškeré náklady na další doménu, avšak přináší také určité výhody, které mohou být pro vaši organizaci zajímavé:

- Správce domény v kořenové doméně doménové struktury bude schopen pracovat se členstvím skupin správců podniku a správců schématu. Můžete mít správce, kteří pro plnění určitých svých povinností vyžadují oprávnění na úrovni správce domény, nechcete však, aby měli možnost manipulovat se skupinami správců pro celou doménovou strukturu. Když vytvoříte samostatnou doménu, nebudete pak muset umisťovat takové správce do skupiny správců kořenové domény doménové struktury.
- Protože je tato doména malá, lze ji snadno replikovat kamkoli na síť a zajistit tak ochranu před geograficky omezenými katastrofami.
- Jelikož jedinou rolí takové domény je fungovat jako kořenová doména doménové struktury, nikdy nebude hrozit její zastarání. V případě, kdy vyberete nějakou doménu ze svého seznamu plánovaných domén a označíte ji za kořenovou doménu doménové struktury, vždy existuje určitá možnost, že právě tato doména zastará, třeba díky změnám ve vaší organizaci. Takovou doménu však nebudete moci nikdy úplně opustit a zrušit, protože bude muset vždy hrát roli kořenové domény doménové struktury.

Přiřazení názvů DNS a vytvoření hierarchie domén

Domény služby Active Directory jsou pojmenovány názvy systému DNS. Protože DNS je základní systém názvů používaný na Internetu, názvy DNS jsou globálně uznávány a mají dobře zavedené registrační úřady. Klienti služby Active Directory požadující přihlášení k síti pomocí DNS vyhledávají řadiče domén.

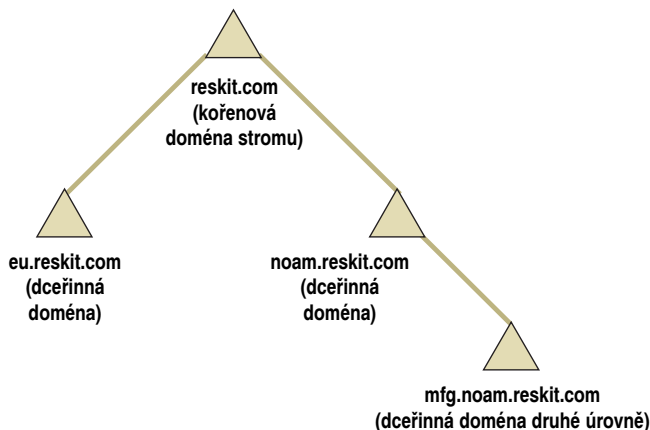
V systému Windows NT 4.0 vycházel lokátor domén ze systému názvů prostředí NetBIOS (NBNS) a domény byly identifikovány názvy systému NetBIOS. Serverová sou-

část NBNS se označuje za server Windows Internet Name Service (WINS). Názvy NetBIOS jsou jednoduché, jednoduté názvy a obor názvů systému NetBIOS nelze rozdělit. Naproti tomu názvy DNS jsou hierarchické a obor názvů DNS lze rozdělit podle hierarchie. Výsledkem je, že systém DNS je škálovatelnější než systém NBNS a může obsáhnout větší databázi rozptýlenou na rozsáhlé síti. Internetová pošta, která využívá službu DNS podobným způsobem jako služba Active Directory, je dobrým příkladem toho, jak dokáže systém DNS jako mechanismus lokátoru zvládnout i extrémně rozsáhlé sítě, jako je Internet.

Poznámka Pro zachování možnosti spolupráce s počítači s předchozími verzemi systému Windows mají domény služby Active Directory názvy systému NetBIOS a řadiče domén Active Directory je v případě potřeby registrují v systému NBNS a dotazují se na ně systému NBNS. To umožňuje klientům používajícím dřívější verze systému Windows vyhledat řadiče domén služby Active Directory. Navíc se mohou vzájemně vyhledávat řadiče domén Active Directory a řadiče domén systémů Windows NT 3.51 a Windows NT 4.0.

Uspořádání domén do stromů

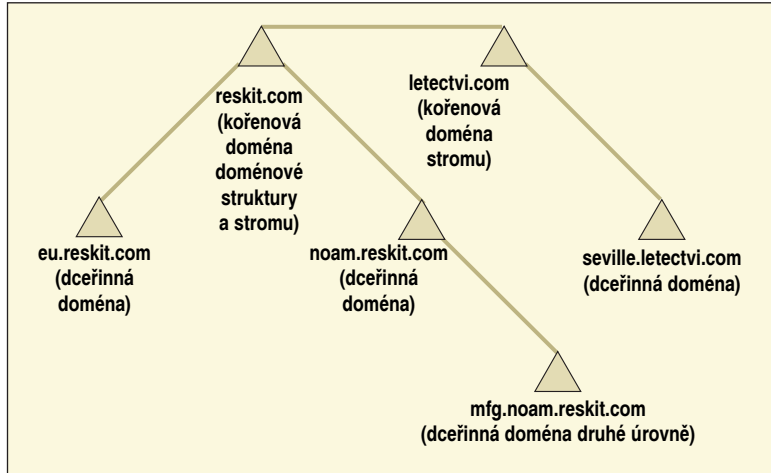
Strom je sada jedné nebo více domén systému Windows 2000 se spojenými názvy. Obrázek 9.6 představuje jediný strom se spojeným oborem názvů. Protože doména reskit.com nemá žádnou nadřazenou doménu, je považována za *kořenovou doménu stromu*. Podřízenými (dceřinými) doménami domény reskit.com jsou domény eu.reskit.com a noam.reskit.com. Podřízenou doménou druhé úrovně domény reskit.com je doména mfg.noam.reskit.com. Tyto názvy domén jsou spojené, protože každý název se od názvu nadřazené domény v hierarchii domén liší jen jedním popiskem.



Obrázek 9.6 Jediný strom se čtyřmi doménami

Doménová struktura může mít více stromů. V doménové struktuře s více stromy nejsou názvy kořenových domén stromů spojené, jak ukazuje obrázek 9.7. Více stromů můžete mít v doménové struktuře, například pokud má nějaké oddělení vaší organizace svůj vlastní registrovaný název DNS a provozuje své vlastní servery DNS.

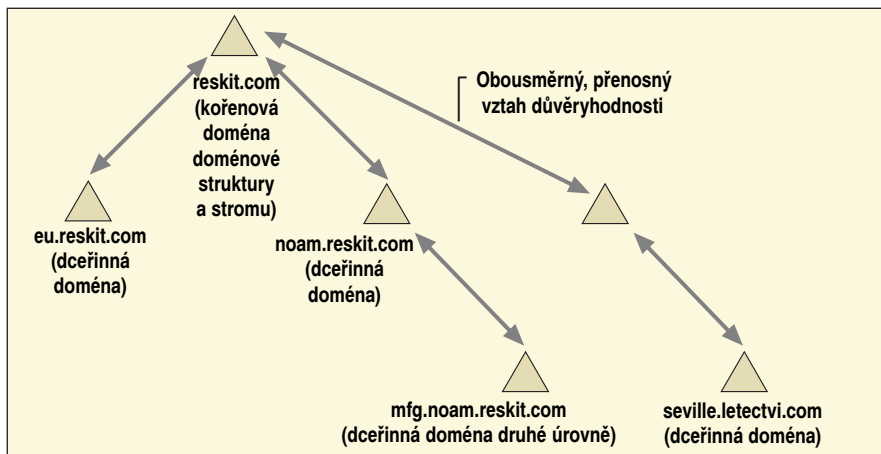
Doménová struktura



Obrázek 9.7 Doménová struktura s více stromy

Hierarchie domén v doménové struktuře určuje přenosné vztahy důvěryhodnosti propojující jednotlivé domény. Každá doména má přímý vztah důvěryhodnosti se svou nadřazenou (mateřskou) doménou a se svými podřízenými (dceřinnými) doménami. Existuje-li v doménové struktuře více stromů, pak se na vrcholu stromu důvěryhodnosti nachází kořenová doména doménové struktury a všechny ostatní kořenové domény stromů jsou jí podřízeny, alespoň z hlediska vztahů důvěryhodnosti. Obrázek 9.8 znázorňuje přenosný vztah důvěryhodnosti mezi dvěma stromy.

Doménová struktura



Obrázek 9.8 Přenosný vztah důvěryhodnosti mezi stromy

Vztah nadřazenosti a podřízenosti domén je pouze vztah vytvoření názvů a důvěryhodnosti. Správci v mateřské doméně nejsou automaticky správci v dceřinných doménách. Zásady zadané v nadřazené doméně se neaplikují automaticky na podřízené domény.

Doporučení vytváření názvů domén

Chcete-li vytvořit hierarchii domén v doménové struktuře, přiřadte název DNS první doméně a pak se u všech následujících domén rozhodněte, zda se jedná o podřízenou doménu existující domény nebo o novou kořenovou doménu stromu. Podle toho pak doménám přiřadte názvy. Dále jsou uvedena určitá doporučení vytváření názvů domén:

Používejte názvy relativní k registrovanému internetovému názvu DNS.

Názvy zaregistrované na Internetu jsou globálně jedinečné. Máte-li jeden nebo více zaregistrovaných internetových názvů, použijte je jako přípony názvů svých domén Active Directory.

Používejte standardní internetové znaky.

Standardní internetové znaky názvů hostitelů systému DNS jsou definovány v dokumentu Request for Comments (RFC) 1123 jako A–Z, a–z, 0–9 a rozdělovník (–). Bude-li používát výhradně standardní internetové znaky, vaše služba Active Directory pak bude kompatibilní s veškerým softwarem, který z těchto standardů vychází. V zájmu podpory inovace dřívějších domén systému Windows s nestandardními názvy na domény systému Windows 2000 podporují klienti společnosti Microsoft a služba DNS systému Windows 2000 téměř všechny znaky sady Unicode v názvu.

Nikdy nepoužívejte jeden název dvakrát.

Dvěma různým doménám nikdy nedávejte stejný název, i když jsou tyto domény na nepropojených sítích s různými obory názvů DNS. Jestliže se například společnost Reskit rozhodne pojmenovat doménu na intranetu reskit.com, neměla by zároveň vytvořit internetovou doménu nazvanou reskit.com. Když je klient domény reskit.com připojen jak k intranetu tak i k Internetu zároveň, vybere během hledání lokátoru doménu, která odpovíděla první. Z hlediska klienta se tento výběr bude jevit náhodným a neexistuje žádná záruka, že si klient vybere „tu správnou“ doménu. Příkladem takové konfigurace je klient, který vytvořil připojení virtuální privátní sítě k intranetu přes Internet.

Používejte rozdílné názvy.

Určitý klientský software proxy, jako je klient proxy zabudovaný do programu Microsoft Internet Explorer nebo klient Winsock Proxy, používá název hostitele k určení, zda se hostitel nachází na Internetu. Většina softwaru tohoto typu nabízí přinejmenším možnost vyloučení názvů s určitými příponami jako místní názvy, u kterých se pak již nepředpokládá, že jsou na Internetu.

Chce-li společnost Reskit nazvat nějakou doménu Active Directory na svém intranetu reskit.com, musí zadat reskit.com do seznamu výjimek jejich klientského softwaru proxy. To zabrání klientům na intranetu společnosti Reskit v zobrazení hostitele na Internetu nazvaného www.reskit.com, pokud není neposkytnuto identické sídlo na intranetu.

Aby se společnost Reskit vyhnula tomuto problému, může používat nějaký zaregistrovaný název, který se neobjevuje na Internetu, jako je například reskit-int01.com, nebo vytvořit zásady společnosti říkající, že názvy končící konkrétní příponou reskit.com, například corp.reskit.com, se nesmějí nikdy objevit na Internetu. V obou případech je

snadné nakonfigurovat seznamy výjimek klientů proxy, aby dokázali určit, které názvy se nacházejí na intranetu a které na Internetu.

Existuje mnoho různých technik přístupu k Internetu ze soukromého intranetu. Ještě než použijete nějaký název, ujistěte se, že jej klienti na vašem intranetu (v rámci vaší konkrétní strategie přístupu k Internetu) dokáží správně přeložit.

Používejte co nejmenší možný počet stromů.

Minimalizování počtu stromů v doménové struktuře sebou přináší určité výhody. Pro vaše prostředí mohou být užitečné následující výhody:

- Jakmile vám bylo předáno řízení určitého názvu DNS, vlastníte také všechny názvy, které jsou mu podřízeny. Čím menší je počet stromů, tím menší je také počet názvů DNS, jejichž vlastnictví musíte pro organizaci zařídít.
- Do seznamů výjimek klientů proxy je zapotřebí zadávat méně názvů.
- Klientské počítače LDAP, které nejsou klienty programů společnosti Microsoft, mohou při prohledávání adresáře nepoužívat globální katalog. Tito klienti budou při prohledávání na úrovni adresáře využívat spíš hloubková hledání. Hloubkové hledání se týká všech objektů v určitém podstromu. Čím menší je počet stromů v doménové struktuře, tím méně hloubkových hledání bude zapotřebí vykonat při prohledávání celé doménové struktury.

První část názvu DNS zadejte stejnou jako název systému NetBIOS.

Je možné přiřadit doméně název DNS a název NetBIOS, které spolu vůbec nesouvisí. Například název DNS domény může být sales.reskit.com, ale název systému NetBIOS může být „Marketing“. Pamatujte, že software nespolečupracující se službou Active Directory a počítače s předchozími systémy budou zobrazovat a přijímat názvy systému NetBIOS, zatímco počítače se systémem Windows 2000 a software podporující službu Active Directory budou zobrazovat a přijímat názvy DNS. To může vést ke zmatení koncových uživatelů a správců.

Nesouhlasící názvy systémů NetBIOS a DNS použijte, pouze pokud:

- chcete svou síť migrovat na nové konvence vytváření názvů,
- inovujete název systému NetBIOS obsahující nestandardní znaky, chcete však, aby se název DNS skládal výhradně ze standardních znaků.

Podívejte se na své názvy z mezinárodního hlediska.

Názvy, které mají příjemný či užitečný význam v jednom jazyku, mohou být v jiném jazyku pohrdavé nebo urážlivé. DNS je globální obor názvů, a proto se na své názvy podívejte ve své organizaci z globálního hlediska.

Poznámka

Provozujete-li na síti více lokalizovaných verzí systému Windows, všechny počítače včetně těch se systémem Windows 2000 Professional a všemi verzemi systému Windows 2000 Server musí ve svých názvech DNS a NetBIOS používat výhradně standardní internetové znaky. Použijete-li jiné než výše uvedené znaky, budou spolu schopny komunikovat pouze počítače se stejnými místními nastaveními.

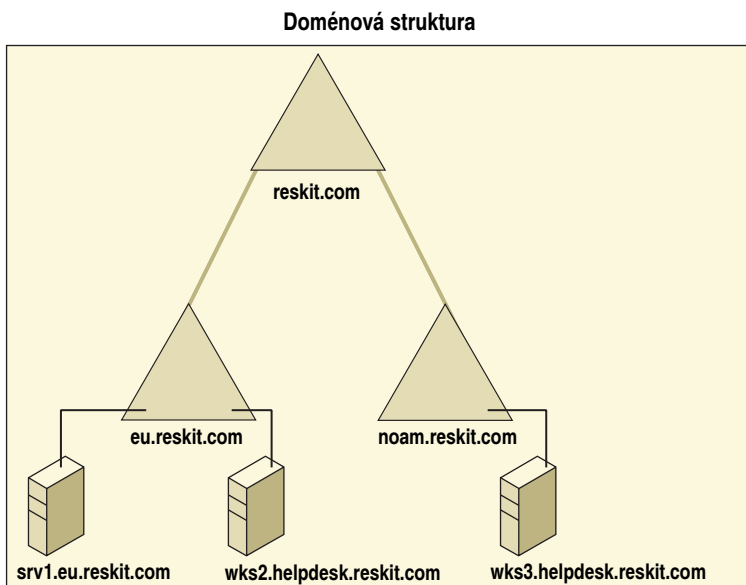
Použijte rozumně dlouhé názvy, které se dobře pamatují.

Délka by neměla při volbě názvů hrát naprosto zásadní roli. Uživatelé obvykle pracují s globálním katalogem a o názvy domén se nezajímají. Ty se obvykle týkají pouze správců. Nástroje pro správu téměř vždy nabízejí seznamy domén, z nichž si lze vybrat,

a počet případů, kdy musí správce skutečně zapisovat úplný název domény, bude poměrně malý. Obecně platí, že pokud si dokážete zapamatovat všechny součásti názvu, pak není tento název příliš dlouhý.

Názvy domén a názvy počítačů

Počítače se systémem Windows 2000, které se přidají do domény, si standardně samy přiřadí název DNS, který je tvořen názvem hostitele počítače a názvem DNS domény, ke které se počítač přidal. Pokud je například na obrázku 9.9 účet počítače Server1 umístěn v doméně eu.reskit.com, počítač se sám pojmenuje výchozím názvem server1.eu.reskit.com. Místo názvu domény Active Directory je však možné použít libovolnou příponu DNS. Proto není nutné pojmenovávat domény Active Directory tak, aby odpovídaly struktuře DNS již zavedené ve vaší organizaci. Vaše domény Active Directory mohou používat libovolné názvy a vaše počítače si mohou ponechat své existující názvy.



Obrázek 9.9 Členské počítače s výchozími a nevýchozími názvy

Další informace o vytváření názvů počítačů najdete v kapitole „Windows 2000 DNS“ v knize *Microsoft Windows 2000 Server Sítě TCP/IP*.

Plánování zavedení serverů DNS

Chcete-li naplánovat zavedení serverů DNS podporujících domény Active Directory, musíte identifikovat servery DNS, které budou pro vaše názvy domén autoritativní, a zajistit, aby splňovaly požadavky systému lokátoru řadiče domény.

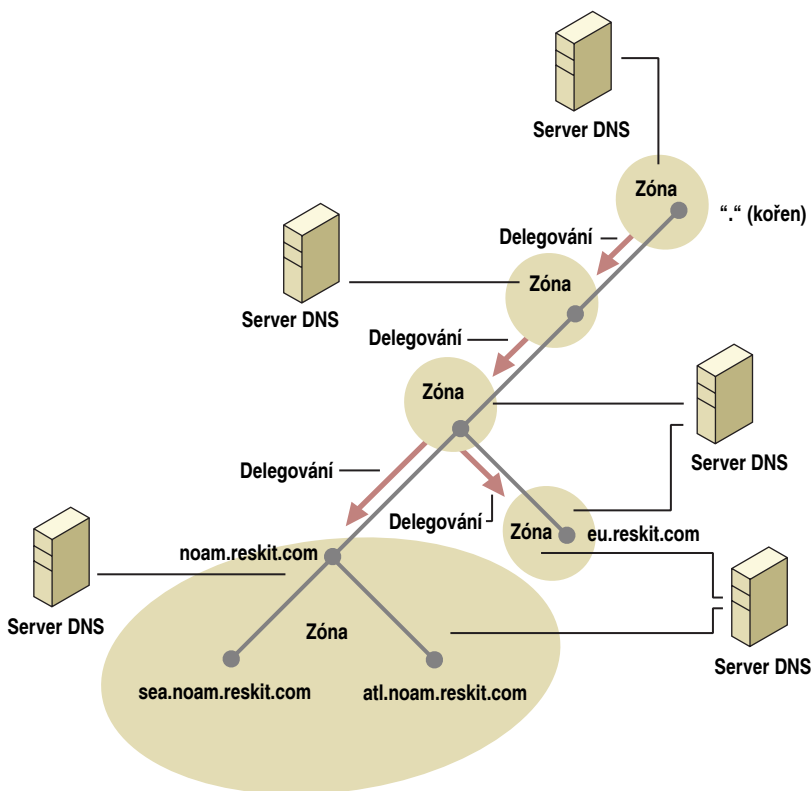
Úřad a delegování v systému DNS

Domain Name System je hierarchická, distribuovaná databáze. Samotná databáze se skládá ze záznamů prostředků, které jsou tvořeny hlavně názvem DNS, typem zázna-

mu a hodnotami dat, které jsou danému typu záznamu přiřazeny. Nejobvyklejšími záznamy v databázi DNS jsou záznamy Address (A – adresa), v nichž je název záznamu typu Address názvem počítače a daty v záznamu je adresa TCP/IP daného počítače.

Podobně jako služba Active Directory je i databáze DNS rozdělena do oddílů, které umožňují výkonné škálování databáze na velmi rozsáhlých sítích. Oddíl databáze DNS se nazývá zóna. Zóna obsahuje záznamy spojitě sady názvů DNS. Server DNS, který nahrává nějakou zónu, se označuje za autoritativní pro názvy v dané zóně.

Zóna začíná určitým názvem a končí v bodu delegování. Bod delegování indikuje, kde jedna zóna končí a další zóna začíná. Například na Internetu existuje registrační úřad zodpovědný za zónu nazvanou „com“. V této zóně jsou tisíce bodů delegování dalších zón, například reskit.com. Data v bodu delegování indikují, které servery jsou pro danou delegovanou zónu autoritativní. Obrázek 9.10 ukazuje vztah mezi servery, zónami a delegováním systému DNS.



Obrázek 9.10 Servery, zóny a delegování v systému DNS

Systém lokátoru řadiče domény

Řadiče domén registrují v systému DNS sadu záznamů. Tyto záznamy se společně označují za záznamy lokátoru (vyhledávače). Když nějaký klient požaduje od domény určitou službu, odešle dotaz na specifický název a typ záznamu nejbližšímu serveru DNS. Odpovědí je seznam řadičů domén, které dokáží požadavek naplnit.

Názvy záznamů lokátoru jednotlivých domén končí konstrukcí `<název-domény-DNS>` a `<název-doménové-struktury-DNS>`. Servery DNS, které jsou autoritativní pro jednotlivé `<název-domény-DNS>`, jsou autoritativní pro záznamy lokátoru.

Poznámka Systém Windows 2000 nevyžaduje konfiguraci zón zpětného vyhledávání. Zóny zpětného vyhledávání však mohou být nezbytné pro jiné aplikace nebo pro zajištění jednoduchosti správy.

Požadavky serverů DNS

Jestliže na své síti ještě nemáte spuštěné servery DNS, doporučujeme vám zavést službu DNS, která je součástí systému Windows 2000 Server. Máte-li již existující servery DNS, pak musí servery autoritativní pro záznamy lokátoru odpovídat následujícím požadavkům podpory služby Active Directory:

- Musí podporovat záznam prostředku Service Location.
Servery DNS autoritativní pro záznamy lokátoru musí podporovat záznamy prostředků typu Service Location (SRV – umístění služby). Další informace o záznamu SRV najdete v kapitole „Introduction to DNS“ v knize *Microsoft Windows 2000 Server Síť TCP/IP*.
- Měly by podporovat protokol dynamické aktualizace DNS.
Servery DNS, které jsou autoritativní pro záznamy lokátoru a které jsou primárními hlavními servery pro tyto zóny, by měly podporovat protokol dynamické aktualizace DNS definovaný v RFC 2136.

Služba DNS, jež je součástí systému Windows 2000 Server, splňuje oba tyto požadavky a nabízí také další důležité funkce:

- Integrace se službou Active Directory
Pomocí této funkce ukládá služba DNS systému Windows 2000 data zón do adresáře. Replikace DNS tak vytváří více hlavních počítačů a umožňuje libovolnému serveru DNS přijímat aktualizace nějaké zóny integrované s adresářovou službou. Použití integrace se službou Active Directory také omezuje potřebu udržovat oddělenou topologii přenosové replikace zóny DNS.
- Zabezpečená dynamická aktualizace
Součástí zabezpečení systému Windows je integrovaná zabezpečená dynamická aktualizace. Umožňuje správci přesně řídit, které počítače mohou aktualizovat určité názvy, a zabráňuje neautorizovaným počítačům v získání existujících názvů od systému DNS.

Zbývající servery DNS na vaší síti, které nejsou autoritativní pro záznamy lokátoru, nemusí uvedené požadavky splňovat. Neautoritativní servery jsou obvykle schopny zodpovědět dotazy na záznamy SRV, i když tento typ záznamu explicitně nepodporují.

Umístěte autoritativní servery

V případě každého vybraného názvu DNS se spojte s týmem správy systému DNS a zjistěte, zda daný server DNS podporuje uvedené požadavky. Objevíte-li server, který je nespĺňuje, můžete vykonat tři základní akce:

Inovovat server na verzi, která tyto požadavky naplňuje.

Pokud na autoritativních serverech běží služba DNS systému Windows NT 4.0, prostě je inovujte na systém Windows 2000. Jedná-li se o jinou implementaci serverů DNS, prostudujte si dokumentaci výrobce a zjistěte, které verze obsahují funkce nezbytné k podpoře služby Active Directory.

Nemáte-li dané autoritativní servery DNS pod svou kontrolou a nedokážete-li přesvědčit jejich vlastníky, aby je inovovali, můžete využít jednu z následujících možností:

Migrujte zónu na systém DNS Windows 2000.

Místo inovace takových serverů na verzi podporující požadavky služby Active Directory můžete zónu migrovat z autoritativních serverů na systém DNS Windows 2000. Migrace zóny na systém DNS Windows 2000 je přímočarý proces. Zaveďte jeden nebo více serverů DNS systému Windows 2000 jako sekundární servery zóny. Jakmile jste spokojeni s výkonem a možností správy těchto serverů, převeďte zónu na jednom ze serverů tak, aby byla primární kopií, a podle potřeby upravte topologii přenosu zóny DNS.

Delegujte daný název serveru DNS, který požadavky splňuje.

Jestliže vám možnosti inovace a migrace autoritativních serverů nevyhovují, můžete autoritativní servery změnit delegováním názvu domény serverům DNS systému Windows 2000. Jak toho lze dosáhnout, závisí na vztahu názvu domény k existující struktuře zóny.

- Neodpovídá-li název domény názvu kořenu zóny, lze daný název delegovat přímo serverům DNS systému Windows 2000. Jestliže je například název domény noam.reskit.com a název zóny, která tento název obsahuje, je reskit.com, delegujte noam.reskit.com nějakému serveru DNS se systémem Windows 2000.
- Odpovídá-li název domény názvu kořenu zóny, nelze daný název delegovat nějakému serveru DNS systému Windows 2000 přímo. Místo toho delegujte serveru DNS systému Windows 2000 všechny poddomény používané záznamy lokátoru. Těmito poddoménami jsou: `_msdcs.<název-domény-DNS>`, `_sites.<název-domény-DNS>`, `_tcp.<název-domény-DNS>` a `_udp.<název-domény-DNS>`. Učiníte-li tak, budete muset ručně zaregistrovat záznamy adres (A) `<název-domény-DNS>`. Další informace o tomto tématu najdete v kapitole „Windows 2000 DNS“ v knize *Microsoft Windows 2000 Server Síť TCP/IP*.

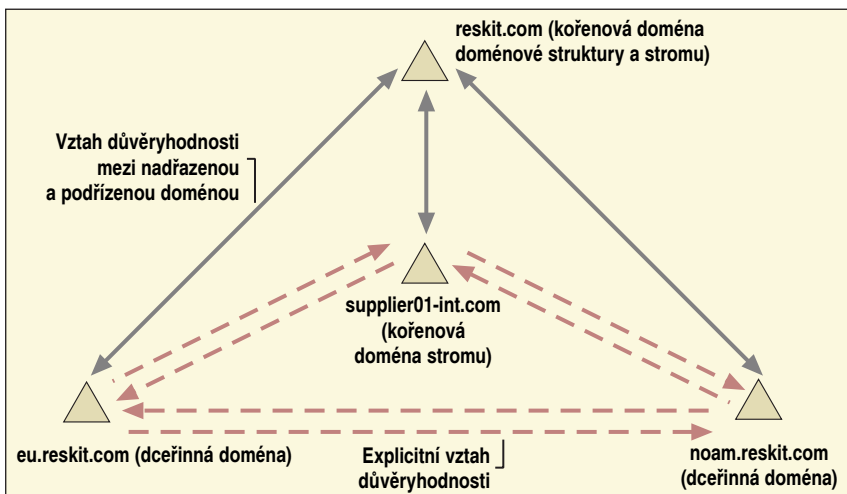
Optimalizace ověřování pomocí explicitních vztahů důvěryhodnosti

Když nějaký uživatel požaduje přístup k určitému síťovému prostředku, musí řadič domény uživatele komunikovat s řadičem domény prostředku. Nejsou-li tyto dvě domény ve vztahu podřízenosti a nadřízenosti, musí řadič domény uživatele komunikovat také s nějakým řadičem domény ve všech doménách ve stromu důvěryhodnosti mezi doménou uživatele a doménou prostředku. V závislosti na síťovém umístění řadičů jednotlivých domén může každý dodatečný přeskok ověření mezi dvěma doménami zvýšit pravděpodobnost možného selhání nebo zvýšit pravděpodobnost přenosu ověřovacího provozu pomalou linkou. Chcete-li omezit množství komunikace potřeb-

né pro takové interakce, můžete libovolné dvě domény spojit *explicitním vztahem důvěryhodnosti*.

Máte-li například více stromů v doménové struktuře, může pro vás být výhodné propojit skupinu kořenových domén stromů vztahy důvěryhodnosti. Nezapomeňte, že ve výchozím uspořádání se všechny kořenové domény stromů považují z hlediska vztahů důvěryhodnosti za podřízené domény kořenové domény doménové struktury. To znamená, že veškerý provoz ověřování mezi jakýmkoli dvěma doménami v různých stromech musí projít kořenovou doménou doménové struktury. Vytvoření naznačených vztahů důvěryhodnosti umožní libovolným dvěma kořenovým doménám stromů komunikovat přímo mezi sebou.

Obrázek 9.11 ukazuje úplné vztahy důvěryhodnosti vytvořené mezi čtyřmi doménami stromů.



Obrázek 9.11 Úplné vztahy důvěryhodnosti mezi čtyřmi doménami

Změna plánu domén po zavedení

Hierarchii domén není jednoduché po jejich vytvoření restrukturalizovat. Proto je nejlepší nevytvářet domény vycházející z dočasné nebo krátkodobé organizační struktury. Například vytvoření domény odpovídající určité obchodní či výrobní jednotce ve vaší organizaci může znamenat zbytečnou práci, dojde-li k rozdělení této jednotky nebo k jejímu zrušení či sloučení s jinou jednotkou v rámci reorganizace společnosti.

Existují však také případy, kdy je rozdělování podle struktury organizace vhodné. Relativně stabilní šablonu pro rozdělování představují geopolitické hranice, avšak pouze v případě, kdy organizace tyto hranice nepřekračuje často. Zamyslete se nad plánem domén armády, která má různé divize rozptýleny na mnoha různých základnách. Přesun divizí mezi základnami bude pravděpodobně velmi častý. Pokud by byla doménová struktura rozdělena podle geografického umístění, správci by museli po každém přesunu divize na jinou základnu přesunovat velké množství účtů uživatelů mezi doménami. Pokud bude doménová struktura rozdělena podle divizí, správci budou muset mezi základnami přesunovat jen řadiče domén. V takovém případě je uspořádání podle struktury organizace vhodnější než geografické rozdělení.

Přidání nových domén a odstranění existujících domén

Do doménové struktury je jednoduché přidat novou doménu, nelze však přesunovat existující domény Active Directory systému Windows 2000 mezi doménovými strukturami.



Důležité rozhodnutí Jakmile je vytvořena kořenová doména stromu, nemůžete do doménové struktury přidat doménu s názvem vyšší úrovně. Nelze také vytvořit nadřazenou doménu existující domény, lze vytvořit pouze podřízenou doménu. Je-li například první doména ve stromu nazvána eu.reskit.com, nemůžete již později přidat nadřazenou doménu nazvanou reskit.com.

Když všechny řadiče nějaké domény převedete na role členských nebo samostatných serverů, odstraníte tak doménu z doménové struktury a vymažete všechny informace, které byly uloženy v dané doméně. Doménu lze z doménové struktury odstranit pouze v případě, že nemá žádné podřízené domény.

Slučování a rozdělování domén

Systém Windows 2000 nenabízí možnost rozdělit doménu na dvě domény nebo sloučit dvě domény jednou operací.



Důležité rozhodnutí Je důležité navrhnout plán domén tak, aby vyžadoval minimální změny rozdělováním během vývoje vaší organizace.

Doménu je možné rozdělit přidáním prázdné domény do doménové struktury a následným přesunutím objektů z jiné domény do nové domény. Stejným způsobem je možné sloučit jednu doménu s jinou doménou přesunutím všech objektů ze zdrojové domény do cílové domény. Jak již bylo řečeno, přesunování komitentů zabezpečení mezi doménami může mít dopady na koncové uživatele. Další informace o přesunování objektů mezi doménami najdete v kapitole „Určení strategií migrace domén“ v této knize.

Změna názvů domén

Systém Windows 2000 nenabízí možnost přímé změny názvu domény. Protože název domény představuje také její pozici v hierarchii stromu, zároveň platí, že doménu nelze v doménové struktuře přesunovat.



Důležité rozhodnutí Při výběru názvů domén volte takové názvy, o kterých si myslíte, že si svůj význam zachovají i během dalšího vývoje vaší organizace.

Alternativou přímého přejmenování je vytvoření nové domény s požadovaným názvem v doménové struktuře a následné přesunutí všech objektů ze staré domény do nové domény.

Vytvoření plánu organizačních jednotek

Organizační útvar nebo jednotka (Organizational Unit – OU) je kontejner, který se používá k vytváření struktury v doméně. Při vytváření struktury v doméně musíte zvážit zejména následující důležité charakteristiky jednotek OU.

Jednotky OU lze vkládat do sebe.

OU může obsahovat podřízené jednotky OU, což vám dovoluje vytvořit v doméně hierarchickou stromovou strukturu.

Jednotky OU lze používat k delegování správy a pro řízení přístupu k objektům adresáře.

Použijete-li kombinaci vkládání jednotek OU a seznamů řízení přístupu, můžete velmi přesně a detailně delegovat správu objektů v adresáři. Můžete tak například skupině pracovníků technické podpory přiřadit oprávnění resetovat hesla určité množiny uživatelů, nikoliv však práva vytvářet uživatele a upravovat jiné atributy objektů uživatelů.

Jednotky OU nejsou komitenty zabezpečení.

Jednotky OU nemůžete učinit členy skupin se zabezpečením, ani nemůžete udělit uživatelům oprávnění k nějakému prostředku na základě toho, že se nacházejí v určité OU. Protože jednotky OU se používají k delegování správy, nadřazená jednotka OU objektu uživatele indikuje, kdo spravuje daný objekt uživatele, neindikuje však prostředky, k nimž může uživatel přistupovat.

Jednotce OU lze přiřadit zásady skupiny.

Zásady skupiny vám umožňují definovat desktopové konfigurace uživatelů a počítačů. Zásady skupiny lze přiřadit sídlům, doménám a jednotkám OU. Definování zásad skupiny na základě OU vám umožňuje používat různé zásady skupiny v rámci jedné domény. Další informace o zásadách skupiny najdete v kapitolách „Aplikování správy změn a konfigurací“ a „Definování standardů správy a konfigurace klientů“ v této knize.

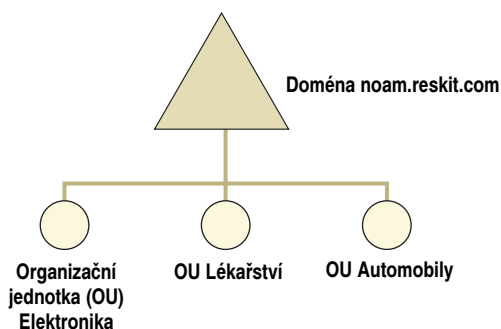
Uživatelé nebudou procházet strukturou jednotek OU.

Není nutné navrhovat takovou strukturu OU, která bude pochopitelná pro koncové uživatele. Uživatelé sice mohou procházet strukturou OU v doméně, není to však nejvhodnější způsob objevování prostředků. Nejvhodnějším způsobem vyhledávání prostředků v adresáři je dotazování globálního katalogu.

Struktura OU a struktura podniku

Fráze „struktura organizační jednotky“ vás může v prvním okamžiku přivést na myšlenku vytvoření nějaké struktury, která bude zrcadlit vaši obchodní či výrobní organizaci a její různá oddělení, divize a projekty. Je sice možné takovou strukturu vytvořit, její správa se však může ukázat být obtížnou a nákladnou. Jednotky OU slouží k delegování správy, takže vytvořená struktura by měla spíše odrážet váš model správy. Model správy vaší organizace nemusí přesně odpovídat celkové struktuře vaší organizace.

Jako příklad si vezměte podnikovou strukturu uvedenou na obrázku 9.12. Jednotky OU byly vytvořeny v odděleních Domácí elektronika (OU Elektronika), Lékařské systémy (OU Lékařství) a Automobilová technika (OU Automobily), přičemž uživatelé týmů automobilové techniky se nacházejí v OU Automobily atd.



Obrázek 9.12 Struktura OU odpovídající struktuře podniku

Předpokládejme, že společnost v tomto příkladu používá model centralizované správy. Jediná skupina správců spravuje všechny uživatele v celé společnosti, bez ohledu na jejich obchodní či výrobní oddělení. V rámci každodenních operací společnosti se může přihodit mnoho věcí. Dojde-li k převedení nějaké osoby z oddělení domácí elektroniky do oddělení automobilové techniky, musí správce přesunout uživatelský účet dané osoby z OU Elektronika do OU Automobily. Je-li počet přesunů velký, může to znamenat značnou zátěž pro skupinu správy. Jaký to však má všechno smysl?

U těžké společnosti si nyní představme strukturu OU, která se skládá z jediné OU obsahující všechny uživatelské účty. Dojde-li k přeřazení nějakého uživatele mezi odděleními, nevzniká pro správce žádný úkol přesunu příslušného objektu. Při vytváření struktury se vždy ujistěte, že slouží nějakému smysluplnému účelu. Struktury vytvořené bez důkladného zdůvodnění budou vždy správcům zbytečně přidělovat práci.

Možná bude vhodné zrcadlit podnikovou strukturu ve struktuře OU, aby bylo snadné vytvářet seznamy uživatelů podle jednotlivých obchodních či výrobních jednotek. Použití jednotek OU je jen jednou z cest, jak toho dosáhnout. Struktura vašeho podniku může blíže odrážet způsob zajištění přístupu k prostředkům pro vaše uživatele. Například uživatelům v určitém projektu lze zajistit přístup k určité sadě souborových serverů, nebo lze uživatelům určitého oddělení povolit přístup k nějakému webovému sídlu. Protože přístup se uděluje pomocí skupin se zabezpečením, můžete přijít na to, že organizační struktura vašeho podniku se bude lépe reprezentovat pomocí struktur skupin se zabezpečením a nikoli pomocí organizačních jednotek (OU).

Proces plánování OU

Kroky vytvoření plánu struktury OU domény vypadají takto:

- Vytvořte jednotky OU pro delegování správy
- Vytvořte jednotky OU pro skrývání objektů
- Vytvořte jednotky OU pro zásady skupiny
- Seznamte se s vlivem změny struktury jednotek OU po jejich zavedení

Je důležité postupovat uvedenými kroky v naznačeném pořadí. Zjistíte, že struktura OU navržená čistě pro delegování správy vypadá jinak, než struktura OU navržená čistě pro zásady skupiny. Protože existuje více možností aplikování zásad skupiny, ale jen jediný způsob delegování správy, musíte nejprve vytvořit jednotky OU pro delegování správy.

Struktura OU se může velmi rychle stát složitou. Kdykoli přidáte nějakou OU do plánu, poznamenejte si konkrétní důvod k tomuto kroku. To vám pomůže zajistit, aby měla každá OU určitý účel, a také čtenáři vašeho plánu snáze pochopí důvody pro vytvoření navrhované struktury.

Při vytváření plánu jednotek OU pro jednotlivé domény spolupracujte s následujícími skupinami v organizaci správy:

- Současní správci domén, kteří zodpovídají za účty uživatelů, skupiny se zabezpečením a účty počítačů.
- Současní vlastníci a správci domén prostředků.

Vytváření jednotek OU pro delegování správy

V předchozích verzích systému Windows bylo delegování správy v doméně omezeno na použití zabudovaných místních skupin, jako je například skupina Account Administrators (správci účtů). Tyto skupiny měly předdefinované schopnosti a v některých případech tyto schopnosti neodpovídaly potřebám konkrétní situace. Výsledkem byly stavy, kdy správci v organizaci potřebovali vysoké úrovně přístupu pro správu, například oprávnění skupiny Domain Administrators (správci domény).

V systému Windows 2000 je delegování správy výkonnější a flexibilnější. Této flexibility se dosahuje kombinací organizačních jednotek, řízení přístupu na úrovni jednotlivých atributů a dědění řízení přístupu. Správu lze libovolně delegovat a umožnit uživatelům vytvářet specifické třídy objektů nebo upravovat určité atributy konkrétních tříd objektů.

Například vaše oddělení lidských zdrojů může získat možnost vytvářet objekty uživatelů v určité OU, ale nikde jinde. Technikům z oddělení podpory lze umožnit resetovat hesla uživatelů v této OU, nikoli však možnost vytvářet uživatele. Dalším správcům adresáře lze dovolit upravovat atributy adresáře objektu uživatele, nikoli však vytvářet uživatele a resetovat hesla.

Delegování správy ve vaší organizaci má několik výhod. Delegování konkrétních práv vám umožňuje minimalizovat počet uživatelů, kteří musejí mít vysokou úroveň přístupu. Nehody nebo chyby způsobené správcem s omezenými možnostmi budou mít vliv jen na oblast jeho zodpovědnosti. V mnoha organizacích bylo dříve nezbytné, aby skupiny s výjimkou oddělení IT předávaly požadavky na změny správcům pracujícím na vyšší úrovni, kteří pak učinili potřebné změny. Pomocí delegování správy můžete zodpovědnost přesunout až na jednotlivé skupiny ve vaší organizaci a vyhnout se tak zdržení a dodatečným nákladům souvisejícím s odesláním požadavků skupinám správců pracujícím na vysoké úrovni.

Úpravy seznamů řízení přístupu

Chcete-li delegovat správu, přidejte nějaké skupině určitá práva vzhledem ke konkrétní OU. Abyste toho dosáhli, musíte upravit seznam řízení přístupu (Access Control List – ACL) dané jednotky OU. Položky řízení přístupu (Access Control Entry – ACE) v seznamu ACL objektu určují, kdo může k objektu přistoupit a jaký druh přístupu je mu zajištěn. Během vytvoření objektu v adresáři se na něj aplikuje výchozí seznam ACL. Výchozí seznam ACL je popsán v definici schématu dané třídy objektu.

Položky ACE mohou být děděny podřízenými (dceřinými) objekty objektu kontejneru. Je-li některý z podřízených objektů také kontejnerem, položky ACE se aplikují také na podřízené objekty tohoto kontejneru. Pomocí dědění můžete aplikovat delegovaná

oprávnění na celý podstrom jednotek OU a nikoli jen na jednu OU. Můžete také zablokovat dědění položky ACE objektu a zabránit tak v aplikování položek ACE z nadřazeného kontejneru na určený objekt nebo jiné podřízené objekty. Položky ACE, které lze dědit, platí pouze v rámci jedné domény a nepřecházejí do podřízených domén.

Chcete-li delegovat řízení nějaké sady objektů v podstromu OU, musíte upravit seznam ACL v dané jednotce OU. Toho nejsnáze dosáhnete použitím Průvodce delegací řízení (Delegation of Control Wizard) v modulu snap-in Uživatelé a počítače služby Active Directory (Active Directory Users and Computers) konzoly Microsoft Management Control (MMC). Chcete-li si zobrazit seznam ACL určitého objektu nebo vykonat pokročilé úpravy seznamu ACL, použijte kartu **Zabezpečení** (Security) okna vlastností daného objektu.

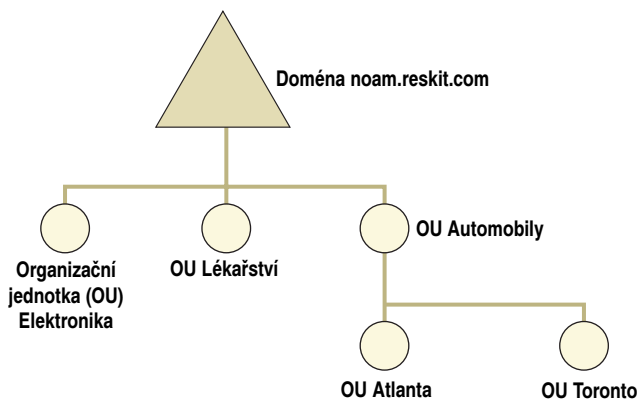
V seznamech ACL se odkazujte vždy na skupiny a nikoli na jednotlivé uživatele. Správa členství v nějaké skupině je jednodušší než správa seznamu ACL určité jednotky OU. Když se změní role uživatelů, je mnohem jednodušší objevit a upravit jejich členství ve skupinách, než zkontrolovat seznamy ACL všech jednotek OU. Je-li to možné, delegujte práva místním skupinám a nikoli globálním nebo univerzálním skupinám. Na rozdíl od globálních skupin mohou místní skupiny obsahovat členy z libovolné důvěryhodné domény, a proto jsou vhodnější k zajištění oprávnění přístupu k prostředkům. Na rozdíl od univerzálních skupin není členství v místních skupinách replikováno do globálního katalogu, a proto jsou místní skupiny méně náročné na prostředky.

Určení vytvořených jednotek OU

Struktura OU, kterou vytvoříte, bude zcela záviset na tom, jak je ve vaší organizaci delegována správa. Možnosti delegování správy jsou:

- Podle fyzického umístění. Například správu objektů v Evropě může mít na starost samostatná skupina správců.
- Podle obchodní či výrobní jednotky. Například správu objektů patřících do oddělení Letectví může mít na starost samostatná skupina správců.
- Podle role nebo úkolu. Toto rozdělení je podle typu spravovaného objektu. Určitá skupina správců tak může být zodpovědná například pouze za objekty účtů počítačů.

Tyto tři dimenze se často kombinují. Například jak je uvedeno na obrázku 9.13, může existovat skupina správy zodpovědná za objekty účtů počítačů v Atlantě pro obchodní jednotku automobilů.



Obrázek 9.13 Dvouvrstvé delegování

To, zda je nebo není OU Atlanta podřízeným objektem OU Automobily, závisí na tom, zda správci jednotky Automobily delegují oprávnění správcům jednotky Atlanta nebo naopak. Je také možné, že správci jednotky Atlanta budou úplně nezávislí na správcích jednotky Automobily – obě jednotky OU si pak budou rovny.

Poznámka Některé organizace mají geograficky rozptýlené skupiny správy, které zajišťují provoz 24 hodin denně. Zkombinovaná normální pracovní doba všech skupin správy dává organizaci pokrytí celých 24 hodin. V takové situaci se dosah jednotlivých skupin správy nevztahuje na konkrétní umístění, protože správci musí být schopni pomáhat uživatelům po celém světě. I když jsou v tomto scénáři správci umístění na mnoha lokacích, nejedná se o příklad delegování vycházející z umístění.

Postupy delegování

Začněte výchozí strukturou v doméně a strukturu OU vytvořte pomocí následujících základních kroků:

- Delegováním plného řízení vytvořte vrchní vrstvy jednotek OU.
- Delegováním řízení podle tříd objektů vytvořte spodní vrstvy jednotek OU.

Delegování plného řízení

Pro začátek si řekněme, že plnou kontrolu nad všemi objekty mají pouze správci domény. V ideálním případě by měli být správci domény odpovědní pouze za tyto činnosti:

- Vytvoření počáteční struktury OU.
- Oprava chyb.

Nejenže mají správci domény standardně k dispozici plné řízení, ale mají také právo převzít vlastnictví libovolného objektu v doméně. Pomocí tohoto práva mohou správci domén získat plnou kontrolu nad libovolným objektem v doméně, bez ohledu na oprávnění nastavená pro daný objekt.

- Vytvoření dalších řadičů domény.

Pouze členové skupiny správců domény mohou vytvářet další řadiče dané domény.

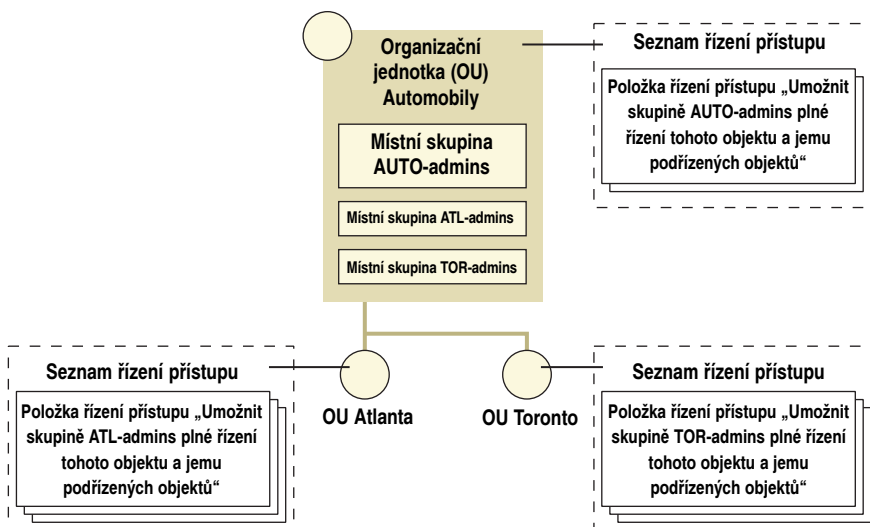
Protože správci domén mohou mít omezené a specifické povinnosti, členství v této skupině lze snadno řídit a počet jejích členů lze udržovat na velmi nízké hodnotě.

Máte-li ve své organizaci oddělení, která si musí sama určit svou strukturu OU a model správy, postupujte takto:

- Pro každé oddělení vytvořte OU.
- Pro každé oddělení představující nejvyšší úroveň správců v daném oddělení vytvořte místní skupinu.
- Odpovídající skupině přiřadte plné řízení její OU.
- Má-li oddělení možnost určovat své členství, umístěte do OU skupinu správců daného oddělení. Nemá-li oddělení možnost samo nastavovat své členství správy, ponechte tuto skupinu mimo OU.

Příklad delegování plného řízení

Oddělení Automobily společnosti Reskit je důsledkem sloučení dvou společností, přičemž si oddělení Automobily ponechalo plně autonomní skupinu IT. V takovém případě obdrží oddělení Automobily z kořene domény svou vlastní jednotku OU. Protože mají také možnost definovat členství ve své skupině správců, tato skupina je vložena do OU Automobily. Má-li samotné oddělení Automobily zcela nezávislé operace v Atlantě a Torontu, správci oddělení Automobily mohou opět vytvořit jednotky OU a delegovat plné řízení. Jak ukazuje obrázek 9.14, správci oddělení Automobily si zachovali možnost nastavovat členství skupin správců v Atlantě a Torontu.



Obrázek 9.14 Delegování plného řízení

Nemáte-li ve své organizaci žádná oddělení vyžadující plné řízení, určí zbývající strukturu OU správci domén.

Delegování řízení podle tříd objektů

Skupiny s plným řízením mohou rozhodnout, zda jsou k delegování omezenějšího řízení zapotřebí další jednotky OU. Nejsnáze toho dosáhnete zvážením jednotlivých tříd objektů vytvářených v adresáři a určením, zda je správa dané třídy objektů dále ve vaší organizaci delegována. Schéma sice definuje mnoho různých druhů tříd objektů, zapotřebí je však zvážit jen třídy objektů, které budou vaši správci vytvářet ve službě Active Directory. Přinejmenším se musíte zabývat:

- objekty účtů uživatelů,
- objekty účtů počítačů,
- objekty skupin,
- objekty organizačních jednotek.

Při zkoumání jednotlivých tříd objektů zvažte samostatně tyto položky:

- Jaká skupina by měla mít plnou kontrolu nad objekty dané třídy? Skupiny s plným řízením mohou vytvářet a odstraňovat objekty zadané třídy a upravovat libovolný atribut objektů zadané třídy.
- Jaké skupiny budou moci vytvářet objekty určité třídy? Standardně mají uživatelé nad objekty, které vytvoří, plnou kontrolu.
- Jaké skupiny budou moci pouze upravovat určité atributy existujících objektů zadané třídy?

V každém případě, kdy se rozhodnete delegovat řízení, musíte:

- vytvořit místní skupinu, která bude moci vykonat specifickou funkci,
- zajistit skupině specifická oprávnění v nejvyšší možné OU.

Poznámka Aby bylo možné přesunout nějaký objekt mezi dvěma jednotkami OU, musí mít správce vykonávající daný přesun možnost vytvořit příslušný objekt v cílovém kontejneru a odstranit objekt ze zdrojového kontejneru. Z tohoto důvodu může být vhodné vytvořit samostatnou skupinu správců, která bude moci přesunovat objekty, a poskytnout jim potřebná oprávnění na společné nadřazené jednotce OU.

Při zavádění aplikací podporujících službu Active Directory může seznam objektů, které je zapotřebí zvážit, narůstat. Některé aplikace však budou v adresáři vytvářet takové objekty, které nevyžadují ruční správu. Například tiskové servery se systémem Windows 2000 automaticky do adresáře publikují tiskové fronty. Protože o správu objektu tiskové fronty se stará samotný tiskový server, není nutné její správu delegovat nějaké speciální skupině správců.

Úpravou seznamu ACL výchozího kontejneru Počítače (Computers) můžete delegovat možnost vytvářet objekty účtů počítačů všem uživatelům, přičemž již není zapotřebí žádná pozornost správy. Účty počítačů se budou ve výchozím kontejneru Počítače vytvářet, když uživatelé připojí nějaký počítač do domény.

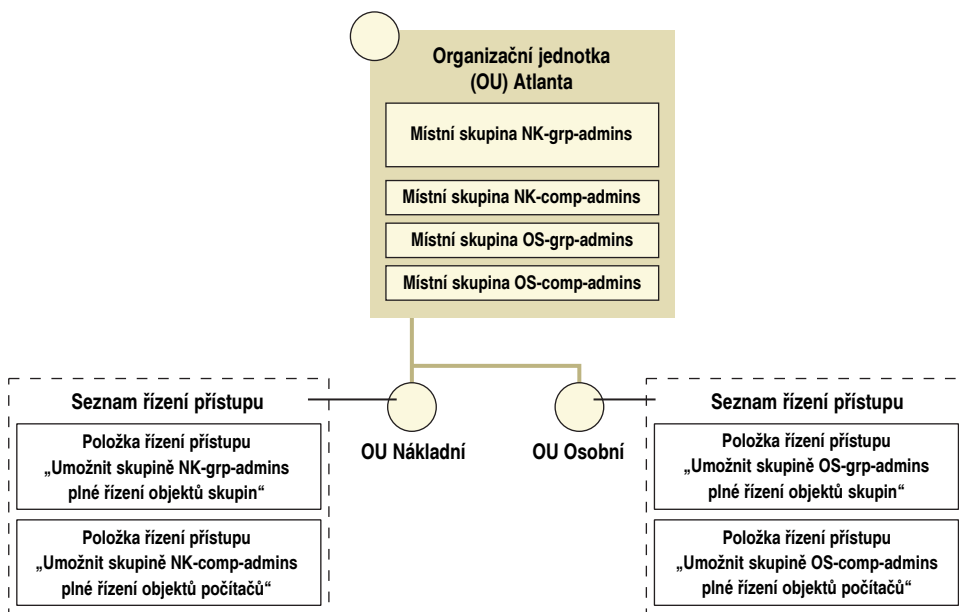
Příklad delegování řízení podle tříd objektů

Lokace Atlanta oddělení Automobily společnosti Reskit je domovem dvou domén prostředků systému Windows NT 4.0, Nákladní a Osobní. Součástí migrace na systém Windows 2000 bude konsolidace těchto dvou domén do domény noam.reskit.com.

Správci domén Nákladní a Osobní používají v současné době tyto domény ke:

- sdílení účtů počítačů mezi členy týmu,
- sdílení místa v systému souborů na záložních řadičích domén (Backup Domain Controllers –BDC) systému Windows NT 4.0, přičemž přístup k systému souborů a místům sdílení je řízen členstvím v místních skupinách.

Pomocí delegování správy je jednoduché nahradit domény prostředků jednotkami OU. V našem případě dojde k vytvoření skupin pro správu jednotlivých druhů objektů – skupinám je následně přiřazeno plné řízení v OU daného projektu. Jednotky OU specifických projektů jsou nezbytné k tomu, aby se zabránilo správcům jednotky Nákladní v možnosti manipulovat s objekty jednotky Osobní a naopak. Obrázek 9.15 ilustruje tento koncept.



Obrázek 9.15 Náhrada domén prostředků

Vytváření jednotek OU pro skrývání objektů

I když uživatel nemá právo číst atributy určitého objektu, jakmile si vytvoří výčet (výpis) obsahu nadřazeného kontejneru, zjistí, že daný objekt existuje. Nejjednodušším a nejvýhodnějším způsobem skrývání objektů je vytvoření speciální OU pro tyto objekty a omezení množiny uživatelů, kteří mají pro danou OU práva Vypisovat obsah (List Contents).

▼ Chcete-li vytvořit OU v zájmu skrývání objektů, postupujte takto:

1. Vytvořte OU, kde budete skrývat objekty.
2. Zobrazte si kartu **Zabezpečení** (Security) okna vlastností dané OU.
3. Z OU odstraňte všechna existující oprávnění.

4. V dialogovém okně **Upřesnit** (Advanced) zrušte zaškrtnutí políčka **Povolit šíření dědičných oprávnění z nadřazeného objektu na tento** (Inherit permissions from parent).
5. Určete skupiny, které mají mít nad danou OU plnou kontrolu. Pomocí karty **Zabezpečení** (Security) okna vlastností těchto skupinám zajistíte plné řízení.
6. Určete skupiny, které mají mít k dané skupině OU a jejímu obsahu obecný přístup pro čtení. Pomocí karty **Zabezpečení** (Security) okna vlastností těchto skupinám zajistíte přístup pro čtení.
7. Určete všechny další skupiny vyžadující nějakou formu přístupu k OU, například právo vytvářet a odstraňovat určitou třídu objektů. Pomocí karty **Zabezpečení** (Security) okna vlastností těchto skupinám zajistíte specifický přístup.
8. Do této OU přesuňte objekty, které chcete skrýt.

Objekty budou moci tímto způsobem skrývat pouze uživatelé, kteří mohou měnit seznam ACL dané jednotky OU.

Vytváření jednotek OU pro zásady skupiny

V systému Windows NT 4.0 můžete k definování konfigurací všech uživatelů a počítačů v doméně použít nástroj Editor systémových zásad (System Policy Editor). V systému Windows 2000 lze k definování konfigurací uživatelů a počítačů použít zásady skupiny (Group Policy) a tyto zásady pak přiřadit sídlům, doménám nebo jednotkám OU. To, zda budete nebo nebudete muset vytvářet dodatečné jednotky OU podporující aplikování zásad skupiny, závisí na vytvořených zásadách a vybraných možnostech implementace. Další informace o zásadách skupiny najdete v kapitolách „Aplikování správy změn a konfigurací“ a „Definování standardů správy a konfigurace klientů“ v této knize.

Změna plánu OU po zavedení

Vytváření nových jednotek OU, přesunování podstromů jednotek OU v doméně, přesunování objektů mezi jednotkami OU v téže doméně a odstraňování jednotek OU, to všechno jsou jednoduché úkoly.

Přesunem objektu nebo podstromu objektů dojde ke změně nadřazeného (mateřského) kontejneru daných objektů. Položky ACE zděděné z bývalého nadřazeného kontejneru již nebudou platit a mohou se tu objevit nové položky ACE zděděné od nového nadřazeného kontejneru. Chcete-li se vyhnout neočekávaným změnám v možnostech přístupu, předem vyhodnoťte, o jaké změny se bude jednat, a určete, zda budou mít tyto změny nějaký vliv na uživatele, které k daným objektům v současné době přistupují a spravují je.

Přesun objektu uživatele, objektu počítače nebo podstromu obsahujícího objekty uživatelů nebo počítačů může změnit zásady skupiny aplikované na dané objekty. Chcete-li se vyhnout neočekávaným změnám konfigurací klientů, vyhodnoťte změny v zásadách skupiny a zajistěte, aby byly pro koncové uživatele přijatelné.

Vytvoření plánu topologie sídel

Topologie sídel služby Active Directory je logická reprezentace fyzické sítě. Topologie sídel je definována na základě jednotlivých doménových struktur. Klienti a servery služby Active Directory používají topologii sídel doménové struktury k výhodnému směrování provozu dotazů a replikací. Topologie sídel vám také pomáhá učit, kam je zapotřebí na síť umístit řadiče domén. Při návrhu topologie sídel pamatujte na následující klíčové koncepty:

Sídlo je množina sítí s rychlým, spolehlivým propojením.

Sídlo (sít) je definováno jako množina podsítí IP propojených rychlými, spolehlivými linkami. Obecně platí, že se za rychlé sítě považují sítě s rychlostí LAN a vyšší.

Propojení sítí je linka s malou šířkou pásma nebo nespolehlivá linka propojující dvě nebo více sídel.

Propojení sítí (spojení mezi sídly) se používají k modelování množství dostupné šířky pásma mezi dvěma sídly. Obecně platí, že libovolné dvě sítě propojené linkou pomalejší než je rychlost LAN, se považují za propojení mezi sídly. Rychlá linka, která však pracuje na hranici své kapacity a má tak nízkou efektivní šířku pásma, může být také považována za propojení mezi sídly. Propojení mezi sídly mají čtyři parametry:

■ Náklady

Hodnota nákladů na propojení mezi sídly pomáhá replikačnímu systému určit, kdy se má použít tato linka a kdy jiné linky. Hodnoty nákladů určují cesty vaší sítí, kdy bude probíhat replikace.

■ Časový plán replikace

Propojení mezi sídly má svůj časový plán určující, v kterých denních hodinách je linka dostupná pro přenos replikačního provozu.

■ Interval replikace

Interval replikace určuje, jak často systém zjišťuje na řadičích domén na druhém konci propojení mezi sídly replikační změny.

■ Přenos

Přenos (transport) používaný pro replikaci.

Klientské počítače se nejprve snaží komunikovat se servery umístěnými na stejném sídle jako daný klient.

Když uživatel zapne klientský počítač, počítač odešle zprávu náhodně vybranému řadiči domény, jejímž členem klient je. Tento řadič domény určí sídlo, v němž se klient nachází, na základě jeho adresy IP a název sídla vrátí klientovi. Klient si tuto informaci uloží do mezipaměti a použije ji v příštím okamžiku, kdy hledá nějaký replikovaný server v sídle.

Replikace služby Active Directory používá topologii sídel k vytváření replikačních spojení.

Kontrolor konzistence znalostí (Knowledge Consistency Checker – KCC) je zabudovaný proces, který vytváří a udržuje replikační spojení mezi řadiči domén. K vytváření těchto spojení se používají informace o topologii sídel. Replikace v rámci sídla je vyladěna na minimalizování čekací doby replikace a replikace mezi sídly je vyladěna na minimalizování využití šířky pásma. Tabulka 9.1 ukazuje rozdíly mezi replikacemi v rámci sídla a mezi sídly.

Tabulka 9.1 Replikace v sídle a mezi sídly

Replikace v sídle	Replikace mezi sídly
Replikační provoz není komprimován, aby se šetřil čas procesorů.	Replikační provoz je komprimován, aby se šetřila šířka pásma.
Replikační partneři se vzájemně upozorňují na potřebu replikace změn, aby se snížila čekací doba replikace.	Replikační partneři se vzájemně neupozorňují na potřebu replikace změn, aby se šetřila šířka pásma.
Replikační partneři se pravidelně vzájemně dotazují na změny.	Replikační partneři se v intervalu dotazování replikace vzájemně dotazují na změny, avšak pouze během naplánovaných period.
Replikace používá přenos voláním vzdálené procedury (Remote Procedure Call – RPC).	Replikace používá přenos protokoly TCP/IP nebo SMTP.
Replikační připojení lze vytvořit mezi libovolnými dvěma řadiči domén, které se nacházejí v jednom sídle. Proces KCC vytváří připojení k více řadičům domén, aby se snížila čekací doba replikace.	Replikační připojení se vytvářejí pouze mezi servery předmostí. Jeden řadič domény z každé domény v sídle je kontrolorem KCC označen za server předmostí. Server předmostí zpracovává veškeré replikace mezi sídly pro danou doménu. Kontrolor KCC vytváří spojení mezi servery předmostí (bridgehead) cestou nejnižších nákladů, podle nákladů na linky propojení sídel. KCC vytvoří připojení cestou vyšších nákladů, pouze pokud není dosažitelný žádný z řadičů domén na cestách s nižšími náklady.

Informace o topologii sídel jsou uloženy v kontejneru konfigurace.

Sídla, propojení mezi sídly a podsítě jsou všechny uloženy v kontejneru konfigurace, který se replikuje na všechny řadiče domén v doménové struktuře. Každý řadič domény v doménové struktuře má úplné znalosti o topologii sídel. Změna topologie sídel má za následek replikaci na každý řadič domény v doménové struktuře.

Poznámka Topologie sídel je naprosto samostatná a nijak nesouvisí s hierarchií domén. Sídlu může obsahovat mnoho domén a stejně tak doména může obsahovat mnoho sídel.

Proces plánování topologie sídel

K vytvoření topologie sídel v doménové struktuře použijte následující postup:

- Začněte topologií fyzické sítě a definujte sídla a spojení mezi sídly.
- Do sídel umístěte servery.
- Zjistěte, jak změny topologie sídel po zavedení ovlivní koncové uživatele.

Při vytváření plánu topologie sídel bude muset nespíše spolupracovat s:

- týmy spravujícími a sledujícími implementaci protokolu TCP/IP na vaší síti,
- správci jednotlivých domén v doménové struktuře.

Další informace o sídlech a všech tématech popisovaných v tomto oddílu najdete v knize *Microsoft Windows 2000 Server Distribuované systémy*

Definování sídel a propojení mezi sídly

Chcete-li vytvořit topologii sídel doménové struktury, vezměte si fyzickou topologii sítě a vytvořte obecnější topologii vycházející z dostupných šířek pásma a spolehlivosti sítě.

Pokud jste při vytváření plánu domén vykonali fyzické rozdělení, můžete jako počáteční bod topologie sídel použít již vytvořený plán topologie sídel a umístění řadičů domén. Pokud jste přeskočili fyzické dělení popsané dříve v této kapitole, doporučujeme vám přečíst si oddíl „Určení počtu domén v jednotlivých doménových strukturách“ a vytvořit základní topologii sídel právě nyní.

Při vytváření topologie sídel je užitečné mít k dispozici úplnou mapu fyzické topologie sítě. Tato mapa by měla obsahovat seznam fyzických podsítí na vaší síti, typ média a rychlost u každé sítě a propojení mezi jednotlivými sítěmi.

Vytváření sídel

Nejprve vytvořte seznam sídel na vaší síti.

- Vytvořte sídlo pro každou síť LAN nebo množinu sídel LAN, které jsou propojeny vysokorychlostním páteřním spojením, a sídlu přiřadte název. Konektivita v rámci sídla musí být spolehlivá a vždy dostupná.
- Vytvořte sídlo pro každou lokaci, která nemá přímou konektivitu ke zbytku vaší sítě a je dosažitelná jen prostřednictvím elektronické pošty SMTP.
- Určete, která sídla nebudou mít místní řadiče domén a tato sídla slučte s jinými sousedními sídly. Sídla pomáhají výhodně směřovat provoz od klientů k řadičům domén a mezi řadiči domén. Není-li v sídle žádný řadič domény, není tu žádný replikační provoz do sídla, který by bylo zapotřebí řídit.

Pro každé sídlo přidávané do plánu si poznamenejte sadu podsítí IP, které dané sídlo tvoří. Tyto informace budete potřebovat později při vytváření sídel v adresáři.

Poznámka Názvy sídel se používají v záznamech registrovaných v systému DNS lokátorem domény, takže se musí jednat o platné názvy DNS. Doporučujeme vám v názvech sídel používat pouze standardní znaky A–Z, a–z, 0–9 a rozdělovník (–).

Pamatujte, že klienti se nejprve budou pokoušet komunikovat s řadiči domén v sídle, ve kterém se nacházejí – pak teprve se budou snažit komunikovat s řadiči domén v jiných sídlech. Jestliže je šířka pásma mezi sadou sítí tak velká, že vám nezáleží na tom, zda klient na jedné síti komunikuje se serverem na jiné síti, pak můžete tyto sítě považovat za jediné sídlo.

Nachází-li se klient na podsíti, která není definovaná v adresáři, nepovažuje se za součást sídla a vybírá si náhodně ze všech řadičů ve své doméně. Můžete se setkat se situacemi, kdy nejsou v adresáři definované všechny podsítě, například po přidání nových podsítí do sítě. Chcete-li tyto klienty přiřadit nějakému sídlu, vytvořte dvě výchozí podsítě ukázané v tabulce 9.2 a pak je přiřadte danému sídlu.

Tabulka 9.2 Výchozí podsítě

ID podsítě	Maska	Popis
128.0.0.0	192.0.0.0	Zachytává všechny klienty na sítích třídy B, kteří nejsou ještě definováni v adresáři.
192.0.0.0	224.0.0.0	Zachytává všechny klienty na sítích třídy C, kteří nejsou ještě definováni v adresáři.

Neexistuje žádná výchozí podsít pro klienty na síti třídy A.

Jestliže jsou dvě sítě odděleny linkami, které jsou výrazně zatěžovány v některých dnech a prakticky volné v jiných časech, pak tyto sítě umístěte do samostatných sídel. Můžete využít možnosti časově naplánovat replikaci mezi sídly a předejít tak tomu, aby replikační provoz bránil během pracovních hodin jinému provozu.

Je-li celá vaše síť tvořena rychlou, spolehlivou konektivitou, můžete ji celou považovat za jediné sídlo.

Propojení sídel linkami

Dále propojte sídla linkami, čímž naznačíte fyzickou konektivitu vaší sítě. Každé lince mezi sídly přiřadte název.

Propojení mezi sítěmi jsou přenosná, takže pokud je sídlo A připojeno k sídlu B a sídlo B je připojeno k sídlu C, pak proces KCC předpokládá, že řadiče domén v sídle A mohou komunikovat s řadiči domén v sídle C. Mezi sídly A a C musíte zakreslit spojení, pouze pokud tu skutečně existuje nějaké nezávislé síťové propojení mezi těmito sídly.

U každého vytvořeného propojení mezi sídly si poznamenejte následující informace:

- Časový plán replikace

K výzvě k replikaci dochází pouze během naplánovaného času či časů v sedmidenním intervalu. Výchozí časový plán linky umožňuje výzvu k replikaci kdykoli v daném sedmidenním intervalu.

- Replikační interval

K výzvě k replikaci dochází v zadaném intervalu, když časový plán replikaci umožňuje. Výchozí interval výzvy je tři hodiny.

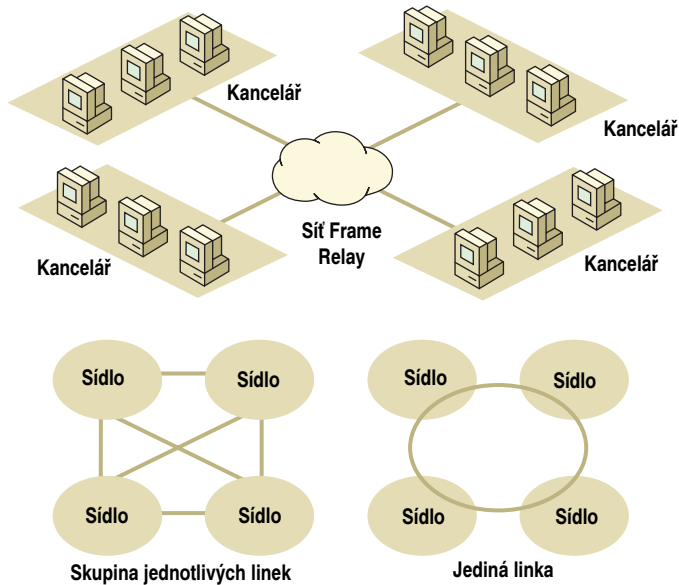
- Replikační přenos

Je-li dané sídlo dostupné pouze protokolem SMTP, vyberte jako protokol přenosu SMTP. Jinak vyberte přenos protokolem TCP/IP.

- Náklady na linku

Každé lince mezi sídly přiřadte náklady, které budou odrážet dostupnou šířku pásma nebo cenu šířky pásma v porovnání s jinými linkami mezi sídly.

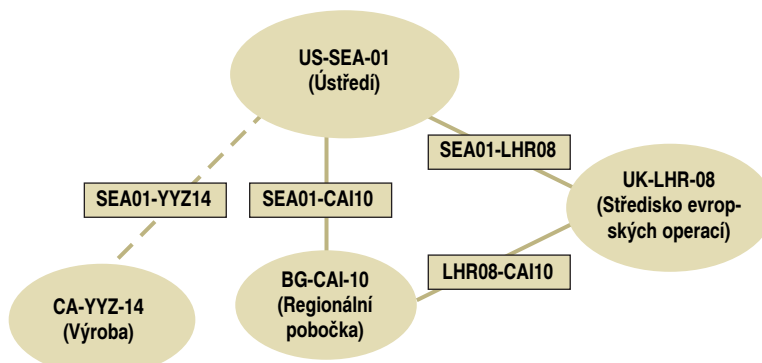
Páteří spojení propojující mnoho sídel lze reprezentovat jedinou linkou mezi sídly propojující mnoho sídel – nemusíte vytvářet skupinu propojení mezi sídly. To je užitečná možnost omezení počtu spojení mezi sídly, které je zapotřebí vytvořit a spravovat, má-li stejné charakteristiky mnoho linek. Obrázek 9.16 ilustruje, jak lze síť Frame Relay propojující čtyři kanceláře znázornit jedinou linkou místo šesti jednotlivých linek.



Obrázek 9.16 Jediná linka a skupina linek

Poznámka Časový plán replikace určuje, kdy se určitý řadič domény dotazuje u svých replikačních partnerů na změny. Pokud při skončení časového okna ještě probíhá replikační cyklus, dojde k jeho dokončení.

Obrázek 9.17 ukazuje topologii sídel společnosti Reskit. Konvence vytváření názvů sídel využívá kombinaci regionálního kódu, kódu nejbližšího letiště a identifikačního čísla. Názvy spojení mezi sídly zahrnují názvy propojených sídel.



Obrázek 9.17 Topologie sídel společnosti Reskit

Tabulka 9.3 zobrazuje parametry jednotlivých spojení mezi sídly v topologii sídel společnosti Reskit.

Tabulka 9.3 Parametry spojení mezi sídly topologie sídel společnosti Reskit

Propojení sídel	Přenos	Náklady	Interval dotazování	Časový plán
SEA01-YYZ14	SMTP	100	30 minut	0500 až 0900 UTC denně
SEA01-CAI10	IP	100	30 minut	2000 až 0400 UTC denně
SEA01-LHR03	IP	25	1 hodina	(stále)
LHR03-CAI10	IP	50	15 minut	2000 až 0400 UTC denně

Replikace je v případě spojení mezi výrobním závodem a ústředím časově naplánována tak, aby k ní docházelo pouze mimo pracovní dobu. Replikace mezi regionální pobočkou a ostatními sídly je také naplánována na mimopracovní dobu. Jelikož jsou náklady na linku mezi regionální pobočkou a střediskem operací nižší, než náklady na linku mezi regionální pobočkou a ústředím, proces KCC se pokusí uskutečnit připojení nejprve se servery předmostí ve středisku operací, pak teprve se servery předmostí v ústředí. Časový plán pro spojení mezi ústředím a střediskem operací je stále otevřený, k omezení provozu však používá delší interval dotazování.

Umístění serverů do sídel

Umístění serverů ve vaší topologii sídel má přímý vliv na dostupnost služby Active Directory. Během fyzického dělení v plánu domén jste vytvořili základní plán umístění řadičů domén. Umístěním serverů do topologie sídel dokončíte podrobnosti tohoto plánu.

Umístění dodatečných řadičů domén

Během rozdělování jste určili, která sídla budou mít jednotlivé řadiče domén, neurčili jste však počet řadičů domén umístěných v jednotlivých sídlech každé domény. Počet řadičů domén vytvořených pro určitou doménu je určen dvěma faktory: požadavky na odolnost proti chybám a požadavky na rozdělování zatížení.

U jednotlivých domén určete, zda jsou zapotřebí další řadiče domény, následujícím postupem:

Vždy vytvořte alespoň dva řadiče domény.

I v případě malých domén s malým počtem uživatelů vytvořte alespoň dva řadiče domény, aby v doméně nevznikal jediný bod selhání.

U každého sídla s jediným řadičem domény určete, zda budete v procesu překlopení důvěřovat spojení WAN.

Dojde-li k selhání jediného řadiče domény, klienti v daném sídle mohou být obsluhováni jinými řadiči téže domény, které se nacházejí v jiných sídlech. Je-li konektivita sítě nespolehlivá nebo občas nedostupná, nemůžete síti důvěřovat, že zvládne překlopení. V takovém případě umístěte do daného sídla druhý řadič domény.

Do sídla umístěte dodatečný řadič domény, který bude zpracovávat zatížení klientů.

Počet klientů, které dokáže určitý server zvládnout, závisí na charakteristikách zatížení a hardwarové konfiguraci serveru. Klienti si náhodně vybírají dostupné řadiče domény v sídle, čímž se zatížení klientů rovnoměrně distribuuje.

Umístění serverů globálního katalogu

Dostupnost serverů globálního katalogu je pro operaci adresáře naprosto zásadní. Server globálního katalogu musí být například dostupný při zpracovávání požadavku na přihlášení uživatele v doméně pracující v nativním režimu nebo při přihlašování uživatele pomocí hlavního uživatelského jména.

Poznámka Při zpracovávání požadavku na přihlášení uživatele v doméně pracující v nativním režimu odesílá řadič domény serveru globálního katalogu dotaz, kterým se určuje členství daného uživatele v univerzálních skupinách. Protože skupinám lze explicitně zakázat přístup k nějakému prostředku, jsou úplné znalosti o členství uživatele ve skupinách nezbytným předpokladem správného zavedení řízení přístupu. Pokud řadič domény pracující v nativním režimu nedokáže kontaktovat server globálního katalogu během požadavku na přihlášení uživatele, řadič domény daný požadavek na přihlášení odmítne.

Obecně platí, že byste v každém sídle měli určit alespoň jeden řadič domény jako server globálního katalogu.

K určení, zda jsou v jednotlivých sídlech zapotřebí další servery globálního katalogu, použijte stejná pravidla překlopení a vyrovnávání zatížení, jako v případě jednotlivých řadičů domén.

Poznámka V prostředí s jedinou doménou nejsou ke zpracování požadavku na přihlášení uživatele servery globálního katalogu zapotřebí. Přesto byste však měli určit servery globálního katalogu uvedeným postupem. Klienti totiž používají servery globálního katalogu při vyhledávání. Navíc budete-li již mít v provozu servery globálního katalogu, umožní to vašemu systému jednoduchou adaptaci, jestliže později přidáte nějaké domény.

Umístění serverů DNS

Dostupnost systému DNS přímo ovlivňuje dostupnost služby Active Directory. Klienti se na službu DNS spoléhají při vyhledávání nějakého řadiče domény a řadiče domén se na službu DNS spoléhají při vyhledávání jiných řadičů domén. I když již na své síti máte zavedené servery DNS, možná budete muset upravit jejich počet a umístění tak, aby to odpovídalo potřebám klientů a řadičům domén služby Active Directory.

Obecně platí, že do každého sídla byste měli umístit alespoň jeden server DNS. Server DNS v sídle musí být autoritativní pro záznamy lokátoru (vyhledávače) domén v sídle, aby klienti nemuseli používat k vyhledání řadičů domén v sídle nějaké servery DNS, které se nacházejí mimo toto sídlo. Řadiče domén budou také periodicky ověřovat, že jsou položky na primárním hlavním serveru pro každý záznam lokátoru správné.

Jednoduchou konfigurací naplňující všechny tyto požadavky je použít službu DNS integrovanou se službou Active Directory, ukládat záznamy lokátoru určité domény přímo v této doméně a spouštět službu DNS systému Windows 2000 na jednom nebo více řadičích domén jednotlivých sídel, kde se tyto řadiče domén nacházejí.

Distribuce záznamů lokátoru celé doménové struktury

Každý řadič domény v doménové struktuře registruje dvě sady záznamů lokátoru: sadu záznamů specifických domén, které končí označením <název-domény-DNS>, a sadu záznamů celé doménové struktury, které končí označením _msdcs.<název-domény-

DNS>. Záznamy celé doménové struktury jsou zajímavé pro klienty a řadiče domén ze všech částí doménové struktury. V záznamech celé doménové struktury jsou například obsaženy záznamy lokátoru globálního katalogu a záznamy používané replikačním systémem k vyhledání replikačních partnerů.

Aby mohlo dojít k replikaci mezi libovolnými dvěma řadiči domén, včetně dvou řadičů v téže doméně, musí být schopny vyhledat záznamy lokátoru celé doménové struktury. Aby se mohl nově vytvořený řadič domény účastnit replikace, musí být schopen zaregistrovat své záznamy celé doménové struktury v systému DNS a ostatní řadiče domén musí být schopny tyto záznamy vyhledat. Proto je důležité zpřístupnit záznamy lokátoru celé doménové struktury všem serverům DNS ve všech sídlech.

Dosáhnete toho tím, že vytvoříte samostatnou zónu nazvanou *_msdcs.<název-domény-DNS>* a tuto zónu replikujete na všechny servery DNS. Používáte-li jednoduchou konfiguraci s integrovanou službou Active Directory, můžete umístit primární kopii této zóny do kořenové domény doménové struktury společně se zónou *<název-domény-DNS>*. Pak můžete tuto zónu replikovat na servery DNS mimo doménu pomocí standardní replikace systému DNS.

Obvykle nedostačuje replikovat tuto zónu pouze na jeden server DNS v jednotlivých sídlech. Nemá-li nějaký server DNS místní kopii zóny *_msdcs.<název-domény-DNS>*, musí k vyhledání nějakého názvu v této zóně použít rekurzi DNS. Při vykonávání rekurze kontaktuje server DNS jiný server DNS, který je autoritativní pro kořen oboru názvů (kořenový server DNS), a postupuje směrem dolů delegováním v systému DNS, dokud nenajde požadovaný záznam. Není-li v sídle kořenový server DNS a spojení mezi tímto sídlem a ostatními sídly selhalo, daný server DNS nemůže rekurzi vykonat. Proto nebude schopen nalézt žádné servery DNS, které jsou autoritativní pro *_msdcs.<název-domény-DNS>*, i když se tyto servery DNS nacházejí v témže sídle.

Konfigurace klientů DNS

Klienti a řadiče domén by měli mít nakonfigurovány alespoň dvě adresy IP serverů DNS: preferovaného místního serveru a alternativního serveru. Alternativní server se může nacházet v místním sídle a může být také vzdálený, pokud důvěřujete své síti v tom ohledu, že zvládne překlopení.

Změna topologie sídel po zavedení

Topologie sídel doménové struktury je po počátečním zavedení velmi flexibilní a snadno se mění. Během vývoje fyzické sítě nezapomínejte vyhodnocovat a upravovat topologii sídel. Jestliže nějaké změny v síti zvýší nebo sníží šířku pásma či spolehlivost, nezapomeňte vytvořit nebo odstranit sídla a spojení mezi sídly a také vyladit parametry spojení mezi sídly a vyrovnat tak čekací dobu replikace s využitím šířky pásma.

Ještě než zadáte změny do topologie sídel, prozkoumejte vliv těchto změn na dostupnost, čekací dobu replikace a šířku pásma replikace a možné dopady těchto položek na koncové uživatele. Protože je topologie sídel uložena v kontejneru konfigurace, změny se budou replikovat na každý řadič domény v doménové struktuře. Časté změny topologie sítě budou způsobovat značný replikační provoz, takže je lepší změny postupně zadávat v několika větších krocích než v mnoha malých. V závislosti na topologii a časovém plánu replikace může trvat velmi dlouho, než změny topologie dosáhnou všech řadičů domén v doménové struktuře.

Seznam úkolů plánování návrhu struktury služby Active Directory

Tabulka 9.4 vám pomůže s kontrolou splnění všech základních úkolů návrhu struktury služby Active Directory.

Tabulka 9.4 Seznam úkolů plánování služby Active Directory

Úkol	Umístění v kapitole
Určete počet doménových struktur.	Vytvoření plánu doménových struktur
Pro každou doménovou strukturu vytvořte zásady řízení změn.	Vytvoření plánu doménových struktur
Určete počet domén v jednotlivých doménových strukturách.	Vytvoření plánu domén
Vyberte kořenovou doménu doménové struktury.	Vytvoření plánu domén
Všem doménám přiřadte názvy DNS.	Vytvoření plánu domén
Naplánujte zavedení serverů DNS.	Vytvoření plánu domén
Optimalizujte ověřování pomocí explicitních vztahů důvěryhodnosti.	Vytvoření plánu domén
Vytvořte jednotky (útvary) OU pro delegování správy.	Vytvoření plánu organizačních jednotek
Vytvořte jednotky OU pro skrývání objektů.	Vytvoření plánu organizačních jednotek
Vytvořte jednotky OU pro zásady skupiny.	Vytvoření plánu organizačních jednotek
Definujte sídla a spojení mezi sídly.	Vytvoření plánu topologie sídel
Umístěte do sídel servery.	Vytvoření plánu topologie sídel

KAPITOLA 10

Určení strategií migrace domén



Úspěšná migrace ze systémů Microsoft Windows NT 3.51 a Microsoft Windows NT 4.0 na systém Microsoft Windows 2000 vyžaduje pečlivou analýzu aktuálního systému a dokonalé plánování. S doporučenými konfiguracemi a postupy popsány v této kapitole se musí seznámit síťoví technici, kteří se starají o logický návrh procesu inovace. Uvedená doporučení sice platí i pro menší organizace, důraz je však v této kapitole kladen na organizace s přinejmenším 2500 osobními počítači.

Jelikož je zaměřením této kapitoly plánování inovace a restrukturalizace domén a plánování oboru názvů adresářové služby Microsoft Active Directory prostřednictvím inovace domén systému Windows NT, musí již být dokončena většina plánování oboru názvů služby Active Directory. Další podmínkou pro plné pochopení této kapitoly je znalost následujících témat: funkcí, které lze zavést v systému Windows 2000, cílů zavádění systému ve vaší organizaci, aktuálního modelu domény vaší organizace a inventáře hardwaru a softwaru ve vaší stávající síťové konfiguraci.

V této kapitole

Začátek procesu plánování migrace 260

Plánování inovace domén 267

Plánování restrukturalizace domén 292

Nástroje migrace domén 305

Seznam úkolů plánování migrace 307

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Postup projektu migrace
- Revidovaný dokument plánování oboru názvů služby Active Directory
- Plán migrace domén

Související informace v sadě Resource Kit

- Další informace o službě Active Directory, návrhu oboru názvů systému Domain Name System (DNS), topologii sídel a skupinách najdete v kapitole „Návrh struktury služby Active Directory“ v této knize.
- Další informace o automatizaci instalace systému Windows 2000 Server najdete v kapitole „Automatizování instalace a inovace serveru“ v této knize.
- Další informaci o automatizaci instalace systému Windows 2000 Professional najdete v kapitole „Automatizování instalace a inovace klientů“ v této knize.

Začátek procesu plánování migrace

Než se pustíte do inovace či restrukturalizace domén, musíte porozumět plánovacímu procesu.

Poznámka Postupy a návrhy v této kapitole vycházejí z inovace neklonovaných počítačů. Inovace na systém Windows 2000 Server je podporována pouze z počítačů se systémy Windows NT Server 3.51 a Windows NT Server 4.0. Starší verze nelze inovovat na systém Windows 2000 Server. V této kapitole označuje termín „Windows NT“ jak verzi 3.51 tak i verzi 4.0 systému Windows NT Server.

Fáze procesu plánování

Proces plánování migrace domén sestává z následujících fází:

1. Návrh doménové struktury systému Windows 2000. Informace o návrhu doménové struktury systému Windows 2000 najdete v kapitole „Návrh struktury služby Active Directory“ v této knize.
2. Plán migrace domén systému Windows NT na nativní domény Windows 2000 a zavedení nových funkcí systému Windows 2000 Server.
3. Plán restrukturalizace domén systému Windows 2000.

Tato fáze není nutná, nebo jí bude zapotřebí až v budoucnosti – to závisí na požadavcích vaší organizace. Další informace o restrukturalizaci domén najdete v oddílu „Plánování restrukturalizace domén“ dále v této kapitole.

Obrázek 10.1 ukazuje základní kroky potřebné k migraci na systém Windows 2000 Server. Tato kapitola podrobně zkoumá jednotlivé uvedené kroky od fáze počátečního plánování přes specifické úkoly inovace a restrukturalizace domén.

Určení postupné migrace

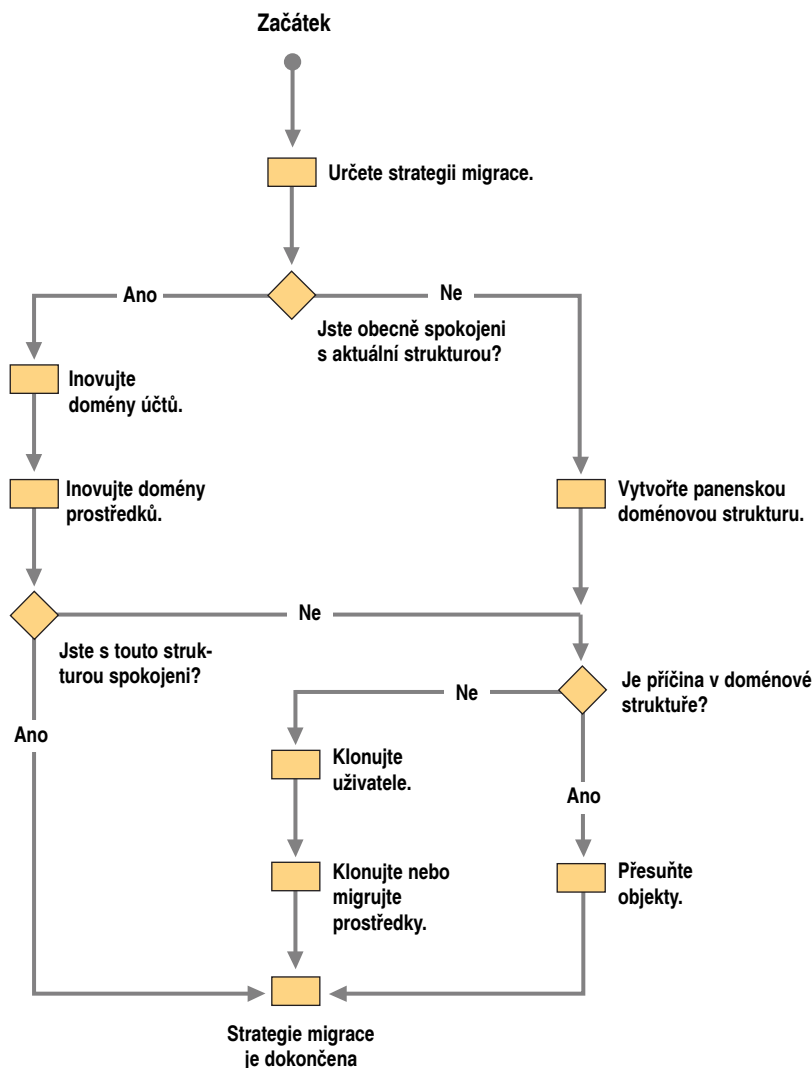
V každém procesu plánování je normální učinit a vyjasnit důležitá rozhodnutí. Rozhodnutí činěná během plánování migrace mohou zapříčinit odložení zavedení určitých funkcí systému až na pozdější dobu. Prvním krokem při vytváření cesty postupné migrace je identifikování a určení priorit cílů migrace a pochopení všech důsledků svých rozhodnutí.

Jestliže jste se rozhodli migrovat na systém Windows 2000, nepochybně jste našli nějaké funkce a výhody, které byste rádi zavedli. Následující oddíl uvádí některé typické cíle migrace a vysvětluje klíčové koncepty a jejich dopady na tyto cíle. Po přečtení tohoto oddílu byste měli mít k dispozici dostatek informací pro dokončení postupu projektu migrace.

Cíle migrace

Plánování migrace musí odrážet vaše primární cíle migrace. Tyto cíle mohou souviset s obchodem či výrobou nebo mohou souviset se samotnou migrací.

Ve většině případů je počáteční rozhodnutí o migraci dáno obchodními či výrobními zájmy. Příklady takových cílů je vyšší škálovatelnost a zlepšené zabezpečení. Obchodní či výrobní cíle jsou také součástí voleb implementace a lze je použít k vyhodnocení možných kompromisů. Obvykle je připravena určitá forma tabulky kompatibility, která se v pozdějších fázích používá k určení technologií a funkcí produktu implemento-



Obrázek 10.1 Vývojový diagram plánu migrace

vaných na konečné platformě. Tyto technologie a funkce vám pomohou dosáhnout obchodních či výrobních cílů.

Cíle související s migrací mohou zahrnovat takové zájmy, jako je vliv přerušení provozu obchodního či výrobního systému, konečný výkon systému a způsoby zvýšení střední doby mezi poruchami. Tyto cíle mohou formulovat testovací plány a kritéria přijatelnosti.

Cíle související s migrací nevycházejí z potřeby implementovat určité technické funkce systému Windows 2000 Server, ale souvisejí spíše se samotným procesem migrace. Některé cíle související s migrací jsou uvedeny v tabulce 10.1.

Tabulka 10.1 Cíle související s migrací

Cíle	Důsledky pro proces migrace
Minimalizace přerušení provozu produkčního prostředí	Uživatelský přístup k datům, prostředkům a aplikacím je zapotřebí udržovat během migrace i po ní. Během migrace a po ní musí také zůstat zachováno prostředí, které již uživatelé znají.
Udržení výkonu systému	Uživatelský přístup k datům, prostředkům a aplikacím je zapotřebí udržovat během migrace i po ní. Během migrace a po ní musí také zůstat zachováno prostředí, které již uživatelé znají.
Zvýšení střední doby mezi poruchami	Uživatelský přístup k datům, prostředkům a aplikacím je zapotřebí udržovat během migrace i po ní. Během migrace a po ní musí také zůstat zachováno prostředí, které již uživatelé znají.
Minimalizace dalších potřeb správy	Je zapotřebí dokonale migrovat uživatelské účty. Je-li to možné, uživatelům musí zůstat zachována hesla. Správci by měli navštěvovat klientský počítač jen minimálně. Je zapotřebí jen minimálně zadávat nová oprávnění k prostředkům.
Maximalizace „rychlých řešení“	Podnik potřebuje získat co nejrychlejší přístup ke klíčovým funkcím nové platformy.
Udržení zabezpečení systému	Zásady zabezpečení by měly být ovlivněny jen minimálně.

Chcete-li získat maximální výhody technologií systému Windows 2000 a plně realizovat své cíle migrace, doporučujeme vám co nejdříve se přepnout do nativního režimu domén Windows 2000. V závislosti na existující síťové konfiguraci však může být možné přepnout se do nativního režimu až po odstranění všech záložních řadičů domén (BDC) Windows NT z domény. Definici nativního režimu najdete v oddílu „Určení okamžiku přechodu na nativní režim“ dále v této kapitole.

Uvědomte si, že klienty a členské servery systému Windows 2000 můžete zavést ještě před inovací infrastruktury domény. Přečtěte si oddíl „Inovace klientů a serverů“ dále v této kapitole.

Koncepty migrace

Požadované infrastruktury můžete dosáhnout dvěma způsoby:

- Inovací domény, která se někdy označuje za „inovaci na místě“ nebo jen „inovaci“.
Inovace domény je proces inovace primárního řadiče domény (Primary Domain Controller – PDC) a záložních řadičů BDC domény Windows NT ze systému Windows NT Server na systém Windows 2000 Server.

- Restrukturalizací domény, která se někdy označuje za „konsolidaci domény“.

Restrukturalizace domény je úplně nový návrh struktury domény, jehož výsledkem je obvykle méně větších domén. Tato možnost je určena těm, kteří nejsou spokojeni s aktuální strukturou domén nebo kteří mají pocit, že nemohou dosáhnout inovace, aniž by to mělo výrazný vliv na produkční prostředí.

Inovace a restrukturalizace se obvykle vzájemně nevylučují; některé organizace mohou nejprve inovovat a pak restrukturalizovat, jiné mohou hned začít restrukturalizací. Obě volby vyžadují před svou implementací důkladné promyšlení a plánování.

Inovace klientů a serverů

Třebaže je zaměřením této kapitoly inovace a restrukturalizace domén, neznamená to, že musíte odložit zavedení klientů a členských serverů systému Windows 2000 až na dobu po dokončení inovace infrastruktury domény. Klienty a servery systému Windows 2000 můžete používat již v existujícím prostředí Windows NT a získat tak okamžité řadu výhod představovaných novými technologiemi. Tabulka 10.2 uvádí některé výhody, které získáte jednoduchou inovací klientů a serverů na systém Windows 2000.

Tabulka 10.2 Výhody jednoduché inovace klientů a serverů

Výhoda	Funkce
Spravovatelnost	Technologie Plug-and-Play Průvodce hardwarem a Správce zařízení (Device Manager) Podpora rozhraní Universal Serial Bus (USB) Konzola Microsoft Management Console Nový nástroj Zálohování (Backup)
Nástroje instalace a řešení problémů	Automatická instalace aplikací umožňuje správcí určit sadu aplikací, které jsou uživateli nebo skupině uživatelů vždy dostupné. Není-li v okamžiku potřeby požadovaná aplikace k dispozici, automaticky se do systému nainstaluje.
Podpora systému souborů	Mezi vylepšení systému NTFS 5.0 patří podpora diskových kvót, schopnost defragmentovat adresářové struktury a používat komprimované síťové vstupy a výstupy. Systém FAT32
Aplikační služby	Model ovladačů Win32 Technologie DirectX 5.0 Nástroj Windows Script Host
Sdílení a publikování informací	Systém Distributed File System (DFS) pro Windows 2000 Server usnadňuje uživatelům vyhledávání a správu dat na síti. Integrované internetové rozhraní
Služby tiskového serveru	Jednodušší vyhledávání tiskárny pomocí služby Active Directory. Tisk z internetu
Škálovatelnost a dostupnost	Zlepšená podpora symetrického multiprocessingu
Zabezpečení	Systém Encrypting File System (EFS)

Úvahy o migraci domén

Tento oddíl vás provede důležitými činnostmi plánování a přípravy, které je zapotřebí vykonat při jakékoli migraci. Váš vlastní proces plánování určí přesné kroky, následující oddíly však zdůrazňují oblasti, kterými se musíte zabývat.

Rozhodnutí o inovaci

Při určování, jak inovovat domény, si zodpovězte následující otázky:

- Je pro vás inovace vhodná?
Pravděpodobně odpovíte „ano“, jsou-li splněny některé nebo všechny následující podmínky:
 - Jste spokojeni se svou aktuální strukturou domén.
 - Jste spokojeni s většinou struktur domén a můžete vykonat migraci ve dvou fázích: inovaci na systém Windows 2000 a následnou restrukturalizaci, která vyřeší všechny problémy.
 - Máte pocit, že zvládnete migraci, aniž by to mělo vliv na produkční prostředí.
- V jakém pořadí musíte inovovat?
Odpověď závisí na tom, zda se zabýváte pořadím inovace řadičů domén nebo pořadím inovace domén:
- V jakém pořadí musíte inovovat řadiče domén?
V rámci domény je pořadí inovace jednoznačné. Nejprve musíte inovovat řadiče PDC, musíte si však být vědomi možných komplikací, které vyplývají například z použití služby replikace systému LAN Manager v inovované doméně, když PDC hostí exportní adresář. V takovém případě musíte ještě před inovací PDC změnit hostitele exportního adresáře. Další informace o replikaci systému LAN Manager najdete v oddílu „Proces služby replikace systému LAN Manager“ dále v této kapitole.
- V jakém pořadí musíte inovovat domény?
Snazší správy a delegování dosáhnete, když budete nejprve inovovat domény účtů. Pak je zapotřebí inovovat domény prostředků.
- V jakém pořadí musíte inovovat servery a klienty?
Servery a klienty můžete inovovat kdykoli – nezávisí to na infrastruktuře systému Windows 2000.
- Kdy musíte přepnout doménu do nativního režimu?
Doménu musíte přepnout do nativního režimu co nejdříve, abyste tak získali přístup ke všem funkcím systému Windows 2000, jako je lepší škálovatelnost adresářů, univerzální a místní skupiny domény a vkládání skupin.

Poznámka Doménu nelze přepnout do nativního režimu, dokud nejsou inovovány všechny řadiče domény.

Rozhodnutí o restrukturalizaci

Při určování, jak restrukturalizovat domény, si zodpovězte následující otázky:

- Musíte restrukturalizovat?
Pravděpodobně odpovíte „ano“, jsou-li splněny některé nebo všechny následující podmínky:
 - Jste spokojeni s většinou struktur domén a můžete vykovat migraci ve dvou fázích: inovaci na systém Windows 2000 a následnou restrukturalizaci, která vyřeší všechny problémy.
 - Nejste spokojeni se svou aktuální strukturou domén.
 - Máte pocit, že zvládnete migraci, aniž by to mělo vliv na produkční prostředí.
- Kdy musíte restrukturalizovat?
Odpověď závisí na důvodu restrukturalizace:
 - Můžete-li vyřešit své požadavky na migrování pomocí migrace se dvěma fázemi, pak musíte restrukturalizovat po inovaci.
 - Máte-li pocit, že strukturu domén nelze zachránit (například rozhodnete-li se změnit návrh infrastruktury adresářových služeb tak, aby využívala lepších možností služby Active Directory), musíte restrukturalizovat na začátku procesu migrace.
 - Máte-li pocit, že se nedokážete vyhnout negativním dopadům na produkční prostředí, musíte restrukturalizovat na začátku procesu migrace.

Poznámka Doporučujeme vám restrukturalizovat po dokončení inovace, ale ještě před využíváním takových prvků, jako je zavádění aplikací nebo nové zásady skupiny. Začnete-li s restrukturalizací až po použití některých z uvedených prvků, může to způsobit více problémů než restrukturalizace hned na začátku procesu migrace.

Kompatibilita aplikací

Jakmile jste určili celkovou strategii migrace domén, musíte ještě zjistit, zda jsou vaše obchodní či výrobní aplikace kompatibilní se systémem Windows 2000. Tento krok je pro úspěch zavádění velmi důležitý a musíte jej vykonat ještě předtím, než se rozhodnete, jak a kdy budete migrovat své aplikační servery. Jakmile určíte své strategické aplikace, nezapomeňte je zahrnout do plánu testování. Všechny strategické aplikace musí být ještě před spuštěním procesu migrace otestovány. Další informace o migrování aplikačních serverů najdete v kapitole „Inovace a instalace členských serverů“ v této knize.

Mezi důležité otázky, které si musíte položit a které souvisejí s aplikacemi, patří také ty následující:

- Bude aplikace fungovat na systému Windows 2000?
Je-li odpověď „ne“, může to mít vliv na vaše plány inovace.
- Musí aplikace běžet na řadiči BDC?
Je-li odpověď „ano“ a aplikace nebude fungovat na systému Windows 2000, bude obtížné přepnout inovovanou doménu do nativního režimu.

■ Máte kontakty na výrobce dané aplikace?

Máte-li nějaké problémy s provozováním aplikace v systému Windows 2000, musíte vědět, jakou plánuje její výrobce podporu v systému Windows 2000.

■ Jestliže byla aplikace vyvinuta interně, plánujete vyvinout její verzi pro systém Windows 2000?

Nemůže-li aplikace běžet na systému Windows 2000, musíte se seznámit s plány její podpory v systému Windows 2000.

■ Jaké operační systémy máte zavedeny na klientech a serverech?

Odpověď na tuto otázku má dopady na cestu vaší migrace. Některé cesty inovace na systém Windows 2000 nejsou podporovány (například ze systému Windows NT 3.5).

Poznámka V doménách prostředků byste neměli ponechávat servery se systémem Windows NT 3.51, protože tento systém nepodporuje členství v univerzálních a místních skupinách domény. Systém Windows NT 3.51 *nerozpozná* funkci SIDhistory uživatelských účtů, které se přesunují mezi doménami systému Windows 2000.

Jakmile budete znát odpovědi na tyto otázky, budete moci formulovat plán testování řešící důležité testovací případy. Také to vám pomůže při vývoji vyhodnocení rizik projektu, které zaznamenává vliv nesprávného fungování různých aplikací včetně navrhovaných opravných prostředků.

Další informace o testování obchodních či výrobních aplikací najdete v kapitole „Testování kompatibility aplikací se systémem Windows 2000“ v této knize.

Poznámka Některé aplikační služby vytvořené pro systém Windows NT, jako je služba Směrování a vzdálený přístup (Routing and Remote Access Service – RRAS) Windows NT, předpokládají neověřený přístup k informacím uživatelského účtu. Výchozí bezpečnostní oprávnění služby Active Directory nedovolují neověřený přístup k informacím o účtu. Průvodce instalací služby Active Directory (Active Directory Installation Wizard) vám umožňuje nakonfigurovat kompatibilní zabezpečení Active Directory tak, aby bylo možné využívat další oprávnění. Máte-li pocit, že toto omezení zabezpečení služby Active Directory umožňující používání serverů RRAS by mělo výrazný dopad na vaše zásady zabezpečení, musíte nejprve inovovat tyto servery.

Jestliže k replikování skriptů v rámci domény používáte službu replikování systému LAN Manager, pak musíte inovovat server hostící exportní adresář až nakonec.

Požadavky spolupráce

Dalším krokem je zvážení rozsahu, v němž musí systém Windows 2000 spolupracovat jak se staršími systémy Windows tak i s operačními systémy nepocházejícími od společnosti Microsoft. Plánujete-li udržet heterogenní prostředí zahrnující také jiné operační systémy než Windows 2000, musíte zjistit, které starší aplikace a služby je zapotřebí zachovat nebo inovovat, aby se na všech platformách udržela přijatelná funkčnost.

Úvahy o spolupráci (interoperabilitě) mají dva aspekty:

- Jaké jsou požadavky na spolupráci z hlediska fungování v heterogenním prostředí? To zahrnuje úroveň, v níž musí migrované prostředí spolupracovat s jinými operačními systémy a síťovými službami.

Mezi důležité úvahy může patřit:

- Potřeba zachovat klienty se systémy dřívějšími než Windows 2000, což znamená, že musíte naplánovat zachování takových služeb, jako je služba Windows Internet Name Service (WINS) podporující překlad názvů.
- Potřeba zachovat domény se systémy dřívějšími než Windows 2000, což znamená, že musíte zachovat a spravovat explicitní vztahy důvěryhodnosti.
- Potřeba spolupracovat s operačními systémy nepocházejícími od společnosti Microsoft, jako je UNIX. To může být důvod pro rychlou migraci a následné rozsáhlé používání ověřování protokolem Kerberos.
- Jaké jsou požadavky na spolupráci z hlediska zdrojových prostředí? (Z jakého systému migrujete?)
Správa přechodného prostředí může být velmi komplikovaná a vyžaduje pečlivé plánování, jak je popsáno v následujících oddílech.

Požadavky objektů služby Active Directory na disková úložiště

Již na počátku plánování migrace je důležité zvážit, kolik diskového prostoru budete potřebovat k uložení objektů vyžadovaných službou Active Directory. Celkový požadovaný diskový prostor závisí na velikosti doménové struktury Windows 2000. Informace o návrhu této doménové struktury najdete v kapitole „Návrh struktury služby Active Directory“ v této knize.

Tabulka 10.3 ukazuje požadavky na diskový prostor jednotlivých typů objektů služby Active Directory.

Tabulka 10.3 Diskový prostor vyžadovaný objekty Active Directory

Objekt	Vyžadovaný diskový prostor (v bajtech)
Objekt User (uživatel)	3,6 K
Objekt Organizational Unit (OU – organizační jednotka)	1,1 K
Atribut (10 bajtů)	100
Certifikát veřejného klíče (certifikát X.509 v3 vystavený certifikačními službami systému Windows 2000)	1.7 K

Plánování inovace domén

Jakmile zvážíte problémy týkající se migrace domén a vytvoříte plán řešení vzniklých potíží, můžete začít plánovat vlastní proces inovace.

Poznámka Návrh doménové struktury systému Windows 2000 musíte dokončit ještě před plánováním inovace. Informace o návrhu takové doménové struktury najdete v kapitole „Návrh struktury službu Active Directory“ v této knize.

Inovace domény je proces inovování řadičů PDC a BDC v doméně Windows NT ze systému Windows NT Server na systém Windows 2000 Server. Inovování představuje nejsnazší a nejbezpečnější cestu migrace, protože zachovává většinu systémových nastavení, preferencí a instalací programů.

Protože systém Windows 2000 Server je vytvořen tak, aby plně podporoval kombinované sítě, nemusíte inovovat všechny servery v doméně a přesto bude možné využívat funkce systému Windows 2000. Inovaci řadičů PDC považujte jen za první krok celého procesu – inovací řadičů BDC a následnou inovací členských serverů budete jen postupně získávat další výhody.

Protože migrace se týká inovace operačního systému a nikoli jeho nové instalace, celý proces zachovává existující strukturu domén, uživatele a skupiny a navíc se zavádějí funkce systému Windows 2000. Jakmile máte po dokončení inovace přístup k pokročilým nástrojům a funkcím správy systému Windows 2000, můžete zvážit restrukturalizaci domén. Buďte si však vědomi toho, že restrukturalizace domén není triviální úkol. Je-li jedním z vašich cílů změna struktury, zamyslete se nad vykonáním restrukturalizace domén během počáteční fáze migrace a nikoli po inovaci. Než postoupíte dále, obě možnosti si opravdu pečlivě promyslete.

Inovací domény docílíte tohoto:

- Udržíte si přístup k doménám systému Windows NT přes existující vztahy důvěryhodnosti Windows NT.
- Udržíte si přístup k serverům systému Windows NT a ke klientům systémů Windows 95 a Windows 98. Tento přístup je pro uživatele na klientských počítačích transparentní.
- Udržíte hesla uživatelských účtů, takže se uživatelé přihlašují ke stejné doméně účtů stejným heslem.

Při plánování inovace musíte uskutečnit toto:

- Určit, jaké cesty inovace jsou podporovány.
- Podrobně prozkoumat existující strukturu domén.
- Vyvinout plán zotavení či obnovení.
- Určit pořadí inovace domén.
- Určit strategii inovace řadičů domén.
- Určit okamžik přechodu na nativní režim.

Poznámka Infrastrukturu serverů nemusíte inovovat na systém Windows 2000 Server před inovací klientů. Dokonce můžete klienty a členské servery inovovat ještě před inovováním řadičů domén, nebudete však moci přistupovat k funkcím služby Active Directory, až dokud neinovujete řadiče domén.

Určení podporovaných cest inovace

Při plánování inovace musíte určit, zda lze aktuální operační systém přímo inovovat na systém Windows 2000. Tabulka 10.4 obsahuje seznam aktuálně podporovaných cest inovací. Zjistíte-li, že přímá inovace vašeho operačního systému není podporována, musíte nejprve vykonat inovaci na nějaký jiný systém, například Windows 95 či Windows 98 v případě klientů, nebo na systém Windows NT v případě klientů a serverů. Nezapomeňte tento mezikrok zahrnout do plánu inovace.

Další informace o inovaci členských serverů najdete v kapitole „Inovace a instalace členských serverů“ v této knize.

Tabulka 10.4 Podporované cesty inovace

Operační systém	Inovace na systém Windows 2000 Professional	Inovace na systém Windows 2000 Server
Windows 3.x	Ne	Ne
Windows NT 3.1	Ne	Ne
Windows NT Workstation 3.51	Ano	Ne
Windows NT Server 3.51	Ne	Ano
Windows 95 a Windows 98	Ano	Ne
Windows NT Workstation 4.0	Ano	Ne
Windows NT Server 4.0	Ne	Ano

Zjištění existující struktury domén

Jakmile jste si jisti, že váš aktuální operační systém lze inovovat na systém Windows 2000, vaším dalším úkolem je prozkoumat existující strukturu domén. Abyste mohli lépe pochopit diskutované koncepty, podívejte se na strukturu domény systému Windows NT uvedenou na obrázku 10.2. Tento příklad vychází z návrhu domén v mnoha organizacích: model domény s více hlavními počítači. Tento příklad ukazuje inovaci začínající s doménou účtů, což je obvykle první inovovaná doména.

Při zkoumání existující struktury domén systému Windows NT zvažte tyto otázky:

- Jaký typ struktury domén máte?

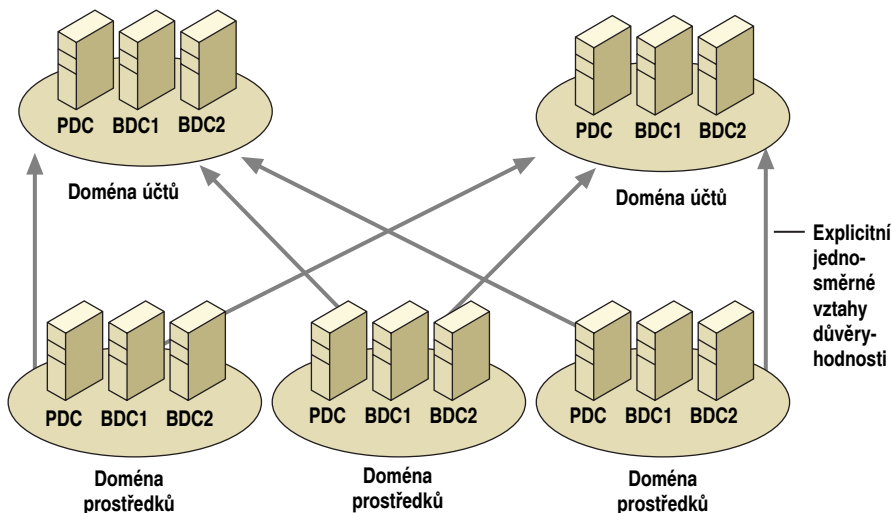
Existující struktura domén vám pomůže určit, jak naplánovat inovaci domén.

- Existují nějaké vztahy důvěryhodnosti (jedno- i obousměrné) a domény, které nemají být součástí doménové struktury?

Tyto domény systému Windows NT používají pro připojení k doménové struktuře explicitní jednosměrné vztahy důvěryhodnosti. Domény inovované na systém Windows 2000 Server a určené jako součást jedné doménové struktury se připojí obousměrnými přenosnými vztahy důvěryhodnosti. Proto je důležité vědět, které vztahy důvěryhodnosti musí zůstat explicitní. Zachovány budou všechny vztahy důvěryhodnosti existující před inovací.

- Kolik řadičů domény máte a kde se v jednotlivých doménách nacházejí?

Tyto informace vám pomohou odhadnout, jak náročná bude inovace dané domény.



Obrázek 10.2 Příklad modelu domény s více hlavními počítači

- Jaký(é) obor(y) názvů systému DNS existují ve vaší organizaci?

Protože ve Windows 2000 nelze přejmenovávat domény, musíte znát existující obor(y) používaný(é) ve vaší organizaci a také musíte vědět použití jakých dalších oborů názvů vaše organizace umožňuje, abyste mohli vytvořit jedinečný obor názvů pro doménovou strukturu.

Vývoj plánu zotavení

Je důležité vyvinout plán zotavení zabraňující náhodné ztrátě dat během inovace. Tento plán musí podrobně uvádět, jak budete zálohovat řadiče domén, aplikace a další data. Hloubka tohoto plánu určí, zda budete v případě potřeby schopni vrátit se zpět k původní konfiguraci nebo zda v určitém okamžiku překonáte bod, ze kterého již není návratu. Při vývoji plánu zotavení určete, zda existuje nějaký bod, v němž se může ukončit postupná migrace a je možné začít s plnou migrací.

Před migrací splňte následující úkoly:

- Přidejte řadič BDC do všech domén systému Windows NT, které obsahují jen jeden řadič domény, PDC. Zajistíte tak fungování domény i v případě, kdy se inovace PDC nezdaří.
- Určete, zda na řadičích PDC a BDC běží služby, jako jsou souborové a tiskové služby nebo protokol Dynamic Host Configuration Protocol (DHCP).

Tyto služby zálohujte na pásky a záložní pásky otestujte.

- Plně synchronizujte všechny řadiče BDC s řadičem PDC.

Před inovací řadiče PDC a dalších řadičů BDC na systém Windows 2000 Server převedte jeden z řadičů BDC do režimu offline. Ještě před započítím migrace zkušebně vykonajte tyto kroky:

1. Povyšte offline řadič BDC na PDC a zkontrolujte data.
2. Tento řadič PDC ponechte v režimu offline a dostupný po migraci a zajistěte pravidelné zálohování zbývajících řadičů BDC.

Upozornění Zatímco offline řadič PDC zůstává v režimu offline, sledujte všechny změny v doméně (například nové účty a aktualizace hesel). Dojde-li ke zhroucení řadičů domény systému Windows 2000, bude nezbytné vrátit se zpět k offline řadiči PDC. Pokud byste nesledovali všechny změny v doméně v době, kdy offline řadič PDC zůstává v režimu offline, došlo by po replikaci dat offline řadiče PDC na řadiče BDC ke ztrátě zadaných změn. Uvědomte si, že nově vytvořené účty mají jiné identifikátory zabezpečení (security identifier – SID), a proto nemusí mít přístup ke stejným prostředkům.

- U každého kroku vývojového diagramu z obrázku 10.1 si zodpovězte následující otázky:
 - Jak vrátíte systém zpět do stavu zotavení?
 - Jaké nástroje správy potřebujete k dosažení jak inovace tak i stavu zotavení?

Správa přechodu na doménovou strukturu systému Windows 2000

Jako součást plánu inovace domén musíte pečlivě spravovat přechod na navrženou doménovou strukturu systému Windows 2000. Pamatujte na následující:

- Řádně definujte obor názvů doménové struktury. Jestliže to nezajistíte, budete muset restrukturalizovat doménovou strukturu na správný obor názvů.
- Opatrně vytvořte kořenovou doménu doménové struktury. Po jejím vytvoření již nelze doménovou strukturu změnit.
- Opatrně vytvořte podřízené (dceřinné) domény. Jestliže připojíte podřízenou doménu k nesprávné části doménové struktury, budete muset vykonat restrukturalizaci, které nebyla součástí vašeho plánu.
- Nastavte zásady, jako jsou ty popisující použití skupin a seznamů řízení přístupu (Access Control Lists – ACL), které nepřekážejí vašim budoucím plánům.

Další informace o návrhu doménové struktury systému Windows 2000 najdete v kapitole „Návrh struktury služby Active Directory“ v této knize.

Úvahy o inovaci domén prostředků

Jestliže vykonáváte inovaci na místě, zvažte inovování domén prostředků. Domény prostředků se používaly v systému Windows NT k uložení počítačových účtů takových prostředků, jako jsou serverové a klientské počítače. Domény prostředků existovaly především proto, aby:

- se omezila velikost databáze účtů.

V systému Windows NT má maximální doporučená velikost databáze účtů nástroje Správce zabezpečení účtů (Security Account Manager – SAM) hodnotu 40 MB. V doméně obsahující uživatelské účty, skupiny se zabezpečením a účty klientů a serverů systému Windows NT to může představovat méně než 20 000 uživatelských účtů. Aby byla zajištěna škálovatelnost organizací s větším počtem uživatelů, uživatelské a počítačové účty se musely ukládat v samostatných doménách, tedy v doménách uživatelských účtů pro účty uživatelů a v doménách prostředků pro úč-

ty počítačů. To je norma pro systém Windows NT, kde se domény prostředků obvykle vytvářejí se vztahy explicitní jednosměrné důvěryhodnosti buď k jediné doméně uživatelských účtů (model domény s jedním hlavním počítačem) nebo k více doménám uživatelských účtů (model domény s více hlavními počítači).

- byla zajištěna možnost místní správy.

V decentralizovaných organizacích s geograficky vzdálenými centry je často vhodné umožnit správu prostředků místnímu personálu. Aby bylo možné používat tento druh decentralizované zodpovědnosti v systémech Windows NT, bylo doporučeno vytvářet domény prostředků s jejich vlastní strukturou správy. Stejně jako u problémů s omezením velikosti SAM bylo důsledkem tohoto opatření vytváření struktur domén s jedním nebo více hlavními počítači, které měly explicitní jednosměrné vztahy důvěryhodnosti k doménám uživatelských účtů v organizaci. Jednosměrná podstata těchto vztahů zaručovala, že správci domén prostředků měli oprávnění správy skutečně jen nad danou doménou prostředků.

Poznámka Součástí plánu inovace musí být také to, jak váš model správy odráží implikace inovace domény prostředků. Pokud jste již inovovali doménu uživatelských účtů a následně inovujete doménu prostředků jako podřízenou doménu domény účtů, vytvoří se mezi nimi přenosný (tranzitivní) vztah důvěryhodnosti. Proto se musíte zamyslet nad tím, jak tento přenosný vztah důvěryhodnosti ovlivňuje místní správu prostředků.

Nechcete-li, aby oprávnění správy přesahovaly doménu prostředků, můžete použít další možnosti, kam patří také ty dále popsané:

Restrukturalizace domén prostředků na organizační jednotky

Můžete zvážit vytvoření jiné struktury domén a pozdější sloučení domén prostředků ve formě organizačních jednotek (OU) do inovované domény uživatelských účtů. Tato volba pochopitelně ovlivní vaše úvahy o pořadí inovace domén.

Inovace domény prostředků v rámci existující doménové struktury a delegování funkcí správou systémem Windows 2000

Můžete inovovat doménu prostředků tak, aby byla ve stejné doménové struktuře jako doména(y) účtů, a k omezení možností místních správců použít funkce delegování a správy systémem Windows 2000. Ještě než tak učiníte, zkontrolujte skupiny správy v doméně prostředků a odstraňte všechny správce, kteří nejsou správci v doménách účtů. Jsou-li tu jen místní správci domény prostředků, přidejte sem jednoho nebo více správců domény uživatelských účtů. Tito správci budou schopni spravovat doménu během její inovace. Chcete-li se dále pojistit, přesvědčte se, že správci domény prostředků nemají přístup pro správu k řadičům domény přes místní účty počítačů.

Po inovaci řadiče PDC můžete vytvořit novou místní skupinu domény, která bude obsahovat správce prostředků, a zajistit jim dostatečná oprávnění k vykonávání jejich rolí pomocí delegování správy systémem Windows 2000.

Inovování domény prostředků jako stromu v nové doménové struktuře

Můžete inovovat doménu prostředků a učinit z ní strom v nové doménové struktuře, přičemž tento strom připojíte k doméně účtů pomocí explicitního jednosměrného vztahu důvěryhodnosti. Tím budete efektivně zrcadlit strukturu existující před inovací.

Určení strategie inovace řadičů domény

Prvním krokem procesu inovace domén je inovace řadiče PDC na systém Windows 2000 Server. Po inovaci PDC je vaším dalším cílem co nejrychlejší inovace všech řadičů BDC v doméně. Tento krok zajišťuje minimalizování vlivu funkcí Windows 2000, které nejsou podporovány na řidičích BDC systému Windows NT.

Režimy domén systému Windows 2000

Doména je považována za doménu Windows NT, pokud nebyl na systém Windows 2000 inovován řadič PDC. Během procesu inovace řadičů PDC a BDC se doména nachází v přechodném operačním stavu označovaném za *kombinovaný režim*. Doménu můžete ponechat v kombinovaném režimu navždy nebo se můžete posunout do provozního stavu označovaného za *nativní režim*.

Kombinovaný režim

Doména se nachází v *kombinovaném režimu*, je-li splněna jedna z následujících podmínek:

- Řadič PDC byl inovován, nebyly však inovovány všechny řadiče BDC.
- Řadič PDC a všechny řadiče BDC byly inovovány, nebyl však zadán přechod do nativního režimu.

Tabulka 10.5 shrnuje funkce systému Windows 2000 dostupné v kombinovaném režimu a funkce dostupné pouze po přechodu do nativního režimu. Nejste-li si jisti přepnutím domény do nativního režimu, podívejte se na cíle své migrace a určete, zda aktuální kombinovaný režim narušuje vaše cíle nebo zda jsou kompromisy přijatelné.

Tabulka 10.5 Dostupnost funkcí systému Windows 2000 v kombinovaném režimu

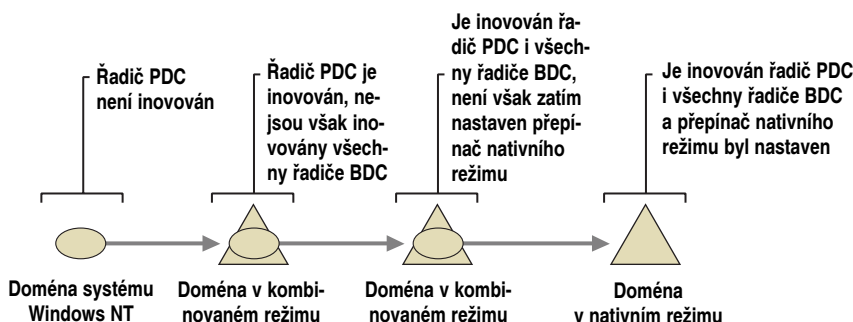
Funkce	Dostupná v kombinovaném režimu?
Přenosné vztahy důvěryhodnosti pro ověřování protokolem Kerberos	Ano. Systémy Windows 2000 Server a Windows 2000 Professional používají služby protokolu Kerberos dostupné na řadiči domény se systémem Windows 2000.
Organizační jednotky (OU) služby Active Directory	Ano, ale zobrazují se pouze při používání nástrojů pro správu systému Windows 2000. Nelze je spravovat z řadičů BDC systému Windows NT nebo ze členských serverů.
Skupiny se zabezpečením služby Active Directory	Ne, dostupné jsou pouze globální a lokální skupiny.
Funkce IntelliMirror	Ano, ale pouze pro klientské počítače se systémem Windows 2000 Professional v prostředí služby Active Directory.
Nástroj Windows Installer	Ano.
64bitová architektura paměti	Ano, s příslušnou hardwarovou podporou.
Škálovatelnost služby Active Directory	Ano, ale pouze pokud byly inovovány všechny řadiče BDC a běží na nich služba Active Directory. Při využívání této služby musíte být opatrní, jelikož řadiče BDC systému Windows NT mohou být do domény pracující v kombinovaném režimu stále přidávány. Tato funkce může být důležitou součástí vašeho plánování návratu zpět, takže nesmí být narušena.

Ověřování protokolem Kerberos	Ano, pro počítače se systémem Windows 2000 a spuštěnou službou Active Directory.
Konzola Microsoft Management Console (MMC)	Ano.
Zásady skupiny	Ano, ale pouze pro klientské počítače se spuštěným systémem Windows 2000 Professional a v prostředí služby Active Directory.
Konfigurace a analýza zabezpečení	Ano.
Replikování s více hlavními počítači	Ano, mezi inovovanými řadiči PDC a BDC. služby Active Directory

Dokud se nerozhodnete přepnout doménu do nativního režimu, zůstává doména v kombinovaném režimu i po inovaci všech řadičů BDC.

Uvědomte si, že i když nastavíte přepínač do nativního režimu, doména může stále obsahovat členské servery se spuštěným systémem Windows NT Server 4.0 nebo klienty se systémy Windows NT Workstation 4.0 či Windows 95 a Windows 98.

Obrázek 10.3 ukazuje přechod z domény systému Windows NT do nativního režimu domény systému Windows 2000.



Obrázek 10.3 Režimy inovace domény

Nativní režim

Nativní režim je konečným operačním stavem domény Windows 2000 a aktivuje se nastavením přepínače v uživatelském rozhraní. Znamená to, že inovovaná doména je nyní považována za doménu systému Windows 2000 a může využívat všechny funkce Windows 2000, jak je popisuje oddíl „Důvody pro přechod do nativního režimu“ dále v této kapitole. Po inovaci všech řadičů domény na systém Windows 2000 můžete zadat přechod domény do nativního režimu. Během přepnutí dojde k těmto událostem:

- Vypne se synchronizace Netlogon a doména používá pouze replikaci s více hlavními počítači služby Active Directory mezi řadiči domény.
- Protože je nyní synchronizace Netlogon vypnuta, nelze již do domény přidávat řadiče BDC systému Windows NT.
- Jelikož je umožněno replikování s více hlavními počítači, dřívější řadič PDC již není hlavním počítačem domény a aktualizace adresářů nyní mohou vykonávat všechny řadiče domény. Přesto však systém Windows 2000 přiřazuje dřívějšímu řadiči PDC roli emulátoru PDC. Dřívější řadič PDC obvykle dál funguje jako emulátor PDC,

což v prostředí nativního režimu znamená, že se změny hesel replikují do dřívějšího řadiče PDC před dalšími řadiči domény.

Všichni klienti se systémem dřívějším než Windows 2000 používají emulátor PDC k vyhledání řadiče PDC a k vykonání změn hesel. Navíc domény prostředků systému Windows NT používají informace o umístění PDC k vytváření vztahů důvěryhodnosti. Emulátor řadiče PDC je definován dále v této kapitole.

K dispozici je také vkládání skupin a další typy skupin systému Windows 2000, jako jsou univerzální skupiny a lokální skupiny domény.



Důležité rozhodnutí Dokud se nerozhodnete přepnout doménu do nativního režimu, zůstává v kombinovaném režimu. Doménu můžete ponechat fungovat v kombinovaném režimu navždy, i když inovujete všechny řadiče BDC v doméně. Jakmile se však jednou přepnete do nativního režimu, nelze doménu vrátit do kombinovaného režimu nebo z ní učinit doménu systému Windows NT.

Inovace řadiče PDC systému Windows NT

Po synchronizaci všech řadičů BDC v doméně tak, aby byly plně aktualizovány všemi nedávnými změnami v řadiči PDC, můžete inovaci PDC začít s procesem inovace domény uživatelských účtů. Jakmile je na řadiči PDC instalováno jádro operačního systému, instalační program systému Windows 2000 detekuje, že dochází k inovaci řadiče domény. Instalační program vás pak vyzve k instalaci služby Active Directory na server automatickým spuštěním Průvodce instalací služby Active Directory (Active Directory Installation Wizard).

Další informace o tom, jak instalovat systém Windows 2000 Server, najdete v kapitole „Automatizování instalace a inovace serveru“ v této knize.

Průvodce instalací služby Active Directory vám dává následující možnosti:

- Vytvořit první strom v nové doménové struktuře
- Vytvořit nový strom v existující doménové struktuře
- Vytvořit novou repliku existující domény
- Instalovat podřízenou doménu

Vybraná možnost závisí na výsledku plánování oboru názvů. Další informace o plánování oboru názvů najdete v kapitole „Návrh struktury služby Active Directory“ v této knize, kterou byste si měli prostudovat ještě před čtením této kapitoly.

Během procesu inovace se obsah databáze účtů (SAM) systému Windows NT kopíruje do služby Active Directory. Těmito objekty jsou komitenti zabezpečení (uživatelské účty, místní a globální skupiny a účty počítačů). V případě větších domén účtů může tento proces trvat poměrně dlouho.

Služba Active Directory také zahrnuje podporu ověřování protokolem Kerberos. Po dokončení Průvodce instalací služby Active Directory je systémům Windows 2000 dostupná ověřovací služba Kerberos. Jestliže se v tomto okamžiku rozhodnete připojit doménu obsahující inovovaný řadič PDC do již existujícího stromu, vytvoří se přenosný (obousměrný) vztah důvěryhodnosti s nadřazenou doménou. Všechny vztahy důvěryhodnosti vytvořené před inovací řadiče PDC jsou zachovány, zůstávají však explicitními jednosměrnými vztahy.

Emulace řadiče PDC v systému Windows 2000

Protože služba Active Directory podporuje aktualizace s více hlavními počítači, řadič domény systému Windows 2000 není stejným řadičem PDC jako v systému Windows NT 4.0. Jakmile inovujete řadič PDC systému Windows NT na řadič domény systému Windows 2000, funguje jako PDC jen tím, že si podrží roli *emulátoru řadiče PDC*. V systému Windows 2000 existuje jeden emulátor PDC v každé doméně v doménové struktuře.

Emulátor PDC podporuje klienty, členské servery a řadiče domény systému Windows NT a klienty systémů Windows 95 a Windows 98 pomocí těchto položek:

- Klienti systémů Windows NT, Windows 95 a Windows 98 vykonávají zápis do adresářů (například změny hesel) na emulátoru PDC.
- Kontroly hesel.
- Řadiče BDC systému Windows NT se replikují z emulátoru PDC.
- Na síti se spuštěnou službou procházení systému Windows NT hraje emulátor PDC roli hlavního prohlížeče domény. Registruje název systému NetBIOS Název domény<0x1B>.

Tyto funkce emulátoru řadiče PDC jsou zbytečné, jakmile jsou inovováni všichni klienti, členské servery a řadiče domény systému Windows NT a klienti systémů Windows 95 a Windows 98.

Poznámka Klienti systému Windows 2000 (a všichni klienti systémů Windows 95 a Windows 98 s instalovaným balíčkem ADClient) mohou k zápisu do adresářů například při změně hesel použít libovolný řadič domény v doméně. Tyto činnosti již nejsou omezeny na řadič domény, který sám sebe inzeroval jako řadič PDC.

Emulátor PDC si i v plně inovovaných doménách systému Windows 2000 ponechává určité funkce. Změny hesel vykonané jinými řadiči domény v doméně se replikují přednostně na emulátor PDC. Neproběhne-li na jiných řadičích domény v doméně řádně požadavek na ověření díky nesprávnému heslu, řadiče domény předají požadavek na ověření emulátoru PDC a pak jej teprve odmítnou. To je pro případ, že došlo k nedávné změně hesla. Uzamčení účtů se zpracovávají na emulátoru PDC. Při úpravě objektů zásad skupiny na serveru se také vychází ze zásad skupiny na emulátoru PDC.

Další informace o zásadách zabezpečení najdete v knize *Microsoft Windows 2000 Server Distribuované systémy*.

Vlastnosti emulátoru řadiče PDC

Emulátor PDC zajišťuje zpětnou kompatibilitu tím, že vystavuje během replikování data služby Active Directory jako nestrukturované skladiště počítačům se systémy Windows 95, Windows 98 a Windows NT, kam patří také řadiče BDC. Tato kompatibilita se projevuje v těchto ohledech:

- Emulátor PDC se jeví jiným počítačům se systémem Windows 2000 jako řadič domény systému Windows 2000 a neinovovaným počítačům se jeví jako řadič PDC systému Windows NT.
- Emulátor PDC lze stále používat k vytváření nových komitentů zabezpečení a k replikování těchto změn do řadičů BDC systému Windows NT.
- Klienti systémů Windows 95, Windows 98 a Windows NT mohou používat emulátor PDC jako možný přihlašovací server.

- Jestliže emulátor PDC přejde do režimu offline nebo se stane nedostupným a v doméně existuje ještě další řadič domény se systémem Windows 2000, pak se musí daný řadič domény stát emulátorem PDC. Jestliže v doméně neexistuje žádný další řadič domény se systémem Windows 2000, lze na řadič PDC povýšit jiný řadič BDC Windows NT a pak jej inovovat na systém Windows 2000 Server.

Řešení konfliktů

Replikace s více hlavními počítači znamená, že aktualizaci můžete vykonat na libovolném řadiči domény systému Windows 2000, i když je daný řadič domény odpojen od zbytku sítě. Jestliže například zadáte aktualizaci na odpojeném řadiči domény a zároveň někdo jiný zadá takovou aktualizaci na jiném řadiči, která bude s vaší úpravou kolidovat, po obnovení připojení k síti se replikují obě změny. Přestože jsou tu kolidující změny, všechny řadiče domény se nakonec dohodnou na stejné hodnotě. Tento proces postupného dohadování se označuje jako *řešení konfliktů*.

Některé konflikty jsou však na řešení velmi obtížné. Představme si, že různé řadiče domény mají kolidující verze schéma adresářů. Konflikty schématů pak lze vyřešit stejnými pravidly, jakými řeší služba Active Directory normální konflikty („poslední zápis vítězí“).

Součásti řízení přístupu

Jakmile během inovace řadiče PDC přesunete komitenty zabezpečení do služby Active Directory, jedním z důležitých problémů se stane vliv tohoto přesunu na přístup k prostředkům. Následující oddíly popisují součásti, které řídí přístup k prostředkům.

Identifikátory zabezpečení

Model zabezpečení systému Windows NT (základ zabezpečení systémů Windows NT a Windows 2000) identifikuje komitenty zabezpečení, jako jsou uživatelé, skupiny a domény, pomocí identifikátorů zabezpečení (security identifier – SID). Identifikátory SID jsou v rámci domény jednoznačné hodnoty, vystavené během vytváření uživatele či skupiny nebo při registraci počítače či vztahu důvěryhodnosti v doméně.

Součásti SID jsou uspořádány podle hierarchické konvence. SID obsahuje části, které určují číslo verze, úřad, který identifikátor SID přiřadil, doménu a proměnné číslo podřízeného úřadu nebo hodnoty relativního identifikátoru (Relative Identifier – RID), které jednoznačně identifikují komitenta zabezpečení vzhledem k vystavujícímu úřadu.

Důležité Třebaže existují dobře známé identifikátory SID, které identifikují generické skupiny a uživatele ve všech systémech, zde popisování komitentů zabezpečení se identifikují v kontextu domény. Tyto komitenty zabezpečení nelze přenášet mezi doménami, aniž by přitom zároveň nedošlo ke změně jejich SID. Dojde-li k nějaké změně identifikátorů SID, má to vliv na přístup k prostředkům. Během inovace však komitenti zabezpečení zůstávají v téže doméně, ve které byli vytvořeni, takže hodnoty SID identifikující dané komitenty zabezpečení zůstávají beze změn. Výsledkem je, že inovace nemá vliv na přístup k prostředkům.

Ověřování a přístupové tokeny

Ověřování je důležitou součástí modelu zabezpečení systému Windows NT. Termín *ověřování* představuje prostředky, kterými je uživatel identifikován v doméně pomocí nějakých informací o totožnosti, které mají obvykle formu uživatelského jména a hesla. Jsou-li tyto informace o totožnosti přijatelné, podsystém zabezpečení vytvoří pro uživa-

tele přístupový token, který obsahuje primární SID (identifikátor SID uživatele) a hodnoty SID všech skupin domény a místních počítačů, jejich členem daný uživatel je. Každý proces vytvořený uživatelem, například spuštění aplikace, nese přístupový token uživatele.

Přístupový token uživatele lze považovat za určitou formu prezentace identifikátoru ID uživatele systému. Systém jeho pomocí určuje, zda má být uživateli umožněn přístup k systémovým prostředkům.

Ověřování a popisovače zabezpečení

Protějškem přístupového tokenu uživatele je popisovač zabezpečení přiřazený prostředkům, jako jsou soubory nebo tiskárny. Popisovač zabezpečení obsahuje seznam řízení přístupu (access control list – ACL), který se skládá z položek řízení přístupu (access control entry – ACE). Položka ACE se dále skládá z identifikátoru SID spojeného s indikátorem, že komitentu zabezpečení identifikovanému pomocí SID je zaručen nebo odepřen nějaký druh přístupu k prostředku, jakými jsou například oprávnění ke čtení, zápisu a k vykonávání. Systém vykoná ověření kontroly přístupu tím, že porovná hodnoty SID v přístupovém tokenu s identifikátory SID v seznamu ACL – tak určí, zda má umožnit požadovaný přístup.

Určení pořadí inovace domén

Jakmile máte vytvořenu strategii inovace řadičů domén, vaším dalším krokem bude určení toho, které domény se budou inovovat nejdříve. Vaše volba závisí na celkových cílech inovace. Jestliže například plánujete restrukturalizovat určité domény, nemá smysl je inovovat jako první. Jestliže se má nějaká existující doména stát kořenem doménové struktury, musíte naopak danou doménu inovovat jako první.

Doporučujeme vám inovovat domény v tomto pořadí:

1. Domény uživatelských účtů
1. Domény prostředků

Pokyny pro inovaci domén uživatelských účtů

Nejvíce výhod obvykle získáte tím, že budete nejprve inovovat domény účtů, jelikož v mnoha případech je zapotřebí spravovat více uživatelů než počítačů. Inovace domén účtů na systém Windows 2000 vám poskytuje tyto výhody:

- Zlepšená škálovatelnost služby Active Directory: Mnoho organizací dosahuje svými existujícími počty uživatelů a počítačů horní hranice doporučené velikosti databáze SAM. Služba Active Directory zajišťuje zlepšenou škálovatelnost a podporuje větší populace uživatelů spouštějících širší rozsah aplikací.
- Delegování správy: Infrastruktura systému Windows 2000 umožňuje velmi přesně delegovat možnosti správy, přičemž není nutné dávat místním správcům absolutní moc.

Máte-li více domén účtů, následující rady vám pomohou s volbou pořadí jejich inovace:

Omezit rizika a udržet řízení.

Třebaže jste otestovali strategii inovace v laboratoři nebo v pilotním programu, první migrace v produkčním prostředí je vždy nejriskantnější. Chcete-li toto riziko omezit, inovujte domény účtů, z nichž máte nejsnazší přístup k řadičům domény.

Minimalizovat přerušení.

Nejprve inovujte domény účtů s méně uživateli a s místním řízením řadičů domény. To minimalizuje přerušení práce většího počtu uživatelů, zejména jestliže zatím ještě získáváte zkušenosti s procesem zavádění.

Vykonejte práci.

Jakmile získáte zkušenosti, procesu budete důvěřovat a omezíte faktor rizika, začnete inovovat větší domény účtů, které se nejpravděpodobněji stanou konsolidačními body pro další domény. Jak bude růst základna vašich uživatelů, budou nabývat funkce systému Windows 2000 stále větší hodnoty.

Identifikujte domény účtů, které jsou cíli restrukturalizace.

Plánujete-li restrukturalizovat domény účtů, nejprve inovujte ty, které jsou pravděpodobnými cíli restrukturalizace. Nelze konsolidovat domény do cílové domény, která neexistuje. Určete domény účtů, které se budou restrukturalizovat.

Pokyny pro inovaci domén prostředků

Máte-li více domén prostředků, následující rady vám pomohou s volbou pořadí jejich inovace:

Vyberte domény, v nichž budou nové aplikace vyžadovat platformu nebo funkce systému Windows 2000.

Vaším prvním krokem bude inovovat domény, kam plánujete zavést aplikace vyžadující infrastrukturu nebo funkce systému Windows 2000, jako je služba Active Directory potřebná pro program Exchange Platinum (další zásadní verze programu Microsoft Exchange).

Vyberte domény s mnoha klienty.

Vaším dalším krokem je inovovat domény, které mají mnoho klientů systému Windows NT, abyste mohli využívat součásti infrastruktury systému Windows 2000, jako je funkce Microsoft IntelliMirror.

Vyberte domény, které jsou cíli restrukturalizace.

Stejně jako u domén účtů platí, že plánujete-li restrukturalizovat domény prostředků, nejprve inovujte ty domény, které jsou pravděpodobnými cíli restrukturalizace. Identifikujte menší domény prostředků, které se budou restrukturalizovat.

Podřízené domény a vztahy důvěryhodnosti

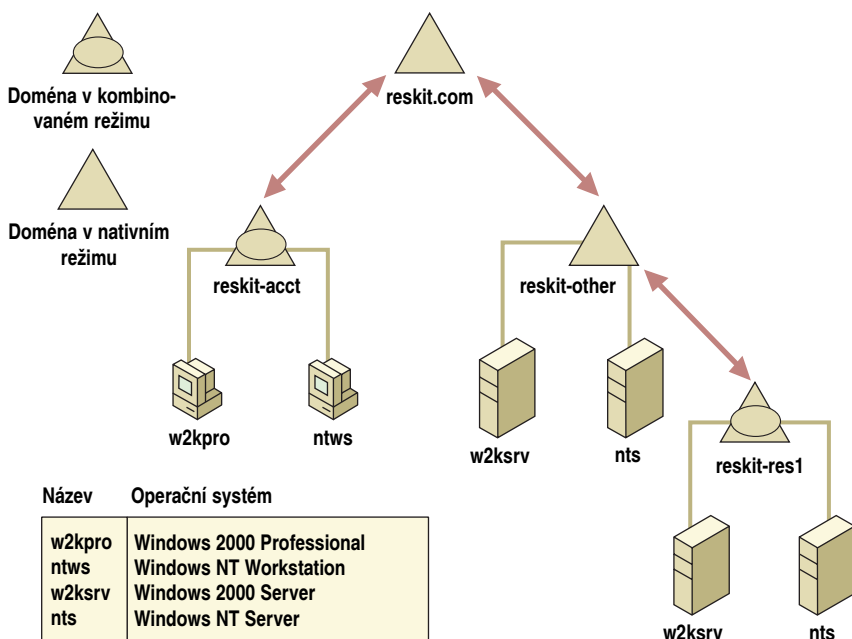
Řadič domény nadřízené domény nakonec zkopíruje veškeré informace o schématu a konfiguraci do nové podřízené domény. Po replikaci těchto informací, se stane inovovaná doména plně funkčním členem stromu Windows 2000. Uvědomte si, že dokud se nerozhodnete pro přechod na nativní režim, zůstává doména v kombinovaném režimu a má omezený přístup k funkcím služby Active Directory.

Klienti podporující službu Active Directory, jako jsou počítače se systémem Windows 2000 Professional nebo Windows 95 či Windows 98 (se spuštěným klientským softwarem Active Directory), mohou nyní využívat službu Active Directory a vykonávat takové úkoly, jako je dotazování globálních katalogů (global catalog – GC) při vyhledávání prostředků a lidí. Přenosné vztahy důvěryhodnosti umožňují klientům v doménové struktuře přistupovat k prostředkům v celém rozsahu dané doménové struktury. Jak k tomu dochází, závisí na tom, zda klient provozuje systém Windows 2000 nebo nějaký předchozí operační systém, jako jsou Windows NT, Windows 95 nebo Windows 98,

a také na tom, jaký je stav inovace cílové domény. Prostředky jsou přenosnými vztahy důvěryhodnosti dostupné v celé doménové struktuře, nacházejí-li se klienti na některé z následujících domén:

- Doménách v nativním režimu.
- Doménách kombinovaném režimu, v nichž byly všechny řadiče domény inovovány na systém Windows 2000.
- Doménách v kombinovaném režimu, v nichž byl řadič domény obsluhující požadavky na ověření protokolem Kerberos nebo NTLM inovován na systém Windows 2000.

Ve všech ostatních případech mají klienti přístup jen k prostředkům dostupným přes existující jednosměrné vztahy důvěryhodnosti, které se inovací nemění. Obrázek 10.4 ukazuje fungování přenosných vztahů důvěryhodnosti mezi nadřízenými a podřízenými doménami.



Obrázek 10.4 Příklad přenosných vztahů důvěryhodnosti mezi nadřízenými a podřízenými doménami

Použití ověřování protokolem NTLM

NTLM je ověřovací protokol, který je výchozím protokolem síťového ověřování v systému Windows NT. V systému Windows 2000 je zachován v zájmu kompatibility s klienty a servery, na nichž běží nějaké verze Windows NT.

Uživatel se například přihlašuje k doméně *reskit-acct.reskit.com*, doméně pracující v kombinovaném režimu, z pracovní stanice systému Windows NT nazvané *ntws*, která se nachází ve stejné doméně (viz obrázek 10.5). Uživatel se pak pokouší o skuteč-

nění síťového připojení k serveru Windows NT, *nts*, v doméně *reskit-other.reskit.com*, což je nativní doména systému Windows 2000. Protože *ntus* je klient dřívější než Windows 2000, použije protokol NTLM.

Počítač *nts* určí, že název domény zadaný v jemu předaných identifikačních informacích, *reskit-acct.reskit.com*, se neodkazuje do jeho databáze účtů. Takže *nts* odešle požadavek na přihlášení k ověření řadiči domény ve své vlastní doméně. Řadič domény zkontroluje název domény, a protože neodpovídá názvu domény řadiče domény, řadič domény prověří, zda je daná doména důvěryhodnou doménou. Domény *reskit-acct.reskit.com* a *reskit-other.reskit.com* jsou obě podřízenými doménami stejné kořenové domény, *reskit.com*, takže mezi těmito dvěma doménami existuje přenosný vztah důvěryhodnosti. Proto řadič domény předá požadavek na přihlášení řadiči domény v důvěryhodné doméně. Tento řadič domény ověří uživatelské jméno a heslo ve své databázi účtů domény a pokud předané informace odpovídají zadaným údajům, předá informace o identifikaci účtu a seznam členství ve skupinách zpět řadiči domény, který jej kontaktoval. Ten je následně odešle zpět původnímu serveru.

Server pak vytvoří přístupový token zosobnění pro uživatele. Tento token obsahuje identifikátor SID uživatele a identifikátory SID všech skupin domény, jejich členem uživatel je. Server zpracovávající požadavek klienta používá k zosobnění kontextu zabezpečení uživatele podproces, jenž nese token zosobnění a pokouší se o přístup k prostředkům jménem uživatele.

Tento příklad ukazuje, že klient s dřívějším systémem než Windows 2000 může v doméně v kombinovaném režimu přistupovat k serveru s dřívějším systémem než Windows 2000 v doméně v nativním režimu prostřednictvím přenosných vztahů důvěryhodnosti pomocí protokolu NTLM. Protože všechny stromy jedné doménové struktury jsou propojeny přenosnými vztahy důvěryhodnosti, totéž bude platit i pro dvě domény v různých stromech.

Vyplývá z toho také skutečnost, že pokud se uživatel pokusí přistoupit k nějakému prostředku na serveru Windows NT *nts* v doméně v kombinovaném režimu *reskit-res1.reskit-other.reskit.com*, daný prostředek je přístupný přes doménovou strukturu prostřednictvím přenosného vztahu důvěryhodnosti za předpokladu, že na řadiči domény přijímajícím požadavek na přihlášení od serveru běží systém Windows 2000.

Použití ověřování protokolem Kerberos

Služba Kerberos je výchozím síťovým ověřovacím protokolem pro počítače se systémy Windows 2000. Pro síťové ověřování v rámci domén Windows 2000 a mezi nimi je také k dispozici ověřování protokolem Secure Sockets Layer (SSL) a protokolem NTLM. Ověřování protokolem Kerberos vychází z použití lístků – uživatelům jsou vydávány centrem distribuce klíčů (Key Distribution Center – KDC) na řadiči domény Windows 2000 při počátečním přihlášení k doméně lístky pro přidělování lístků (Ticket Granting Ticket – TGT). Lístky TGT obsahují ověřovací informace o uživateli a jsou zašifrovány klíčem známým středisku KDC. Jakmile klient obdrží lístek TGT, může jej prezentovat zpět řadiči domény jako součást požadavků na lístky dalších služeb umožňujících připojení k jiným serverům v doméně. Když získá uživatel lístek TGT, následné kontroly jsou rychlé a výkonné, protože řadiči domény stačí ke kontrole informací o uživateli jen dešifrovat lístek TGT. Lístky služeb se podobají lístkům TGT, jsou však zašifrovány pomocí klíče sdíleného serverem a řadičem domény.

V příkladu uvedeném na obrázku 10.4 se uživatel přihlašuje stejně jako dříve k doméně *reskit-acct.reskit.com*, nyní však z počítače *w2kpro* ve stejné doméně, v níž je provozován systém Windows 2000. Uživatel chce uskutečnit síťové připojení k serveru sy-

stému Windows 2000 Server, *w2ksrv*, v doméně *reskit-other.reskit.com*. Protože *w2kpro* je klient systému Windows 2000, klient se pokusí použít protokol Kerberos.

Protokol Kerberos může podobně jako protokol NTLM fungovat i za hranicemi domén. Klient v jedné doméně se může ověřit serveru v jiné doméně, pokud je mezi oběma doménami vytvořen vztah důvěryhodnosti. Když se vytváří vztah důvěryhodnosti mezi doménami, dochází k výměně mezidoménových klíčů. Ověřovací služba jednotlivých domén použije tento mezidoménový klíč k zašifrování lístků pro středisko KDC druhé domény.

Požaduje-li klient přístup k serveru ve vzdálené doméně, klient kontaktuje řadič domény ve své domovské doméně a chce lístek TGT. Klient pak daný lístek TGT předá středisku KDC na řadiči vzdálené domény, má-li klient přímý vztah důvěryhodnosti s danou vzdálenou doménou, nebo své nadřízené doméně. Tento proces se opakuje ve všech prostřednických doménách, až dokud nedojde k vytvoření cesty důvěryhodnosti mezi domovskou doménou klienta a vzdálenou doménou.

Klient předá odkazovací lístek TGT středisku KDC řadiči vzdálené domény a požaduje lístek přístupu k serveru v doméně klienta. Řadič vzdálené domény použije k dešifrování lístku TGT klienta svůj mezidoménový klíč. Je-li dešifrování úspěšné, řadič vzdálené domény si bude jistý, že daný lístek TGT byl vystaven důvěryhodným úřadem. Řadič vzdálené domény pak vystaví klientovi lístek k požadovanému serveru.

Obrázek 10.4 ukazuje, že mezi doménami *reskit-acct.reskit.com* a *reskit-other.reskit.com* lze vytvořit cestu důvěryhodnosti, protože jsou podřízenými doménami jedné kořenné domény a existuje mezi nimi přenosný vztah důvěryhodnosti. Při příjmu odkazovacího lístku TGT zkontroluje řadič domény v cílové doméně, zda má k dispozici sdílený klíč pro požadovaný server. Je-li tomu tak, řadič domény vystaví klientovi lístek služby. Protože *w2ksrv* je počítač se systémem Windows 2000, existuje tu sdílený klíč, takže počítači *w2kpro* lze lístek vystavit.

Důležitými faktory v tomto příkladu jsou existence řadiče domény se spuštěným střediskem KDC protokolu Kerberos v cílové doméně a existence klíče sdíleného řadičem domény a serverem. U řadičů domén Windows 2000 je služba Kerberos povolena během procesu instalace služby Active Directory a vytvoření sdíleného klíče je také součástí přidání členského serveru do domény Windows 2000. Z toho vyplývá, že počítač *w2kpro* může přistupovat k *w2ksrv.reskit-res1.reskit-other.reskit.com* pomocí protokolu Kerberos, pokud je k dispozici řadič domény se systémem Windows 2000, který dokáže vystavit lístek relace.

Pokusí-li se počítač *w2kpro* přistoupit k nějakému prostředku na počítači se systémem Windows NT, jako je například *nts.reskit-res1.reskit-other.reskit.com*, ověření protokolem Kerberos se nezdaří a klient se pak pokusí použít ověření protokolem NTLM, jak bylo popsáno v předchozím oddílu „Použití ověřování protokolem NTLM“.

Určení okamžiku přechodu na nativní režim

Je jednoduché přepnout doménu z kombinovaného do nativního režimu, toto přepnutí však nelze vrátit. Při určování okamžiku přepnutí musíte zvážit všechny faktory popsané v tomto oddílu. Nemůžete přepnout doménu do nativního režimu, jestliže doména ještě obsahuje nebo bude obsahovat nějaké řadiče domény se systémem Windows NT.

Důvody pro pokračování v kombinovaném režimu

Hlavními důvody pro ponechání domény v kombinovaném režimu jsou:

Nelze inovovat aplikační servery

Máte aplikační servery, které nelze inovovat nebo převést na členské servery. Chcete-li například dosáhnout vysoké propustnosti dat, některé aplikace musí být instalovány na řadičích BDC, abyste se vyhnuli průchozímu ověřování. Řadiče BDC hostící takové aplikace se označují za *aplikační servery*.

Neodpovídající fyzické zabezpečení řadičů BDC

Zabezpečení je důležitou součástí plánování domén. Základním aspektem zabezpečení je fyzické zajištění samotného počítače; každý jednoduše přístupný počítač lze snadno napadnout. Předmětem k zamyšlení zde může být rozdíl mezi aktualizací databáze SAM jediným hlavním počítačem prostřednictvím samostatného řadiče PDC a aktualizací databáze účtů více hlavními počítači ve službě Active Directory všemi řadiči domény.

Z důvodu podstaty aktualizací adresářů jedním hlavním počítačem systému Windows NT vám může vyhovovat poměrně volné zajištění řadičů BDC. Je-li to váš případ, musíte se znovu zamyslet nad uvedeným problémem při jejich inovaci na řadiče domény se systémem Windows 2000. Nemůžete-li potřebným způsobem zlepšit zajištění určitého řadiče BDC, zvažte převedení daného řadiče BDC během inovace na členský server a přidání nového řadiče domény se systémem Windows 2000 na jiné místo, popřípadě se znovu podívejte na navrhovanou strukturu domén.

Je zapotřebí zajistit úplný návrat k systému Windows NT

Jednou z výhod kombinovaného režimu je stupeň zpětné kompatibility. Kombinovaný režim v případě problémů umožní přidat do domény nové řadiče BDC. Jakmile se nový řadič BDC připojí k doméně, můžete opakovaně synchronizovat databázi účtů. Nejsou-li tu žádné další domény Windows 2000, můžete povýšit řadič BDC na PDC.

Musíte také plánovat přechod na původní systém nebo zotavení, v určitém okamžiku se však budete chtít úplně přepnout do nového prostředí, což vám umožní plně využít všechny funkce systému Windows 2000.

Jedním z dobrých důvodů pro přechod do nativního režimu je možnost následně používat všechny skupiny systému Windows 2000 včetně vkládaných skupin. Pak si musíte ujasnit, které skupiny by bylo vhodné povýšit na univerzální skupiny.

Důvody pro přechod do nativního režimu

I když pouhou inovací řadičů PDC a BDC a ponecháním domény v kombinovaném režimu také získáte mnoho výhod, doporučujeme vám přejít co nejdříve do nativního režimu. Nativní režim vám pomůže zvýšit celkovou funkčnost vaší sítě takto:

- Budou dostupné nové typy skupin v systému Windows 2000.
- Domény v nativním režimu mohou používat univerzální skupiny a vkládání skupin.

Jak již bylo řečeno, k přepnutí do nativního režimu nedojde automaticky – tuto změnu musíte inicializovat prostřednictvím modulu snap-in Domény a vztahy důvěryhodnosti služby Active Directory (Active Directory Domains and Trusts) konzoly Microsoft Management Console (MMC). Podrobnosti použití této konzoly najdete v souborech nápovědy systému Windows 2000 Server.

Popis skupin systému Windows 2000

Je důležité určit, jaký bude mít migrace na systém Windows 2000 vliv na zásady zabezpečení a vaši strukturu skupin předchozího systému. Změny zásad zabezpečení budou pravděpodobně vyžadovat restrukturalizaci skupin.

Systém Windows 2000 podporuje čtyři typy skupin se zabezpečením:

- Místní
- Místní domény
- Globální
- Univerzální

Místní skupiny

Místní skupiny, které existovaly také v systému Windows NT, mohou obsahovat členy z libovolných míst doménové struktury, z jiných důvěryhodných doménových struktur a z důvěryhodné domény systému dřívějšího než Windows 2000. Místní skupiny však mohou zajistit oprávnění k prostředkům pouze na počítači, na němž existují.

Zvláštním případem místních skupin v systému Windows NT jsou skupiny vytvořené na řadiči PDC. Důsledkem replikace databáze SAM domény mezi řadiči BDC bylo sdílení těchto místních skupin mezi řadičem PDC a řadiči BDC. V kombinovaném režimu se místní skupiny chovají stejně v systému Windows NT i Windows 2000. V nativním režimu se místní skupiny na řadiči domény stávají místními skupinami domény, které jsou popsány v následujícím oddílu. Místní skupiny se obvykle používají k zajištění specifického přístupu k prostředkům na místním počítači.

Místní skupiny domény

Místní skupiny domény jsou novým prvkem systému Windows 2000, i když se svou koncepcí a použitím podobají místním skupinám vytvořeným na řadiči PDC v doméně Windows NT.

Místní skupiny domény jsou dostupné pouze v doménách pracujících v nativním režimu a mohou obsahovat členy z libovolné části doménové struktury, z důvěryhodných doménových struktur a z důvěryhodné domény systému dřívějšího než Windows 2000. Místní skupiny domény zajišťují přístup pouze k prostředkům v doméně, v níž existují. Místní skupiny domény se obvykle používají k soustředění komitentů zabezpečení z celé oblasti doménové struktury v zájmu lepší možnosti řízení přístupu k prostředkům v doméně.

Globální skupiny

Globální skupiny systému Windows 2000 se velmi podobají globálním skupinám systému Windows NT. Globální skupiny systému Windows 2000 mohou obsahovat výhradně členy z domény, v níž existují. Těmto skupinám lze přiřadit oprávnění přístupu k prostředkům ve všech doménách v doménové struktuře nebo v důvěryhodných doménových strukturách.

Univerzální skupiny

Univerzální skupiny mohou obsahovat členy z libovolné domény systému Windows 2000 v doménové struktuře a lze jim přiřadit oprávnění v libovolné doméně v doménové struktuře nebo v důvěryhodných doménových strukturách. Univerzální skupiny

sice mohou mít členy z domén v kombinovaném režimu v téže doménové struktuře, členům z takových domén se však do přístupových tokenů daná univerzální skupina nepřidá, protože univerzální skupiny nelze v kombinovaném režimu používat. Do univerzální skupiny můžete přidávat uživatele, doporučujeme vám však omezit její členství na globální skupiny. Univerzální skupiny jsou k dispozici pouze v doménách pracujících v nativním režimu.

Univerzální skupiny můžete použít k vytvoření skupin, které v podniku vykonávají nějakou společnou funkci. Příkladem jsou virtuální týmy. Členství v takových týmech ve velké společnosti může být na úrovni národa nebo celosvětové a prakticky jistě na úrovni doménové struktury, přičemž prostředky týmu jsou podobně distribuovány. V takových podmínkách lze univerzální skupiny používat jako kontejner globálních skupin z jednotlivých oddělení či poboček, přičemž prostředky týmu budou chráněny jedinou položkou ACE pro univerzální skupinu.

Univerzální skupiny a jejich členové jsou uvedeni v globálním katalogu (Global Catalog – GC). V GC jsou sice uvedeny také globální a místní skupiny domény, nikoli však jejich členové. To má dopady na provoz replikace GC. Doporučujeme vám používat univerzální skupiny opatrně. Podporuje-li celá vaše síť vysokorychlostní propojení, můžete prostě označit všechny skupiny za univerzální skupiny a těžit z toho, že nemusíte dále spravovat globální skupiny a místní skupiny domény. Jestliže však vaše síť zasahuje přes rozlehlé sítě (wide area network – WAN), dosáhnete lepšího výkonu použitím globálních skupin a místních skupin domény.

Používáte-li globální skupiny a místní skupiny domény, můžete za univerzální skupiny označit také všechny široce používané skupiny, které se mění jen zřídka.

Tabulka 10.6 uvádí vlastnosti skupin systému Windows 2000.

Tabulka 10.6 Vlastnosti skupin systému Windows 2000

Typ skupiny	Členství ze	Rozsah na úrovni	Dostupné v kombinovaném režimu?
Místní	stejně doménové struktury dalších důvěryhodných doménových struktur důvěryhodných domén systému dřívějšího než Windows 2000	počítače	Ano
Místní domény	stejně doménové struktury dalších důvěryhodných doménových struktur důvěryhodných domén systému dřívějšího než Windows 2000	místní domény	Ne
Globální	místní domény	všech důvěryhodných domén	Ano
Univerzální	stejně doménové struktury	všech důvěryhodných domén v nativním režimu	Ne

Vkládání skupin

Doporučujeme vám omezit velikost skupiny na přibližně 5000 členů, protože úložiště Active Directory musí být schopno aktualizace v jediné transakci. Jelikož jsou členství ve skupinách uložena v jediném atributu s více hodnotami, změna členství vyžaduje replikaci celého seznamu členů mezi řadiči domény a jeho aktualizaci v jediné transakci. Společnost Microsoft testovala a podporuje členství ve skupinách do 5000 členů.

Efektivní počet uživatelů však můžete zvýšit vkládáním skupin. To vám pomůže omezit provoz způsobený replikací změn členství ve skupinách. Možnosti vkládání závisejí na tom, zda pracuje doména v nativním nebo v kombinovaném režimu. Následující seznam popisuje, co může být obsaženo ve skupině existující v doméně v nativním režimu. Tato pravidla jsou určena rozsahem skupiny.

- Univerzální skupiny mohou obsahovat účty uživatelů, účty počítačů, univerzální skupiny a globální skupiny z libovolné domény.
- Globální skupiny mohou obsahovat účty uživatelů a účty počítačů z téže domény a globální skupiny z téže domény.
- Místní skupiny domény mohou obsahovat účty uživatelů, účty počítačů, univerzální skupiny a globální skupiny z libovolné domény. Mohou také obsahovat další místní skupiny domény pocházející z téže domény.

Skupiny se zabezpečením mohou v doménách pracujících v kombinovaném režimu obsahovat pouze tyto položky:

- Místní skupiny, které mohou obsahovat globální skupiny a účty uživatelů z důvěryhodných domén.
- Globální skupiny, které mohou obsahovat výhradně účty uživatelů.

Rozšíření členství ve skupinách

Když se uživatel přihlásí ke klientovi nebo uskuteční síťové připojení k serveru, během tvorby přístupového tokenu uživatele se rozšíří členství uživatele ve skupinách. K rozšíření členství ve skupinách dochází takto:

- Během interaktivního přihlašování ke klientovi kontaktuje klient řadič domény a ověřuje tu předložené pověřovací údaje uživatele a získává lístek TGT protokolu Kerberos. Řadič domény rozšíří seznam členství uživatele ve skupinách o následující typy skupin:
- Univerzální skupiny definované kdekoli v doménové struktuře
- Globální skupiny
- Místní skupiny domény ve stejné doméně, jako je účet uživatele

Tyto seznamy skupin jsou součástí lístku TGT jako data ověření.

- Jestliže klient inicializuje síťové připojení k nějakému serveru a pokud se daný server nachází v jiné doméně než účet uživatele, použije se k získání lístku služby ze střediska KDC na daném serveru odkazování mezi doménami. Jakmile je lístek služby vystaven, rozšíření skupin přidá k doméně serveru místní skupiny domény, jejichž členem uživatel je. Tyto skupiny se přidávají do dat ověření v lístku služby společně se seznamem skupin v lístku TGT. Nachází-li se server ve stejné doméně jako účet uživatele, jsou místní skupiny domény dostupné v lístku TGT již od počátečního interaktivního přihlášení.

- Když se uživatel připojí k danému serveru, dojde k rozšíření místních skupin, pokud je účet uživatele nebo některá ze skupin, jejímž členem uživatel již je, také členem nějaké místní skupiny na serveru.

Při vytváření přístupového tokenu uživatele se k identifikaci uživatele používají veškeré informace o členství rozšířené řadičem domény nebo serverem prostředků.

Vliv inovace na skupiny

Inovace řadiče PDC na systém Windows 2000 nemá na skupiny žádný okamžitý vliv: místní skupiny Windows NT se stanou místními skupinami Windows 2000 a globální skupiny Windows NT se stanou globálními skupinami Windows 2000. Ke skutečné změně dojde po přepnutí domény do nativního režimu – v tom okamžiku se z místních skupin na řadiči PDC stanou místní skupiny domény.

Používání systému NetBIOS v systému Windows 2000

NetBIOS je rozhraní síťového programování na vysoké úrovni, které se používalo v dřívějších síťových součástech. Síťové prostředky jsou identifikovány v oboru názvů systému NetBIOS jednoznačnými názvy NetBIOS. WINS je služba dodávaná jako součást systému Windows NT Server 4.0, která podporuje registrování dynamických připojování (mapování) názvů NetBIOS k adresám IP a k zajištění překladu názvů systému NetBIOS.

Po uvedení systému Windows 2000 je podpora rozhraní vytváření názvů systému NetBIOS požadována pouze pro klastrové servery. Z tohoto důvodu, k němuž se dále připojuje používání systému DNS a příchod služby Active Directory, bude používání systému NetBIOS postupně mizet.

Uvědomte si však, že inovace domény na systém Windows 2000 nemusí automaticky znamenat, že již na své síti nemusíte podporovat systém NetBIOS, a ani neovlivňuje váš aktuální stupeň potřebné podpory tohoto systému. Má-li například vaše síť více segmentů, k vytvoření seznamu procházení systému NetBIOS je zapotřebí služba WINS. Bez služby WINS se síť musí ohledně prostředku procházení spoléhat na službu Active Directory. To může mít výrazný vliv na klienty s dřívějším systémem.

Po inovaci můžete ukončit používání systému NetBIOS a služby WINS, pokud jsou splněny následující podmínky:

- Neexistují žádní klienti (jako jsou Windows for Workgroups, Windows 95, Windows 98 nebo Windows NT) a žádné servery se spuštěným systémem Windows NT, které používají systém NetBIOS. Klienti se spuštěnými předchozími verzemi operačních systémů Windows mohou však stále potřebovat názvy systému NetBIOS pro zajištění tiskových a souborových služeb a k podpoře starších aplikací.

V plánu testování nezapomeňte vyhodnotit vliv starších aplikací a služeb. Další informace o testování najdete v kapitole „Vytvoření testovací laboratoře systému Windows 2000“ v této knize.

- Máte čistou síť systému Windows 2000 a jste si jisti, že všechny počítače a aplikace na vaší síti mohou fungovat s využitím nějaké jiné služby práce s názvy, jako je například služba DNS. Práce s názvy v síti je důležitá pro vyhledávání počítačů a prostředků v rámci celé sítě i tam, kde nejsou vyžadovány názvy systému NetBIOS.

Klient WINS systému Windows 2000 si místně ukládá přeložené názvy do mezipaměti a před předáním požadavku službě DNS tuto mezipaměť prohledá pomocí součásti nazvané Caching Resolver. Soubor HOST se ukládá do mezipaměti okamžitě po spuštění klienta a veškeré aktualizace souboru HOST se okamžitě projeví v mezipaměti. Pořadí překladu názvů je toto:

1. Klient se pokusí o překlad názvu z mezipaměti.
2. Jestliže se překlad názvu z mezipaměti klienta nepodaří, klient se pokusí o překlad názvu pomocí služby DNS.
3. Pokud se překlad názvu pomocí DNS nepodaří, klient se pokusí přeložit název pomocí služby WINS.

Jsou-li splněny tyto podmínky, ukončení služeb NetBIOS a WINS je bezproblémové, jestliže jste tedy odstranili všechny starší podmínky a implementovali jste dostatečné řízení změn v nově inovovaných klientech.

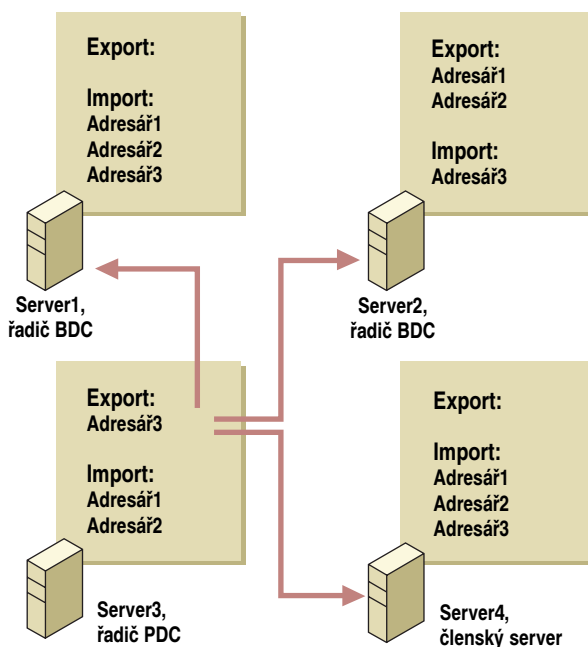
Přechod na službu replikace souborů

Systém Windows NT Server poskytuje replikační nástroj označovaný za službu replikace systému LAN Manager. V systému Windows 2000 je služba replikace systému LAN Manager nahrazena službou replikace souborů (File Replication Service – FRS).

Poznámka Systém Windows 2000 Server nepodporuje službu replikace systému LAN Manager ani v kombinovaném ani v nativním režimu. Pokud jste tedy replikaci programem LAN Manager používali, musíte do svého plánu inovace zahrnout také strategii přechodu na službu FRS a zajištění stejných funkcí.

Proces služby replikace systému LAN Manager

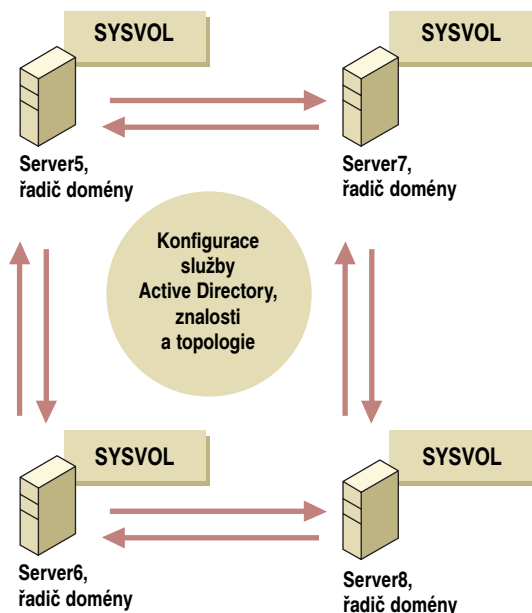
Služba replikace systému LAN Manager používá koncepci importních a exportních adresářů. Služba replikace systému LAN Manager se konfiguruje výběrem serveru, který bude hostit exportní adresář, a řady serverů, které budou hostit importní adresáře. Servery hostící tyto adresáře nemusí být radiči domény – mohou to být obyčejné členské servery. Obrázek 10.5 ilustruje proces služby replikace systému LAN Manager.



Obrázek 10.5 Proces služby replikace správce LAN Manager

Proces služby FRS

Služba FRS v systému Windows 2000 Server se automaticky konfiguruje, takže každý řadič domény má replikovaný systémový svazek (System Volume – SYSVOL). Všechny změny zadané v přihlašovacím skriptu uloženém ve svazku SYSVOL libovolného řadiče domény se replikují stylem více hlavních počítačů na ostatní řadiče domény. Na rozdíl od replikace systémem LAN Manager, kde mohou importní a exportní adresáře hostit i obyčejné členské servery, ve službě FRS mohou hostit svazek SYSVOL pouze řadiče domény. Obrázek 10.6 ilustruje proces služby FRS.



Obrázek 10.6 Proces služby FRS

Ponechání služby replikace systému LAN Manager v kombinovaném prostředí

Během inovace můžete udržovat kombinované prostředí řadičů BDC a členských serverů systému Windows NT spolupracujících s řadiči domény se systémem Windows 2000. Protože systém Windows 2000 Server nepodporuje službu replikace systému LAN Manager, její udržování v kombinovaném prostředí může být problém. Chcete-li takovou podporu zajistit, musíte vytvořit most mezi službou replikace systému LAN Manager a službou FRS, který zajistí fungování obou služeb. Tohoto dosáhnete výběrem řadiče domény se systémem Windows 2000, z něhož se budou kopírovat replikované soubory do exportního adresáře systému Windows NT. Kopírování je zajištěno pravidelně vykonávaným skriptem nazvaným *L-bridge.cmd*.

Poznámka Nezaměňujte termín *kombinované prostředí (environment)* s označením *kombinovaný režim (mode)*, který představuje řadič PDC a žádný nebo několik řadičů BDC v doméně Windows 2000. *Kombinované prostředí* znamená doménu Windows 2000 v kombinovaném nebo nativním režimu, která obsahuje klienty nebo servery se systémy dřívějšími než Windows 2000.

Vytvoření mostu mezi službou replikace systému LAN Manager a službou FRS

Ještě před nastavením mostu mezi službou replikace systému LAN Manager a službou FRS musíte učinit toto:

- Určit exportní server systému Windows NT pro daný adresář.
- Vybrat počítač systému Windows 2000, který může do daného adresáře ukládat soubory.

Doporučujeme vám ještě před inovací jednotlivých řadičů domény a členských serverů ručně zakázat služby replikace systému LAN Manager z ovládacího panelu Služby. Replikaci adresářů můžete zakázat z konzoly MMC i po inovaci, i když to není doporučený postup.

▼ **Chcete-li inovovat exportní server před inovací na systém Windows 2000, vykonejte následující kroky:**

1. Na současném exportním serveru spusíte program SrvMgr.exe a odstraníte exportní adresář.
2. Pomocí programu SrvMgr.exe přidejte z nového exportního serveru exportní adresář do exportního seznamu.

Propojení mezi adresářem skriptů systému Windows NT a systémovým svazkem systému Windows 2000 zajišťuje dávkový soubor. Výhodou tohoto přístupu je, že oba replikační mechanismy jsou fyzicky odděleny, takže na řadiči domény se systémem Windows 2000 nedochází k zavádění žádných starších služeb.

▼ **Chcete-li nastavit dávkový soubor zřizující most mezi službou replikace systému LAN Manager a službou FRS, vykonejte následující kroky:**

1. Vyberte nějaký řadič domény se systémem Windows 2000.
2. Vytvořte dávkový soubor nazvaný *L-bridge.cmd*, který bude kopírovat přihlašovací skripty na exportní server systému Windows NT, jako v tomto příkladě:

```
xcopy \\domain.com\Sysvol\domain.com\scripts \\Srv3\Export\scripts /s /D
```

Všimněte si, že přepínač **/D** příkazového řádku říká programu **xcopy**, aby zkopíroval pouze novější soubory. Přepínač **/s** příkazového řádku říká programu **xcopy**, aby zkopíroval daný adresář a všechny jeho neprázdné podadresáře.

3. Pomocí služby pro plánování (Schedule) systému Windows 2000 nastavte rozumný interval spouštění dávkového souboru. Interval dvou hodin je více než dostatečný, zejména díky tomu, že přepínač **/D** zabraňuje vytváření zbytečných kopií souborů.

Ukázková verze souboru *L-bridge.cmd* je obsažena na kompaktním disku sady *Windows 2000 Resource Kit*.

Udržení dostupnosti služby replikace systému LAN Manager během inovace

Chcete-li udržet službu replikace systému LAN Manager dostupnou během inovace, musíte server hostící exportní adresář inovovat až po skončení inovace všech ostatních serverů hostících importní adresáře. Je-li serverem hostícím exportní adresář řadič PDC, musíte vybrat nový exportní server a překonfigurovat službu replikace systému LAN Manager. Doporučujeme vám vybrat za nový server takový počítač, o kterém si myslíte, že jej budete na systém Windows 2000 inovovat jako poslední; jinak budete muset

později vybrat jiný exportní server a celým procesem projít znovu, protože servery se inovují postupně.

Použití služby Směrování a vzdálený přístup v kombinovaném prostředí

Jestliže v prostředí Windows NT používáte službu Směrování a vzdálený přístup (Routing and Remote Access Service – RRAS) a umožňujete tak vzdálený přístup uživatelů k podnikové síti, zvažte brzkou inovaci serveru RRAS v procesu inovace členských serverů. Hodnota včasné inovace spočívá v tom, jak proces RRAS funguje v systému Windows NT – zejména způsob, jímž kontrolujete vlastnosti RRAS, jako je dostupnost přístupu RRAS nebo zpětné volání uživatelům.

Služba RRAS musí běžet i když k systému nejsou přihlášení žádní uživatelé. Tato služba běží jako LocalSystem. Když se služba přihlásí jako LocalSystem, přihlásí se s informacemi totožnosti s hodnotou NULL, což znamená, že služba nepředá uživatelské jméno ani heslo. To dále znamená, že účet nelze používat pro přístup k síťovým prostředkům prostřednictvím ověřování protokolem NTLM, jestliže vzdálený počítač nedovoluje přístup s informacemi pověření o hodnotě NULL (což se označuje za relaci a NULL). Služba RRAS v systému Windows NT používá účet LocalSystem.

Služba Active Directory standardně nepřijímá dotazy na atributy objektů přes relaci NULL, takže v kombinovaném prostředí není server RRAS systémem Windows NT schopen získat uživatelské vlastnosti RRAS, nejsou-li splněny všechny následující podmínky:

- Doména je v kombinovaném režimu a server RRAS systému Windows NT je zároveň řadičem BDC. V takovém případě má služba RRAS místní přístup k databázi SAM.
- Doména se nachází v kombinovaném režimu a server RRAS systému Windows NT kontaktuje řadič BDC systému Windows NT – výsledkem je chování identické současnému chování systému Windows NT. Toto chování vychází ze zabezpečeného kanálu.
- Doména se nachází v kombinovaném nebo nativním režimu a zabezpečení služby Active Directory bylo rozšířeno tak, aby měli členové zabudované skupiny Everyone (každý) oprávnění číst vlastnosti všech uživatelských objektů. Průvodce instalací služby Active Directory (Active Directory Installation Wizard) umožňuje uživateli vybrat tuto konfiguraci pomocí možnosti **Rozšířit oprávnění** (Weaken the permissions) u určitých objektů služby Active Directory.

Postup uvedený v poslední podmínce použijte, pouze pokud plně chápete jeho dopad na zabezpečení služby Active Directory. Jestliže tento způsob koliduje s vašimi požadavky na zabezpečení, doporučujeme vám inovovat server RRAS se systémem Windows NT na systém Windows 2000 a učinit jej členem kombinované nebo nativní domény Windows 2000. Zabráníte tak nekonzistentnímu chování v doméně v kombinovaném režimu, jak bylo popsáno ve druhé podmínce.

Plánování restrukturalizace domén

Zatímco inovace domény vám umožňuje v co nejvyšší možné míře zachovat aktuální prostředí včetně struktury domén, restrukturalizace domén vám dovoluje změnit návrh doménové struktury podle potřeb vaší organizace. Restrukturalizací domény sice mo-

hou být různé výsledky, obvykle se však současná struktura uspořádává do méně větších domén.

Systém Windows 2000 poskytuje nativní funkce umožňující restrukturalizaci domén:

- Komitenty zabezpečení lze přesunovat mezi doménami a přitom zachovávat přístup k prostředkům dostupným před přesunem.
- Řadiče domény lze přesunovat z jedné domény do druhé, aniž by bylo nutné úplně přeinstalovat operační systém.

Poznámka Restrukturalizace domén není požadavkem zavedení systému Windows 2000 Server. Restrukturalizovat můžete později podle potřeb. Přesun počítačů do nových domén a aktualizace nebo kontrola řízení přístupu však může být složitý a časově náročný úkol.

Společnost Microsoft vytvořila sadu nástrojů Domain Migration Basic Utilities, které vám s migrací domén pomohou. Tyto nástroje jsou sadou objektů Component Object Model (COM) a ukázkových skriptů, které společně tvoří základ zákaznický upravených nástrojů pro správu a podporují řadu příkladů migrace domén, které společnost Microsoft zdokumentovala a otestovala. Tyto příklady byly vyvinuty na základě informací zákazníků týkajících se jejich požadavků na migraci. Dále v této kapitole je popsán základní nástroj ClonePrincipal.

Určení důvodů restrukturalizace domén

Hlavním zaměřením této kapitoly je počáteční migrace ze systému Windows NT na systém Windows 2000. Některé metody restrukturalizace popsané v této kapitole lze však aplikovat také v době po migraci.

Možná máte řadu důvodů k restrukturalizaci domén, hlavním však bude plné využití funkcí systému Windows 2000. Tyto funkce vám umožňují lépe využívat domény k odražení požadavků vaší organizace. Mezi klíčové výhody získané restrukturalizací domén patří:

Vyšší škálovatelnost.

Svou předchozí strukturu domén systému Windows NT jste možná vytvořili podle omezení velikosti databáze účtů SAM, což mělo za následek implementaci modelů domén s jedním nebo více hlavními počítači. Protože služba Active Directory nabízí mnohem vyšší škálovatelnost dosahující milionů uživatelských účtů nebo počítačů, můžete své současné domény Windows NT restrukturalizovat na méně větších domén Windows 2000.

Delegování správy.

Ve svém současném modelu máte možná zavedeny domény prostředků, které umožňují delegování zodpovědnosti správců. Organizační jednotky systému Windows 2000 mohou obsahovat libovolný typ komitenta zabezpečení a správu lze delegovat podle potřeby. V mnoha případech je převod domén prostředků na organizační jednotky pro delegování správy mnohem vhodnější.

Lepší detailní členění správy.

Jestliže jste chtěli dosáhnout lepšího rozčlenění zodpovědností správců, což byl důsledek třeba nákupů společnosti, propojili jste svou strukturu domén složitými a zmatenými vztahy důvěryhodnosti. Můžete se zamyslet nad implementováním některých z těch-

to domén jako organizačních jednotek, což zjednoduší správu, nebo můžete znovu navrhnout model domén a využívat méně explicitních vztahů důvěryhodnosti.

Pamatujte si, že příklady popsané v následujícím oddílu nevyžadují úplné dokončení inovace, třebaže některé z metod restrukturalizace mohou vyžadovat již inovovaný nějaký řadič BDC v doméně, kterou plánujete restrukturalizovat.

Určení okamžiku restrukturalizace domén

Podle svého plánu migrace si můžete vybrat restrukturalizaci domén okamžitě po inovaci, místo inovace, nebo obecně změnit návrh domén někdy v budoucnosti. Tyto možnosti jsou popsány dále:

Po inovaci

Nejpravděpodobnější čas restrukturalizace domén nastává po inovaci jako druhá fáze migrace na systém Windows 2000. Inovace se pak zabývá méně složitými situacemi, jako jsou skupiny domén, v nichž je struktura vztahů důvěryhodnosti v zásadě správná a v nichž nevznikají žádné problémy se správou.

Zvolíte-li restrukturalizaci po inovaci, vaše plány se pravděpodobně budou týkat přepracování struktury domén a omezení její složitosti nebo bezpečného přenesení domén prostředků se správci s nízkými pravomocemi do doménové struktury.

Místo inovace

Možná máte pocit, že současnou strukturu domén již nelze zachránit (například potřebujete-li změnit návrh infrastruktury adresářových služeb a moci plně využívat službu Active Directory) nebo že si nemůžete dovolit ohrozit stabilitu současného produkčního prostředí během migrace. V obou případech může být nejjednodušší cestou migrace vytvoření panenské doménové struktury – ideální doménové struktury systému Windows 2000 izolované od aktuálního produkčního prostředí. Zajistíte tím normální obchodní či výrobní činnost během zkoušení pilotního projektu. Pilotní projekt se nakonec stane produkčním prostředím.

Po vytvoření pilotního projektu můžete začít s restrukturalizací domén migrací menšího počtu uživatelů, skupin a prostředků do pilotního programu. Po úspěšném dokončení této fáze převedete pilotní projekt na postupnou migraci do nového prostředí. Následně učiňte ze systému Windows 2000 produkční prostředí, odstavte starou strukturu domén a zbývající prostředky zaveďte na nových místech.

Po migraci

V této fázi se restrukturalizace domén uskutečňuje jako součást celkové změny návrhu domén v čistém prostředí systému Windows 2000. K tomu může dojít až po několika letech, kdy je již stávající struktura nevyhovující z takových důvodů, jako je změna organizace nebo nákup nějaké společnosti.

Zkoumání dopadů restrukturalizace domén

Jakmile určíte proč a kdy musíte restrukturalizovat domény, je zapotřebí se zamyslet nad dopady takové restrukturalizace. Následující oddíly popisují:

- přesun komitentů zabezpečení, uživatelů a globálních skupin, počítačů a členských serverů,
- vytváření vztahů důvěryhodnosti,
- klonování komitentů zabezpečení.

Přesun komitentů zabezpečení

To, co v zásadě umožňuje restrukturalizaci domén, je schopnost systému Windows 2000 přesunovat komitenty zabezpečení a řadiče domény mezi doménami. To má řadu důležitých dopadů na způsob identifikování komitentů zabezpečení v systému a metodu udržení přístupu k prostředkům. Tyto dopady mohou ovlivnit váš upřednostňovaný přístup k restrukturalizaci domén.

Vliv na identifikátory SID

Podstata identifikátorů SID, které se váží ke konkrétním doménám, má následující dopad: když přesunete nějakého komitenta zabezpečení, jako je uživatel nebo skupina, mezi doménami, danému komitentovi zabezpečení je zapotřebí vystavit nový identifikátor SID pro účet v nové doméně.

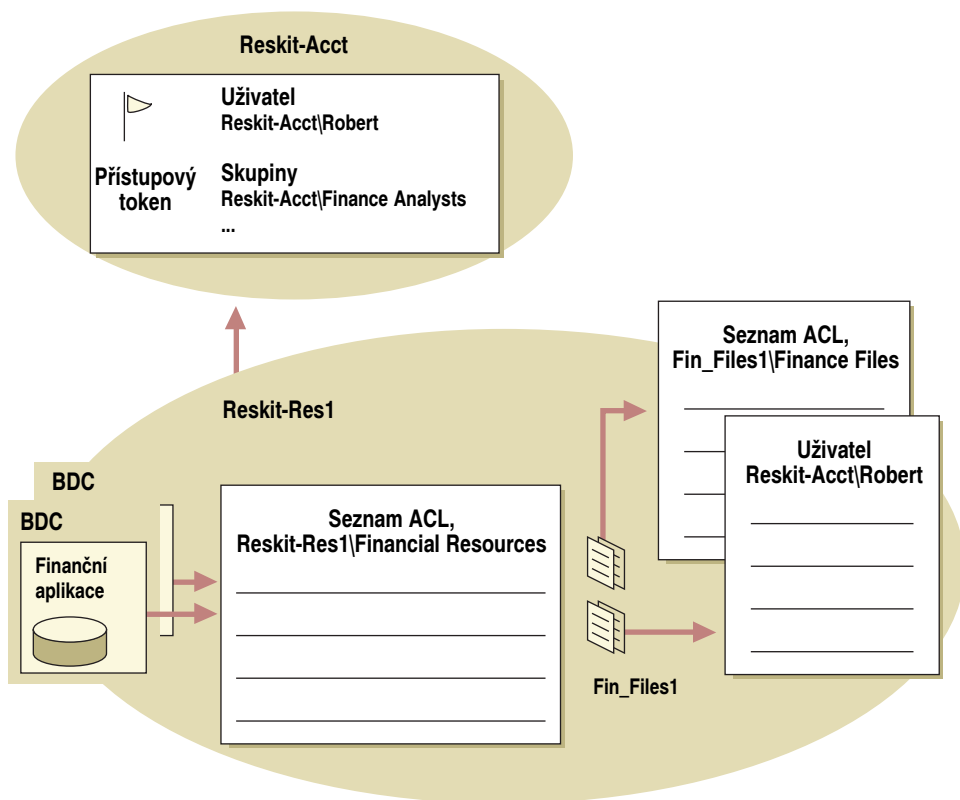
V modelu zabezpečení systému Windows NT je přístup k prostředkům ovlivněn způsobem, jakým se operační systém dívá na přístupový token uživatele a porovnává primární identifikátor SID uživatele (i další identifikátory SID všech skupin, jejichž členem uživatel je) se seznamem ACL na popisovači zabezpečení prostředku. Protože seznam identifikátorů SID obsažených v seznamu ACL obsahuje informace zajišťující nebo znemožňující přístup komitentům zabezpečení identifikovaným jejich hodnotami SID, změna identifikátoru SID má rozsáhlé dopady.

Vlivy změny identifikátoru SID jsou uvedeny v následujícím příkladu a na obrázku 10.7. Robert je zaměstnanec společnosti Reskit Corporation a má účet v doméně uživatelských účtů systému Windows NT nazvané Reskit-Acct. Robert je členem globální skupiny „Finance Analysts“ v téže doméně.

Společnost Reskit Corporation používá finanční aplikaci systému Windows NT, která běží na řadě serverů Windows NT v doméně prostředků Reskit-Res1. Protože místní skupiny vytvořené na řadiči PDC jsou sdíleny mezi všemi řadiči domény v doméně, servery s běžící aplikací jsou zároveň nastaveny jako řadiče BDC pro doménu. Na řadiči PDC byla vytvořena sdílená místní skupina „Financial Resources“, které se používá v seznamech ACL souborů využívaných danou aplikací. Globální skupina „Reskit-Acct\Finance Analysts“ je členem skupiny „Reskit-Res1\Financial Resources“.

Robert má také přístup k souborovému serveru Fin_Files1 v doméně prostředků. Fin_Files1 je server Windows NT nastavený jako členský server. Fin_Files1 používá místní skupinu „Finance Files“ v seznamech ACL souborů souvisejících s Reskit-Acct\Finance Analysts, která je členem Fin_Files1\Finance Files. Robert pracuje na nějakém soukromém projektu a má na serveru Fin_Files1 adresář, který je chráněn tak, že k souborům v tomto adresáři má přístup pouze Robert. Tento adresář má seznam ACL obsahující jedinou položku umožňující Robertovi plné řízení adresáře.

Dopady přesunu komitentů zabezpečení lze vysledovat tím, co se stane, když dojde během migrace zahrnující restrukturalizaci domény k přesunu účtu Reskit-Acct\Robert. V našem případě došlo k inovaci domény Reskit-Acct na systém Windows 2000 a k jejímu připojení do doménové struktury Windows 2000 jako podřízené domény kořenové domény reskit.com. Doména Reskit-Acct byla přepnuta do nativního režimu, byla však restrukturalizována a její členové byly přesunuti do jiné domény Windows 2000 nazvané Reskit-Acct2 v jiné části doménové struktury.



Obrázek 10.7 Příklad přístupu k prostředkům

Poznámka Tento příklad ukazuje, k čemu dojde, není-li k dispozici funkce systému Windows 2000 označovaná za „SIDhistory“. Je důležité, abyste dokázali zvládnout podobné situace, jestliže se během restrukturalizace objeví. Atribut SIDhistory je popsán dále v této kapitole.

Vliv na členství v globálních skupinách

Reskit-Acct\Robert je členem globální skupiny Reskit-Acct\Finance Analysts. Protože globální skupina může obsahovat pouze členy ze své vlastní domény, přesunutím Roberta do nové domény dojde k vyloučení jeho nového účtu ze skupiny Reskit-Acct\Finance Analysts. Robert tak ztratí přístup k cenným prostředkům dostupným v Reskit-Acct\Finance Analysts.

Jestliže mezi novou doménou a doménou prostředků existují dostatečné vztahy důvěryhodnosti, tuto situaci je možné vyřešit několika způsoby.

Přidání nového identifikátoru SID do seznamu ACL prostředků

Přístup k prostředkům lze zajistit přidáním nového identifikátoru SID Roberta do seznamů ACL všech prostředků, k nimž měl dříve přístup jako člen skupiny Reskit-Acct\Finance Analysts. Taková oprava však z následujících důvodů bude časově náročná a komplikovaná:

- Mnoho operací restrukturalizace domén se vykonává postupně. Není zaručeno, že v této době nedojde k vytvoření nových prostředků pro Reskit-Acct\Finance Analysts. Proto bude muset toto „opakované opravňování“ probíhat během celé doby restrukturalizace.
- Pokud by Robert změnil své pracovní zařazení a nemusel by již být členem skupiny Reskit-Acct\Finance Analysts, bylo by mnohem jednodušší odstranit Roberta ze skupiny Reskit-Acct\Finance Analysts než měnit seznamy ACL prostředků, která se na něj odkazují. Doporučujeme vám vytvářet seznamy ACL pomocí skupin a nikoli pomocí jednotlivců, protože uživatelé a jejich konkrétní pracovní funkce se časem mohou měnit.

Přesunutí skupiny

Protože v systému Windows 2000 lze přesunovat komitenty zabezpečení, skupinu Reskit-Acct\Finance Analysts lze přesunout do nové domény. Seznamy ACL odkazující se na danou skupinu se však také odkazují na identifikátor SID skupiny, takže bude zapotřebí opakovaně nastavit oprávnění prostředků tak, aby se odkazovaly na nový identifikátor SID.

Vytvoření „paralelní“ skupiny v cílové doméně

Dojde-li k přesunutí skupiny Reskit-Acct\Finance Analysts do jiné domény, nastane problém, pokud nedojde k přesunutí všech členů skupiny v jedné transakci. To znamená, že bude zapotřebí ponechat skupinu ve staré doméně a zároveň vytvořit novou „paralelní“ skupinu v nové doméně. Přístup k prostředkům bude zajištěn pro původní skupinu a její členy, aby však prostředky umožňovaly přístup nové skupině, budou muset být upravena jejich oprávnění. Znovu platí, že opakované vytváření oprávnění bude muset pokračovat po celou dobu, kdy dané skupiny existují v obou doménách.

Uvědomte si, že k tomu dojde, nebude-li dostupná funkce SIDhistory. Funkce SIDhistory je vysvětlena dále v této kapitole.

Vliv na seznamy ACL přímo se odkazující na daného uživatele

Účtu Reskit-Acct\Robert je také zaručen přímý přístup k určitým prostředkům členského serveru Fin_Files, protože jeho identifikátor SID se objevuje na seznamu ACL daného serveru. Je naprosto v pořádku přidávat uživatele na seznamy ACL prostředků, ale po přesunu účtu Reskit-Acct\Robert bude zapotřebí změnit oprávnění prostředků na daném serveru. Tím se k účtu Roberta přidá identifikátor SID nové domény.

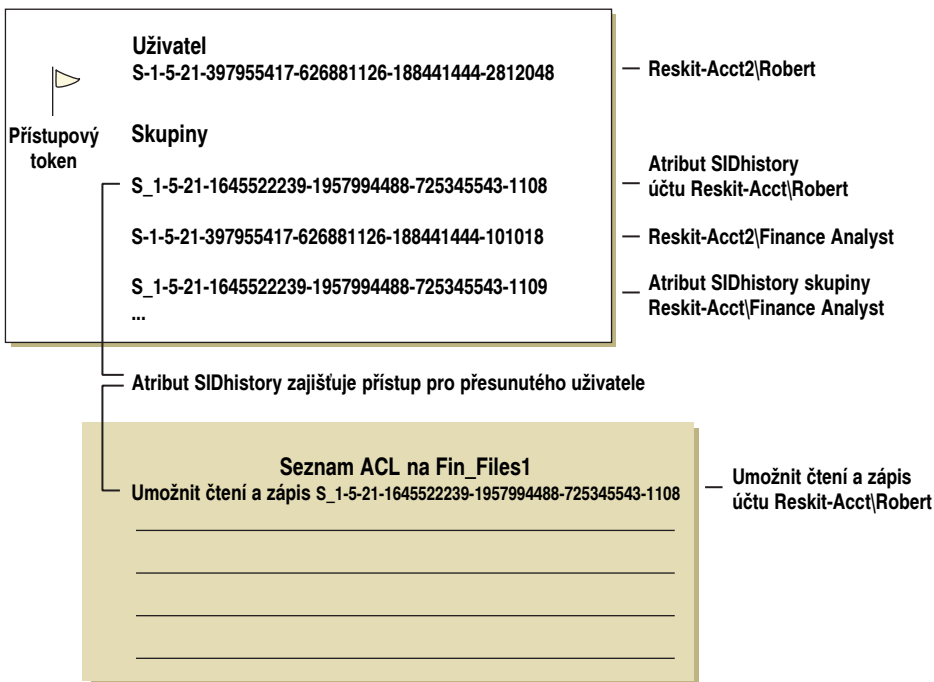
Atribut SIDhistory

V mnoha případech jsou činnosti společnosti Reskit Corporation v příkladu zbytečné, což je dáno funkcí systému Windows 2000 nazvanou *SIDhistory*. SIDhistory je atribut komitentů zabezpečení služby Active Directory a používá se k uložení dřívějších identifikátorů SID přesunutých objektů, jako jsou uživatelé a skupiny se zabezpečením.

Dojde-li k přesunu uživatele nástroji systému Windows 2000 dodanými společností Microsoft, aktualizuje se atribut SIDhistory uživatelského objektu ve službě Active Directory předchozím identifikátorem SID. Když se pak uživatel přihlásí do systému, systém převezme položky atributu SIDhistory uživatele a přidá je k přístupovému tokenu uživatele. Protože je možné skupiny přesunovat, systém také zjistí atributy SIDhistory všech skupin, kterých je uživatel členem, a také je přidá do přístupového tokenu uživatele.

Položky SIDhistory v tokenu se systému během kontrol ověření jeví jako normální členství ve skupinách a zajišťují příslušný přístup dokonce i na dřívějších systémech, které

nevědí nic o systému Windows 2000 ani o službě Active Directory. Obrázek 10.8 ukazuje, jak je zajištěn přístup k prostředkům pomocí atributu SIDhistory.



Obrázek 10.8 Přístup k prostředkům zajištěný pomocí atributů SIDhistory

Systém Windows NT 3.51 a atribut SIDhistory

Se členstvím ve skupinách a s použitím systémů Windows NT 3.51 v doménách Windows 2000 souvisí jeden problém. Ten spočívá ve způsobu, jakým systém Windows NT 3.51 přijímá identifikátory SID členství ve skupinách od řadiče domény a vytváří token zabezpečeného přístupu. Jakmile je uživatel ověřen, vytvoří se přístupový token systému Windows NT 3.51 pouze pomocí identifikátorů SID odpovídajících doméně uživatelských účtů a místním skupinám serveru nebo klienta, kde k ověření dochází. Výsledkem je, že systémy Windows NT 3.51 nemohou rozpoznat univerzální skupiny vně domény účtů ani místní skupiny domény z domény prostředků.

Protože položky atributu SIDhistory uživatele a všech univerzálních skupin, jejichž členem uživatel je, pocházejí z jiných domén než je doména účtů, tyto položky se na tokenu neobjeví. Výsledkem je, že při práci se systémem Windows NT 3.51 se při vyhodnocování řízení přístupu ignorují identifikátory SID členství ve skupinách v jiných doménách, než je doména účtů přihlašovaného uživatele. Ve většině případů dojde k odmítnutí přístupu, i když to není žádoucí.

Přesun uživatelů a globálních skupin

Protože místní skupina může obsahovat pouze členy ze své vlastní domény, jakmile dojde k přesunu uživatele mezi doménami, musí se také přesunout všechny globální sku-

piny, jichž členem uživatel je. K tomu musí dojít v zájmu zachování přístupu k prostředkům chráněným seznamy ACL, jež se odkazují na globální skupiny. Podobně platí, že dojde-li k přesunu globální skupiny, musí se přesunout také její členové.

V takovém případě je uzavřenou sadou uživatelů a globálních skupin sada, v níž platí následující:

- S každým přesunovaným uživatelem se přesunují také všechny globální skupiny sady.
- S každou přesunovanou skupinu se přesunují také všichni její členové.

Pracuje-li zdrojová doména v nativním režimu, globální skupiny mohou také obsahovat další globální skupiny. To znamená, že musí dojít k přesunu všech členů všech vložených skupin a všech globálních skupin, které mají členy v daných vložených skupinách.

Přesun profilů a atributů SIDhistory

Při formulování plánu restrukturalizace domén si musíte být vědomi toho, že migrování uživatelé dostávají nové identifikátory SID, což může ovlivnit použití jejich profilu. Uživatelé, kteří se po migraci přihlašují ke svým počítačům, mohou ztratit přístup ke svým přihlašovacím profilům, protože jejich primární identifikátory SID se změnily, zatímco jejich staré profily mohou být stále ještě uloženy pod jejich původními identifikátory SID. K tomu dojde při splnění následujících podmínek:

- Uživatel byl klonován z domény Windows NT 4.0.
- Uživatel byl klonován z domény Windows 2000.
- Uživatel byl klonován z domény Windows 2000, ale stále se přihlašuje na systému Windows NT 4.0 Workstation.

Ztratí-li uživatelé přístup ke svým přihlašovacím profilům, můžete je migrovaným uživatelům opět zpřístupnit dvěma způsoby: zkopírováním profilů nebo sdílením profilů. Upřednostňovanou metodou je zkopírování profilů.

Kopírování profilů

První možností je zkopírovat původní profil z jeho aktuálního místa pod klíčem pojmenovaným podle původního identifikátoru SID uživatele do klíče pojmenovaného podle nového identifikátoru SID uživatele. Každý účet má přiřazen svou vlastní samostatnou kopii v profilu. Aktualizace jednoho se neprojeví v druhém.

Výhodou použití této metody je, že chování systému Windows 2000 je předvídatelnější. Protože data se mezi profily nesdílejí, není možné, aby jeden profil přistupoval k účtu s daty příslušnými pouze jinému účtu v jiné doméně nebo doménové struktuře.

Mezi nevýhody této metody patří:

- Zabírá další diskový prostor, protože jsou uloženy dva profily.
- Vytváří nepředvídatelné výsledky při návratu k původnímu systému. Musíte dokonale otestovat důsledky instalace aplikací používajících zásady skupiny, abyste byli připraveni na všechny krizové situace.

Sdílení profilů

Tato volba zpřístupní jeden profil jak původnímu účtu tak i novému účtu uživatele. V takových podmínkách oba účty přistupují pouze k jediné kopii profilu a také ji aktualizují. Mezi výhody této metody patří:

- Aktualizace profilu (například změny ve složce Dokumenty, zástupců atd.) zadané při přihlášení jedním účtem jsou dostupné, když se uživatel následně přihlásí druhým účtem.
- Šetří se diskovým prostorem, protože se ukládá jen jedna kopie profilu.

Nevýhodou této metody je, že jsou tu neznámé proměnné, které mohou ovlivnit její použití. Jestliže například vytvoříte nový profil účtu systému Windows 2000, který bude obsahovat odkazy na zásady skupiny, musíte otestovat vliv na návrat zpět ke zdrojovému účtu, kde se zásady skupiny liší nebo nebyly vůbec používány.

Přesun počítačů

Jelikož sdílené místní skupiny a místní skupiny domény mají rozsah pouze v rámci domény, v níž byly vytvořeny, přesun takové skupiny poruší všechny odkazy na danou skupinu v seznamech ACL zdrojové domény.

V takovém případě je uzavřenou sadou počítačů a sdílených místních skupin nebo místních skupin domény sada, v níž platí následující podmínky:

- S každým přesunovaným počítačem se přesunují také všechny sdílené místní skupiny a místní skupiny domény odkazované v seznamech ACL prostředků počítače.
- S každou přesunovanou skupinou se přesunují také všechny počítače v doméně obsahující seznamy ACL odkazující na danou skupinu.

Omezení přesunu zaplněných globálních skupin a uzavřených sestav jsou velmi přísná. Odstranění uživatelů z velkých globálních skupin a jejich opětovné zaplnění může být časově náročné. V některých případech je nejmenší dosažitelnou uzavřenou sadou celá zdrojová doména. Mezi tři způsoby řešení tohoto problému patří:

1. Vytvoření paralelních globálních skupin všech přesunovaných skupin v cílové doméně, následné vyhledání všech prostředků v podniku, které obsahují seznamy ACL odkazující se na původní skupinu, a změna jejich oprávnění tak, aby obsahovaly odkazy na paralelní skupinu.

Při přesunu globálních skupin bude tato metoda pravděpodobně velmi náročná v následujících případech:

- Odkazy na skupinu se mohou vyskytovat v prostředcích libovolné důvěřující domény.
 - Jedná se o místní skupiny domény ze zdrojových domén pracujících v nativním režimu, kde místní skupiny domény lze používat na libovolném počítači v doméně.
2. Přepnutí zdrojové domény do nativního režimu a následná změna typu přesunovaných skupin na univerzální. Protože univerzální skupiny mají rozsah v rámci celé doménové struktury, změna skupin na univerzální skupiny znamená, že je lze bezpečně přesunovat a přitom jim zůstane zachován přístup k nepřesunovaným prostředkům.

Při použití této metody buďte opatrní, jelikož členství v univerzálních skupinách se ukládá v globálním katalogu (GC), což má dopady na provoz replikace GC. Proto může být vhodné použít tuto metodu výhradně jako přechodnou strategii při migraci uživatelů a skupin do nové domény. Po dokončení migrace můžete nastavit původní typy skupin.

3. Klonování skupin ze zdrojové domény do cílové domény, přičemž zůstane zachován atribut SIDhistory. Tato technika má určitá omezení a je popsána v oddílu „Klonování komitentů zabezpečení“ dále v této kapitole.

Přesun členských serverů

V našem příkladu má Robert přístup k určitým prostředkům na členském serveru `Fin_Files1` prostřednictvím seznamu ACL, který se odkazuje na místní skupinu počítače `Fin_Files1\Finance Files`, a přímým odkazem na jeho účet v doméně.

Důsledky přesunutí řadičů domén včetně potřeby zajistit, aby byly zachovány sdílené místní skupiny a místní skupiny domény, byly popsány již dříve v této kapitole. Tyto důsledky se však liší od těch, které souvisejí s přesunem klientského serveru, jako je `Fin_Files`, nebo klienta.

Jestliže budeme předpokládat, že došlo k přesunu členského serveru do domény se vztahem důvěryhodnosti k nové doméně účtů Roberta, atribut `SIDhistory` zajistí, že Robert bude moci přistupovat k prostředkům se seznamy ACL, která se odkazují přímo na něj. Seznamy ACL odkazující na místní skupinu počítače budou také stále fungovat, protože daná skupina existuje v databázi účtů místního počítače. To znamená, že na skupinu nemá přesun žádný vliv a její identifikátor SID není zapotřebí měnit.

Vytvoření vztahů důvěryhodnosti

Během inovace domény se předpokládá, že mezi cílovou doménou a všemi souvisejícími doménami prostředků existovaly dostatečné vztahy důvěryhodnosti, takže přístup k prostředkům je zachován. Takové vztahy důvěryhodnosti je však v každém scénáři restrukturalizace domén zapotřebí nejprve vytvořit.

K vykonávání takových úkolů, jako jsou včty vztahů důvěryhodnosti domén a ustavení nových vztahů důvěryhodnosti, se používá nástroj `Netdom`. Tento nástroj je užitečný také k vytváření účtů počítačů a k aktualizaci členství klienta nebo serveru v doméně.

Klonování komitentů zabezpečení

Až do tohoto okamžiku zahrnovala restrukturalizace přesun komitentů zabezpečení. Po přesunu komitenta zabezpečení se v cílové doméně vytváří nový identický účet a ze zdrojové domény se účet odstraňuje. Operace přesunu neumožňuje návrat ke stavu starému účtu pro případ, že se při migraci objeví problémy.

Chcete-li si zajistit možnost zotavení z problémů během pilotního programu nebo migrace výroby či obchodu, doporučujeme vám postupně migrovat uživatele do domény `Windows 2000` a přitom ponechávat staré účty ve zdrojové doméně. To je umožněno procesem klonování, který vytváří pomocí nástroje `ClonePrincipal` duplikát uživatele nebo skupiny. Tento nástroj obsahuje sadu skriptů jazyka `Microsoft Visual Basic (VB)`, které vykonávají úkoly klonování globálních skupin a klonování uživatelů.

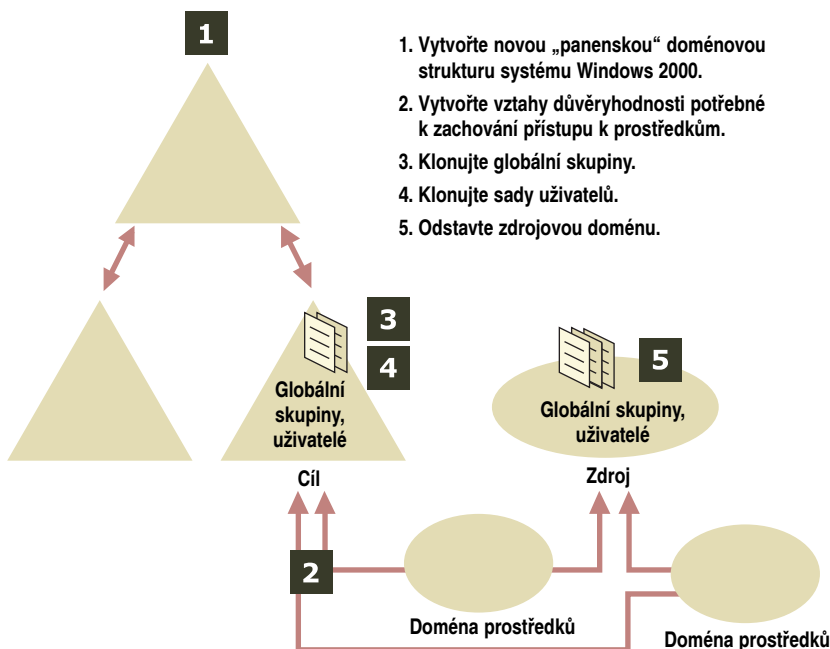
Scénáře restrukturalizace domén

Oba scénáře popsané v tomto oddílu naplňují většinu potřeb restrukturalizace. Scénáře využívají přesun uživatelů a počítačů ze zdrojových domén `Windows NT` do cílových domén `Windows 2000`. Příklady jsou:

- Postupná migrace uživatelů na systém `Windows 2000` (v rámci doménové struktury)
- Migrace prostředků do organizační jednotky systému `Windows 2000` (v rámci doménové struktury)

Scénář #1:**Postupná migrace uživatelů z Windows NT na Windows 2000**

V tomto scénáři postupně migrujete uživatele do panenského prostředí systému Windows 2000, aniž by to mělo vliv na produkční prostředí systému Windows NT. Obrázek 10.9 ilustruje tento příklad. Tento oddíl popisuje také kroky a nástroje potřebné pro postupnou migraci.



Obrázek 10.9 Postupná migrace uživatelů

Poznámka Ochrana současného produkčního prostředí před změnami migrací zaručuje jeho nedotčenost v celém procesu. To vám umožní v případě potřeby vrátit se zpět ke starému produkčnímu prostředí.

Po dokončení migrace můžete odstavit starou doménu účtů a změnit přiřazení řadičů domén. Pak vykonajte tyto kroky:

1. Vytvořte panenskou doménovou strukturu systému Windows 2000. K vytvoření cílové doménové struktury systému Windows 2000, která odráží požadavky a strukturu definovanou v rámci činností plánování oboru názvů organizace, použijte standardní postup. Domény vytvořené v nové doménové struktuře budou doménami Windows 2000 pracujícími v nativním režimu.
2. Vytvořte vztahy důvěryhodnosti potřebné k tomu, aby byl v doménové struktuře udržen přístup k prostředkům. To zahrnuje zjištění všech existujících vztahů důvěryhodnosti mezi doménami prostředků a zdrojovou doménou Windows NT pomocí nástroje Netdom.

Výstup programu Netdom pak můžete porovnat se seznamem vztahů důvěryhodnosti potřebnými k tomu, aby byl uživatelům a skupinám v cílové doméně umožněn přístup k prostředkům. Pak pomocí nástroje Netdom vytvořte všechny potřebné vztahy důvěryhodnosti, které ještě neexistují.

3. Klonujte všechny zdrojové globální skupiny do cílové domény. Většina prostředků je chráněna seznamy ACL, které se odkazují na globální skupiny a to obvykle nepřímo přes sdílené místní skupiny nebo místní skupiny počítače. Po vytvoření vztahů důvěryhodnosti musíte zajistit dostupnost odpovídajících globálních skupin v cílové doméně.

Nejjednodušší metodou, jak toho dosáhnout, je klonovat všechny globální skupiny pomocí nástroje ClonePrincipal.

4. Identifikujte a klonujte sady uživatelů. Po dokončení klonování zdrojových globálních skupin do cílové domény můžete začít s úkolem migrace uživatelů.

To je interaktivní úkol, protože většinou chcete přesunovat sady uživatelů. To znamená, že musíte určit migrované sady uživatelů a následně zdrojové uživatele klonovat do cílové domény pomocí nástroje ClonePrincipal.

5. Odstavte zdrojovou doménu. Jakmile dojde k trvalému přesunutí všech uživatelů a skupin do cílové doménové struktury, vaším posledním úkolem bude odstavit zdrojovou doménu. To zahrnuje vypnutí a odstranění nejprve řadičů BDC zdrojové domény a následně vypnutí řadiče PDC zdrojové domény. Doporučujeme vám uložit si PDC pro účely zotavení po havárii.

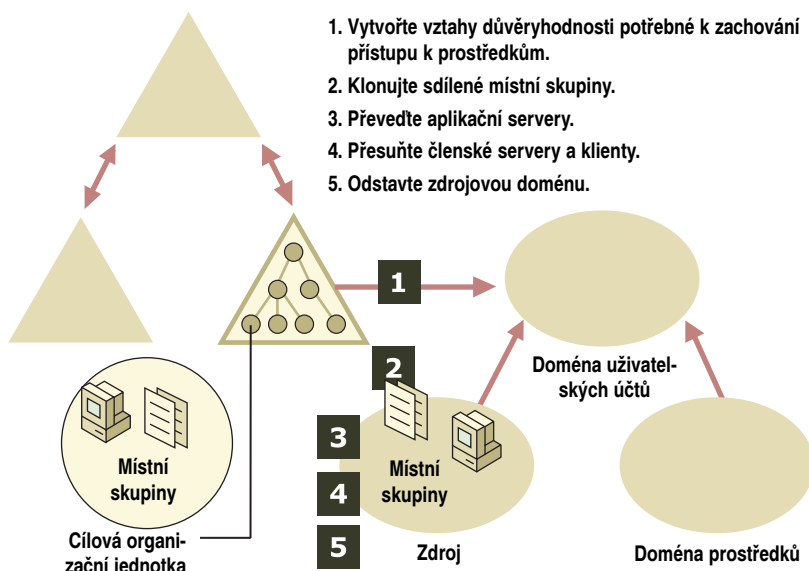
Máte-li v úmyslu dané řadiče domény přiřadit do nové doménové struktury, můžete je inovovat na systém Windows 2000 a pak je buď povýšit na řadiče domény nebo je ponechat jako členské servery.

Zejména během fáze migrace uživatelů je moudré otestovat přihlášení určitých uživatelů během každé migrace. Dojde-li k chybě v nějaké fázi ještě před odstavením zdrojové doménové struktury, můžete celý proces zastavit a práce může pokračovat ve zdrojové produkční doméně.

Scénář #2:

Konsolidace domény prostředků do organizační jednotky

V tomto příkladu konsolidujete nějakou doménu prostředků do organizační jednotky v doméně Windows 2000 pracující v nativním režimu. To můžete učinit v zájmu omezení nákladů na správu složitých vztahů důvěryhodnosti. Obrázek 10.10 ukazuje tento příklad. V tomto oddílu jsou také popsány kroky a základní nástroje potřebné pro postupnou migraci.



Obrázek 10.10 Konsolidace zdrojové domény do organizační jednotky systému Windows 2000

V tomto příkladu se aplikační servery stávají členskými servery v cílové organizační jednotce (OU). Předpokládá se, že aplikační servery v jednotlivých doménách používají sdílené místní skupiny. Také se předpokládá, že domény mohou obsahovat některé členské servery a klienty.

Po dokončení restrukturalizace domén můžete přestat používat staré domény. Proces konsolidace domény prostředků do OU systému Windows 2000 vypadá takto:

1. Vytvořte všechny požadované vztahy důvěryhodnosti od cílové domény k doménám účtů mimo doménovou strukturu. To zahrnuje zjištění všech existujících vztahů důvěryhodnosti mezi doménami prostředků a doménami účtů pomocí nástroje Netdom. Výstup programu Netdom pak můžete porovnat se vztahy důvěryhodnosti které již mezi cílovou doménou a doménami účtů existují. Pak pomocí nástroje Netdom vytvořte všechny potřebné vztahy důvěryhodnosti, které ještě neexistují.
2. Klonujte všechny sdílené místní skupiny. Sdílené místní skupiny mají rozsah jen v rámci domény, v níž byly vytvořeny, a jsou sdílené pouze mezi řadiči v dané doméně. Nemusíte okamžitě přesunovat všechny řadiče domény do cílového místa. Chcete-li zajistit udržení přístupu k prostředkům v době, kdy jsou řadiče domén a prostředky rozděleny mezi zdrojovou a cílovou doménou, musíte klonovat sdílené místní skupiny do cílové domény pomocí nástroje ClonePrincipal.
3. Převedte aplikační servery na členské servery. Po dokončení klonování všech místních sdílených skupin můžete začít převádět aplikační servery na členské servery v cílové OU.

Inovujte řadič PDC domény prostředků na systém Windows 2000 a během přechodného období provozujte doménu v kombinovaném režimu. Pak můžete inovovat všechny převáděné řadiče BDC. Při inovování řadiče BDC spusťte Průvodce insta-

lací službou Active Directory (Active Directory Installation Wizard) a zvolte změnu řadiče BDC na členský server.

Není-li inovace řadiče PDC možná nebo žádoucí, pak musíte během jednotlivých inovací převádět řadiče BDC do režimu offline a povyšovat je na PDC. Po povýšení řadiče BDC na PDC jej můžete inovovat na systém Windows 2000, čímž vlastně učiníte z offline řadiče domény řadič PDC v „klonované“ doméně Windows 2000 pracující v kombinovaném režimu. Po inovaci řadiče PDC offline můžete spustit Průvodce instalací služby Active Directory (Active Directory Installation Wizard) a převést daný řadič PDC na členský server. Členský server pak připojíte k cílové doméně.

4. Přesuňte členské servery (včetně dřívějších řadičů BDC) a klienty. V tomto kroku můžete pomocí nástroje Netdom vytvořit pro přesunovaný členský server nebo klienta účet počítače v OU cílové domény. Počítač připojte k cílové doméně.
5. Odstavte zdrojovou doménu. Jakmile dojde k trvalému přesunutí všech skupin a počítačů do cílové doménové struktury, vašim posledním úkolem bude zrušit zdrojovou doménu. To zahrnuje vypnutí a odstranění nejprve řadičů BDC zdrojové domény a následně vypnutí řadiče PDC zdrojové domény.

Máte-li v úmyslu dané řadiče domény přiřadit do nové doménové struktury, můžete je inovovat na systém Windows 2000 a pak je buď povýšit na řadiče domény Windows 2000 nebo je ponechat jako členské servery.

Poznámka V tomto scénáři musíte řadiče BDC převedené na členské servery co nejdříve přesunout do cílové domény. Nenachází-li se doména v nativním režimu a jestliže nebyly sdílené místní skupiny převedeny na místní skupiny domény, prostředky přístupné přes tyto skupiny nebudou na členských serverech dostupné.

Nástroje migrace domén

Tento oddíl obsahuje obecné informace o sadách Domain Migration Basic Utilities a *Windows 2000 Server Resource Kit* zmíněných na jiných místech této kapitoly. Úplnou dokumentaci funkcí a použití najdete ve zdrojích uvedených v jednotlivých oddílech.

Nástroj ClonePrincipal

ClonePrincipal je nástroj, který se skládá z následujících objektů COM a ukázkových skriptů. Skripty si můžete upravit v jazyku Visual Basic.

- **DSUtils.ClonePrincipal**, objekt COM podporující tři metody:
- **AddSidHistory** Kopíruje identifikátor SID zdrojového komitenta do atributu SIDhistory existujícího cílového komitenta.
- **CopyDownlevelUserProperties** Kopíruje vlastnosti zdrojového komitenta systému Windows NT do cílového komitenta.
- **Connect** Vytváří ověřená připojení k řadičům zdrojové a cílové domény.

ClonePrincipal vám umožňuje postupně migrovat uživatele do prostředí systému Windows 2000, aniž by to mělo vliv na existující produkční prostředí systému Windows NT. Toho se dosahuje vytvářením klonů uživatelů a skupin systému Windows NT v prostředí systému Windows 2000. Výhody dosažené tímto využitím nástroje ClonePrincipal jsou tyto:

- Uživatelé se mohou připojovat k cílovému účtu (klonu), ale přitom mít stále možnost během zkušebního období se v případě havárie vrátit ke zdrojovému účtu.
- Do cílového prostředí systému Windows 2000 lze uvést několik uživatelů najednou.
- Zdrojové produkční prostředí není během migrace uživatelů do cílového prostředí systému Windows 2000 narušeno.
- Není nutné aktualizovat seznamy ACL v zájmu zachování členství ve skupinách a síťového přístupu pro cílové účty.
- Více skupin se stejným názvem nebo účelem z různých zdrojových domén lze „sloučit“ do jediného cílového objektu.

Navíc můžete konsolidovat větší počty malých domén prostředků do organizačních jednotek systému 2000 tak, že pomocí nástroje ClonePrincipal klonujete místní skupiny.

Pamatujte, že metoda AddSidHistory je bezpečnostně citlivá operace, pro kterou platí následující omezení:

- Metoda AddSidHistory vyžaduje, abyste ve zdrojové a cílové doméně měli nebo zadali pověření na úrovni Domain Administrator (správce domény). Zdroj a cíl se NESMÍ nacházet ve stejné doménové struktuře. Mezi zdrojovou a cílovou doménou sice může existovat externí vztah důvěryhodnosti, takový vztah však není pro tuto funkci nutný.
- Události metody AddSidHistory lze auditovat, což zajišťuje, že správci jak zdrojové tak i cílové domény mohou detekovat spuštění této funkce. Auditování ve zdrojové doméně je doporučeno, nikoli však vyžadováno, zatímco auditování v cílové doméně MUSÍ být povoleno, aby funkce AddSidHistory proběhla úspěšně.
- Ukázkové skripty nástroje ClonePrincipal volají metodu AddSidHistory, a proto pro další součásti nástroje ClonePrincipal platí stejná bezpečnostní omezení a pravidla jako pro metodu AddSidHistory.

Program Netdom

Netdom je nástroj, který vám umožňuje spravovat domény a vztahy důvěryhodnosti systému Windows 2000 z příkazového řádku.

Program Netdom lze použít pro:

- připojení počítače se systémem Windows 2000 k doméně Windows NT nebo Windows 2000 a k:
 - zajištění možnosti určit OU pro účet počítače,
 - vytvoření náhodného hesla počítače při počátečním připojení,
- správu účtů počítačů pro členské klienty a členské servery domény:
 - přidání, odstranění a dotaz,
 - zajištění možnosti určit OU pro účet počítače (zajištění možnosti přesunout existující účet počítače členského klienta z jedné domény do druhé a udržet popiso-
vač zabezpečení na účtu počítače),

- vytvoření (jedno- nebo obousměrných) vztahů důvěryhodnosti mezi doménami včetně vztahu důvěryhodnosti pro následující typy domén:
 - domény systému Windows NT,
 - nadřízené a podřízené domény Windows 2000 v doménové struktuře,
 - část systému Windows 2000 propojení vztahu důvěryhodnosti ke sféře protokolu Kerberos,
- ověření a reset zabezpečeného kanálu pro následující konfigurace:
 - členské servery a klienti,
 - řadiče BDC v doméně Windows NT,
 - specifické repliky systému Windows 2000,
- správy vztahů důvěryhodnosti mezi doménami:
 - zobrazení všech vztahů důvěryhodnosti,
 - vytvoření výčtu přímých vztahů důvěryhodnosti,
 - vytvoření výčtu všech (přímých a nepřímých) vztahů důvěryhodnosti.

Seznam úkolů plánování migrace

Tabulka 10.7 představuje souhrn úkolů souvisejících s plánováním migrace.

Tabulka 10.7 Souhrn úkolů plánování migrace

Úkol	Umístění v kapitole
Určete cestu postupné migrace.	Začátek procesu plánování migrace
Určete podporované cesty inovace.	Plánování inovace domén
Prozkoumejte existující strukturu domén.	Plánování inovace domén
Vyviňte plán zotavení.	Plánování inovace domén
Určete strategii inovace řadičů domén.	Plánování inovace domén
Určete pořadí inovace domén.	Plánování inovace domén
Určete okamžik přechodu na nativní režim.	Plánování inovace domén
Určete důvody restrukturalizace domén.	Plánování restrukturalizace domén
Určete okamžik restrukturalizace domén.	Plánování restrukturalizace domén
Přesuňte uživatele a skupiny.	Plánování restrukturalizace domén
Přesuňte počítače.	Plánování restrukturalizace domén
Přesuňte členské servery.	Plánování restrukturalizace domén
Vytvořte vztahy důvěryhodnosti.	Plánování restrukturalizace domén
Klonujte komitenty zabezpečení.	Plánování restrukturalizace domén
Přepněte se do nativního režimu.	Plánování inovace domén
	Plánování restrukturalizace domén

KAPITOLA 11

Plánování distribuovaného zabezpečení

Plán zabezpečení je základní součástí vašeho plánu zavedení systému Microsoft Windows 2000. Na jeho tvorbě se budou podílet zástupci mnoha podřízených týmů zavádění. Tato kapitola vás provede strategií plánování distribuovaného zabezpečení ve vaší síti systému Windows 2000. Načrtává zásadní cíle plánu distribuovaného zabezpečení a představuje také funkce zabezpečení systému Windows 2000.

Tato kapitola staví do správného kontextu důležité faktory, které je třeba zvážit, chcete-li využívat zabezpečení systému Microsoft Windows 2000 efektivně. Distribuované počítačové zabezpečení je však velmi složité téma, které budete muset dále studovat.

V této kapitole

Vývoj plánu zabezpečení sítě 310

Ověřování veškerého přístupu uživatelů 315

Aplikování řízení přístupu 322

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Analýza bezpečnostních rizik
- Strategie zabezpečení
- Popisy skupin se zabezpečením a související zásady
- Strategie přihlašování k síti a ověřování
- Strategie zabezpečení informací
- Zásady správy

Související informace v sadě Resource Kit

- Další informace o distribuovaném zabezpečení najdete v knize *Microsoft Windows 2000 Server Distribuované systémy*.
- Další informace o skupinách se zabezpečením najdete v kapitole „Návrh struktury služby Active Directory“ v této knize.
- Další informace o infrastruktuře veřejných klíčů najdete v kapitole „Plánování infrastruktury veřejných klíčů“ v této knize.

Vývoj plánu zabezpečení sítě

Distribuované zabezpečení zahrnuje koordinaci mnoha bezpečnostních funkcí na počítačové síti, jejímž cílem je zavést celkové zásady zabezpečení. Distribuované zabezpečení umožňuje uživatelům přihlašovat se k příslušným počítačovým systémům, vyhledávat informace, které potřebují, a používat je. Mnoho z informací na počítačových sítích si může přečíst kdokoli, ale jen malá skupina lidí je může aktualizovat nebo upravit. Jedná-li se o citlivé nebo soukromé informace, mohou odpovídající soubory číst pouze oprávnění jednotlivci nebo skupiny. Důležitá je také ochrana a soukromí informací přenášených přes veřejné telefonní sítě, internet a dokonce i segmenty interních sítí společnosti.

Technologie zabezpečení patří sice mezi nejpokročilejší technologie, ale samotné zabezpečení je ještě zapotřebí zkombinovat s dobrými obchodními a sociálními praktikami. Nezáleží na tom, jak pokročilá a dobře implementovaná daná technologie je – vždy bude jen tak dobrá, jak vhodné budou metody jejího zavádění a správy.

Plán zabezpečení sítě vyvíjí váš tým zavedení zabezpečení. Plán zavedení zabezpečení sítě popisuje, jak se použijí funkce distribuovaného zabezpečení systému Windows 2000 k zavedení řešení distribuovaného zabezpečení a k zajištění informací. Typický plán zabezpečení obsahuje oddíly ukázané v tabulce 11.1.

Tabulka 11.1 Oddíly v plánu zabezpečení

Oddíl v plánu	Popis
Bezpečnostní rizika	Uvádí typy bezpečnostních rizik ovlivňujících váš podnik.
Strategie zabezpečení	Popisuje obecné strategie zabezpečení nezbytné k odstranění rizik.
Zásady infrastruktury veřejných klíčů	Obsahuje vaše plány zavedení certifikačních úřadů podporujících funkce interního a externího zabezpečení.
Popisy skupin se zabezpečením	Zahrnuje popisy skupin se zabezpečením a jejich vzájemné vztahy. Tento oddíl přiřazuje zásady skupiny ke skupinám se zabezpečením.
Zásady skupiny	Ukazuje, jak se nakonfigurují bezpečnostní nastavení zásad skupiny, jako jsou zásady síťových hesel.
Strategie přihlášení k síti a ověřování	Obsahuje strategie ověřování pro přihlašování k síti a pro přihlašování vzdáleným přístupem a pomocí karet Smart Card.
Strategie zabezpečení informací	Říká, jak budou implementována řešení zabezpečení informací, jako je zabezpečené elektronická pošta a zabezpečená webová komunikace.
Zásady správy	Zahrnuje zásady delegování úkolů správy a sledování protokolů událostí v zájmu odhalení podezřelých činností.

Váš plán zabezpečení sítě může obsahovat ještě další oddíly, minimem by však měly být ty uvedené v tabulce. Vaše organizace také může potřebovat více plánů zabezpečení, což bude záviset na rozsahu vašeho zavádění. Mezinárodní organizace může potřebovat samostatné plány pro všechna svá oddělení nebo lokace, zatímco regionální

organizaci postačí jediný plán. Organizace s různými zásadami pro různé skupiny uživatelů mohou vyžadovat samostatný plán zabezpečení sítě pro každou skupinu.

Plány zabezpečení sítě otestujte a revidujte v testovací laboratoři, která představuje počítačové prostředí ve vaší organizaci. Pro další testování a ladění plánů zabezpečení sítě použijte pilotní programy.

Bezpečnostní rizika

Ještě než se v této kapitole podíváme na funkce zabezpečení systému Windows 2000, musíme se seznámit s typy problémů zabezpečení sítě, kterým manažeri oddělení IT čelí. Tabulka 11.2 popisuje několik typů bezpečnostních rizik a představuje obecný základ následujícího pojednání o funkcích, strategiích a technologiích zabezpečení. Vytvoříte-li si podobný seznam ve svém plánu zabezpečení, lépe si uvědomíte složitost bezpečnostních problémů, které před vámi stojí, a pomůže vám to k určení sady standardních popisů jednotlivých kategorií rizik.

Tabulka 11.2 Typy bezpečnostních rizik v organizaci

Bezpečnostní riziko	Popis
Zachycení identity	Narušitel odhalí uživatelské jméno a heslo nějakého platného uživatele. K tomu může dojít mnoha různými sociálními i technologickými metodami.
Maskování	Neoprávněný uživatel se tváří jako platný uživatel. Narušitel například převezme adresu IP důvěryhodného systému a použije ji k získání přístupových oprávnění přiřazených danému zařízení nebo systému.
Útok opakováním	Narušitel si zaznamená síťovou výměnu mezi uživatelem a serverem a jejím pozdějším přehráním se vydává za původního uživatele.
Zachycení dat	Jestliže se data přenášejí přes síť v prostém textu, mohou je sledovat a zachycovat neoprávněné osoby.
Manipulace	Narušitel způsobí změnu nebo poškození síťových dat. K manipulaci jsou náchylné nešifrované síťové finanční transakce. Síťová data mohou poškodit také viry.
Popření, odvolání	Síťové obchodní a finanční transakce jsou kompromitovány, jestliže si nemůže být příjemce transakce jistý, kdo zprávu odeslal.
Makroviry	Viry specifické jednotlivým aplikacím mohou zneužít makrojazyk složitých dokumentů a pracovních listů.
Nedostupnost služby	Narušitel zahltní server požadavky spotřebovávajícími systémové prostředky a buď způsobí zhroucení serveru nebo zabrání jeho užitečnému využívání. Zhroucení serveru někdy nabízí možnosti průniku do systému.
Zlomyslný mobilní kód	Tento termín představuje zlomyslný kód spuštěný jako automaticky vykonávaný ovládací prvek ActiveX nebo applet jazyka Java nahráný z internetu na webový server.

Zneužití privilegií	Správce počítačového systému vědomě nebo chybně použije svá plná privilegia v operačním systému k získání soukromých dat.
Trojský kůň	Jedná se o obecný termín zlomyslných programů, které se tváří jako zajímavé a neškodné nástroje.
Útok sociálním inženýrstvím	Průnik do sítě může být někdy velmi jednoduchý – stačí zavolat novému zaměstnanci, oznámit mu, že jste z oddělení IT, a požádat ho o ověření jeho hesla pro vaše záznamy.

Koncepty zabezpečení

Následující koncepty jsou užitečné při popisu strategií distribuovaného zabezpečení v systému Windows 2000. Možná bude vhodné vložit je do plánu zabezpečení, aby se jeho čtenáři seznámili s distribuovaným zabezpečením.

Model zabezpečení

Zabezpečení systému Windows 2000 vychází z jednoduchého modelu ověřování a autorizování, který využívá adresářovou službu Microsoft Active Directory. Ověřování identifikuje uživatele při přihlašování a při síťových připojení ke službám. Po ověření je uživateli na základě oprávnění umožněn přístup k určité sadě síťových prostředků. Autorizování se uskutečňuje pomocí mechanismů řízení přístupu a využívá seznamy řízení přístupu (access control list – ACL) definující oprávnění v systému souborů, na síťových místech sdílení souborů a tiskáren a v položkách Active Directory.

Model domény

V systému Windows 2000 je doména kolekcí síťových objektů, jako jsou uživatelské účty, skupiny a počítače, které sdílejí z hlediska zabezpečení společnou adresářovou databázi. Doména určuje bezpečnostní autoritu a formuje hranice zabezpečení s konzistentními interními zásadami a explicitními vztahy zabezpečení s jinými doménami.

Správa důvěryhodnosti

Důvěryhodnost je logický vztah ustavený mezi doménami, který umožňuje průchozí ověřování – důvěřující doména věří přihlašovacím ověřením důvěryhodné domény. Termín tranzitivní či přenosná důvěryhodnost představuje ověřování přes řetězec vztahů důvěryhodnosti. V systému Windows 2000 podporují vztahy důvěryhodnosti ověřování mezi doménami pomocí protokolu Kerberos v5 a ověřování NTLM, což zajišťuje zpětnou kompatibilitu.

Zásady zabezpečení

Nastavení zásad zabezpečení definují bezpečnostní chování systému. Pomocí objektů zásad skupiny služby Active Directory mohou správci centrálně aplikovat přesně zadané bezpečnostní profily na různé třídy počítačů v podniku. Součástí systému Windows 2000 je například výchozí objekt zásad skupiny nazvaný Default Domain Controllers Policy (výchozí zásady řadičů domén), který řídí bezpečnostní chování řadičů domény.

Konfigurace a analýza zabezpečení

Konfigurace a analýza zabezpečení (Security Configuration and Analysis), funkce systému Windows 2000, nabízí možnost porovnat nastavení zabezpečení počítače se stan-

dardní šablonou, zobrazit si výsledky a vyřešit všechny nesoulady zjištěné touto analýzou. Šablonu zabezpečení lze také importovat do objektu zásad skupiny a aplikovat daný profil zabezpečení na mnoho počítačů najednou. Systém Windows 2000 obsahuje několik předdefinovaných šablon zabezpečení vhodných pro různou úroveň zabezpečení a pro různé typy serverů a klientů na síti.

Šifrování symetrickým klíčem

Šifrování symetrickým klíčem, které se také označuje za šifrování tajným klíčem, používá k šifrování i k dešifrování dat stejný klíč. Zaručuje rychlé zpracování dat a používá se v mnoha formách šifrování dat na sítích a v systémech souborů.

Šifrování veřejným klíčem

Šifrování veřejným klíčem má dva klíče, jeden veřejný a jeden soukromý. Oba klíče mohou zašifrovat data, které pak lze dešifrovat pouze druhým z klíčů. Tato technologie otevírá řadu strategií zabezpečení a je základem několika funkcí zabezpečení systému Windows 2000. Tyto funkce vycházejí z infrastruktury veřejných klíčů (public key infrastructure – PKI). Další informace o PKI najdete v kapitole „Plánování infrastruktury veřejných klíčů“ v této knize.

Ověřování

Ověřování potvrzuje identitu všech uživatelů, kteří se pokoušejí přihlásit k síti nebo přistoupit k síťovým prostředkům. Ověřování systému Windows 2000 umožňuje jediné přihlášení ke všem síťovým prostředkům. Při jediném přihlášení se může uživatel přihlásit ke klientskému počítači jen jednou pomocí jediného hesla nebo karty Smart Card, a ověřit se tak pro všechny počítače v doméně. Ověřování je v systému Windows 2000 implementováno pomocí protokolu Kerberos v5, protokolu NTLM, nebo funkcí přihlašování systému Windows NT pro doménu Windows NT 4.0.

Jediné přihlášení

Uživatelům se nelíbí, když se musí zvlášť přihlašovat na různé síťové servery a aplikace. Uživatel tak někdy musí zadávat různá hesla pro přihlášení k místnímu počítači, při přístupu na souborový nebo tiskový server, při odesílání elektronické pošty, při použití databáze atd. Různé servery mohou v různých intervalech vyžadovat změnu hesel a často přitom neumožňují opakované používání hesel. Normální uživatel si tedy musí pamatovat na půl tuctu hesel. Nejenže je pak ověřování pro uživatele únavné, v určitý okamžik si však navíc začnou někde zapisovat seznam aktuálních hesel. Tímto způsobem může být síť používající více hesel náchylná k zachycení identity.

Strategie jediného přihlášení vyžaduje, aby se uživatelé interaktivně ověřili jen jednou – následně je umožněno ověřené přihlášení k dalším síťovým aplikacím a službám. Tyto další události přihlášení jsou pro uživatele transparentní.

Dvoufaktorové ověřování

Dvoufaktorové ověřování vyžaduje, aby uživatelé poskytli nějaký fyzický objekt, v němž je zakódována jejich identita, a navíc ještě heslo. Nejobvyklejším případem dvoufaktorového ověřování jsou karty výdejních bankomatů, které ještě navíc vyžadují osobní identifikační číslo (PIN).

Další formou dvoufaktorového ověřování je biometrická identifikace. Speciální zařízení skenuje namísto nějaké karty otisk ruky nebo prstu, duhovku, sítnici nebo hlas. Pak

uživatel zadá příslušné heslo. Toto pojetí zabezpečení je sice drahé, ale velmi znesnadňuje zachycení identity a maskování.

Pro obchodní podniky se nejlepší dvoufaktorovou technologií jeví být karty Smart Card. Takové karty nejsou o mnoho větší než karty do bankomatů a uživatel je fyzicky nosí s sebou. Karty obsahují čip, v němž je uložen digitální certifikát a soukromý klíč uživatele. Po vložení karty do čtečky na klientském počítači zadá uživatel heslo nebo PIN. Protože soukromý klíč se nachází na čipu v kapse uživatele, narušitel sítě jej bude jen velmi obtížně získávat. Systém Windows 2000 přímo podporuje ověřování kartami Smart Card.

Řízení přístupu

Řízení přístupu je modelem implementování ověřování. Jakmile je uživatel ověřen v nějaké doméně a pokusí se přistoupit k určitému prostředku, jako je soubor na síti, určí se typ povolené operace na základě oprávnění přiřazených prostředku, tedy například pouze pro čtení nebo pro čtení i zápis. Řízení přístupu je v systému Windows 2000 zavedeno pomocí seznamů ACL specifických jednotlivým objektům. Seznam ACL si můžete zobrazit na kartě **Zabezpečení** (Security) okna vlastností souboru nebo složky. Tento seznam obsahuje názvy skupin uživatelů, které mají k danému objektu přístup.

Integrita dat

Zajistit integritu dat znamená chránit data před zlomyslnými i náhodnými úpravami a změnami. V případě uložených dat to znamená, že je mohou upravovat, přepisovat a odstraňovat jen autorizovaní uživatelé. Na síti to znamená, že datový paket musí obsahovat digitální podpis, aby mohl cílový počítač případnou manipulaci s paketem detekovat.

Důvěrnost dat

Strategie důvěrnosti dat znamená šifrování dat před jejich průchodem sítí a následné dešifrování. Tato strategie brání ve čtení dat někým, kdo odposlouchává síť (zachytává data). Paket nezašifrovaných dat přenášený přes síť si lze jednoduše zobrazit na libovolném síťovém počítači pomocí nějakého programu sledování paketů nahrانého z internetu.

Neodvolatelnost

Strategie neodvolatelnosti má dvě části. První zajišťuje, aby určitý uživatel nemohl popřít, že odeslal nějakou zprávu. Druhá část zaručuje, že zprávu nemůže odeslat někdo jiný, kdo se jen maskuje a vydává za daného uživatele.

Jedná se o další aplikaci infrastruktury veřejných klíčů. Jako digitální podpis zprávy se používá soukromý klíč uživatele. Jestliže příjemce dokáže přečíst zprávu pomocí veřejného klíče odesílatele, pak mohl danou zprávu odeslat jen daný uživatel a nikdo jiný.

Ověřování kódu

Tato strategie vyžaduje, aby byl kód nahrانý z internetu podepsán digitálním podpisem důvěryhodného tvůrce softwaru. Webové prohlížeče lze nakonfigurovat tak, aby nespouštěly nepodepsaný kód. Podepisování softwaru potvrzuje autenticitu kódu, tedy že s ním po publikování nebylo manipulováno, a nezaručuje tak bezpečnost kódu. Sami se musíte rozhodnout, jakým tvůrcům softwaru budete důvěřovat. (Digitální podpis spustitelného souboru je dalším příkladem infrastruktury veřejných klíčů.)

Protokolování událostí

Auditování správy uživatelských účtů i přístupu k důležitým síťovým prostředkům je důležitou zásadou zabezpečení. Auditování zaznamenává síťové operace a ukazuje, o co se kdo pokoušel. Nejenže to pomáhá detekovat narušení, dojde-li však k odhalení narušitele a k jeho trestnímu stíhání, záznamy událostí představují také právní důkaz obvinění. Vyhledávání a vymazávání či úprava protokolů událostí představuje pro zkušeného narušitele další časově náročný úkol, takže je jeho detekce a včasný zásah jednodušší.

Fyzické zabezpečení

Snad bychom ani nemuseli říkat, že servery důležitých síťových služeb společnosti musí být v nepřístupných prostorách. Jestliže si mohou narušitelé sednout ke konzole síťového serveru, mohou také převzít kontrolu nad síťovým serverem. Nejsou-li důležité síťové servery fyzicky zajištěny, může zhrzený zaměstnanec poškodit váš hardware takovými jednoduchými a starými nástroji, jako je třeba kladivo. Vaše data jsou také otevřená fyzickému útoku: každý začínající uživatel ví, jak se tiskne klávesa Delete. Škody z takových průniků mohou mít za následek právě tak rozsáhlou ztrátu dat a výpadek, jaké mohou být zapříčiněny promyšlenějším, externím útokem na vaši síť. Útoky na síť nemusí být promyšlené, aby byly efektivní.

Školení uživatelů

Nejlepší ochranou před útokem sociálním inženýrstvím je vyškolení uživatele v tom smyslu, že mají svá hesla udržovat v tajnosti a zabezpečená. Je zapotřebí jasně stanovit obchodní zásady distribuce kritických informací. Vydejte zásady zabezpečení a trvejte na tom, aby se jimi všichni řídili. Jedním ze způsobů školení je jít příkladem: ujistěte se, že vaši profesionálové oddělení IT si chrání svá hesla a že k tomu také vyzývají uživatele.

Strategie distribuovaného zabezpečení

Distribuované zabezpečení představuje logické funkce zabezpečení, které fungují převážně v podnikové síti. Chcete-li zajistit své síťové prostředky, musíte se věnovat sedmi základním strategiím zabezpečení:

- Ověřovat veškerý přístup uživatelů k síťovým prostředkům.
- Aplikovat příslušné řízení přístupu ke všem prostředkům.
- Vytvořit vhodné vztahy důvěryhodnosti mezi doménami.
- Umožnit ochranu citlivých dat.
- Vytvořit jednotné zásady zabezpečení.
- Zavést zabezpečené aplikace.
- Spravovat uspořádání zabezpečení.

Těchto sedm témat musí být centrem vašeho plánu distribuovaného zabezpečení. Na následujících stránkách najdete podrobné pojednání o jednotlivých strategiích.

Ověřování veškerého přístupu uživatelů

Chcete-li zajistit zabezpečení sítě systému Windows 2000, musíte umožnit přístup oprávněným uživatelům, ale vyloučit narušitele, kteří se snaží proniknout dovnitř. To

znamená, že musíte nastavit funkce zabezpečení tak, aby ověřovaly veškerý přístup uživatelů k systémovým prostředkům. Strategie ověřování tvoří jednu úroveň ochrany před narušiteli, kteří se pokoušejí ukrást identity nebo se vydávat za jiné uživatele.

V systému Windows 2000 vychází ověřování uživatelů domény z uživatelských účtů ve službě Active Directory. Správci spravují tyto účty pomocí modulu snap-in Uživatelé a počítače služby Active Directory (Active Directory Users and Computers) konzoly Microsoft Management Console (MMC). Uživatelské účty lze uspořádat do kontejnerů označovaných za „organizační jednotky“, které odrážejí návrh vašeho oboru názvů Active Directory. Výchozím umístěním uživatelských účtů je složka Users (uživatelé) tohoto modulu snap-in.

Když organizace přijme nového uživatele, správce vytvoří pro daného uživatele jediný účet a nebude vytvářet půl tuctu nebo ještě více samostatných účtů na různých serverech a aplikačních databázích. Protože je do podnikového adresáře integrována služba doménového ověřování, daný jediný účet uživatele je také položkou adresáře globálních adresářových informací a poskytuje přístup ke všem síťovým službám. Uživatel se může přihlásit k různým klientským počítačům nebo notebookům v doméně pomocí jediného hesla.

Systém Windows 2000 automaticky podporuje jediné přihlášení pro uživatele v doménové struktuře. Vztahy důvěryhodnosti mezi doménami jsou v doménové struktuře standardně obousměrné, takže ověření v jedné doméně je dostatečné pro odkazované nebo předávané ověřování přístupu k prostředkům v jiných doménách doménové struktury. Uživatel se interaktivně přihlásí na začátku relace a poté již protokoly zabezpečení sítě (protokol Kerberos v5, protokol NTLM a protokol Secure Sockets Layer/Transport Layer Security) transparentně dokazují identitu uživatele všem požadovaným síťovým službám.

Systém Windows 2000 volitelně podporuje přihlašování kartami Smart Card zajišťujícími silné ověřování. Karta Smart Card je identifikační karta, kterou s sebou nosí uživatel a která se používá k interaktivnímu přihlášení namísto hesla. Lze ji také využít v případě vzdálených telefonických připojení k síti a jako místo pro ukládání certifikátů veřejných klíčů používaných pro klientské ověřování protokolem Secure Sockets Layer (SSL) nebo zabezpečenou elektronickou poštu.

Ověřování se neomezuje jen na uživatele. Ověřují se také počítače a služby, když se síťově připojují k jiným serverům. Například serverové a klientské počítače se systémem Windows 2000 se během spouštění připojují ke své službě Active Directory domény a přebírají informace o zásadách. Ověřují se ve službě Active Directory a nahrávají si odtud zásady počítače ještě předtím, než se k danému počítači může přihlásit nějaký uživatel. Počítače a služby poskytují svou identitu také klientům, kteří vyžadují vzájemné ověření. Vzájemné ověřování zabráňuje narušiteli v přidání dalšího počítače mezi klienta a skutečný síťový server, přičemž tento další počítač se bude vydávat za něco jiného.

Počítačům a službám lze „důvěřovat pro delegování“. To znamená, že služby mohou skutečňovat další síťová připojení „jménem“ uživatele, aniž by znaly jeho heslo. Než bude moci služba vytvořit nové síťové připojení k jinému počítači jménem uživatele, musí mít k této službě uživatel již vytvořené vzájemně ověřené síťové připojení. To je užitečné pro vícevrstvé aplikace vytvořené tak, aby využívaly možnost jediného přihlášení při přístupu na více počítačů. Tato funkce je užitečná zejména v kontextu systému Encrypting File System (EFS) běžícího na souborovém serveru. Chcete-li používat nějakou službu k delegování síťového připojení, použijte modul snap-in Uživatelé a počí-

tače služby Active Directory (Active Directory Users and Computers) konzoly MMC. V okně vlastností pak zaškrtněte políčko **Důvěřovat počítači pro delegování** (Trust computer for delegation).

Úvahy o plánování

Při plánování zásad ověřování se zabývejte také následujícími úvahami a doporučenými postupy.

Nejednodušším způsobem ochrany před nástroji útočícími brutální silou nebo odhalováním hesel postupným zkoušením podle slovníku je zavést a vynutit si používání dlouhých, složitých hesel. Systém Windows 2000 vám umožňuje nastavit zásady řídicí složitost, délku a životnost hesel a možnost opakovaně je používat. Složitě heslo má deset nebo více znaků, obsahuje malé i velké znaky, interpunkční znaménka a čísla. Příkladem složitěho hesla je: „NarodilJsem,Se,623“.

Mnohem silnější ověřování než hesla nabízejí karty Smart Card, vyžadují však ještě dodatečná opatření a zařízení. Karty Smart Card vyžadují konfiguraci certifikačních služeb, zařízení pro čtení karet a samotné karty Smart Card. Další informace o zavádění karet Smart Card najdete v oddílu „Přihlašování pomocí karet Smart Card“ dále v této kapitole a v kapitole „Plánování infrastruktury veřejných klíčů“ v této knize.

Nezávislí výrobci nabízejí různé výrobky poskytující dvoufaktorové ověřování, jako jsou „bezpečnostní odznaky“ a biometrické příslušenství. Tato příslušenství používají rozšiřitelné funkce grafického rozhraní přihlašování uživatele systému Windows 2000 a poskytují alternativní metody ověřování uživatelů.

Velmi mocnou schopností je „důvěřování počítači pro delegování“. Standardně není tato možnost aktivní a její umožnění na určitých účtech počítačů a služeb vyžaduje privilegia správce domény. K počítačům a účtům, kterým je důvěřováno pro delegování, musí být omezený přístup, aby nemohlo dojít k zavedení programů trojských koňů, které by této schopnosti vytváření síťových připojení jménem uživatelů zneužily.

Některé účty jsou příliš citlivé na to, aby na nich bylo možno povolit delegování dokonce i důvěryhodným serverem. Jednotlivé uživatelské účty lze nastavit tak, aby je nebylo možné delegovat, i když lze dané službě důvěřovat pro delegování. Chcete-li využít tuto funkci, přejděte do modulu snap-in Uživatelé a počítače služby Active Directory (Active Directory Users and Computers) konzoly MMC a otevřete si okno vlastností příslušného účtu. Vyhledejte políčko **Účet je citlivý a nelze jej delegovat** (Account is sensitive and cannot be delegated) na kartě **Účet** (Account) okna vlastností.

Ověřování protokolem Kerberos a důvěryhodnost

Protokol ověřování Kerberos je technologie umožňující jediné přihlášení k síťovým prostředkům. Systém Windows 2000 používá protokol Kerberos v5 k zajištění rychlého, jediného přihlášení k síťovým službám v doméně a ke službám, jež se nacházejí v důvěryhodných doménách. Protokol Kerberos ověřuje jak identitu uživatele tak i síťových služeb a zajišťuje tak vzájemné ověření.

Fungování ověřování protokolem Kerberos

Jakmile uživatel zadá svá oprávnění v doméně (prostřednictvím přihlášení uživatelským jménem a heslem nebo kartou Smart Card), systém Windows 2000 vyhledá server služby Active Directory a ověřovací službu Kerberos. Služba Kerberos vydá uživateli „lístek“. Jedná se o dočasný certifikát obsahující informace, jež identifikují uživatele síťo-

vým službám. Po úvodním interaktivním přihlášení se první lístek služby Kerberos použije k požadování dalších lístků služby Kerberos umožňujících přihlášení k následným síťovým službám. Tento proces je složitý a zahrnuje vzájemné ověřování uživatele a serveru, pro uživatele je však úplně transparentní. (Další informace o ověřování protokolem Kerberos v5 najdete v nápovědě systému Windows 2000 Server.)

Ověřování protokolem Kerberos omezuje počet hesel, která si uživatel musí pamatovat, a snižuje tak riziko zachycení identity. Vztahy důvěryhodnosti mezi doménami v doménové struktuře rozšiřují rozsah ověřování protokolem Kerberos na širokou oblast síťových prostředků.

Implementace ověřování protokolem Kerberos

Implementace ověřování protokolem Kerberos si neklade žádné předběžné požadavky. Protokol Kerberos se používá v celém systému Windows 2000 a nemusíte jej ani instalovat ani inicializovat.

Parametry zásad zabezpečení protokolu Kerberos lze nastavit v modulu snap-in Zásady skupiny (Group Policy) konzoly MMC. V objektu zásad skupiny se nastavení protokolu Kerberos nacházejí pod položkou Zásady účtů (Account Policies):

Objekt Zásady skupiny (Group Policy)
Konfigurace počítače (Computer Configuration)
Nastavení systému Windows (Windows Settings)
Nastavení zabezpečení (Security Settings)
Zásady účtů (Account Policies)
Zásady modulu Kerberos (Kerberos Policy)

Tato nastavení smějí používat jen kvalifikovaní správci, kteří jsou s protokolem Kerberos dobře obeznámeni.

Další úvahy o zabezpečení protokolem Kerberos

Chcete-li naplno využít všechny výhody vylepšeného výkonu a zabezpečení ověřování protokolem Kerberos, zvažte zavedení přihlašování protokolem Kerberos jako jediný způsob přihlašování k síti ve vaší společnosti. Systém Windows 2000 implementuje standardní verzi IETF ověřovacího protokolu Kerberos v5 umožňující meziplatformní interoperabilitu. Například uživatelé systémů UNIX mohou použít ověřovací údaje protokolu Kerberos k přihlášení na systémy UNIX a k zabezpečenému připojení ke službám systému Windows 2000 u aplikací, které ověřování protokolem Kerberos podporují. Podnikové sítě, které již využívají ověřování protokolem Kerberos vycházející ze sfér systému UNIX, mohou vytvářet vztahy důvěryhodnosti s doménami systému Windows 2000 a pomocí mapování názvů protokolu Kerberos integrovat ověřování systému Windows 2000 pro účty systému UNIX.

Uvědomte si, že počítače na síti s ověřováním protokolem Kerberos obvykle musí mít svá časová nastavení synchronizována se společnou časovou službou v rámci pěti minut, jinak se ověření nepodaří. Počítače systému Windows 2000 automaticky upravují aktuální čas pomocí řadiče domény, který využívají jako časovou službu sítě. Řadiče domény využívají jako autoritativní časovou službu primární řadič dané domény. I když se aktuální čas na počítačích v jedné doméně nebo mezi doménami liší, systém Windows 2000 automaticky zpracovává rozdíly v hodinách a řeší tak problémy s přihlašováním v těchto situacích.

Při použití přenosné důvěryhodnosti mezi doménami v doménové struktuře, vyhledává služba Kerberos cesty důvěryhodnosti mezi doménami a vytváří systém odkazování

mezi doménami. V rozsáhlých doménových strukturách může být výhodnější vytvořit specificky definované obousměrné vztahy důvěryhodnosti mezi doménami, které často spolupracují. To umožní rychlejší ověření, protože tak předáte protokolu Kerberos „zkratky“, které používá při vytváření systému odkazů.

Ověřování protokolem Kerberos používá transparentní přenosnou (tranzitivní) důvěryhodnost mezi doménami v doménové struktuře, nepodporuje však ověřování mezi doménami v různých doménových strukturách. Chce-li uživatel použít prostředek v jiné doménové struktuře, musí poskytnout údaje platné pro přihlášení k nějaké doméně v dané doménové struktuře. Jestliže existuje jednosměrná důvěryhodnost, aplikace použijí ověřování protokolem NTLM, pokud to zásady zabezpečení povolují.

Systém Windows 2000 zachovává kompatibilitu s ověřovacím protokolem NTLM, aby tak podporoval kompatibilitu s předchozími verzemi operačních systémů společnosti Microsoft. Protokol NTLM můžete nadále používat pro klienty systémů Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows NT 4.0 Server a Windows NT 4.0 Workstation. Ověřování protokolem NTLM se také v systému Windows 2000 používá v aplikacích vytvořených pro předešlé verze Windows NT, jež specificky vyžadují zabezpečení NTLM.

Přihlašování pomocí karet Smart Card

Systém Windows 2000 podporuje volitelné ověřování kartami Smart Card. Karty Smart Card představují velmi bezpečný prostředek ověření uživatelů, interaktivního přihlášení, podepisování kódu a používání zabezpečené elektronické pošty. Zavedení a údržba programu karet Smart Card však vyžaduje další prostředky a náklady.

Fungování karet Smart Card

Karta Smart Card obsahuje čip, v němž je pro různé účely uložen soukromý klíč uživatele, přihlašovací informace a certifikát veřejného klíče. Uživatel vloží kartu do čtečky karet Smart Card připojené k počítači. Pak uživatel zadá své osobní identifikační číslo (PIN), je-li to požadováno.

Karty Smart Card umožňují prostřednictvím uloženého soukromého klíče ověřování, které nelze obejít. Soukromý klíč pak dále zajišťuje další formy zabezpečení související s digitálními podpisy a šifrováním.

Karty Smart Card přímo implementují dvoufaktorové zásady ověřování a nepřímo zajišťují důvěrnost dat, integritu dat a neodvolatelnost více různých akcí, mezi které patří mimo jiné přihlašování k doméně, používání zabezpečená elektronická pošta a zabezpečený přístup k síti WWW.

Požadavky na implementaci karet Smart Card

Karty Smart Card se spoléhají na infrastrukturu veřejných klíčů (PKI) systému Windows 2000. Další informace o PKI najdete v kapitole „Plánování infrastruktury veřejných klíčů“ v této knize.

Implementace karet Smart Card

Kromě PKI a samotných karet potřebuje každý počítač čtečku karet Smart Card. Nastavte alespoň jeden počítač jako stanici zápisu karet Smart Card a k její obsluze autorizujte přinejmenším jednoho uživatele. Kromě čtečky karet není zapotřebí žádný speciální hardware, uživateli obsluhujícímu stanici zápisu však musíte vydat certifikát agenta pro zápis certifikátu (Enrollment Agent).

Podrobné postupy implementování karet Smart Card najdete v nápovědě systému Windows 2000 Server.

Další úvahy o kartách Smart Card

K podpoře přihlašování k doménám systému Windows 2000 kartami Smart Card budete potřebovat podnikový certifikační úřad a nikoli samostatný certifikační úřad nebo certifikační úřad od nezávislého výrobce.

Společnost Microsoft podporuje karty Smart Card a čtečky karet odpovídající průmyslovému standardu Personal Computer/Smart Card (PC/SC) a poskytuje ovladače pro komerčně dostupné čtečky karet Smart Card vyhovující technologii Plug-and-Play. Přihlašování kartami Smart Card je podporováno v systémech Windows 2000 Professional, Windows 2000 Server a Windows 2000 Advanced Server. Výhody zabezpečení vyplývající z použití karet Smart Card se ještě zvýší, jakmile bude moci stále více uživatelů podniku používat karty Smart Card pro ověřování v doméně, vzdálený telefonický přístup k síti a další aplikace.

Systém Microsoft Windows 2000 nepodporuje čtečky karet Smart Card neodpovídající standardům PC/SC a Plug-and-Play. Někteří výrobci mohou sice nabízet ovladače pro čtečky karet Smart Card neodpovídající standardu Plug-and-Play, které budou v systému Windows 2000 fungovat, doporučujeme vám však koupit výhradně čteček karet Smart Card odpovídajících standardům Plug-and-Play a PC/SC.

Karty Smart Card lze zkombinovat s karetními klíči zaměstnanců a identifikačními odznaky a zajistit tak jedinou kartou podporu více funkcí.

Celkové náklady na správu programu karet Smart Card závisejí na několika faktorech, kam patří:

- Počet uživatelů zapsaných v programu karet Smart Card a jejich umístění.
- Vaše postupy vydávání karet Smart Card uživatelům včetně požadavků na ověření identit uživatelů. Budete například požadovat, aby uživatelé prostě předložili platnou osobní identifikační kartu, nebo ještě budete sledovat nějaké další informace? Vaše zásady ovlivní úroveň poskytovaného zabezpečení i vlastní náklady.
- Vaše postupy pro uživatele, kteří svou kartu ztratí nebo někam založí. Vydáte například dočasné karty Smart Card, umožníte dočasné alternativní přihlášení k síti, nebo pošlete uživatele domů, aby svou kartu Smart Card našli? Vaše zásady ovlivní to, kolik pracovní doby se tím ztratí a jaká technická podpora je zapotřebí.

Váš plán zavedení zabezpečení sítě musí popisovat používané metody přihlášení k síti a ověření. Do plánu zabezpečení zahrňte také následující informace:

- Určete strategie přihlášení k síti a ověření, které chcete zavést.
- Popište úvahy o zavedení karet Smart Card a jejich problémy.
- Popište certifikační služby PKI potřebné k podpoře karet Smart Card.

Vzdálený přístup

Směrování a vzdálený přístup (Routing and Remote Access) je služba umožňující vzdáleným uživatelům připojení k vaší síti přes telefonní linky. Tento oddíl se týká pouze funkcí zabezpečení vzdáleného připojení služby Směrování a vzdálený přístup. Vzdálený přístup je už svou podstatou pozvánkou pro narušitele, takže systém Windows 2000 nabízí mnoho funkcí zabezpečení dovolujících povolit oprávněný přístup a omezit možnosti podvodů.

Fungování vzdáleného přístupu

Klient se telefonicky připojí k severu vzdáleného přístupu na vaší síti. Klientovi je umožněn přístup k síti, pokud:

- požadavek odpovídá jedné ze zásad vzdáleného přístupu definovaných na serveru,
- uživatelský účet obsahuje povolení vzdáleného přístupu,
- ověření klient/server proběhne úspěšně.

Jakmile byl klient identifikován a ověřen, lze přístup k síti omezit jen na zadané servery, podsítě a typy protokolů v závislosti na profilu vzdáleného připojení klienta. Jinak se prostřednictvím připojení vzdáleného přístupu zpřístupní uživateli všechny služby typicky dostupné uživateli připojenému k místní síti (včetně sdílení souborů a tiskáren, přístupu k webovému serveru a používání systému zpráv).

Zásady vzdáleného přístupu

Servery se systémem Windows 2000 jsou řízeny zásadami zabezpečení, které určují jejich chování ke vzdálenému připojení. Tyto zásady stanovují, zda server přijme požadavky na vzdálený přístup a pokud ano, v jakých hodinách určitých dnů, jaké protokoly se použijí a jaké typy ověření jsou vyžadovány.

Zásady vzdáleného přístupu se definují pomocí modulu snap-in Správa počítače (Computer Management) konzoly MMC. Zásady se definují v uzlu Zásady vzdáleného přístupu (Remote Access Policies):

Správa počítače (místní) (Computer Management)
Služby a aplikace (Services and Applications)
Směrování a vzdálený přístup (Routing and Remote Access)
Zásady vzdáleného přístupu (Remote Access Policies)

Klepněte pravým tlačítkem myši na zásadu ve stromu konzoly a zadejte příkaz **Vlastnosti** (Properties). Zásady vzdáleného přístupu jsou definovány jako pravidla s podmínkami a akcemi. Jsou-li splněny podmínky, dojde k akci. Jestliže požadavku na vzdálený přístup odpovídá zadaná denní doba, je-li povolen požadovaný protokol a je-li dostupný požadovaný typ portu, pak je přístup umožněn. Je-li přístup umožněn, omezuje se podle profilu přístupu zásad. Dostupné možnosti profilu si zobrazíte stiskem tlačítka **Upravit profil** (Edit Profile).

Povolení vzdáleného přístupu

Chcete-li povolit vzdálený přístup určitému uživateli, otevřete si modul snap-in Uživatelé a počítače služby Active Directory (Active Directory Users and Computers) konzoly MMC. Klepněte pravým tlačítkem myši na uživatele a zadejte příkaz **Vlastnosti** (Properties). V okně vlastností si zobrazte kartu **Telefonické připojení** (Dial-In).

Další informace o vzdáleném přístupu a instalaci a konfigurování serveru vzdáleného přístupu najdete v nápovědě systému Windows 2000 Server. Další informace o ověřování vzdáleného přístupu najdete v kapitole „Server vzdáleného přístupu“ v knize *Microsoft Windows 2000 Server Networking*.

Další úvahy o vzdáleném přístupu

Zaručení vzdáleného přístupu uživateli je neefektivní, neexistují-li příslušné zásady vzdáleného přístupu pro server vzdáleného přístupu.

Systém Windows 2000 podporuje následující možnosti ověřování vzdáleného přístupu:

- Standardní metody ověřování výzvou a reakcí protokolu Point-to-Point Protocol (PPP) vycházející z uživatelského jména a hesla.
Standardní metody ověřování protokolem PPP nabízejí jen omezené zabezpečení.
- Vlastní ověřovací metody protokolu Extensible Authentication Protocol (EAP).
Moduly EAP, které lze vyvinout nebo zakoupit u nezávislých společností, rozšiřují možnosti ověřování protokolu PPP. EAP můžete například použít k zajištění silného ověřování pomocí identifikačních odznaků, karet Smart Card, biometrického hardwaru nebo systémů hesel použitelných jen jednou.
- Ověřování protokolem EAP Transport Layer Security (EAP-TLS) vycházejícím z digitálních certifikátů a karet Smart Card.
EAP-TLS poskytuje silné ověřování. Identifikační údaje uživatelů jsou uloženy na kartách Smart Card, které nelze zneužít. Každému uživateli můžete vydat jednu kartu Smart Card, kterou bude používat pro veškeré přihlašování.

Doporučujeme vám, aby váš plán zabezpečení sítě zahrnoval strategie vzdáleného přístupu a ověřování včetně následujících informací:

- Použité strategie ověřování při přihlašování.
- Strategie vzdáleného přístupu při využití služby Směrování a vzdálený přístup (Routing and Remote Access) a virtuálních privátních sítí.
- Certifikační služby potřebné pro podporu ověřování uživatelů při přihlašování pomocí digitálních certifikátů.
- Postupy a strategie zápisu uživatelů pro certifikáty ověřování při přihlašování a vzdálený přístup.
- Zda se budou eliminovat útoky maskováním pomocí funkce zpětného volání vzdáleného přístupu.

Aplikování řízení přístupu

Jakmile se uživatel přihlásí, je mu umožněn přístup k různým síťovým prostředkům, jako jsou souborové servery a tiskárny, dovolující přístup skupině Authenticated Users (ověření uživatelé). Nezapomeňte omezit zobrazení síťových prostředků uživatelům na zařízení, služby a adresáře, které souvisejí s jejich prací. Tím se omezuje škoda, jakou může způsobit narušitel vydávající se za legitimního uživatele.

Přístup k síťovým prostředkům vychází z oprávnění. Oprávnění identifikují uživatele a skupiny, které mohou s využitím určitých prostředků vykonat určité akce. Například skupina Účetní může mít přístup pro čtení a zápis k souborům ve složce Finanční hlášení. Skupina Audit má zase k souborům ve složce Finanční hlášení přístup pouze pro čtení.

Oprávnění se povolují použitím seznamu ACL přiřazeného jednotlivým prostředkům. Seznam ACL najdete na kartě **Zabezpečení** (Security) okna vlastností. ACL je seznam skupin se zabezpečením (a výjimečně také jednotlivců), které mají přístup k danému prostředku.

Skupiny se zabezpečením představují nejefektivnější způsob správy oprávnění. Oprávnění můžete sice přiřazovat jednotlivcům, ale ve většině případů je snazší přiřadit oprávnění skupině a pak přidávat nebo odstraňovat uživatele jako členy této skupiny.

Systém Windows 2000 obsahuje skupinu se zabezpečením nazvanou „Everyone“ (každý), která se standardně objevuje v seznamech ACL nově vytvořených síťových míst sdílení. Chcete-li omezit přístup k síťovým místům sdílení položek, musíte odstranit skupinu Everyone a nahradit ji vhodnější skupinou nebo skupinami. Nepředpokládejte, že výchozí oprávnění přístupu k prostředku jsou vždy těmi správnými oprávněními.

Oprávnění systému souborů jsou standardně přiřazena skupině se zabezpečením nazvané Users (uživatelé). Všichni uživatelé ověření v doméně patří do skupiny nazvané Authenticated Users (ověření uživatelé), která je také členem skupiny Users. Podívejte se, k čemu se prostředek používá, a určete příslušné zásady. Některé prostředky jsou veřejné zatímco jiné musí být dostupné jen určitým lidem. Někdy má větší skupina oprávnění pouze ke čtení souboru nebo adresáře a menší skupina má oprávnění ke čtení a zápisu stejného prostředku.

Seznamy řízení přístupu

Seznamy ACL popisují skupiny a jednotlivce, kteří mají přístup k určitému objektu v systému Windows 2000. Jednotlivci a skupiny se zabezpečením se definují v modulu snap-in Uživatelé a počítače služby Active Directory (Active Directory Users and Computers) konzoly MMC. Seznamy ACL jsou přiřazeny mnoha typům objektů systému Windows 2000; patří sem také všechny objekty Active Directory, soubory a složky místního systému NTFS, registr a tiskárny. Zrnitost seznamů ACL je tak jemná, že lze omezení zabezpečení přístupu aplikovat dokonce na jednotlivá písmena.

Fungování seznamů ACL

Seznamy řízení přístupu implementují strategie omezení využití. Systém Windows 2000 nabízí velmi přesnou možnost řízení zabezpečení přístupu k velkému množství objektů. Chcete-li umožnit nějaké skupině přístup k objektu, přidáte skupinu do seznamu ACL daného objektu. Pak můžete upravit specifická oprávnění, která bude skupina nad objektem mít. Například z hlediska místní složky souborů začínají možná oprávnění pro skupinu čtením, zápisem, úpravou a odstraněním – to jsou však jen první čtyři ze třínácti nabízených povolení.

Požadavky na implementaci seznamů ACL

Seznamy řízení přístupu se vyskytují v celém prostředí systému Windows 2000. Jedinou podmínkou je, že seznamy ACL musí být seznamy skupin se zabezpečením a uživatelů. Před přidáním skupin, které popisují projektové týmy nebo obchodní či výrobní role uživatelů vaší organizace, do seznamů ACL musíte příslušné skupiny definovat.

Implementace seznamů ACL

Seznam řízení přístupu je objekt, který obvykle naleznete na kartě **Zabezpečení** (Security) okna vlastností. Tato karta zobrazuje seznam skupin, které mají k danému objektu přístup, a navíc souhrn oprávnění, jimž se jednotlivé skupiny těší. Najdete tu také tlačítko **Upřesnit** (Advanced), jež podrobně zobrazuje oprávnění skupin a umožňuje používání pokročilejších funkcí přiřazení oprávnění, jako je definování možností dědění přístupu.

Chcete-li si například zobrazit seznam řízení přístupu k nějaké tiskárně, stiskněte tlačítko **Start** a pak zadejte příkaz **Nastavení** (Settings). Ukažte na položku **Ovládací panely** (Control Panel) a následně klepněte na položku **Tiskárny** (Printers). Klepněte

pravým tlačítkem myši na danou tiskárnu a zadejte příkaz **Vlastnosti** (Properties). Seznam řízení přístupu k dané tiskárně najdete na kartě **Zabezpečení** (Security).

Chcete-li si zobrazit seznam řízení přístupu k místní složce souborů, otevřete si okno **Tento počítač** (My Computer) a procházením si zobrazte příslušnou složku. Klepněte na ni pravým tlačítkem myši. Zadejte příkaz **Vlastnosti** (Properties) a zobrazte si kartu **Zabezpečení** (Security).

Chcete-li si zobrazit seznam řízení přístupu k organizační jednotce (složce) v modulu snap-in Uživatelé a počítače služby Active Directory (Active Directory Users and Computers) konzoly MMC, musíte rozevřít nabídku **Zobrazit** (View) a vybrat příkaz **Upřesňující funkce** (Advanced Features). Jinak se v dialogovém okně vlastností karta **Zabezpečení** (Security) nezobrazuje.

Další informace o řízení přístupu a seznamech ACL najdete po otevření nápovědy systému Windows 2000 Server a klepnutí na kartu **Rejstřík** (Index). Přesuňte se k položce **řízení přístupu** (Access Control). V rejstříku najdete odkazy na mnoho příbuzných témat, protože seznamy ACL se používají v celém rozsahu produktu.

Skupiny se zabezpečením

Systém Windows 2000 vám umožňuje uspořádat uživatele a další objekty domény do skupin, které pak umožňují jednoduchou správu oprávnění přístupu. Definování skupin se zabezpečením je hlavním úkolem vašeho plánu distribuovaného zabezpečení.

Skupiny se zabezpečením systému Windows 2000 vám umožňují jedinou operací přiřadit stejná bezpečnostní oprávnění velkému počtu uživatelů. Tím jsou zaručena konzistentní bezpečnostní oprávnění všech členů dané skupiny. Přiřazování oprávnění pomocí skupin se zabezpečením má za následek skutečnost, že řízení přístupu k prostředkům zůstává velmi statické a jednoduše se řídí a audituje. Uživatelé, kteří potřebují určitý přístup, se podle potřeby přidávají do příslušných skupin se zabezpečením nebo se z nich odstraňují a vlastní seznamy řízení přístupu se mění jen výjimečně.

Fungování skupin se zabezpečením

Služba Active Directory systému Windows 2000 podporuje skupiny se zabezpečením a distribuční skupiny. Skupiny se zabezpečením mohou mít přiřazeny bezpečnostní oprávnění a mohou také fungovat jako seznamy adresátů. Distribuční skupiny se používají pouze pro seznamy adresátů a nemají žádnou bezpečnostní funkci.

Když vytvoříte nového uživatele, můžete jeho oprávnění a omezení přístupu plně definovat přidáním do nějaké existující skupiny se zabezpečením. Změna oprávnění pro skupiny ovlivňuje všechny uživatele v dané skupině. Systém Windows 2000 obsahuje několik předdefinovaných skupin se zabezpečením, ale snadno si můžete vytvořit také své vlastní.

Typy skupin se zabezpečením

Systém Windows 2000 podporuje čtyři typy skupin se zabezpečením, které se liší svým rozsahem:

- Místní skupiny domény se nejlépe hodí pro zajištění přístupových práv k takovým prostředkům, jako jsou systémy souborů nebo tiskárny, umístěné na libovolném počítači v doméně, jež vyžadují společná oprávnění pro přístup. Výhodou místních skupin domény používaných k ochraně prostředků je, že členové místních skupin domény mohou pocházet jak zevnitř dané domény tak i zvenjšku. Servery prostřed-

ků jsou obvykle v doménách, které důvěřují jedné nebo více hlavním uživatelským doménám neboli doménám označovaným za domény účtů. (Místní skupinu domény lze použít pro zajištění přístupu k prostředkům na libovolném počítači pouze v doménách pracujících v nativním režimu. V doménách kombinovaného režimu mohou být místní skupiny domény jen na řadičích domény.)

- Globální skupiny se používají ke kombinování uživatelů, kteří sdílejí společný profil přístupu vycházející z pracovní funkce nebo role v podniku. Organizace obvykle používají globální skupiny pro všechny skupiny, kde se očekává častá změna členství. Členy těchto skupin mohou být pouze uživatelské účty definované ve stejné doméně jako globální skupina. Globální skupiny lze vládat do sebe a umožnit tak překrývání potřeb přístupu či škálování struktur velmi rozsáhlých skupin. Nejvhodnější možností zajištění přístupu globálním skupinám je učinit globální skupinu členem skupiny prostředků, která má zajištěna přístupová oprávnění k určité sadě souvisejících projektových prostředků.
- Univerzální skupiny se používají ve větších organizacích s více doménami, kde je zapotřebí zajistit přístup podobným skupinám účtů definovaným v různých doménách. Je lepší používat globální skupiny jako členy univerzálních skupin, protože to snižuje celkový replikační provoz daný změnami členství v univerzálních skupinách. Uživatelé pak mohou být přidáváni do odpovídající globální skupiny a odstraňováni z ní v rámci jejich domény uživatelského účtu a přímým členem univerzální skupiny bude menší počet globálních skupin. Univerzálním skupinám lze jednoduše přiřadit přístup tím, že se učiní členy místní skupiny domény, jež slouží k zajištění oprávnění přístupu k prostředkům.

Univerzální skupiny se používají pouze ve vícedoménových stromech nebo strukturách, které mají globální katalog. Doména systému Windows 2000 musí pracovat v nativním režimu, aby bylo možné používat univerzální skupiny. Model domény s jen jedinou doménou nepotřebuje a ani nepodporuje univerzální skupiny.

- Místní skupiny počítače jsou skupiny se zabezpečením, které jsou specifické pro daný počítač a jinde v doméně nejsou rozpoznány. Jestliže je členský server souborovým serverem a hostí 100 gigabajtů (GB) dat na více místech sdílení, můžete pro přímo vykonávané úkoly správy nebo k definování místních skupin přístupových oprávnění na daném počítači použít místní skupinu serveru.

Výchozí oprávnění skupin se zabezpečením

Výchozí oprávnění řízení přístupu systému Windows 2000 poskytují členským serverům a klientským počítačům následující úroveň zabezpečení:

- Členové skupin Everyone a Users (normální uživatelé) nemají na rozdíl od systému Windows NT 4.0 široká oprávnění ke čtení a zápisu. Tito uživatelé mají oprávnění pouze pro čtení k většině částí systému a oprávnění ke čtení a zápisu výhradně v jejich vlastních složkách profilu. Uživatelé nemohou instalovat aplikace vyžadující úpravu systémových adresářů ani nemohou vykonávat úkoly správy.
- Členové skupiny Power Users mají všechna přístupová oprávnění jako měli členové skupin Users a Power Users v systému Windows NT 4.0. Členové skupiny Power Users mají kromě svých vlastních složek profilu oprávnění pro čtení a zápis k dalším částem systému. Členové skupiny Power Users mohou instalovat aplikace a vykonávat řadu úkolů správy.
- Členové skupiny Administrators mají stejnou úroveň práv a oprávnění jako měli v systému Windows NT 4.0.

U serverů nakonfigurovaných jako řadiče domény poskytují výchozí skupiny se zabezpečením systému Windows 2000 následující zabezpečení:

- Členové skupin Everyone a Users nemají na rozdíl od systému Windows NT 4.0 rozsáhlá oprávnění pro čtení a zápis. Normální uživatelé mají k většině částí systému oprávnění pouze pro čtení a oprávnění pro zápis v jejich vlastních složkách profilu. Normální uživatelé však mohou přistupovat k řadičům domény pouze přes síť – interaktivní přihlašování k řadičům domény není na rozdíl od systému Windows NT 4.0 pro uživatele zajištěno.
- Členové skupin Account Operators, Server Operators a Print Operators mají stejná oprávnění jako v systému Windows NT 4.0.
- Členové skupiny Administrators mají k dispozici úplné řízení systému, stejně jako ve Windows NT 4.0.

Požadavky na implementaci skupin se zabezpečením

Skupiny se zabezpečením jsou zabudovanou funkcí služby Active Directory. Není vyžadována žádná instalace a nejsou kladeny žádné další podmínky.

Implementace skupin se zabezpečením

Chcete-li vytvořit nové uživatele a umístit je do skupin se zabezpečením, použijte modul snap-in Uživatelé a počítače služby Active Directory (Active Directory Users and Computers) konzoly MMC. Další informace o vytváření nových uživatelů najdete v nápovědě systému Windows 2000 Server.

Další úvahy o skupinách se zabezpečením

Při návrhu možných skupin se zabezpečením je z hlediska vlastníků projektu nebo prostředků výhodné definovat své vlastní místní skupiny vycházející z požadavků na přístupová oprávnění a delegovat možnost spravovat členství v těchto skupinách, což je samo o sobě oprávněním skupin. Tato strategie umožní vlastníkům prostředků nebo vedoucím projektů spravovat přístup aktualizací příslušné skupiny.

Skupina se zabezpečením se skládá z lidí, kteří mají v oddělení nebo v podniku podobné role. Skupina je často pojmenována podle této role – příklady jsou zabudované skupiny systému Windows 2000 Account Operators (operátoři účtů), Administrators (správci) a Backup Operators (operátoři zálohování). Personál, který přirozeně patří do jednoho seznamu adresátů projektu nebo oddělení pravděpodobně patří do stejné skupiny se zabezpečením ve službě Active Directory. Skupiny se zabezpečením systému Windows 2000 mají druhotnou roli jako seznamy adresátů, takže tato analogie není náhodná.

Použití skupin odpovídajících projektovým týmům nebo odpovědnosti je efektivní způsob řádného zajištění přístupu. Každý v oddělení potřebuje přístup k tiskárnám oddělení. Technici na softwarovém projektu potřebují přístup ke společným adresářům zdrojového kódu. To jsou přirozené skupiny.

Uvědomte si, že systém musí během přihlašování určit všechny vztahy daného uživatele k univerzálním a globálním skupinám. Je-li uživatel členem mnoha skupin, má to vliv na výkon v okamžiku, kdy systém určuje členství ve všech skupinách.

Existuje určité omezení počtu skupin, ve kterých může být uživatel zapsán. V případě jednotlivého uživatele pracujícího v jedné doméně nemůže celkový počet skupin univerzálních a globálních, místních skupin domény a místních skupin počítače překročit

hranici 1000 skupin. Uživatel však není omezen přesně na 1000 skupin, protože tento limit platí z hlediska jedné domény. V modelu s více doménami může být uživatel hypoteticky členem 500 univerzálních a globálních skupin v jejich doméně účtu, 400 místních skupin domény v jedné doméně prostředků, 400 místních skupin domény v jiné doméně prostředků, 50 místních skupin na jednom serveru a 100 místních skupin na jiném serveru. Pro většinu praktických cílů je však počet 1000 skupin více než dostačující.

Chcete-li si usnadnit správu členství ve skupinách v případě velkých skupin, používejte vkládané skupiny. (Taková velká skupina může obsahovat třeba 5000 členů.) Neuvádějte ve své skupině zahrnující celou společnost každého zaměstnance jednotlivě. Skupina celé společnosti se vám bude snáze spravovat, bude-li definována jako skupina obsahující skupiny oddělení. Skupiny oddělení tak lze vložit do skupiny celé společnosti.

To je důležité, zejména je-li vaše skupina celé společnosti univerzální skupinou. Organizace s jediným sídlem místní síť (LAN) může používat univerzální skupiny, aniž by to mělo vliv na výkon. Organizace používající rozlehlou síť (WAN) však musí zvážit vliv častých změn členství v univerzálních skupinách na replikační provoz probíhající na spojeních mezi sídly. Jestliže jsou členy univerzální skupiny jen jiné skupiny, nemění se příliš často a replikační provoz je prakticky nulový. Naproti tomu univerzální skupina obsahující tisíce jednotlivých uživatelů bude pravděpodobně vyžadovat časté aktualizace přes více spojení WAN, protože všechny změny se replikují na všechny servery globálního katalogu v podniku. Definováním univerzálních skupin jako skupin s dalšími skupinami se tato síťová činnost omezuje.

Můžete přijít na to, že váš systém Windows 2000 Server nepovoluje používání vložených skupin. Systém Windows 2000 Server zpočátku funguje v kombinovaném režimu, což znamená, že na jedné síti mohou spolupracovat systémy Windows 2000 Server a Windows NT 4.0 Server. Kombinovaný režim určitým způsobem omezuje použití skupin se zabezpečením. Jakmile jsou všechny servery inovovány na systém Windows 2000, můžete se přepnout do nativního režimu. Jedná se o jednosměrný přechod umožňující dále využívat pokročilé funkce, jako je vkládání skupin se zabezpečením.

Pokud se jedná o jeden počítač, mají uživatelé v místní skupině správy se zabezpečením plná práva a oprávnění pro daný počítač. Jakmile je počítač se systémem Windows 2000 připojen k doméně, stane se členem místní skupiny správy také skupina Domain Administrators. Místní uživatelé počítače obvykle nemusí být členy skupiny správců. Skupina správy s plnými oprávněními musí být použita pro činnosti místní správy, jako je změna konfigurace systému.

Váš plán zavedení zabezpečení sítě popisuje strategie pro skupiny se zabezpečením. Do svého plánu zavedení zahrňte tyto informace:

- Určete univerzální a globální skupiny se zabezpečením, kterými doplníte zabudované skupiny.
- Určete požadavky na členství v univerzálních a globálních skupinách a v místních skupinách se zabezpečením včetně zabudovaných skupin.

Skupiny se zabezpečením a konflikty při replikaci

Jestliže správci na dvou různých řadičích domény v různých sídlech změní současně členství ve skupinách, jedna změna se může ztratit. Tato situace může nastat, pouze pokud zadáváte změny členství ve skupinách rychleji, než je systém dokáže replikovat. Když správce přidá nebo odstraní členy skupiny, replikuje se celé členství ve skupině

a nikoli jen změnění členové. Jestliže dva správci změní členství ve skupině na dvou různých řadičích domény a k replikaci na druhém řadiči dojde dříve, než dokončí replikaci první řadič, po vyřešení konfliktu replikace službou Active Directory bude platit jen jedna ze změn. Druhá změna se ztratí. Výsledkem může být neočekávané zachování přístupu uživatele k nějakému prostředku.

Jednou z možností minimalizování tohoto problému je používat vložené skupiny. Vytvořte skupiny specifické pro jednotlivá sídla a učíte je členy nadřazené (mateřské) skupiny, která se bude používat k zajištění nebo odmítnutí přístupu k nějakému prostředku. Správci v sídle pak mohou změnit členství skupiny příslušné sídlu – tyto změny se neztratí, pokud není členství ve skupině specifické sídlu aktualizováno na více řadičích domén rychleji, než je možné dokončit replikaci v rámci sídla. Jestliže budete delegovat odpovědnost za změny členství ve skupinách jedinému správci na sídle, všechny změny se budou zadávat na jediném řadiči domény a k žádným konfliktům při replikování nebude moci dojít.

Poznámka V rámci jednoho sídla Active Directory bude čas potřebný k tomu, aby změna dosáhla všech řadičů domény, růst s počtem řadičů domény, přičemž maximální čekací doba bude rovna přibližně trojnásobku intervalu upozornění replikátoru. Obecně platí, že replikace se v rámci jednoho sídla dokončí rychle. Replikace mezi dvěma a více sídly Active Directory obvykle trvá déle a závisí na časovém plánu replikace nakonfigurovaném správcem i na tom, zda správce nakonfiguruje upozornění replikátoru v rámci sídla.

Chcete-li se úplně vyhnout této situaci, zadávejte veškeré změny členství ve skupinách na jediném řadiči domény. Zabráníte tak možné ztrátě změn způsobené konflikty při replikování. Další informace jak o zásadách řešení konfliktů služby Active Directory tak i o konfigurování služby Active Directory pro minimalizaci čekací doby replikace najdete v kapitole „Replikace služby Active Directory“ v knize *Microsoft Windows Server Distribuované systémy*.

Vytvoření vztahů důvěryhodnosti

Váš plán distribuovaného zabezpečení musí zahrnovat navrhovanou strukturu vašich domén, stromů domén, doménových struktur a serverů jiného systému než Windows 2000. Systém Windows 2000 sice vytváří vztahy důvěryhodnosti automaticky, váš plán však musí určovat, jaké domény musí být součástí doménové struktury a jaké domény ve vaší síti mohou požadovat explicitní důvěryhodnost.

V případě počítačů se systémem Windows 2000 v jedné doménové struktuře je ověřování účtů mezi doménami umožněno obousměrnou, tranzitivní (přenosnou) důvěryhodností. Tranzitivní vztah důvěryhodnosti se automaticky vytvoří v okamžiku připojení nové domény k doménové struktuře. Vztah důvěryhodnosti je definován tajným klíčem sdíleným oběma doménami, který se pravidelně aktualizuje. Vztahy důvěryhodnosti používá ověřování Kerberos v5 v případě, kdy se klienti a servery nacházejí v samostatných doménách v doménové struktuře. Tajný klíč důvěryhodnosti používá služba Kerberos k vytvoření lístku odkazu pro důvěřující doménu. Vztah důvěryhodnosti také používá ověřování NTLM pro průchozí ověřování. Průchozí ověřování použije k vytvoření zabezpečeného kanálu mezi doménami právě tajný klíč vztahu důvěryhodnosti. V systému Windows 2000 podporuje ověřování NTLM také tranzitivní důvěryhodnost, pokud se domény nacházejí v nativním režimu.

Doménová důvěryhodnost

Doménová důvěryhodnost představuje užitečnou možnost, jak dovolit uživatelům z důvěryhodné domény přistupovat k službám v důvěřující doméně. Je-li možné všechny uživatele a služby spravovat v jediné podnikové doméně, nejsou vztahy důvěryhodnosti zapotřebí. Vytvoření samostatných domén však nabízí několik výhod. Domény představují prospěšnou možnost rozdělit rozsah odpovědnosti správců domén. Každý správce je zodpovědný za uživatele a prostředky v jedné doméně. Domény jsou také rozsahem nastavení bezpečnostních zásad, např. zásad účtů. Většina vztahů důvěryhodnosti v doménové struktuře systému Windows 2000 jsou implicitní obousměrné tranzitivní (přenosné) vztahy, které nevyžadují žádné plánování. Ve vašem plánu však musí být zmíněn *externí* vztah důvěryhodnosti k doménám systému Windows NT 4.0 nebo k doménám systému Windows 2000 v jiné doménové struktuře.

Fungování vztahu důvěryhodnosti

Všechny doménové vztahy důvěryhodnosti zahrnují pouze dvě domény: důvěřující doménu a důvěryhodnou doménu. Vztah důvěryhodnosti domény může být následující:

- obousměrný;
- jednosměrný;
- přenosný;
- nepřenosný.

Jednosměrná důvěryhodnost představuje jeden vztah důvěryhodnosti, kdy doména A důvěřuje doméně B. Všechny jednosměrné vztahy jsou nepřenosné. Požadavek na ověření může předat pouze důvěřující doména doméně důvěryhodné. To znamená, že pokud má doména A jednosměrnou důvěryhodnost s doménou B a doména B má jednosměrnou důvěryhodnost s doménou C, nemá doména A vztah důvěryhodnosti s doménou C.

Domény, s nimiž může doména systému Windows 2000 navázat jednosměrnou důvěryhodnost, jsou:

- domény systému Windows 2000 v jiných doménových strukturách;
- domény systému Windows NT 4.0;
- sféry MIT Kerberos v5.

Protože jsou všechny domény systému Windows 2000 v doménové struktuře automaticky propojeny přenosnou důvěryhodností, mezi doménami systému Windows 2000 v rámci jedné doménové struktury není obvykle nutné vytvářet jednosměrnou důvěryhodnost.

Všechny vztahy důvěryhodnosti domény v doménové struktuře systému Windows 2000 jsou obousměrné přenosné vztahy. Přenosné vztahy jsou vždy obousměrné: obě domény ve vztahu si vzájemně důvěřují. Mezi nově vytvořenou podřízenou doménou a nadřazenou doménou se automaticky vytvoří obousměrná přenosná důvěryhodnost. Tímto způsobem se přenosné vztahy důvěryhodnosti pohybují směrem vzhůru stromem domény v okamžiku jeho formování, a vytvářejí tak přenosné důvěryhodnosti mezi všemi doménami ve stromu.

Pokud vytvoříte nový strom v doménové struktuře, je mezi kořenovou doménou doménové struktury a novou doménou (kořenem nového stromu doménové struktury) vytvořen obousměrný vztah přenosné důvěryhodnosti. Tímto způsobem se přenosné

vztahy důvěryhodnosti vytvářejí mezi všemi doménami ve struktuře. Požadavky na ověření sledují tyto cesty důvěryhodnosti, takže účty z libovolné domény ve struktuře mohou být ověřeny v jakékoli jiné doméně doménové struktury.

Mezi doménami systému Windows 2000 v různých větvích jednoho doménového stromu nebo mezi různými stromy doménové struktury můžete přenosnou důvěryhodnost vytvořit také explicitně (ručně). Tyto vztahy důvěryhodnosti mohou být použity ke zkrácení cesty v rozsáhlých a komplexních stromech nebo doménových strukturách. Právě takové explicitní vztahy důvěryhodnosti by měl váš plán distribuované bezpečnosti zahrnovat.

Nepřenosná důvěryhodnost je omezena na dvě domény ve vztahu důvěryhodnosti a nepostupuje do žádných jiných domén ve stromu. Nepřenosné důvěryhodnosti jsou standardně jednosměrné, i když je možné vytvořit obousměrný vztah aplikováním dvou jednosměrných vztahů. Všechny vztahy důvěryhodnosti vytvořené mezi doménami, které se nenacházejí ve stejné struktuře, jsou nepřenosné.

Přenosné vztahy důvěryhodnosti mohou existovat výhradně mezi doménami Windows 2000 v jedné doménové struktuře.

Lze tedy říci, že nepřenosné vztahy důvěryhodnosti domén jsou jediným možným vztahem důvěryhodnosti mezi:

- doménou systému Windows 2000 a doménou systému Windows NT;
- doménou systému Windows 2000 v jedné doménové struktuře a doménou systému Windows 2000 v jiné struktuře;
- doménou systému Windows 2000 a sférou MIT Kerberos v5.

Požadavky na implementaci vztahů důvěryhodnosti

Vztahy důvěryhodnosti nevyžadují žádné další znalosti. Stačí si jen uvědomit, že jde o propojení mezi doménami. Než budete moci definovat vztah důvěryhodnosti, budete muset vytvořit alespoň dvě domény.

Implementace vztahů důvěryhodnosti

Explicitní vztah důvěryhodnosti mezi doménami ve struktuře vytvoříte tak, že si otevřete modul snap-in konzoly MMC Domény a vztahy důvěry služby Active Directory (Active Directory Domains and Trusts). Pak klepněte pravým tlačítkem myši na nějakou doménu a otevřete si okno vlastností. Zobrazte si kartu **Vztahy důvěryhodnosti** (Trusts), která vám umožňuje přidávat, upravovat a odstraňovat vztahy důvěryhodnosti mezi vybranou doménou a dalšími doménami ve stejné struktuře.

Další úvahy o vztazích důvěryhodnosti

Domény s kombinovaným režimem (kde jsou záložní řadiče domén Windows NT 4.0 dočasně zkombinovány s primárním řadičem domény Windows 2000 během inovace sítě) implementují vztahy důvěryhodnosti způsobem, který je konzistentní s doménami systému Windows NT 4.0 pro systémy Windows NT 4.0 Workstation a Server. Jinými slovy, všechny vztahy důvěryhodnosti požadované systémy Windows NT 4.0 Workstation a Server jsou v doménách s kombinovaným režimem zapotřebí. Domény s nativním režimem (kde na všech serverech běží systém Windows 2000) podporují přenosné důvěryhodnosti.

Správce libovolné domény ve struktuře domén může převzít vlastnictví a upravit libovolné informace v konfiguračním kontejneru Active Directory. Tyto změny se projeví

a budou replikovány do všech řadičů domén ve struktuře. Proto si při připojování domény do struktury musíte uvědomit, že správce dané domény tak bude postaven na úrovni všech ostatních správců domén.

Problém s doménami, jejímž správcům nelze plně důvěřovat, lze vyřešit dvěma způsoby. Prvním z nich je vytvoření explicitního jednosměrného vztahu důvěryhodnosti (neboli externího vztahu) k dané doméně. Pak nemají uživatelé, kteří se přihlašují k podezřelé doméně, automatický přístup k ostatním částem struktury.

Chcete-li mít takovou situaci ještě lépe pod kontrolou, zvažte převedení zdrojů podezřelé domény do organizační jednotky (složky Active Directory) v nějaké doméně, kterou má na starost důvěryhodný správce. Samostatnou doménu tak úplně odstraňte. Správci podezřelé domény pak mohou být poskytnuty jen prostředky pro řízení počítačů a místních skupin, které mu patří.

Zavedení ochrany dat

Strategie zabezpečení informací chrání vaše data na serverech i klientských počítačích a zároveň ukrývají a chrání pakety putující nezabezpečenými sítěmi. Váš plán distribuovaného zabezpečení musí určit, které informace je zapotřebí chránit v případě ztráty nebo zcizení počítačového vybavení. V plánu musí být zároveň obsaženy citlivé nebo soukromé typy síťového provozu, které je zapotřebí chránit před sledovacími programy.

Z hlediska uživatelů na podnikové síti je hlavním mechanismem ochrany citlivých souborů před neoprávněným přístupem technika řízení přístupu. Řízení přístupu bylo popsáno dříve v této kapitole. I samotné počítače však mohou být fyzicky odcizeny, a proto k ochraně dat uložených na těchto počítačích není řízení přístupu dostatečné. To je problém zejména u přenosných počítačů, které lze odcizit velmi snadno. Řešení tohoto problému nabízí systém Windows 2000 prostřednictvím technologie šifrování systému souborů - Encrypting File System (EFS).

Chcete-li zajistit důvěrnost síťových datových paketů, použijte k šifrování síťového provozu mezi některými nebo všemi servery zabezpečený protokol IPSec (Internet Protocol security). Protokol IPSec umožňuje vytvoření ověřených a šifrovaných spojení mezi dvěma počítači. Lze například nakonfigurovat server elektronické pošty tak, aby požadoval zabezpečenou komunikaci s klienty a zabráňoval tím programům sledování paketů ve čtení zpráv elektronické pošty mezi klienty a serverem. Protokol IPSec je ideální pro ochranu dat v existujících aplikacích, které nenabízejí žádné možnosti zabezpečení.

Síťová a telefonická připojení (vzdálený přístup) vždy chrání síťová data odesílaná přes Internet nebo linky veřejné telefonní sítě. Vzdálený přístup používá virtuální privátní síť pracující s tunelovými protokoly PPTP nebo L2TP přes IPSec.

Šifrovaný systém souborů - Encrypting File System (EFS)

Systém souborů EFS (Encrypting File System) Windows 2000 dovoluje uživateli zašifrovat určené soubory nebo složky na místním počítači, čímž zajistí další ochranu místně uložených dat. Systém EFS automaticky dešifruje soubor při jeho použití a znovu jej zašifruje v okamžiku ukládání. S výjimkou uživatele, který soubor zašifroval, a správce s certifikátem obnovení EFS nemůže takové soubory nikdo číst. Protože je šifrovací mechanismus zabudován do systému souborů, jeho funkce jsou pro uživatele transparentní a je velmi obtížné na takový systém zaútočit.

Systém EFS je užitečný zejména při ochraně dat na počítači, který je možné fyzicky odcizit, jako jsou notebooky. Systém EFS můžete aplikovat na přenosném počítači a zajistit tak šifrování všech obchodních informací ve složkách dokumentů uživatele. Šifrování chrání dokumenty i v případě, kdy někdo obejde systém EFS a pokusí se číst informace nějakými diskovými nástroji pracujícími na nízké úrovni.

Systém EFS slouží především k ochraně uživatelských souborů na disku místního systému souborů NTFS. Když tento model opustíte (jako je tomu v případě vzdálených jednotek, více uživatelů nebo úpravy zašifrovaných souborů), existuje tu mnoho výjimek a speciálních podmínek, kterých si musíte být vědomi.

Fungování systému EFS

Systém EFS šifruje soubor pomocí symetrického klíče, který je pro každý soubor jiný. Pak pomocí veřejného klíče z certifikátu EFS vlastníka souboru zašifruje samotný šifrovací klíč. Protože vlastník souboru je jedinou osobou s přístupem ke svému soukromému klíči, je také jedinou osobou, která může dešifrovat klíč a následně i soubor.

Existuje také možnost šifrovat původní šifrovací klíč pomocí veřejného klíče certifikátu obnovení souborů EFS správce. Soukromý klíč tohoto certifikátu pak lze použít v případě nouze k obnovení daného souboru. Všem organizacím doporučujeme, aby zřídili funkci agenta obnovení.

Soubor je sice možné odcizit, ať už přes síť nebo fyzicky, nelze jej však dešifrovat, dokud se příslušný uživatel nepřihlásí do sítě. A protože soubor nelze číst, nelze jej ani skrytě změnit. Systém EFS tak řeší jeden z aspektů zásad důvěrnosti dat.

Požadavky na implementaci systému EFS

Chcete-li používat systém EFS, musíte mít vytvořenu infrastrukturu veřejných klíčů a alespoň jeden správce musí mít certifikát obnovení dat EFS (EFS Data Recovery), aby mohl být soubor dešifrován, kdyby se něco přihodilo jeho původnímu autorovi. Autor souboru musí mít certifikát EFS. Šifrované soubory a složky musí být uloženy v systému souborů NTFS verze obsažené ve Windows 2000.

Implementace systému EFS

Otevřete si Průzkumníka Windows a klepněte pravým tlačítkem myši na složku nebo soubor. Zadejte příkaz **Vlastnosti** (Properties). Na kartě **Obecné** (General) stiskněte tlačítko **Upřesnit** (Advanced) a pak zaškrtněte políčko **Šifrovat obsah a zabezpečit tak data** (Encrypt Contents to Secure Data). Obsah souboru nebo všech souborů ve vybrané složce bude nyní šifrován, dokud zaškrtnutí uvedeného políčka nezrušíte.

Další informace o nejlepších postupech při použití systémů šifrování souborů najdete v nápovědě systému Windows 2000. Viz také kapitola „Šifrování systému souborů“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.

Další úvahy o systému EFS

Systém EFS je podporován pouze ve verzi NTFS použité ve Windows 2000. Nefunguje v žádném jiném systému souborů včetně předchozích verzí NTFS.

Systém EFS lze používat k zabezpečenému ukládání citlivých dat na sdílené servery a umožnit tak obvyklou správu dat (zálohování). Takové servery musí být dobře chráněny a musí být „důvěryhodné pro delegování“. Služby EFS „zosobní“ daného uživatele EFS a při šifrování a dešifrování souborů jeho jménem uskuteční další potřebná síťová připojení.

Systém EFS používá zásady obnovení dat (Data Recovery) umožňující autorizovanému agentovi obnovení dat dešifrovat zašifrované soubory. Systém EFS vyžaduje existenci alespoň jednoho agenta obnovení. Agenti obnovení mohou pomocí EFS obnovit šifrované soubory, když uživatelé opustí organizaci nebo ztratí svá šifrovací pověření. Musíte naplánovat aplikování komponent PKI a vydání jednoho nebo více certifikátů obnovení dat EFS. Tyto certifikáty musí být zabezpečeně uloženy offline, aby nemohlo dojít k jejich prozrazení. Systém EFS může vygenerovat své vlastní certifikáty pro uživatele EFS a agenty obnovení EFS. Systém EFS standardně vydá certifikáty obnovení EFS pro účet správce domény, který je tak agentem obnovení pro danou doménu. V případě samostatných počítačů, které nejsou připojeny k doméně, vydá EFS certifikáty obnovení EFS pro uživatelský účet místního správce, který je tak agentem obnovení pro daný počítač. Mnoho organizací může potřebovat určit další agenty obnovení EFS, aby byla možná centrální správa programu obnovení EFS. Můžete například vytvořit organizační jednotky pro skupiny počítačů a určit konkrétní účty agentů obnovení, kteří se budou starat o obnovení EFS v jednotlivých organizačních jednotkách.

K vydávání certifikátů agentům obnovení EFS a uživatelům EFS můžete použít službu Microsoft Certificate Services. Je-li certifikační služba k dispozici online, systém EFS použije k vytvoření certifikátů EFS právě certifikační službu.

Uvědomte si, že protože služba klastru nepodporuje body změny zpracování na sdílených úložištích, systém EFS nelze použít, je-li souborový server ve skutečnosti klastrem Windows.

Do svého plánu zavedení síťového zabezpečení zahrňte také strategie EFS a obnovení EFS. Strategie EFS mohou obsahovat následující informace:

- Strategie systému souborů pro notebooky a další počítače.
- Agenti obnovení EFS.
- Doporučený proces obnovení EFS.
- Doporučený proces archivace a správy soukromého klíče agenta obnovení EFS.
- Certifikační služby potřebné pro podporu certifikátů obnovení EFS.

Zabezpečený protokol IP

Systém Windows 2000 obsahuje zabezpečený protokol IPSec sloužící k ochraně dat síťového provozu. IPSec je sada protokolů umožňujících zabezpečenou a šifrovanou komunikaci mezi dvěma počítači přes nezabezpečenou síť. Šifrování se aplikuje na síťové vrstvě IP, což znamená, že je transparentní pro většinu aplikací používajících určité protokoly síťové komunikace. IPSec zajišťuje zabezpečení mezi dvěma koncovými body, což zase znamená, že pakety IP odesílající počítač zašifruje, takže jsou během transportu nečitelné a dešifrovat je dokáže jen přijímající počítač. Díky speciálnímu algoritmu vytváření stejného sdíleného šifrovacího klíče na obou koncích spojení není zapotřebí přenášet tento klíč přes síť.

Fungování protokolu IPSec

Protokol IPSec má mnoho složitých komponent a voleb, které stojí za podrobnější studium, na vyšší úrovni však celý proces funguje tímto způsobem:

1. Aplikace na počítači A vygeneruje odchozí pakety, které se mají přes síť odeslat na počítač B.
2. V rámci protokolu TCP/IP porovná ovladač IPSec odchozí pakety s filtry IPSec a zkontroluje, zda je zapotřebí pakety zabezpečit. Filtry jsou v rámci pravidel zabezpečení IPSec přiřazeny k určité akci filtru. V jediné skupině zásad IPSec přiřazené počítači může být obsaženo mnoho pravidel zabezpečení IPSec.
3. Je-li zapotřebí, aby odpovídající filtr vyjednal nějakou akci zabezpečení, počítač A začne vyjednávání o zabezpečení s počítačem B, přičemž používá protokol internetové výměny klíčů (Internet Key Exchange) neboli IKE. Oba počítače si vymění potvrzení identity podle metody ověření zadané v pravidle zabezpečení. Metodami ověření může být ověření Kerberos, certifikáty veřejných klíčů nebo předem sdílená hodnota klíče (podobá se heslu). Vyjednávání IKE vytvoří mezi dvěma počítači dva typy dohod nazývané přidružení zabezpečení (security associations neboli SA). První typ (nazývaný „fáze I IKE SA“) určuje, jak si počítače vzájemně důvěřují a ochraňují svá vyjednávání. Druhým typem je dohoda, jak chránit určitý typ komunikace aplikací. Ta se skládá ze dvou zabezpečení SA (nazývaná „fáze II IPSec SA“) specifikujících metody zabezpečení a klíče pro oba směry komunikace. IKE automaticky vytvoří a aktualizuje sdílený tajný klíč pro každé přiřazení zabezpečení. Tajný klíč se vytváří nezávisle na obou koncích a nepřenáší se přes síť.
4. Ovladač IPSec na počítači A podepíše odchozí pakety, aby zajistil jejich integritu, a může také data pro zaručení důvěrnosti zašifrovat metodami dohodnutými během vyjednávání. Pak odvysílá zabezpečené pakety na počítač B.

Poznámka Firewally, směrovače a servery v síťové trase od počítače A k počítači B nemusí podporovat IPSec. Úplně normálně pošlou příchozí pakety dál.

5. Ovladač IPSec na počítači B zkontroluje integritu paketů a v případě potřeby dešifruje jejich obsah. Pak přenese pakety k příjmací aplikaci.

Protokol IPSec zajišťuje ochranu před manipulací s daty, jejich zachytáváním a útoky opakovaným přehráváním.

Protokol IPSec je důležitý pro strategie důvěrnosti dat, integrity dat a jejich neodvolatelnost.

Požadavky na implementaci protokolu IPSec

Počítače na vaší síti musí mít definované zásady zabezpečení IPSec tak, aby to odpovídalo vaší strategii zabezpečení sítě a typu síťové komunikace, jakou vykonávají. Počítače v jedné doméně lze organizovat do skupin a zásady zabezpečení IP pak aplikovat na tyto skupiny. Počítače v různých doménách mohou mít doplňkové zásady zabezpečení IPSec, aby podporovaly zabezpečenou síťovou komunikaci.

Implementace protokolu IPSec

Výchozí zásady zabezpečení IP si můžete zobrazit v modulu snap-in Zásady skupiny (Group Policy) konzoly MMC. Tyto zásady jsou uvedeny pod položkami **Zásady zabezpečení protokolu IP – Active Directory** (IP Security Policies on Active Directory)

nebo **Zásady zabezpečení protokolu IP – Místní počítač** (IP Security Policies (Local Computer)):

Objekt Zásady skupiny (Group Policy)
Konfigurace počítače (Computer Configuration)
Nastavení systému Windows (Windows Settings)
Nastavení zabezpečení (Security Settings)
Zásady zabezpečení protokolu IP – Active Directory
(IP Security Policies on Active Directory)

Zásady IPsec si také můžete zobrazit v modulu snap-in Správa zásad zabezpečení protokolu IP (IP Security Policy Management) konzoly MMC. Každá zásada zabezpečení IP protokolu obsahuje pravidla zabezpečení určující, kdy a jak je provoz chráněn. Klepněte pravým tlačítkem myši na zásadu a zadejte příkaz **Vlastnosti** (Properties). Karta **Pravidla** (Rules) uvádí seznam pravidel zásad. Pravidla lze dále rozložit na seznamy filtrů, akce filtrů a další vlastnosti.

Další informace o zabezpečeném protokolu IP najdete v nápovědě systému Windows 2000 Server a v knize *Microsoft Windows 2000 Server Sítě TCP/IP* v kapitole „Zabezpečení protokolu IP“.

Další úvahy o protokolu IPsec

Protokol IPsec zajišťuje šifrování odchozích a příchozích paketů za cenu spotřeby části výkonu procesoru během šifrování dat operačním systémem. V mnoha případech mohou mít servery a klienti k dispozici značné zdroje procesoru, takže šifrování IPsec nemusí mít na výkon systému pozorovatelný vliv. V případě serverů podporujících mnoho současných síťových připojení nebo serverů vysílajících velké objemy dat jiným serverům jsou však další náklady na šifrování významné. Proto je zapotřebí před zavedením protokolu IPsec nejprve otestovat simulovaný síťový provoz. Testování je důležité také v případě, kdy používáte k zajištění zabezpečení protokolu IP hardwarový nebo softwarový produkt jiného výrobce.

Systém Windows 2000 obsahuje rozhraní zařízení umožňující hardwarovou akceleraci šifrování IPsec po paketech inteligentními síťovými kartami. Výrobci síťových karet mohou nabízet několik verzí klientských a serverových karet, nemusejí však podporovat všechny kombinace metod zabezpečení protokolu IP. Prostudujte dokumentaci každé karty a ujistěte se, že podporuje metody zabezpečení a počet připojení, které ve svém nasazení očekáváte.

Zásady zabezpečení protokolu IP (IPsec) lze definovat pro každou doménu nebo organizační jednotku. Můžete také definovat místní zásady IPsec na počítačích, jimž není přiřazena doménová zásada IPsec. Konfigurací zásad IPsec lze:

- Určit úroveň ověření a důvěrnosti požadované mezi klienty IPsec.
- Určit nejnižší úroveň zabezpečení, při níž může docházet ke komunikaci mezi klienty podporujícími protokol IPsec.
- Povolit nebo zakázat komunikaci s klienty nepodporujícími protokol IPsec.
- V zájmu důvěrnosti vždy požadovat šifrovanou komunikaci nebo povolit komunikaci prostým textem.

Zamyslete se nad použitím protokolu IPSec v zájmu zajištění zabezpečení následujících typů komunikace:

- Komunikace typu peer-to-peer přes intranet vaší organizace, jako jsou komunikace právního oddělení nebo výkonného výboru.
- Komunikace typu klient/server za účelem ochrany citlivých (důvěrných) informací uložených na serveru. V případě bodů sdílení souborů vyžadujících řízení přístupu uživatelů zvažte použití protokolu IPSec v zájmu zajištění toho, aby si jiní uživatelé sítě nemohli zobrazovat přenášená data.
- Komunikace vzdáleného přístupu (telefonické nebo virtuální privátní sítě). (U virtuálních privátních sítí používajících protokol IPSec ve spojení s protokolem L2TP nezapomeňte nastavit zásady skupiny tak, aby bylo možné automaticky zapisovat certifikáty IPSec počítačů. Podrobné informace o certifikátech počítačů protokolu L2TP přenášených přes připojení IPSec virtuálních privátních sítí (VPN) naleznete v nápovědě systému Windows 2000.)
- Zabezpečená komunikace mezi směrovači na rozsáhlé síti.

Ve svém plánu zavedení síťového zabezpečení také zvažte tyto strategie IPSec:

- Určete klienty a servery, které budou používat komunikaci IPSec.
- Určete, zda bude ověření klientů vycházet z protokolu Kerberos nebo z digitálních certifikátů.
- Popište, jak jednotlivé počítače přijmou počáteční zásady IPSec a jak budou přijímat aktualizace těchto zásad.
- Popište pravidla zabezpečení v jednotlivých zásadách IPSec. Zvažte, jak musí certifikační služby podporovat ověřování klientů pomocí digitálních certifikátů.
- Popište proces zápisu a strategie zápisu certifikátů IPSec počítačů.

Nastavení jednotných zásad zabezpečení

Jednotné zásady zabezpečení umožňují aplikování a zaručení konzistentních nastavení zabezpečení na různé třídy počítačů, například na třídu řadičů domén. Jde o jednoduchou záležitost vytvoření organizační jednotky, složky v systému Active Directory, sběru příslušných objektů účtů počítačů do této organizační jednotky a aplikování objektu zásad skupiny na tuto organizační jednotku. Zásady zabezpečení specifikované v zásadách skupiny se pak automaticky a konzistentně vynuceně použijí na všech počítačích představovaných účty počítačů v organizační jednotce (OU).

Systém Windows 2000 obsahuje výběr výchozích objektů zásad skupin, které se automaticky aplikují na nové domény a řadiče domén. Existuje tu také několik *šablon* zabezpečení představujících různé úrovně zabezpečení pro různé typy podnikových počítačů. Šablonu lze použít k vytvoření zásad skupiny pro skupinu počítačů nebo ke kontrole nastavení zabezpečení na určitém počítači.

Uvědomte si, že toto pojednání se omezuje na nastavení *zabezpečení* zásad skupiny. Když aplikujete zásady skupiny na nějakou organizační jednotku, aplikujete tím také mnoho zásad nesouvisejících se zabezpečením. Podrobnější pojednání o tomto mechanismu najdete v nápovědě Windows 2000 a v kapitole „Definování standardů správy a konfigurace klientů“ v této knize.

Zásady skupiny

Objekt zásad skupiny obsahuje rozsáhlý profil oprávnění zabezpečení, která platí především pro nastavení zabezpečení domény nebo počítače (nikoli uživatele). Jediný objekt zásad skupiny může být aplikován na všechny počítače v organizační jednotce. Zásady skupiny se aplikují, když se spouští jednotlivý počítač, a bez restartu se periodicky aktualizují, dojde-li ke změnám.

Fungování zásad skupin

Objekt zásad skupiny se přiřazuje doménám a organizačním jednotkám (složkám) v modulu snap-in Uživatelé a počítače služby Active Directory (Active Directory Users and Computers) konzoly MMC. Povolení zajištěná zásadami skupiny se aplikují na počítače uložené v dané složce. Zásady skupiny lze pomocí modulu snap-in Sítě a služby Active Directory (Active Directory Sites and Services) aplikovat také na síťová sídla.

Nastavení zásad skupiny se dědí z nadřazených složek do podřízených složek, které mohou mít dále své objekty zásad skupiny. Jediná složka může mít přiřazených více objektů zásad skupiny. Další informace o nadřazenosti zásad skupiny a řešení konfliktů mezi více objekty zásad najdete v nápovědě Windows 2000.

Zásady skupiny je doplňková komponenta skupin zabezpečení. Zásady skupiny vám dovolují aplikovat jediný profil zabezpečení na více počítačů. Vynucují konzistentnost a zaručují jednoduchou správu.

Objekty zásad skupiny obsahují oprávnění a parametry implementující více typů strategií zabezpečení.

Požadavky na implementaci zásad skupiny

Zásady skupiny jsou funkcí služby Active Directory systému Windows 2000. Než tedy bude možné upravovat a aplikovat zásady skupiny, musí být na serveru služba Active Directory nainstalována.

Implementace zásad skupiny

Chcete-li si zobrazit ukázkovou organizační jednotku a jí přiřazené zásady skupiny, otevřete si modul snap-in Uživatelé a počítače služby Active Directory (Active Directory Users and Computers) konzoly MMC a klepněte pravým tlačítkem myši na organizační jednotku **Domain Controllers** (řadiče domény). Otevřete si okno vlastností a zobrazte si kartu **Zásady skupiny** (Group Policy). Vyberte položku **Default Domain Controllers Policy** (výchozí zásady řadičů domény) a stiskněte tlačítko **Upravit** (Edit). Otevře se modul snap-in Zásady skupiny (Group Policy) konzoly MMC. V tomto modulu se přesuňte do kontejneru **Nastavení zabezpečení** (Security Settings):

Objekt Zásady skupiny (Group Policy)
Konfigurace počítače (Computer Configuration)
Nastavení systému Windows (Windows Settings)
Nastavení zabezpečení (Security Settings)

Pod položkou **Nastavení zabezpečení** je devět podadresářů nastavení zásad zabezpečení. Těchto devět skupin je krátce popsáno dále v této kapitole.

Implementace zásad skupiny se skládá z vytvoření nového objektu zásad skupin (nebo úpravy existujícího objektu), zadání příslušných nastavení v objektu a následném napojení objektu zásad skupiny k organizační jednotce obsahující počítače dané domény.

Další úvahy o zásadách skupiny

Počítače s podobnou rolí v podniku rozdělíte do organizačních jednotek. Jednu organizační jednotku použijte pro řadiče domén. Další jednotku vytvořte pro servery aplikací. Jiná jednotka může obsahovat všechny vaše klientské počítače. Na každé seskupení pak aplikujete jediný objekt zásad skupiny, čím dosáhnete konzistentního nastavení zabezpečení.

Doporučujeme vám, abyste se snažili o minimalizaci počtu objektů zásad skupiny aplikovaných na uživatele a počítače. To udělejte nejprve, protože každý objekt zásad skupiny počítače a uživatele se musí na počítač přenést během jeho spouštění a do uživatelských profilů během přihlašování uživatele. Větší množství objektů zásad skupiny prodlužuje čas spouštění počítače a přihlašování uživatele. Aplikováním více objektů zásad skupiny může navíc docházet ke konfliktům, které se obtížně řeší.

Obecně platí, že zásady skupiny lze předávat z nadřazených na podřízená síťová sídla, domény a organizační jednotky. Jestliže přiřadíte určité zásady skupiny nadřazenému prvku vysoké úrovně, dané zásady skupiny platí pro všechny organizační jednotky pod nadřazenou jednotkou, včetně objektů uživatelů a počítačů ve všech kontejnerech. Další informace o dědičnosti nastavení zásad skupiny najdete v kapitole „Definování standardů správy a konfigurace klientů“ v této knize.

Šablony pro zabezpečení (popsané dále v této kapitole) vám mohou sloužit jako modely nastavení zabezpečení vhodné pro různé typy zásad skupiny.

Váš plán zavedení síťového zabezpečení by měl popisovat významné volby zásad pro jednotlivé kategorie a podkategorie. Do svého plánu zabezpečení můžete zahrnout tyto informace:

- Určení těch nastavení zásad skupiny, která se od výchozích nastavení budou lišit.
- Popis všech problémů souvisejících se změnou nastavení zásad skupiny.
- Popis zvláštních požadavků na zabezpečení a nastavení zásad skupiny k jejich naplnění.

Nastavení zabezpečení zásad skupiny

Existuje devět typů funkcí zabezpečení zásad skupiny, o kterých se již tato kapitola zmínila. Jedná se o kontejnery umístěné v uzlu **Nastavení zabezpečení** (Security Settings) objektu Zásady skupiny (Group Policy). Jde o tyto funkce:

- Zásady účtů (Account Policies)
- Místní zásady (Local Policies)
- Protokol událostí (Event Log)
- Skupiny s omezeným členstvím (Restricted Groups)
- Systémové služby (Systems Services)
- Registr (Registry)
- Systém souborů (File System)
- Zásady veřejných klíčů (Public Key Policies)
- Zásady zabezpečení protokolu IP v Active Directory (Internet Protocol Security Policies on Active Directory)

Některé z těchto oblastí zásad platí pouze pro rozsah domény, což znamená, že daná nastavení zásad platí pro celou doménu. Například zásady účtů platí jednotně pro

všechny uživatelské účty v doméně a nelze definovat různé zásady účtů v různých organizačních jednotkách v rámci jedné domény.

Z hlediska oblastí zásad zabezpečení mají doménový rozsah zásady účtů a zásady veřejných klíčů. Všechny ostatní oblasti zásad lze zadat na úrovni organizační jednotky.

Zásady účtů

Zásady účtů jsou první podkategorií Nastavení zabezpečení (Security Settings). Mezi zásady účtů patří:

Zásady hesla (Password Policy) Zásady hesla můžete změnit podle potřeb své organizace. Můžete tak určit například minimální délku hesla a dobu platnosti. Lze také vyžadovat složitá hesla a bránit uživatelům v opakovaném používání hesel nebo v jejich jednoduchých obměnách.

Zásady zamknutí účtů (Account Lockout Policy) Účet uživatele můžete uzamknout po zadaném počtu chybných pokusů o přihlášení. Lze také zadat dobu, po jakou je účet uzamčený.

Zásady modulu Kerberos (Kerberos Authentication Policy) Lze změnit výchozí nastavení protokolu Kerberos pro jednotlivé domény. Můžete tak například určit maximální dobu platnosti uživatelského lístku.

Vybrané zásady ovlivňují úroveň náročnosti podpory vyžadované uživateli i zranitelnost vaší sítě z hlediska porušení zabezpečení a útoků na ni. Například omezení zásad zamknutí účtů zvyšuje potenciál útoků odmítnutím služby a nastavení restriktivních zásad hesel má za následek vyšší počet problémů uživatelů, kteří se nemohou přihlásit k síti.

Navíc zadání restriktivních zásad hesel může ve skutečnosti omezit zabezpečení sítě. Budete-li například požadovat hesla delší než sedm znaků, většina uživatelů bude mít problémy s jejich zapamatováním. A tak si je třeba poznamenat na místo, kde je většinou snadno nalezne.

Zásady místního počítače

Druhou podkategorií Nastavení zabezpečení (Security Settings) jsou zásady Místní počítač (Local Computer). Zásady místního počítače zahrnují tyto položky:

Zásady auditu (Audit Policy) Systém Windows 2000 může zaznamenávat velké množství typů událostí zabezpečení, od celosystémových událostí jako je přihlašování uživatele, až po pokusy určitého uživatele číst nějaký soubor. Zaznamenávají se úspěšné i neúspěšné pokusy o vykonání takové akce.

Přirazení uživatelských práv (User Rights Assignment) Lze řídit práva přiřazená uživatelským účtům a skupinám se zabezpečením místních počítačů. Můžete určit uživatele a skupiny se zabezpečením, které budou mít práva vykonávat různé úlohy související se zabezpečením. Lze tak například řídit, kdo může přistupovat k počítačům ze sítě, kdo se může místně přihlašovat a kdo může systém vypnout. Je možné určit, kdo má právo zadat na počítači důležité úlohy správy, jako je zálohování a obnovování souborů, přebírání vlastnictví souborů a objektů a vynucení vypnutí ze vzdáleného systému.

Možnosti zabezpečení (Security Options) Lze ovládat velké množství možností zabezpečení místních počítačů. Můžete například určit zásady nutící uživatele k odhlášení po vypršení doby přihlášení, zakázat požadavek na stisknutí kláves Ctrl+Alt+Del před přihlášením (v zájmu vynucení přihlášení kartou Smart Card) a přinutit počítače, aby se zastavily, jestliže nemohou provádět auditování.

Zásady protokolování událostí

Zásady protokolování událostí se používají k řízení nastavení protokolování událostí aplikací, systému a zabezpečení na místních počítačích. Lze tak například určit maximální velikost protokolů, jak dlouho se budou zaznamenané události uchovávat a metody jejich uchovávání.

Zásady skupin s omezeným členstvím

Zásady skupin s omezeným členstvím lze definovat v zájmu správy a vynucení členství zabudovaných nebo nově definovaných skupin se zvláštními právy a oprávněními. Zásady omezených skupin obsahují seznam členů určitých skupin, jejichž členství je definováno centrálně jako součást zásad zabezpečení. Vynucení omezených skupin automaticky nastavuje členství všech počítačů v místních skupinách tak, aby odpovídalo nastavení seznamu členství definovanému v rámci těchto zásad. Změny členství ve skupinách ze strany správce místního počítače se přepíše zásadami skupin s omezeným členstvím definovanými ve službě Active Directory.

Skupiny s omezeným členstvím lze používat ke správě členství v zabudovaných skupinách. Mezi zabudované skupiny patří místní skupiny jako jsou Administrators, Power Users, Print Operators a Server Operators, a také globální skupiny jako Domain Administrators. Skupiny, které považujete za citlivé nebo privilegované, můžete přidat do seznamu skupin s omezeným členstvím společně s informacemi o jejich členství. To vám umožní vynutit členství těchto skupin podle nastavených zásad a znemožní to různá nastavení na jednotlivých počítačích.

Zásady systémových služeb

Systémové služby představují určité bezpečnostní riziko, protože vetřelci mohou službu převzít nebo ji použít jako vstupní bod k získání přístupu na počítače a síťové prostředky. Vetřelec může například využít slabé stránky spuštěného webového serveru a získat přístup k operačnímu systému nebo souborům počítače. Pomocí zásad systémových služeb lze:

- Určit režim spouštění služeb systému Windows 2000 (ručně nebo automaticky) nebo služby zakázat.

Lze tedy například nakonfigurovat systémové služby tak, aby nepotřebné služby nepracovaly. Tím dosáhnete maximálního zabezpečení speciálních serverů, jako jsou řadiče domén, servery DNS, servery proxy, servery vzdáleného přístupu a servery certifikačního úřadu.

- Určit práva a oprávnění přiřazená spuštěným systémovým službám.

Systémovým službám lze tedy přiřadit minimální práva a oprávnění, čímž se omezí rozsah potenciální škody způsobené vetřelci, kteří se budou snažit službu zneužít.

- Přesně definovat úroveň auditování zabezpečení systémových služeb.

Můžete určit typ neúspěšných i úspěšných událostí, které se budou zaznamenávat. Je-li například povoleno auditování, můžete je přesně nastavit tak, aby sledovalo nepatřičné akce vykonané spuštěnými službami.

Zásady registru

Prostřednictvím zásad registru lze nakonfigurovat zabezpečení a auditování řízení zabezpečení klíčů registru a jejich podklíčů. Chcete-li například zajistit, aby mohli určité informace v registru měnit pouze správci, můžete pomocí zásad registru zaručit správ-

cům úplnou kontrolu nad klíči registru a jejich podklíči a ostatním uživatelům přiřadit pouze oprávnění ke čtení registru. Pomocí zásad registru lze také určitým uživatelům zakázat zobrazování částí registru.

Je-li povoleno auditování, lze zásady registru používat k auditování aktivit uživatele v registru počítače. Můžete zadat, jaké úspěšné i neúspěšné akce uživatelů a události uživatelů se budou protokolovat.

Zásady systému souborů

Pomocí zásad systému souborů je možné nakonfigurovat zabezpečení souborů a složek a řídit auditování zabezpečení souborů a složek. Chcete-li například zajistit, aby mohli systémové soubory a složky měnit pouze správci, můžete pomocí zásad systému souborů zaručit správcům úplnou kontrolu systémovými soubory a složkami a ostatním uživatelům přiřadit pouze oprávnění k jejich čtení. Pomocí zásad systému souborů lze také určitým uživatelům zakázat zobrazování souborů a složek.

Je-li povoleno auditování, lze zásady systému souborů používat k auditování těch aktivit uživatele, které mají vliv na soubory a složky. Můžete zadat, jaké úspěšné i neúspěšné akce uživatelů a události uživatelů se budou protokolovat.

Zásady veřejných klíčů

Tato část nastavení zabezpečení vám dovoluje přidat nového agenta obnovení zašifrovaných dat a nastavit automatické požadavky na certifikáty. Lze tu také spravovat seznamy důvěryhodných certifikačních úřadů.

Zásady zabezpečení protokolu IP

Zásady v této části říkají serveru, jak má reagovat na požadavek na komunikaci protokolem IPsec. Server může vyžadovat zabezpečenou komunikaci, umožnit zabezpečenou komunikaci, nebo komunikovat bez použití protokolu IPsec. Předdefinované zásady byste neměli automaticky používat. Představují jen ukázky různého chování a slouží pro účely testování. Správci sítě si musí důkladně promyslet zásady IPsec a pak je přiřadit počítačům.

Šablony zabezpečení

Systém Windows 2000 obsahuje sadu šablon zabezpečení, které můžete použít při vytváření síťového prostředí. *Šablona zabezpečení* je profil nastavení zabezpečení, které je považováno za odpovídající určité úrovni zabezpečení na řadiči domény, serveru nebo klientském počítači systému Windows 2000. Například šablona *bisecdc* obsahuje nastavení vhodná pro vysoce zabezpečený řadič domény.

Profil zabezpečení lze importovat do objektu zásad skupiny a aplikovat jej na nějakou třídu počítačů. Šablonu lze importovat také do osobní databáze a používat ji při zkoumání a konfigurování zásad zabezpečení místního počítače.

Fungování šablon zabezpečení

Šablony zabezpečení obsahují standardní nastavení zabezpečení, která lze využít jako model vašich zásad zabezpečení. Pomáhají vám řešit problémy s počítači, jejichž zásady zabezpečení neodpovídají celkovým zásadám nebo jsou neznámá. Šablony zabezpečení nejsou aktivní až do okamžiku, než je importujete do objektu zásad skupiny (Group Policy) nebo do modulu snap-in Konfigurace a analýza zabezpečení (Security Configuration and Analysis) konzoly MMC.

Požadavky na implementaci šablon zabezpečení

Šablony zabezpečení jsou standardním prvkem systému Windows 2000 a jejich použití neklade žádné další požadavky.

Implementace šablon zabezpečení

Šablony zabezpečení lze upravit v modulu snap-in Šablony zabezpečení (Security Templates) konzoly MMC.

K importu a exportu šablon a k porovnání šablony s nastaveními zabezpečení na místním počítači lze použít modul snap-in Konfigurace a analýza zabezpečení (Security Configuration and Analysis) konzoly MMC. Chcete-li, můžete tento modul snap-in využít při konfigurování počítače tak, aby šabloně odpovídal.

Chcete-li importovat šablonu zabezpečení do objektu zásad skupiny, otevřete si v konzole MMC modul snap-in Zásady skupiny (Group Policy). Klepněte pravým tlačítkem myši na kontejner **Nastavení zabezpečení** (Security Settings) a zadejte příkaz **Importovat zásady** (Import Policy). Objeví se výběr šablon zabezpečení, které lze importovat.

Další informace o použití šablon zabezpečení a o předdefinovaných šablonách najdete v nápovědě systému Windows 2000 Server.

Další úvahy o šablonách zabezpečení

Výchozí oprávnění čistě nainstalovaného systému Windows 2000 představují výrazný nárůst úrovně zabezpečení oproti předchozím verzím Windows NT. Toto výchozí zabezpečení při čisté instalaci je definováno oprávněními k přístupu rozdělenými do tří skupin: Users, Power Users a Administrators.

Standardně platí, že členové skupiny Users mají příslušné zásady řízení přístupu potřebné pro používání systému (nikoli pro úkoly správy). Členové skupiny Power Users mají práva zpětně kompatibilní s členy skupiny Users v systému Windows NT 4.0 a členové skupiny Administrators jsou všemocní. Proto spočívá zabezpečení systému Windows 2000 převážně v definování, do jaké skupiny jednotliví uživatelé patří.

Jsou-li na vašem síťovém sídle spuštěny výhradně aplikace odpovídající specifikacím aplikací pro Windows 2000, pak je možné všechny uživatele přiřadit do skupiny Users a dosáhnout maximálního zabezpečení řízení přístupu bez omezení funkčnosti aplikací. Pracují-li na vašem síťovém sídle také aplikace, které neodpovídají specifikacím aplikací pro Windows 2000, je pravděpodobné, že budete muset uživatele zařadit do skupiny Power Users, aby měli oprávnění potřebná k provozování takových aplikací. Proto je ještě před rozhodováním o použití dodatečných šablon zabezpečení důležité určit úroveň přístupu (User, Power User nebo Administrator), kterou musí uživatelé mít, aby mohli úspěšně spouštět aplikace, jež pro svou práci potřebují.

Jakmile je o tomto bodu rozhodnuto, lze použít šablony zabezpečení takto:

Základní (Basic) Základní šablony zabezpečení aplikují výše popsaná výchozí nastavení řízení přístupu systému Windows 2000. Základní šablony lze aplikovat také na počítač se systémem Windows NT, který byl inovován na systém Windows 2000. Tím se inovovaný počítač dostane do souladu s novými výchozími nastaveními zabezpečení systému Windows 2000, která se jinak aplikují pouze na počítače s čistou instalací. Základní šablony lze použít také pro návrat k výchozím hodnotám po provedení nevhodných změn.

Kompatibilní (Compatible) Někteří zákazníci nechtějí řadit své uživatele do skupiny Power Users jenom proto, aby mohli spouštět aplikace neodpovídající specifikacím aplikací pro systém Windows 2000. Může tomu tak být proto, že členové skupiny Power Users mají další možnosti (například schopnost vytvářet sdílené položky) přesahující rámec volnějších nastavení řízení přístupu potřebných ke spouštění starších aplikací. Pro zákazníky, kteří nechtějí uživatele řadit do skupiny Power Users, „otevře“ kompatibilní šablona výchozí zásady řízení přístupu skupiny Users způsobem, který odpovídá požadavkům většiny starších aplikací. Například sadu Microsoft Office 97 SR1 úspěšně spustí členové skupiny Power Users i členové skupiny Users s kompatibilní konfigurací. Sada Office 97 se však nespustí člena skupiny Users vytvořené po čisté instalaci systému. Sada Microsoft Office 2000 se úspěšně spustí i člena skupiny Users vzniklé po čisté instalaci systému, protože tato sada odpovídá specifikacím aplikací pro systém Windows 2000. Počítač, nakonfigurovaný pomocí kompatibilní šablony, nelze považovat za zabezpečenou instalaci.

Zabezpečení (Secure) Šablona normálního zabezpečení upravuje nastavení (například zásady hesel, zásady auditování a hodnoty registru), které nemají velký vliv na funkčnost aplikací ale spíše na chování operačního systému a jeho síťových protokolů. Šablona normálního zabezpečení uvádí doporučení, která se od definovaných výchozích zásad řízení přístupu liší. Šablona normálního zabezpečení nemění položky ACL, ale odstraňuje všechny členy skupiny Power Users.

Vysoké zabezpečení (High Secure) Šablona vysokého zabezpečení zvyšuje zabezpečení definované několika parametry v šabloně normálního zabezpečení. Zatímco šablona normálního zabezpečení povolí podepisování paketů SMB, šablona vysokého zabezpečení bude podepisování paketů SMB požadovat. Zatímco šablona normálního zabezpečení bude varovat při instalaci nepodepsaných ovladačů, šablona vysokého zabezpečení instalaci nepodepsaných ovladačů zablokuje. Lze říci, že šablona vysokého zabezpečení konfiguruje mnoho operačních parametrů na jejich extrémní hodnoty bez ohledu na výkonnost, jednoduchost obsluhy nebo konektivitu s klienty používajícími starší verze NTLM nebo verze od jiných výrobců. Podobně jako šablona normálního zabezpečení i šablona vysokého zabezpečení odstraňuje všechny členy skupiny Power Users.

Závěrem můžeme říci, že použití šablon zabezpečení musí být zváženo s ohledem na výchozí zásady řízení přístupu požadované instalovanou základnou aplikací a na komunikační požadavky jiných síťových systémů. Protože šablony upravují nastavení operačního systému, nesmíte je aplikovat bez kontroly prostředků zajištění řádné kvality.

Zavádění zabezpečených aplikací

Nestačí jen zavést distribuované zabezpečení a pak se vrátit k obvyklým činnostem. Zabezpečená podniková síť potřebuje software, při jehož tvorbě hrála možnost zabezpečení významnou úlohu. Příkladem archetypu (typické) aplikace bez podpory zabezpečení je program, který posílá hesla přes síť v prostém textu. Zabezpečené prostředí potřebuje zabezpečené aplikace.

Až budete zvažovat koupi softwaru, hledejte aplikace s funkcemi zabezpečení. Hledejte integraci se schopnostmi jediného přihlášení v ověřených síťových připojeních a možnost správné funkce v konfiguracích zabezpečených počítačů. Software nemusí vyžadovat privilegia správce, pokud tedy nejde o nástroj správy systému.

Specifikace aplikací pro systém Windows 2000 (*Application Specification for Windows 2000*) definuje technické požadavky, jaké musí aplikace splnit, aby získala značku certifikace (Certified for Microsoft Windows). Tento dokument vymezuje oblasti minimálních požadavků, které musí zabezpečené aplikace podporovat:

- Fungování na zabezpečených serverech Windows 2000.
- Jediné přihlášení pomocí ověření Kerberos při vytváření síťových spojení.
- Použití zosobnění klienta, aby byl podporován konzistentní mechanismus řízení přístupu systému Windows 2000 využívající oprávnění a skupiny se zabezpečením.
- Služby aplikace musejí pracovat prostřednictvím účtů služeb a nikoli prostřednictvím místního systému (který má úplná systémová privilegia).

To jsou minimální požadavky. Je zároveň důležité používat dobře vytvořené aplikace a vyhýbat se přetečením zásobníku a dalším slabým místům, kterých může vetřelec využít.

Jedním z možných přístupů je požadovat, aby byly komponenty aplikace digitálně podepsány. Technologie Microsoft Authenticode umožňuje skrze program Microsoft Internet Explorer uživatelům ještě před přenesením komponenty z Internetu zjistit, kdo danou softwarovou komponentu publikoval, a prověřit, že s ní nikdo jiný nemanipuloval.

Také pravidelně připomínejte uživatelům, aby nespouštěli programy přímo z příloh zpráv elektronické pošty, pokud přesně nevědí odkud pocházejí nebo z daného zdroje nějakou zprávu neočekávají.

Authenticode a podepisování softwaru

Software přenesený z Internetu do počítačů uživatelů může obsahovat neautorizované programy nebo viry způsobující škodu či otevírající skrytý síťový přístup pro vetřelce. Protože sítě jsou stále více vzájemně propojeny, hrozba záškodných programů a virů existuje již i na intranetu.

Fungování Authenticode

V boji proti této rostoucí hrozbě vyvinula společnost Microsoft technologii Authenticode umožňující vývojářům digitálně podepisovat software pomocí standardních certifikátů veřejných klíčů X.509. Uživatelé si pak mohou ověřit výrobce digitálně podepsaného softwaru a mohou si také prověřit, že daný software nebyl nikým změněn, protože jeho kód je podepsán.

K vydávání digitálních certifikátů pro své interní vývojáře můžete použít službu Microsoft Certificate Services. Vaši vývojáři pak mohou svůj software ještě před jeho distribucí na intranetu podepsat pomocí podpisových certifikátů. Abyste svou síť ochránili před záškodnými programy a viry, zamyslete se také nad zavedením takových zásad, které zabrání uživatelům v nahrávání a spouštění nepodepsaného softwaru z intranetu i Internetu.

V případě softwaru distribuovaného přes Internet bude většina uživatelů důvěřovat softwaru podepsanému certifikátem vydaným komerčním certifikačním úřadem s dobrou pověstí. Použitím komerčních certifikačních úřadů se také vaše organizace zbaví závazků vyplývajících z toho, že na sebe bere odpovědnost komerčního certifikačního úřadu za distribuci externího softwaru. Budete-li tedy distribuovat software na Internetu, zvažte využití služeb komerčního certifikačního úřadu, který vydá digitální podpisové certifikáty pro vaše externí vývojáře softwaru.

Implementace sledování Authenticode

Sledování nahrávaného softwaru pomocí technologie Authenticode můžete povolit v Internet Exploreru takto: V nabídce **Nástroje** (Tools) vyberte položku **Možnosti síť Internet** (Internet Options) a pak si zobrazte kartu **Zabezpečení** (Security). Vyšší úrovně zabezpečení nastavené na této kartě sledují v softwarových komponentách důvěryhodné digitální certifikáty.

Řízení těchto nastavení zabezpečení Internet Exploreru můžete převzít prostřednictvím zásad skupiny (jak bylo popsáno dříve v této kapitole). Otevřete si modul snap-in Zásady skupiny (Group Policy) konzoly MMC a přejděte do kontejneru Internet Exploreru:

Objekt Zásady skupiny (Group Policy)
Konfigurace počítače (Computer Configuration)
Šablony pro správu (Administrative Templates)
Součásti systému Windows (Windows Components)
Internet Explorer

Zásady Internet Exploreru vám umožňují uzamknout nastavení zabezpečení, takže je uživatelé nemohou měnit, a požadovat, aby měly všechny nahrávané součásti důvěryhodné podpisy.

Další úvahy o Authenticode a podepisování softwaru

Mezi strategiemi podepisování softwaru ve vašem plánu zavedení mohou být uvedeny také následující informace:

- Interní nebo externí skupiny, které potřebují mít možnost podepisovat software.
- Strategie podepisování softwaru pro interní distribuci.
- Strategie podepisování softwaru pro externí distribuci.
- Zavedení certifikačního úřadu a správy důvěryhodnosti potřebné na podporu strategií podepisování softwaru.
- Proces a strategie zapisování uživatelů s možností podepisovat software.
- Školení uživatelů s cílem informovat je, aby nespouštěli nepodepsané nebo nedůvěryhodné součásti.

Zabezpečená elektronická pošta

Dnes se stále ještě obvykle posílají zprávy elektronické pošty obsahující citlivé osobní a obchodní informace přes nezabezpečené části intranetu nebo dokonce přes Internet. Agenti špionáže nebo hackeři mohou jednoduše přijímat zprávy elektronické pošty psané v prostém textu. Navíc může kdokoli snadno zachycovat zprávy elektronické pošty a měnit je na jejich cestě nebo falšovat adresu IP odesílatele elektronické pošty a odesílat nesprávné zprávy.

Mnoho dnešních řešení zabezpečené elektronické pošty, například Microsoft Exchange Server, vychází z otevřeného standardu Secure/Multipurpose Internet Mail Extensions (S/MIME). Používání otevřených standardů je důležité, chcete-li zajistit interoperabilitu s aplikacemi zabezpečené elektronické pošty používanými vašimi obchodními partnery, prodejci a zákazníky.

Fungování zabezpečené elektronické pošty

Systémy zabezpečené elektronické pošty S/MIME vycházejí ze standardních digitálních certifikátů X.509 a technologie veřejného klíče, čímž zaručují zabezpečení elektronické pošty mezi odesílateli a příjemci zpráv. Zabezpečené systémy elektronické pošty obvykle zajišťují následující funkce zabezpečení:

- Odesílatelé mohou digitálně podepisovat zprávy elektronické pošty a zaručovat tak integritu jejich dat.
- Příjemci mohou ověřovat identitu odesílatele zprávy a kontrolovat, že zpráva nebyla po cestě změněna.
- Odesílatelé nemohou zapírat podepsané zprávy, protože pouze odesílatel je vlastním pověřením k podpisu.
- Odesílatelé mohou zprávy elektronické pošty šifrovat, čímž dosahují důvěrné komunikace.
- Označení příjemci mohou zprávu dešifrovat pomocí soukromých pověření, nikdo jiný však nemůže zprávu dešifrovat ani číst.
- Správci mohou centrálně uložit soukromá pověření uživatelů v zabezpečené databázi. Dojde-li k poškození nebo ztrátě soukromých pověření uživatele, správci je mohou v případě potřeby získat a dešifrovat zprávy.

Další úvahy o zabezpečené elektronické poště

Chcete-li se zmínit o strategiích používání zabezpečené elektronické pošty, vložte do svého plánu zavedení také tyto informace:

- Používaný server zabezpečené elektronické pošty a klientské aplikace.
- Servery elektronické pošty a skupiny uživatelů vyžadující inovaci nebo migraci na systém zabezpečené elektronické pošty.
- Obecné zásady použití zabezpečené elektronické pošty v organizaci.
- Použitá šifrovací technologie včetně mezinárodních exportních omezení.
- Certifikační služby potřebné pro podporu zabezpečení elektronické pošty.
- Proces zápisu a strategie zápisu uživatelů v programu zabezpečení elektronické pošty.
- Možnosti zálohování databáze obnovení klíčů a doporučená praxe zálohování a obnovení.
- Možnosti obnovení klíčů a doporučená obecná praxe obnovení.

Zabezpečená webová sídla a komunikace

Webová sídla a prohlížeče se staly centrálními mechanismy otevřené výměny informací a spolupráce na intranetech společností i na Internetu. Standardní webové protokoly, jako je například protokol http (Hypertext Transfer Protocol), poskytují jen omezené možnosti zabezpečení. Většinu webových serverů lze nakonfigurovat tak, aby zajišťovaly zabezpečení na úrovni adresářů a souborů na základě uživatelských jmen a hesel. Zabezpečení webového sídla lze také zajistit naprogramováním různých řešení jazyky Common Gateway Interface (CGI) nebo Active Server Pages (ASP). Tyto tradiční metody zajištění webového zabezpečení však již nedostačují, protože útoky na webové servery jsou dnes častější a sofistikovanější.

Vyšší úroveň zabezpečení webových sídel a komunikací prostřednictvím standardních zabezpečených komunikačních protokolů a standardních certifikátů X.509 můžete dosáhnout pomocí služby Internet Information Services (IIS), která je součástí systému Windows 2000 Server. Lze tak zajistit následující zabezpečení webových sídel a webových komunikací:

- Ověření uživatelů a vytvoření zabezpečených kanálů důvěrně šifrované komunikace za použití protokolů Secure Sockets Layer (SSL) a Transport Layer Security (TLS).
- Ověření uživatelů a vytvoření zabezpečených kanálů důvěrných šifrovaných finančních transakcí za použití protokolu Server Gated Cryptography (SGC).
- Připojení certifikátů uživatelů k síťovým účtům uživatelů v zájmu ověření uživatelů a řízení uživatelských práv a oprávnění přístupu k webovým prostředkům na základě toho, že uživatelé vlastní platné certifikáty vydané důvěryhodným certifikačním úřadem.

Další úvahy o zabezpečených webových sídlech

Zvažte vložení těchto informací do svého plánu zavedení:

- Webová sídla a skupiny uživatelů, které je zapotřebí inovovat nebo migrovat na zabezpečená webová sídla.
- Strategie použití protokolů SSL nebo TLS v zájmu zajištění zabezpečené webové komunikace mezi klienty a webovými servery.
- Strategie použití připojování certifikátů v zájmu řízení uživatelských práv a oprávnění vzhledem k prostředkům webového sídla.
- Zavedení certifikačního úřadu potřebného pro podporu webových sídel.
- Proces zápisu a strategie zápisu uživatelů do programu zabezpečených webových sídel.

Řízení správy

Určité zásady vašeho plánu zabezpečení budou zahrnovat denní povinnosti lidí z vašeho oddělení IT. Systém Windows 2000 podporuje delegování oprávnění správy a předává tak určitým osobám omezená práva správy svých vlastních skupin a souborů. Systém Windows 2000 také podporuje auditové protokolování aktivit systému s možností podrobného určení typů zaznamenávaných událostí a jejich kontextu.

Také je velmi důležité, aby váš plán popisoval, jak budou chráněny účty správce domén před možností proniknutí vetřelce. Doporučujeme vám, abyste nastavili zásady doménových účtů tak, aby ve všech účtech musela být použita dlouhá a složitá hesla, která nelze snadno odhalit. To je celkem samozřejmé, je však důležité tuto okolnost v plánu zdůraznit.

Není už tak zřejmé, že zabezpečení se významně sníží, pokud bude znát heslo správce příliš mnoho lidí. Správce kořenové domény doménového stromu je také automaticky členem skupiny Schema Administrators a skupiny Enterprise Administrators. To je velmi privilegovaný účet, s jehož pomocí může vetřelec způsobit neomezené škody. Váš plán musí říkat, že přístup k tomuto účtu bude omezen na velmi malý počet důvěryhodných osob.

Účet správce domény musí být používán výhradně pro úkoly vyžadující oprávnění správce. Počítač, na němž je tento účet aktivní, nesmí nikdy zůstat bez dozoru. Doporučte správcům, aby pro jiné aktivity nesouvisející se správou (čtení zpráv elektronické pošty, procházení webem apod.), používali druhý, nepriviligovaný účet.

Serverové konzoly používané pro správu domény musí být fyzicky zabezpečeny, aby k nim měly přístup výhradně oprávněné osoby. To musí váš plán také zdůraznit a navíc uvést seznam osob, které mohou konzoly používat. Nemusí být také zřejmé, že uživatelé s účty správce se nikdy nesmějí přihlásit na klientské počítače spravované někým, komu zcela nedůvěřují. Správce jiného klientského počítače totiž může na daném počítači použít kód, který mu umožní využívat oprávnění správce.

Delegování

Delegování úkolů správy je v podnikovém prostředí systému Windows 2000 prakticky nezbytné. Je obvyklé delegovat určitá oprávnění nejen na členy skupiny IT, ale také na osoby starající se o lidské zdroje a různé manažery, aby mohli provádět činnosti související s jejich povinnostmi. Delegování distribuuje pracovní zatížení správce, aniž by přitom každý asistent získal příliš velká privilegia. To je vyjádřením konceptu zabezpečení „principu nejmenších privilegií“, což znamená přiřazení pouze takových oprávnění, která jsou pro určitou činnost nezbytná.

Systém Windows 2000 vám různými prostředky umožňuje delegovat skupinám a jednotlivcům předepsaný stupeň řízení omezené sady objektů. Jedinou podmínkou je, že příslušné delegované prvky (uživatelé, skupiny, objekty zásad skupiny, adresáře atd.) musejí být před vlastním delegováním již připraveny.

Systém Windows 2000 podporuje delegování oprávnění správy pomocí různých funkcí, z nichž některé jsou uvedené v následujících oddílech. (Uvědomte si, že některé úkoly vyžadují privilegia správce domény a nelze je delegovat.)

Skupiny se zabezpečením, zásady skupiny a seznamy řízení přístupu

Tyto funkce byly popsány již dříve v této kapitole a formují mechanismy funkcí popísaných v dalších odstavcích.

Zabudované skupiny se zabezpečením

Systém Windows 2000 obsahuje předdefinované skupiny se zabezpečením, přičemž každá z nich již má delegované určité speciální oprávnění. Otevřete si modul snap-in Uživatelé a počítače služby Active Directory (Active Directory Users and Computers) konzoly MMC. Z nabídky **Zobrazit** (View) zadejte příkaz **Upřesňující funkce** (Advanced Features). Předdefinované skupiny se zabezpečením se nacházejí ve složkách **Builtin** a **Users**.

Chcete-li přímo delegovat řízení některé z těchto skupin, otevřete si okno vlastností dané skupiny a zobrazte si kartu **Zabezpečení** (Security). Přidejte manažera skupiny na seznam řízení přístupu a určete příslušná privilegia.

Průvodce delegováním řízení

Otevřete si modul snap-in Sítě a služby Active Directory (Active Directory Sites and Services) konzoly MMC. Klepněte pravým tlačítkem myši na nějakou organizační jednotku a zadejte příkaz **Delegovat řízení** (Delegate Control). Zobrazený průvodce nastaví oprávnění skupin uživatelů ke správě určitých síťových sídel a služeb. Příkladem může být právo vytvářet nové účty vzdáleného přístupu.

Průvodce delegováním správy

Otevřete si modul snap-in Uživatelé a počítače Active Directory (Active Directory Users and Computers) konzoly MMC. Klepněte pravým tlačítkem myši na nějakou organizač-

ní jednotku a zadejte příkaz **Delegovat řízení** (Delegate Control). Zobrazený průvodce nastaví oprávnění skupin uživatelů ke správě určitých organizačních jednotek obsahujících počítače a skupiny uživatelů. Příkladem může být delegované právo vytvářet nové účty uživatelů.

Delegování řízení objektů zásad skupiny

Delegování správy přes zásady skupiny zahrnuje následující tři úkony, které lze vykonat společně nebo samostatně, podle toho, jak to vaše situace vyžaduje:

- Správa propojení zásad skupiny na síťovém sídle, v doméně nebo v organizační jednotce.
- Vytvoření objektů zásad skupiny.
- Úprava objektů zásad skupiny.

Tyto úkony jsou podrobněji popsány v kapitole „Definování standardů správy a konfigurace klientů“ v této knize.

Auditování

Důležitými bezpečnostními prvky jsou auditování a protokolování síťových aktivit. Systém Windows 2000 vám dovoluje monitorovat velké množství událostí, s jejichž pomocí lze sledovat aktivity vetřelce. Položky v protokolu událostí mohou po identifikaci vetřelce sloužit jako právní doklad.

Fungování auditování

Lze zadat, aby se do protokolu událostí zapsala nějaká položka auditu, kdykoli dojde k vykonání určitých akcí nebo k přístupu k určitým souborům. Položka auditu ukazuje vykonanou akci, uživatele, který ji vykonal, a datum a čas akce. Auditovat lze úspěšné i neúspěšné pokusy o akce, takže záznam auditu ukazuje, kdo vykonal nějaké akce na síti a kdo se pokusil vykonat nepovolené akce. Protokol zabezpečení si můžete zobrazit v nástroji Prohlížeč událostí (Event Viewer).

Budete-li protokol zabezpečení pravidelně kontrolovat, můžete detekovat určité typy útoků ještě předtím, než budou mít úspěch (například útoky na hesla). I po prolomení zabezpečení vám může záznam zabezpečení pomoci určit způsob, jakým vetřelec vniknul do systému, a jaké akce tam vykonal.

Protokolování auditu jsou samostatné zásady. Zaznamenávání událostí zabezpečení je formou detekce pronikání do systému.

Požadavky na implementaci funkce auditování

Nemusíte nic instalovat ani kupovat. Musíte jen nakonfigurovat nastavení zásad skupiny tak, aby bylo auditování umožněno. Musíte také povolit auditování obecných oblastí nebo specifických položek, které chcete sledovat.

Implementace funkce auditování

Auditování zabezpečení není standardně povoleno. Požadované typy auditování musí te aktivovat pomocí modulu snap-in Zásady skupiny (Group Policy) konzoly MMC.

Objekt Zásady skupiny (Group Policy)

Konfigurace počítače (Computer Configuration)

Nastavení systému Windows (Windows Settings)

Nastavení zabezpečení (Security Settings)

Místní zásady (Local Policies)

Zásady auditu (Auditing Policies)

Mezi kategorie událostí, jež lze auditovat, patří: události přihlášení k účtu, správa účtu, přístup k adresářové službě, události přihlášení, přístup k objektům, změny zásad, používání privilegií, sledování procesů a systémové události. Uvědomte si, že pro zásady auditu platí princip dědičnosti a že tedy zásady nastavené na místním počítači mohou být přepsány zásadami nastavenými pro doménu jako celek.

Jakmile nastavíte zásady auditu, můžete se ponořit hlouběji a povolit specifické typy zpráv auditu jednotlivých objektů. Chcete-li například povolit audit nějakého adresáře souborů, klepněte pravým tlačítkem myši na příslušnou složku v Průzkumníkově Windows. Zadejte příkaz **Vlastnosti** (Properties) a zobrazte si kartu **Zabezpečení** (Security). Stiskněte tlačítko **Upřesnit** (Advanced) a v dialogovém okně upřesňujících vlastností si zobrazte kartu **Auditování** (Auditing). Objeví se seznam událostí složky, které lze auditovat. V případě adresářů souborů lze nastavení auditování volitelně aplikovat na obsažené soubory a podadresáře.

Zprávy auditu si zobrazte položkou **Protokol zabezpečení** (Security Log) nástroje **Prohlížeč událostí** (Event Viewer).

Další informace o auditování událostí zabezpečení najdete v nápovědě systému Windows 2000.

Další úvahy o auditování

Vytváření protokolu zabezpečení má vliv na diskový prostor serveru. Prohlížeč událostí můžete nastavit tak, aby přepisoval položky záznamu starší než „n“ dnů nebo můžete zadat, aby se po naplnění protokolu událostí zabezpečení server zastavil. Další informace o zastavení počítače v okamžiku, kdy se zaplní protokol zabezpečení, najdete v nápovědě systému Windows 2000.

Výše popsané funkce auditování adresářů a souborů vyžadují systém souborů NTFS.

Podezřelé aktivity můžete odhalit sledováním serverů firewallu a kritických serverů uvnitř firewallu. Také byste měli sledovat servery vně firewallu, třebaže jsou považovány za nezabezpečené, protože představují vstupní bránu do vašeho podniku.

Tabulka 11.3 uvádí různé události, které byste měli sledovat, a příslušné ohrožení zabezpečení, jež daná událost auditu sleduje.

Tabulka 11.3 Zásady detekce ohrožení auditu zabezpečení

Údlost auditu	Detekované ohrožení
Neúspěšný audit přihlášení/odhlášení.	Útok náhodným heslem
Úspěšný audit přihlášení/odhlášení.	Průnik zcizeným heslem
Úspěšný audit uživatelských práv, správy uživatelů a skupin, zásad změny zabezpečení, restartu, vypnutí systému a systémových událostí.	Zneužití privilegií
Úspěšný a neúspěšný audit událostí přístupu k souborům a přístupu k objektům. Úspěšný a neúspěšný audit správce souborů přístupu pro čtení/zápis do citlivých souborů ze strany podezřelých uživatelů nebo skupin.	Nesprávný přístup k citlivým souborům
Úspěšný a neúspěšný audit tiskáren přístupu k souborům a událostí přístupu k objektům. Úspěšný a neúspěšný audit správce tisku pro přístup k tiskárnám ze strany podezřelých uživatelů nebo skupin.	Nesprávný přístup k tiskárnám

Úspěšný a neúspěšný audit přístupu pro zápis k programovým souborům (s příponami .exe a .dll). Úspěšný a neúspěšný audit sledování procesu. Spusťte podezřelé programy; vyhledejte v protokolu zabezpečení neočekávané pokusy upravit programové soubory nebo vytvořit neočekávané procesy. Spusťte pouze při aktivním sledování systémového protokolu událostí.

Průnik viru

Seznam úkolů plánování distribuovaného zabezpečení

Plán zavedení síťového zabezpečení vytvoříte splněním úkolů uvedených v tabulce 11.4.

Tabulka 11.4 Seznam úkolů plánování zabezpečení

Úkol	Kapitola
Určete bezpečnostní rizika, která je zapotřebí zvážit v případě vaší sítě. V plánu zabezpečení je vysvětlíte a uveďte do tabulek.	Bezpečnostní rizika
Zajistěte základní materiály a slovníček konceptů zabezpečení, aby se čtenář vašeho plánu dokázal v tématicke orientovat.	Koncepty zabezpečení
Ve svém plánu uveďte a vysvětlíte strategie zabezpečení, které řeší bezpečnostní rizika.	Strategie distribuovaného zabezpečení
Zajistěte, aby veškerý přístup k síťovým prostředkům vyžadoval ověření pomocí doménových účtů.	Ověřování všech přístupů uživatelů
Určete, jaká část uživatelů musí během interaktivního přihlašování nebo přihlašování vzdáleného přístupu používat silné ověřování.	Ověřování všech přístupů uživatelů
Definujte délku hesla, interval změny a požadavky na složitost pro uživatelské účty domény a vytvořte plán předání těchto požadavků uživatelům.	Ověřování všech přístupů uživatelů
Definujte zásady vaší organizace zamezující vysílání hesel v prostém textu na všech sítích a vytvořte strategii jediného přihlašování či ochrany přenosu hesla.	Ověřování všech přístupů uživatelů
Určete plán zavedení zabezpečení pomocí veřejného klíče pro přihlašování kartou Smart Card, pokud silné ověření splňuje vaše bezpečnostní cíle.	Přihlašování kartou Smart Card
Popište své zásady umožnění vzdáleného přístupu uživatelů.	Vzdálený přístup
Vytvořte plán předání procedur vzdáleného přístupu (včetně metod připojení) uživatelům.	Vzdálený přístup
Určete, jak vaše společnost v současné době používá skupiny, a vytvořte konvence názvů skupin a použití různých typů skupin.	Aplikování řízení přístupu
Popište skupiny se zabezpečením nejvyšší úrovně, které budete používat k širokému zabezpečenému přístupu k prostředkům v rámci celé společnosti. Půjde pravděpodobně o univerzální skupiny vašeho podniku.	Aplikování řízení přístupu
Popište zásady řízení přístupu a specificky ukažte, jak se budou konzistentním způsobem používat skupiny se zabezpečením.	Aplikování řízení přístupu

Definujte procedury vytváření nových skupin a určete, kdo má odpovědnost za správu členství ve skupinách.	Aplikování řízení přístupu
Určete, které existující domény patří do doménové struktury a které domény používají externí vztahy důvěryhodnosti.	Vytvoření vztahů důvěryhodnosti
Popište své domény, doménové stromy a struktury a přesně uveďte vztahy důvěryhodnosti mezi nimi.	Vytvoření vztahů důvěryhodnosti
Definujte zásady určování a správy citlivých či důvěrných informací a požadavky na ochranu citlivých dat.	Zavedení ochrany dat
Identifikujte síťové servery s citlivými daty, které budou potřebovat ochránit.	Zavedení ochrany dat
Vytvořte plán zavedení protokolu IPsec s cílem zajistit ochranu dat při vzdáleném přístupu nebo při přístupu k citlivým datům aplikací na serverech.	Zavedení ochrany dat
Používáte-li systém EFS, popište zásady obnovení dat včetně role agenta obnovení ve vaší organizaci.	Šifrovaný systém souborů
Používáte-li systém EFS, popište procedury, jejichž prostřednictvím plánujete zavést proces obnovení dat a ověřit, že tento proces bude v rámci vaší organizace fungovat.	Šifrovaný systém souborů
Používáte-li protokol IPsec, určete scénáře jeho použití ve vaší síti a seznámte se s jeho vlivem na výkon systému.	Zabezpečený protokol IP
Definujte zásady účtů pro celou doménu a předejte tyto zásady a další pokyny uživatelům.	Nastavení jednotných zásad zabezpečení
Určete požadavky místních zásad zabezpečení pro různé kategorie síťových systémů, jako jsou stolní počítače, souborové a tiskové servery a servery elektronické pošty. Definujte nastavení zabezpečení zásad skupiny vhodná pro jednotlivé kategorie.	Nastavení jednotných zásad zabezpečení
Určete servery aplikací, kde lze ke správě nastavení zabezpečení používat určité šablony zabezpečení, a zvažte jejich správu prostřednictvím zásad skupiny.	Nastavení jednotných zásad zabezpečení
Na systémy aktualizované z verze Windows NT 4.0 (nikoli čistě instalované) zaveďte vhodné šablony zabezpečení.	Šablony zabezpečení
Pomocí šablon zabezpečení popište úroveň zabezpečení, kterou plánujete zavést pro různé třídy počítačů.	Šablony zabezpečení
Vytvořte plán testování, který bude mít za cíl ověřit, že vaše aplikace budou v řádně nakonfigurovaných zabezpečených systémech fungovat.	Zavádění zabezpečených aplikací
Definujte, jaké další aplikace jsou zapotřebí k zajištění zvýšeného zabezpečení, které bude odpovídat bezpečnostním cílům vaší společnosti.	Zavádění zabezpečených aplikací
Určete úroveň zabezpečení kladenou na přenášený kód.	Authenticode a podepisování softwaru
Zaveďte interní procedury implementace podepisování kódu vnitřně vytvořeného softwaru, který je veřejně distribuován.	Authenticode a podepisování softwaru
Uveďte zásady zabezpečení účtu Administrator a konzol správy.	Řízení správy
Určete situace, při kterých plánujete delegovat řízení správy určitých úkolů.	Delegování
Určete zásady týkající se auditování včetně správy osob.	Auditování

KAPITOLA 12

Plánování infrastruktury veřejných klíčů

Systém Microsoft Windows 2000 podporuje infrastrukturu veřejných klíčů (Public Key Infrastructure - PKI). PKI je systém digitálních certifikátů, certifikačních úřadů a dalších registračních úřadů ověřujících a potvrzujících prostřednictvím šifrování s veřejným klíčem platnost jednotlivých účastníků elektronické transakce.

Infrastrukturu PKI splňující vaše požadavky na zabezpečení veřejnými klíči lze vytvořit pomocí služby Microsoft Certificate Services nebo jiných certifikačních služeb.

V této kapitole

Přehled infrastruktury veřejných klíčů 354

Vytváření infrastruktury veřejných klíčů 358

Návrh infrastruktury veřejných klíčů 359

Vývoj vlastních aplikací 369

Plánování prostředků 370

Zavedení infrastruktury veřejných klíčů 371

Seznam úkolů plánování infrastruktury veřejných klíčů 377

Cíle kapitoly

Tato kapitola vám pomůže při vytváření následujících dokumentů plánů:

- Požadavky na certifikáty veřejných klíčů
- Zásady vydávání a používání certifikátů
- Návrh hierarchie důvěryhodnosti certifikačních úřadů
- Zásady životního cyklu a procesů certifikátů
- Zásady odvolávání certifikátů
- Strategie zálohování a nouzové obnovy certifikátů
- Časový plán zavedení a zápisu PKI

Související informace v sadě Resource Kit

Další informace o základních konceptech zabezpečení pomocí šifrování, PKI a technologii veřejného klíče naleznete v knize *Microsoft Windows 2000 Server Distribuované systémy* v kapitole „Šifrování na síti a zabezpečení informací“.

Další informace o řešení zabezpečení pomocí technologie veřejného klíče naleznete v knize *Microsoft Windows 2000 Server Distribuované systémy* v kapitole „Volba řešení zabezpečení s použitím technologie veřejného klíče“.

Přehled infrastruktury veřejných klíčů

Infrastruktura veřejných klíčů (public key infrastructure – PKI) je podpůrnou technologií systému Windows 2000, která zajišťuje řadu funkcí souvisejících s ověřováním a šifrováním. Proto je nutné, aby byly plány PKI definovány velmi brzy v rámci procesu zavádění.

V této části najdete krátký přehled funkcí a nástrojů PKI v systému Windows 2000.

Fungování PKI

Struktura PKI vychází z *certifikátů*. Certifikát je digitálně podepsané prohlášení obsahující veřejný klíč a název subjektu. V certifikátu mohou být různé typy názvů, pod kterými je subjekt znám, jako je třeba název adresáře, název účtu elektronické pošty a název DNS. Podepsáním certifikátu certifikační úřad potvrzuje, že soukromý klíč patřící k veřejnému klíči v certifikátu je vlastnictvím subjektu pojmenovaného v certifikátu.

Certifikační úřad, což je často nějaká samostatná společnost, vydá důvěryhodnému uživateli certifikát obsahující veřejný klíč. Tento certifikát lze volně distribuovat. Veřejný klíč lze použít k zašifrování dat, která pak lze dešifrovat pouze přiřazeným soukromým klíčem, jenž uživatel také získá. Uživatel udržuje svůj soukromý klíč v tajnosti, aby k němu neměl nikdo jiný přístup. Soukromý klíč lze použít k vytvoření digitálního podpisu, který lze ověřit pomocí veřejného klíče.

Základní myšlenka šifrování s veřejným klíčem spočívá v tom, že existují dva klíče, mezi kterými je nějaký vztah. První z klíčů lze předávat naprosto volně různým subjektům nebo jej lze publikovat v nějakém veřejném adresáři; druhý klíč však musí zůstat soukromý. Existují dva různé typy algoritmů s veřejným klíčem a každý z nich má své zvláštní charakteristiky. To znamená, že není vždy možné nahradit jeden algoritmus druhým. I když dokáží oba algoritmy vykonat stejnou funkci, přesný mechanismus získání výsledku se liší. V případě šifrování s veřejným klíčem se oba klíče používají po pořadě. Je-li jako první použit veřejný klíč a po něm klíč soukromý, pak se jedná o operaci výměny klíčů. Je-li jako první použit soukromý klíč a po něm klíč veřejný, jedná se o operaci digitálního podepisování.

Ve své společnosti si můžete vytvořit své vlastní certifikační úřady nebo můžete využít produkty jiných společností, které poskytují certifikační služby na komerčním základě.

PKI zpracovává informace takovým způsobem, že zároveň identifikuje i ověřuje jejich zdroj. Narušení identity je tak velmi obtížné a zároveň se tím zabráňuje možnosti vydávat se za někoho jiného a manipulovat s daty. Popis některých možností použití PKI v podnikovém prostředí najdete v tabulce 12.1.

Tabulka 12.1 **Nejdůležitější aplikace digitálních certifikátů**

Aplikace	Použití
Zabezpečená elektronická pošta	Klienti zabezpečené elektronické pošty používají certifikáty v zájmu zajištění integrity zprávy elektronické pošty a k šifrování zpráv elektronické pošty pro zajištění důvěrnosti.
Zabezpečená webová komunikace	Webové servery mohou ověřit klienty webové komunikace (pomocí klientských certifikátů) a zajistit tak důvěrnou, šifrovanou webovou komunikaci (pomocí serverových certifikátů).
Zabezpečené webové servery	Webová sídla serverů Internet Information Services (IIS) mohou připojovat (mapovat) klientské certifikáty k ověřeným uživatelům a řídit tak jejich práva a oprávnění vzhledem k prostředkům webového sídla.
Digitální podepisování softwarových souborů	Nástroje podepisování kódu používají certifikáty k digitálnímu podepisování souborů softwaru, čímž garantují původnost souboru a zajistí integritu jeho dat.
Ověřování pomocí karty Smart Card na místní síti	Přihlašovací protokol Kerberos může k ověřování síťových uživatelů, kteří se přihlašují na síť, využívat certifikáty a soukromý klíč uložený na kartách Smart Card.
Ověřování pomocí karty Smart Card při vzdáleném přístupu	Servery se spuštěnou službou Směrování a vzdálený přístup (Routing and Remote Access) mohou k ověřování síťových uživatelů, kteří se přihlašují na síť, využívat certifikáty a soukromý klíč uložený na kartách Smart Card.
Ověřování IPSec	Protokol IPSec může při vytváření zabezpečené komunikace IPSec používat k ověření klientů certifikáty.
Agent obnovení Encrypting File System (EFS)	Certifikáty agentů obnovení umožňují obnovit soubory jiných uživatelů zašifrované systémem EFS.

Požadavky na implementaci PKI

Implementace PKI ve vašem podniku je proces skládající se z více částí, který vyžaduje plánování a experimentování prostřednictvím pilotních programů. Některé z funkcí systému Windows 2000, například Encrypting File System (EFS) a zabezpečení protokolu IP (IPSec), mohou používat své vlastní certifikáty, aniž by byla nutná nějaká speciální příprava na straně správce sítě. Tyto funkce lze používat okamžitě. Další funkce zabezpečení mohou požadovat hierarchii certifikačních úřadů (CA). Hierarchie CA vyžaduje plánování.

Prvním rozhodnutím, které budete muset v rámci určení své obchodní politiky učinit, bude výběr certifikačních úřadů (interního a externího), které budou zdroji vašich certifikátů. Typická hierarchie CA má architekturu se třemi úrovněmi. Doporučujeme vám,

abyste měli jeden hlavní úřad CA, který bude offline. Druhou úroveň CA potřebujete pro zavedení zásad certifikátů. Tato úroveň by také měla být offline. Třetí úrovní jsou úřady CA vystavující certifikáty. Na této úrovni můžete mít interní i externí certifikační úřady. Interní ověřování v síti a integritu dat může spravovat místní certifikační úřad, například vaše oddělení informační technologií (IT). Internetové transakce a podepisování softwaru může v zájmu obecné důvěryhodnosti vyžadovat využití služeb jiné společnosti.

Při výběru CA věnujte také pozornost poskytovateli kryptografických služeb (cryptographic service provider – CSP). CSP je software nebo hardware zajišťující šifrovací služby pro váš úřad CA. Je-li CSP softwarový, vygeneruje na vašem počítači veřejný a soukromý klíč, které se také často označují za pár klíčů. Je-li CSP hardwarový, jako je například karta CSP Smart Card, může CSP o vygenerování páru klíčů požádat daný hardware.

Standardním CSP pro prostředí Windows je poskytovatel kryptografických služeb Microsoft Base CSP, který zajišťuje klíče s délkou 40 bitů. Systém Windows 2000 podporuje 40/56bitové šifrování, které lze exportovat. Chcete-li dosáhnout nejvyššího zabezpečení (a největší rychlosti), zvažte použití hardwarového CSP, který nabízejí různí výrobci.

Vyšší zabezpečení obvykle znamená vyšší náklady z hlediska výdajů za hardware i cyklů CPU věnovaných šifrování. Vyšší zabezpečení tak nemusí být vždy z hlediska nákladů efektivní, v případě potřeby je však k dispozici. Zajímá-li vás extrémní zabezpečení, zvažte použití hardwarových CSP v případě certifikačních úřadů a karet Smart Card pro uživatele.

Implementace PKI

Podpora infrastruktury veřejných klíčů je zabudována do systému Windows 2000 a většiny programů podporujících podnikovou sféru. Více se o funkcích PKI systému Windows 2000 dozvíte v následujících oddílech.

Vytvoření místního certifikačního úřadu

Na serveru Windows 2000 můžete vytvořit místní CA. Můžete si vybrat z několika typů CA. Jedním typem je podnikový certifikační úřad, který dokáže vystavovat certifikáty pro účely, jako jsou digitální podpisy, šifrované zprávy elektronické pošty, webové ověřování a doménové ověřování systému Windows 2000 pomocí karet Smart Card. Podnikový úřad CA vystaví certifikáty na základě žádostí uživatelů a dalších entit a pro svou funkci potřebuje adresářové služby Active Directory.

Samostatný certifikační úřad vystavuje certifikáty na základě žádostí uživatelů a dalších entit, na rozdíl od podnikového úřadu CD však nevyžaduje použití Active Directory. Samostatné úřady CA jsou určeny především pro extranety a Internet.

Certifikační úřady mohou také plnit různé role v hierarchii, jako je hlavní (kořenový, root) certifikační úřad, podřízený (subordinate) úřad a vystavující (issuing) úřad. Úvahy o certifikačních hierarchiích najdete v oddílu „Definování zásad certifikátů a postupů certifikačního úřadu“ dále v této kapitole.

▼ Chcete-li vytvořit místní CA na serveru se systémem Windows 2000, postupujte takto:

1. Stiskněte tlačítko **Start**, vyberte příkaz **Nastavení** (Settings) a pak zvolte položku **Ovládací panely** (Control Panel).

2. Poklepejte na panel Přidat nebo odebrat programy (Add/Remove Programs) a stiskněte tlačítko Přidat nebo odebrat součásti systému Windows (Add/Remove Windows Components).
3. Přidejte položku Služba Certificate Services (Certificate Services) a nainstalujte hlavní podnikový certifikační úřad.

Další informace o instalování místního certifikačního úřadu najdete v nápovědě systému Windows 2000 Server.

Jakmile vytvoříte místní certifikační úřad, můžete jej sledovat a spravovat pomocí modulu snap-in Certifikační úřad Certification Authority) nástroje Microsoft Management Console (MMC).

Certifikáty PKI si také můžete zobrazovat.

▼ **Chcete-li si zobrazit svou osobní sadu certifikátů PKI, postupujte takto:**

1. Otevřete si program Microsoft Internet Explorer.
2. Zadejte příkaz **Možnosti sítě Internet** (Internet Options) nabídky **Nástroje** (Tools).
3. V dialogovém okně si zobrazte kartu **Obsah** (Content). Tlačítka v prostřední části této karty zobrazují vaše aktuální certifikáty, důvěryhodné certifikační úřady a důvěryhodné výrobce softwaru.

Správa certifikátů

Ke správě certifikátů použijte modul snap-in Certifikáty (Certificates) konzoly MMC. Pamatujte, že tento modul má dva režimy zobrazení: podle logických úložišť certifikátů a podle účelu certifikátů. Uzel vyberte klepnutím na položku Certifikáty (Certificates) nejvyšší úrovně. Pak v nabídce **Zobrazit** (View) zadejte příkaz **Možnosti** (Options). Seznamte se s oběma režimy zobrazení.

Chcete-li v rámci tohoto modulu snap-in požadovat nový certifikát, klepněte pravým tlačítkem myši na příslušný uzel v zobrazení podle účelu certifikátů a pak zadejte příkaz **Požádat o nový certifikát** (Request New Certificate) podnabídky **Všechny úkoly** (All Tasks).

Použití webových stránek služby Certificate Services

Jakmile vaše síťové sídlo systému Windows 2000 funguje, můžete dovolit uživatelům požadovat od vašeho interního certifikačního úřadu své vlastní certifikáty. CA musí být nakonfigurován a spuštěn a zároveň musí být nakonfigurována a spuštěna také služba IIS. Webové stránky zápisu se nachází na adrese http://název_DNS_počítače/certsrv/.

Nastavení zásad veřejných klíčů v objektech zásad skupiny

Mnoho zásad PKI lze nastavit v objektu zásad skupiny (Group Policy object) a pak je jednoduše aplikovat na celý rozsah počítačů v doméně a organizační jednotce. V konzole MMC si otevřete modul snap-in Zásady skupiny (Group Policy) příslušného objektu zásad skupiny. Položky PKI se nacházejí v oblasti Konfigurace počítače (Computer Configuration):

Objekt Zásady skupiny (Group Policy)
Nastavení počítače (Computer Configuration)
Nastavení systému Windows (Windows Settings)
Nastavení zabezpečení (Security Settings)
Zásady veřejných klíčů (Public Key Policies)

Součástí objektů zásad skupiny jsou seznamy důvěryhodných certifikátů a kořenové certifikáty CA, které obsahují certifikační úřady, jimž mají příjemci daných zásad skupiny důvěřovat. Jedná se o kontejner Důvěryhodnost v rámci rozlehlé sítě (Enterprise Trust) resp. kontejner Důvěryhodné kořenové certifikační úřady (Trusted Root Certification Authority) položky Zásady veřejných klíčů (Public Key Policies).

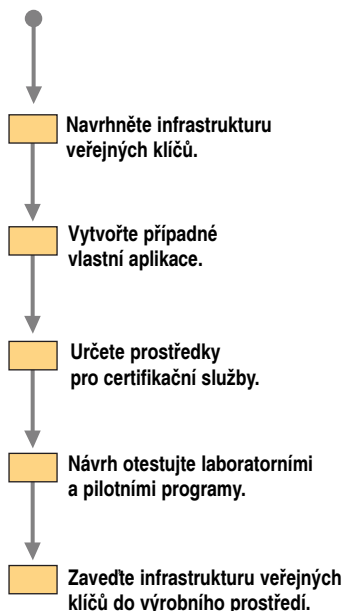
Vytváření infrastruktury veřejných klíčů

PKI systému Windows 2000 poskytuje rámec služeb, technologií a protokolů založených na standardech, jež vám prostřednictvím technologie veřejného klíče umožňují vytvářet a spravovat systém se silným zabezpečením informací. Systém Windows 2000 podporuje různé funkce zabezpečení veřejným klíčem požadované službami distribuovaného zabezpečení. Systém Windows 2000 tak například podporuje operace šifrování s veřejným klíčem potřebné pro EFS, aniž by bylo nutné zavádět nějakou další infrastrukturu nebo certifikační úřady.

Mnoho zabezpečených řešení (například zabezpečená elektronická pošta, ověřování kartami Smart Card a zabezpečené webové komunikace) však vyžaduje, abyste pro podporu těchto typů aplikací navrhli, otestovali a zavedli další komponenty PKI včetně certifikačních úřadů, zápisů certifikátů a obnovení. Můžete také požadovat zavedení certifikačních služeb v zájmu podpory uživatelů a více agentů obnovení EFS nebo ověření IPSec pro klienty bez spuštěného ověřování Kerberos či pro klienty, kteří při vytváření vztahů důvěryhodnosti nemohou ověřování Kerberos používat (přes nedůvěryhodné domény Windows 2000 nebo s počítačem, který není členem domény Windows 2000). V zájmu naplnění specifických požadavků vaší společnosti může být také nutné vyvinout a zavést své vlastní aplikace a certifikační služby.

Na obrázku 12.1 je základní proces, který můžete použít při návrhu, testování a zavádění PKI ve své organizaci.

Začátek



Obrázek 12.1
Vývojový graf procesu návrhu
PKI ve vaší organizaci

Infrastrukturu PKI můžete navrhnout a zavést prostřednictvím certifikačních služeb (Microsoft Certificate Services). Pro vytvoření části nebo celé struktury PKI lze použít také jiné certifikační úřady kompatibilní se systémem Windows 2000. Základní proces vytváření PKI je vždy stejný a nezávisí na používaných certifikačních službách. Podrobnosti vlastní implementace vytváření PKI se však budou lišit podle specifické technologie certifikačních služeb. Další informace o komponentách a funkcích infrastruktury veřejných klíčů systému Windows 2000 najdete v knize *Microsoft Windows 2000 Server Distribuované systémy* v kapitole „Volba řešení zabezpečení s použitím technologie veřejného klíče“. Další informace o komponentách a funkcích certifikačních služeb jiných výrobců získáte u příslušného výrobce této certifikační služby.

Návrh infrastruktury veřejných klíčů

V systému Windows 2000 lze navrhnout PKI naplňující široký rozsah potřeb zabezpečení s veřejným klíčem. Tyto potřeby je nutné přesně specifikovat, aby bylo možné navrhnout vytvoření a rozsah infrastruktury, která je bude podporovat.

Určení požadavků na certifikáty

Než budete moci určit, jaké certifikační služby PKI potřebujete, musíte identifikovat aplikace, které budete používat a které požadují digitální certifikáty. Musíte také určit všechna využití certifikátů, kteří uživatelé, počítače a služby budou certifikáty potřebovat a jaké typy certifikátů máte v úmyslu vydávat. Můžete zavést služby Microsoft Certificate Services nebo můžete potřeby svých veřejných klíčů podporovat pomocí jiných certifikačních služeb. Určete kategorie uživatelů, počítačů a služeb, které budou potřebovat certifikáty, a v jednotlivých kategoriích specifikujte tyto informace:

- Název nebo popis
- Důvod potřebnosti certifikátů
- Počet entit (uživatelů, počítačů nebo služeb)
- Umístění uživatelů, počítačů a služeb

Budete potřebovat certifikační služby podporující identifikované kategorie všech jednotek a lokací ve vaší organizaci. Zaváděné certifikační služby jsou určeny typy vydávaných certifikátů, počtu entit vyžadujících certifikáty a umístěním skupin. Můžete tak například zavést dva vystavující certifikační úřady zajišťující certifikáty pro všechny skupiny správců ve vaší organizaci. Protože je však nepochybně ve vaší organizaci mnohem více normálních uživatelů než správců, budete asi muset zavést samostatné vystavující certifikační úřady v jednotlivých oblastech a tímto způsobem naplnit potřeby uživatelů.

Další informace o řešeních zabezpečení využívajících digitální certifikáty najdete v knize *Microsoft Windows 2000 Server Distribuované systémy* v kapitole „Volba řešení zabezpečení s použitím technologie veřejného klíče“.

Základní požadavky zabezpečení certifikátů

Při použití certifikátů je úroveň celkového zabezpečení ovlivněna několika základními faktory. Pro certifikáty, které plánujete vystavovat, určete požadavky těchto faktorů:

- **Délka soukromého klíče.** V obvyklém nasazení mají klíče certifikátů uživatelů délku 1024 bitů a klíče kořenových certifikačních úřadů mají délku 4096 bitů.

- **Šifrovací algoritmy používané v certifikátech.** Doporučujeme použití výchozích algoritmů.
- **Doba životnosti certifikátů a soukromých klíčů a cyklus jejich obnovení.** Doba životnosti certifikátů je určena typem certifikátu, vašimi požadavky na zabezpečení, standardní praxí ve vašem oboru a vládními nařízeními.
- **Požadavky na speciální ukládání a správu soukromých klíčů.** Například jde o ukládání na karty Smart Card a neexportovatelné klíče.

Obvyklým požadavkům na zabezpečení vyhoví standardní nastavení certifikátů vydávaných službou Microsoft Certificate Services. Můžete však definovat silnější nastavení zabezpečení certifikátů používaných určitými skupinami uživatelů. Lze například určit větší délky soukromých klíčů a kratší doby životnosti certifikátů používaných k zajištění zabezpečení velmi cenných informací. Dalšího zabezpečení ukládání soukromých klíčů lze dosáhnout specifikováním použití karet Smart Card.

Určení typů vydávaných certifikátů

Určete typy certifikátů, jaké budete vydávat. Typy vydávaných certifikátů závisejí na zavedených certifikačních službách a požadavcích zabezpečení určených pro vydávané certifikáty. Lze vydávat typy certifikátů s více možnostmi použití, které splňují různé požadavky na zabezpečení.

V případě podnikových certifikačních úřadů je možné vydávat různé typy certifikátů vycházejících z šablon certifikátů a privilegií účtů v doméně Windows 2000. Každý podnikový certifikační úřad lze nakonfigurovat na vydávání určitého výběru typů certifikátů. Různé typy nabízených šablon certifikátů a jejich účel najdete v tabulce 12.2.

Tabulka 12.2 Šablony certifikátů a jejich účel

Název šablony certifikátu	Účel certifikátu	Vystavován pro
Agent pro zápis certifikátu počítače (MachineEnrollmentAgent)	Agent žádosti o certifikát	Počítač
Agent pro zápis certifikátu (EnrollmentAgent)	Agent žádosti o certifikát	Uživatel
Agent pro zápis certifikátu (žádost v režimu offline) (Exchange Enrollment Agent (Offline Request))	Agent žádosti o certifikát	Uživatel
Agent pro zotavení systému souborů EFS (EFSRecovery)	Obnovení souborů	Uživatel
IPSec (IPSECIntermediateOnline)	Zabezpečení protokolu IP	Počítač
IPSec (Žádost v režimu offline) (IPSECIntermediateOffline)	Zabezpečení protokolu IP	Počítač
Ověřená relace (ClientAuth)	Ověření klienta	Uživatel
Počítač (Machine)	Ověření klienta, ověření serveru	Počítač
Podpis kódu (CodeSigning)	Podpis kódu	Uživatel
Podpis seznamu důvěryhodnosti (CTLSigning)	Podpis seznamu důvěryhodných certifikátů	Uživatel
Podpis uživatele Exchange (Exchange User Signature)	Ověření klienta, zabezpečení elektronické pošty	Uživatel

Podřízený certifikační úřad (SubCA)	Libovolný	Počítač
Pouze podpis uživatele (UserSignature)	Zabezpečení elektronické pošty, ověření klienta	Uživatel
Přihlášení pomocí karty Smart Card (SmartcardLogon)	Ověření klienta	Uživatel
Řadič domény (Domain Controller)	Ověření klienta, ověření serveru	Počítač
Server WWW (WebServer)	Ověření serveru	Počítač
Směrovač (Žádost v režimu offline) (OfflineRouter)	Ověření klienta	Počítač/směrovač
Správce (Administrator)	Podpis kódu, podpis seznamu důvěryhodných certifikátů (CTL), systém souborů EFS, zabezpečení elektronické pošty, ověření klienta	Uživatel
Šifrování CEP (CEP Encryption)	Agent žádosti o certifikát	Směrovač (router)
Uživatel (User)	Šifrování systému souborů, zabezpečení elektronické pošty, ověření klienta	Uživatel
Uživatel Exchange (Exchange User)	Ověření klienta, zabezpečení elektronické pošty	Uživatel
Uživatel karty Smart Card (SmartcardUser)	Ověření klienta, zabezpečení elektronické pošty	Uživatel
Základní systém souborů EFS (EFS)	Šifrování systému souborů	Uživatel

U samostatných certifikačních úřadů (stand-alone CA) můžete v požadavku o certifikát určit použití certifikátu. Pomocí vlastních modulů zásad lze také určit typy certifikátů vystavované samostatnými certifikačními úřady. Další informace o vývoji vlastních aplikací pro službu Microsoft Certificate Services najdete v rámci odkazu na sadu SDK na stránce webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Typy certifikátů vystavovaných jinými certifikačními službami jsou určeny specifickými funkcemi a prvky daného produktu. Další informace získáte u výrobce příslušné certifikační služby.

Definování zásad certifikátů a postupů certifikačního úřadu

K vytvoření certifikačních úřadů ve své organizaci můžete použít službu Microsoft Certificate Services nebo jiné certifikační služby. Než ve své organizaci zavedete CA, definujte zásady certifikátů a prohlášení o certifikačních postupech (certificate practice statements – CPS). Zásady certifikátů určují, k čemu se budou certifikáty používat a jaká je odpovědnost přebíraná certifikačním úřadem za takové použití. Prohlášení o certifikačních postupech určuje postupy, které bude CA používat pro správu certifikátů, jež vystavila. CPS popisuje, jak jsou implementovány požadavky zásad certifikátů v kontextu operačních zásad, systémové architektury, fyzického zabezpečení a počítačového prostředí certifikačního úřadu organizace. Zásady certifikátů tak mohou například určovat, že soukromé klíče nelze exportovat, a CPS pak popisuje, jak se toho dosáhne pomocí zavedené infrastruktury PKI.

Zásady certifikátů

Zásady certifikátů mohou obsahovat tyto typy informací:

- Jak budou uživatelé ověřováni pro certifikační úřad
- Právní problémy (například odpovědnost), které se mohou objevit v případě kompromitace CA nebo zneužívání tohoto úřadu
- K jakým účelům se bude daný certifikát používat
- Požadavky na správu soukromých klíčů, například jejich ukládání na kartách Smart Card nebo jiných hardwarových zařízeních
- Zda lze exportovat soukromé klíče
- Požadavky na uživatele certifikátů včetně toho, co musí uživatelé učinit v případě ztráty nebo prozrazení svých soukromých klíčů
- Požadavky na zápis certifikátů a jejich obnovování
- Životnost certifikátů
- Používaný kryptografický algoritmus
- Minimální délka páru veřejného a soukromého klíče

Prohlášení o certifikačních postupech (CPS)

Prohlášení CPS určitého certifikačního úřadu může splňovat požadavky více zásad certifikátů. Každé CPS obsahuje informace specifické pro daný úřad CA. CPS podřízeného certifikačního úřadu se však může odkazovat na obecné a společné informace uvedené v CPS nadřazeného certifikačního úřadu. Prohlášení CPS může obsahovat tyto typy informací:

- Identifikace certifikačního úřadu (včetně názvu CA, názvu serveru a adresy DNS)
- Jaké zásady certifikátů daný certifikační úřad implementuje a jaké typy certifikátů vystavuje
- Zásady, procedury a postupy vystavování a obnovování certifikátů
- Kryptografické algoritmy, CPS a délky klíčů používané daným certifikátem CA
- Životnost certifikátu CA
- Fyzické, síťové a procedurální zabezpečení CA
- Životnost jednotlivých certifikátů vystavených CA
- Zásady odvolávání certifikátů včetně podmínek takového odvolání certifikátu, jako je například odchod zaměstnance nebo zneužívání privilegií zabezpečení
- Zásady seznamů odvolaných certifikátů (certificate revocation lists – CRL) včetně distribučních bodů CRL a intervalů publikování
- Zásady obnovení certifikátu CA před vypršením jeho platnosti

Definování strategie důvěryhodnosti certifikačních úřadů

Před zavedením PKI systému Windows 2000 musíte definovat strategie důvěryhodnosti CA, které budete ve své organizaci používat. V systému Windows 2000 lze vytvořit vztahy důvěryhodnosti mezi úřady CA pomocí hierarchických řetězců důvěryhodnosti CA a seznamů důvěryhodných certifikátů.

Výhody hierarchií důvěryhodnosti certifikačních úřadů

PKI systému Windows 2000 má hierarchickou strukturu CA. Hierarchie CA zajišťuje škálovatelnost, jednoduchou správu a konzistenci se stále větším počtem produktů CA jiných výrobců.

Obecně lze říci, že hierarchie obsahuje více certifikačních úřadů s jasně definovanými vztahy podřízenosti a nadřazenosti. V tomto modelu jsou podřízené certifikační úřady (dceřinné) certifikovány certifikáty vystavenými nadřazeným (mateřským) certifikačním úřadem, čímž se váže veřejný klíč určitého certifikačního úřadu k jeho identitě.

Certifikační úřad na vrcholu hierarchie se označuje za hlavní nebo také kořenový úřad CA (root CA). Úřady CA pod hlavním úřadem se označují za podřízené úřady CA (subordinate CA). V systému Windows 2000 platí, že pokud důvěřujete hlavnímu úřadu CA (protože máte jeho certifikát ve svém úložišti důvěryhodných hlavních certifikačních úřadů), důvěřujete také všem podřízeným úřadům v hierarchii, za předpokladu, že nebyl certifikát některého podřízeného úřadu odvolán úřadem, jenž jej vystavil, nebo nevypršela doba jeho platnosti. Proto jsou všechny hlavní (kořenové) certifikační úřady velmi důležitými body důvěryhodnosti v organizaci a je zapotřebí je odpovídajícím způsobem zabezpečit a spravovat.

Výhodou tohoto modelu je, že ověřování certifikátů vyžaduje důvěryhodnost jen malého počtu hlavních CA. Zároveň zajišťuje flexibilitu z hlediska počtu podřízených CA vystavujících certifikáty. Existuje několik praktických důvodů pro zavedení více podřízených certifikačních úřadů. Mezi ně patří:

Použití. Certifikáty lze vystavovat pro řadu různých účelů (například zabezpečenou elektronickou poštu, ověřování apod.). Zásady vystavování pro tato použití mohou být odlišné a jejich oddělení vytváří základ jednoduché správy těchto zásad.

Organizační oddělení. V závislosti na roli určité entity v organizaci může být zapotřebí používat různé zásady vystavování certifikátů. V zájmu oddělení a správy těchto zásad je opět možné vytvořit podřízené certifikační úřady.

Geografická oddělení. Organizace mohou mít různé entity na různých fyzických lokalitách. Síťová konektivita mezi takovými místy může vyžadovat zavedení více podřízených certifikačních úřadů, aby byly splněny všechny požadavky na použitelnost.

Větší množství úrovní hierarchie důvěryhodnosti nabízí také následující výhody pro správu:

- Flexibilní konfigurování prostředí zabezpečení CA (síla klíčů, fyzická ochrana, ochrana před síťovými útoky atd.). Prostředí CA lze vyladit tak, aby byla zajištěna rovnováha mezi zabezpečením a použitelností. U svého hlavního certifikačního úřadu můžete například použít speciální kryptografický hardware, ponechat jej v nepřístupné místnosti a provozovat jej v režimu offline. V případě vystavujícího certifikačního úřadu by však takové řešení bylo nákladné, celý úřad by se jen obtížně používal a výsledkem by bylo snížení výkonnosti a efektivity CA.
- Možnost často obnovovat klíče a certifikáty těch podřízených a vystavujících certifikačních úřadů, jejichž fungování je nejriskantnější, aniž by bylo nutné měnit již vytvořené vztahy důvěryhodnosti ke kořenové autoritě.
- Schopnost odstavit nějakou část hierarchie CA, aniž by to mělo vliv na vytvořené vztahy důvěryhodnosti ke kořenové autoritě nebo na zbylou část hierarchie.

Navíc vám poskytne zavedení více vystavujících certifikačních úřadů tyto výhody:

- Samostatné zásady certifikátů pro různé kategorie uživatelů a počítačů nebo pro organizační či geografická oddělení. Můžete zavést vystavující CA zajišťující certifikáty pro jednotlivé kategorie, oddělení nebo lokace.
- Rozdělení certifikačního zatížení a zajištění redundantních služeb. Je možné vytvořit více vydávajících certifikačních úřadů a rozdělit tak zatížení vyplývající z požadavků na používání certifikátů v síťovém sídle, v síti nebo na serveru. Například v případě pomalých nebo přerušujících se propojení mezi síťovými sídly může být zapotřebí pro zajištění dostatečné výkonnosti a použitelnosti certifikačních služeb vytvořit vystavující certifikační úřad na každém síťovém sídle. Podle propojení sídel a sítí a požadavků na zatížení lze vystavující certifikační úřady vytvářet také v zájmu rozdělení zatížení vyplývajícího z použití certifikátů. Zavedením více vystavujících úřadů CA zajistíte také duplikaci služeb. Když tedy dojde k poruše na jednom certifikačním úřadu, druhý úřad zajistí nepřerušovanou obsluhu požadavků.

Výhody seznamů důvěryhodných certifikátů

Seznam důvěryhodných certifikátů (certificate trust list – CTL) je seznam podepsaných certifikátů certifikačních úřadů, jejichž certifikátům bude vaše organizace důvěřovat. Seznam důvěryhodných certifikátů vám umožňuje řídit účel a dobu platnosti certifikátů vystavených externími certifikačními úřady nad rámec údajů specifikovaných daným úřadem. Když vytvoříte seznam důvěryhodných certifikátů, musíte jej ještě autorizovat podepsáním certifikátem vystaveným certifikačním úřadem, kterému již důvěřujete.

V rámci jednoho síťového sídla může existovat více seznamů důvěryhodných certifikátů. Protože použití certifikátů v různých doménách nebo organizačních jednotkách (OU) se může lišit, lze vytvořit seznamy důvěryhodných certifikátů odpovídajících daným použitím a přiřadit určitý seznam důvěryhodných certifikátů určitému objektu zásad skupiny.

Po aplikování daného objektu zásad skupiny (Group Policy object) na sídlo, doménu nebo OU dědí tyto zásady odpovídající počítače. Tyto počítače pak důvěřují úřadům CA v seznamu důvěryhodných certifikátů. Do zásad skupiny můžete vložit také hlavní (kořenové) certifikační úřady. Použití seznamů důvěryhodných certifikátů je pohodlnější než používání zásad skupiny, protože mají omezenou dobu platnosti.

Seznamy důvěryhodných certifikátů systému Windows 2000 můžete vytvořit v zájmu získání těchto výhod:

- **Vytváření důvěryhodných certifikátů specifických úřadů CA, aniž by bylo nutné požadovat širší důvěryhodnost hlavního certifikačního úřadu.** Seznamy důvěryhodných certifikátů tak můžete používat například na extranetu a důvěřovat certifikátům vystaveným určitými komerčními certifikačními úřady. Prostřednictvím připojení (mapování) certifikátu k účtu uloženému v Active Directory lze uživatelům s certifikáty vystavenými důvěryhodnými komerčními certifikačními úřady zaručit oprávnění přístupu k chráněným prostředkům extranetu.
- **Omezení povoleného použití certifikátů vystavených důvěryhodným certifikačním úřadem.** Například certifikáty vystavené určitým certifikačním úřadem je možné používat pro zabezpečenou elektronickou poštu, ověřování v síti a podepisování softwarového kódu. Pomocí seznamu důvěryhodných certifikátů na extranetu lze však omezit povolené použití těchto certifikátů výhradně na zabezpečení elektronické pošty.

- **Řízení doby platnosti certifikátů a certifikačních úřadů jiných organizací.** Například certifikační úřad vašeho obchodního partnera může mít dobu platnosti pět let a vydávat certifikáty s platností jednoho roku. Můžete však vytvořit seznam důvěryhodných certifikátů s dobou platnosti šest měsíců a omezit tak dobu, po jakou budou certifikáty vystavené certifikačním úřadem vašeho partnera důvěryhodné na vašem extranetu.

Další úvahy o strategiích důvěryhodnosti certifikačních úřadů

Při definování strategií důvěryhodnosti certifikačních úřadů mějte na paměti také tyto body:

- Hierarchie důvěryhodnosti CA má obvykle čtyři úrovně (hlavní CA, podřízená CA, vystavující CA a vystavené certifikáty).
- Úřady CA jiných společností mohou vytvářet část nebo celou hierarchii důvěryhodnosti CA. O zajištění očekávané interoperability jiných certifikačních úřadů se však přesvědčte testováním v laboratoři.
- Některé produkty jiných společností vyžadují jiné modely důvěryhodnosti CA, které nemusí spolupracovat s kořenovými hierarchiemi CA. Systém Windows 2000 a většina komerčních certifikačních úřadů podporují kořenové hierarchie CA.

Definování požadavků na zabezpečení certifikačních úřadů

Je zapotřebí, abyste definovali požadavky na zabezpečení poskytované certifikačním úřadům. Požadavky na zabezpečení CA mohou zahrnovat tyto body:

- Použití hardwarových CSP u hlavních certifikačních úřadů
- Správa hlavních certifikačních úřadů v nepřístupných místnostech
- Fungování kořenových certifikačních úřadů a někdy také podřízených úřadů v režimu offline.
- Umístění podřízených a vystavujících certifikačních úřadů v centrech zabezpečených dat.
- Delší klíče pro hlavní certifikační úřady a podřízené úřady vyšší úrovně

Chcete-li delegovat oprávnění z nadřazené společnosti na větší počet samostatných organizací, můžete vytvořit podřízený úřad CA, který bude pracovat v režimu offline. Samostatným organizacím pak můžete poskytnout podřízený certifikační úřad.

Rozhodování o požadovaném zabezpečení CA zahrnuje také určení rovnováhy mezi náklady na zavedení a správu zabezpečení a riziky útoků na CA a cenou za případný úspěšný útok. Vyšší riziko útoků na CA a vyšší náklady při jejich úspěchu ospravedlňují vyšší náklady na prostředky zabezpečení CA. Obvykle je zapotřebí zajistit největší ochranu hlavního (kořenového) certifikačního úřadu a podřízeným CA je nutné zařídit větší ochranu než vystavujícím CA.

Ochrana hlavního certifikačního úřadu nemusí být nákladná, zejména v případě menších společností. Někdy může postačovat mít hlavní CA v režimu offline v zabezpečené schránce pro počítač nebo používat vyměnitelné médium, které je jinak uloženo v trezoru. Počítač hlavního certifikačního úřadu by neměl obsahovat síťovou kartu.

Definování životních cyklů certifikátů

Životní cyklus certifikátu zahrnuje tyto události:

- Instalaci certifikačních úřadů a vystavení jejich certifikátů
- Vystavení certifikátů certifikačními úřady
- Odvolání certifikátů (v případě potřeby)
- Obnovení nebo vypršení platnosti certifikátů
- Obnovení nebo vypršení platnosti certifikátů certifikačních úřadů

Životní cyklus certifikátu se obvykle definuje tak, aby bylo nutné vystavené certifikáty periodicky obnovovat. Platnost vystavených certifikátů skončí na konci jejich životnosti a lze je cyklicky obnovovat, dokud nedojde k jejich odvolání, vypršení jejich platnosti, nebo již není k dispozici certifikační úřad, který je vystavil. Každý úřad CA může vystavovat certifikáty v několika cyklech obnovení certifikátů, dokud se CA nepřiblíží ke konci své životnosti. Pak bude funkce daného certifikačního úřadu ukončena, protože jeho klíče již nejsou zapotřebí, nebo dojde k obnovení CA novým párem klíčů.

Životní cykly certifikátů musíte nadefinovat tak, aby splňovaly vaše cíle a požadavky na zabezpečení. Volba životních cyklů závisí na různých faktorech, mezi něž patří i ty následující:

Délka soukromých klíčů CA a vystavených certifikátů Obecně platí, že delší klíče znamenají delší životnost certifikátů a klíčů.

Zabezpečení poskytované CSP Je obvyklé, že hardwarová CPS se překonávají obtížněji než softwarová CSP, a proto mohou podporovat delší životnosti certifikátů a klíčů.

Síla technologie použité v kryptografických operacích Některé šifrovací technologie poskytují silné zabezpečení i podporu silnějších kryptografických algoritmů. K zajištění vyššího zabezpečení, než je možné pomocí karet Smart Card, lze použít karty FORTEZZA Crypto Cards. Platí, že šifrovací technologie, kterou je obtížnější napadnout, podporuje delší životnost certifikátů.

Zabezpečení poskytované certifikačním úřadům a jejich soukromým klíčům Obecně platí, že čím více je certifikační úřad a jeho soukromý klíč fyzicky zabezpečen, tím delší je životnost CA.

Zabezpečení poskytované vystaveným certifikátům a jejich soukromým klíčům Například soukromé klíče uložené na kartách Smart Card lze považovat za zabezpečenější než soukromé klíče uložené ve formě souborů na místních pevných discích, protože karty Smart Card nelze přinutit k exportu soukromého klíče.

Riziko útoku Riziko útoku závisí na tom, jak zabezpečenou máte síť, jak cenné jsou síťové prostředky chráněné řetězcem důvěryhodnosti CA a jaké jsou náklady na spuštění útoku.

Nakolik důvěřujete uživatelům certifikátů Lze říci, že nižší důvěra vyžaduje kratší životní cykly certifikátů a klíčů. Dočasným uživatelům třeba budete důvěřovat méně než normálním uživatelům, takže můžete pro dočasné uživatele vystavit certifikáty s kratší životností. Lze také vyžadovat přísnější kontrolu obnovení certifikátů dočasných uživatelů.

Množství úkonů správy, které jste ochotni věnovat na obnovování certifikátů a CA Chcete-li například omezit úkony správy potřebné k obnovování certifikačních úřadů, můžete ve své hierarchii důvěryhodnosti certifikátů zadat dlouhou, bezpečnou životnost.

Důkladně si promyslete, jak dlouho chcete důvěřovat certifikačním úřadům a vystaveným certifikátům a klíčům. Čím déle jsou certifikáty a soukromé klíče platné, tím větší je riziko a potenciál kompromitace.

Měli byste definovat životní cykly certifikátů, které realisticky vyrovnávají vaše obchodní cíle s požadavky na zabezpečení. Příliš krátké životní cykly mohou mít za následek nadměrné množství úkonů správy potřebných ke správě cyklů. Příliš dlouhé životní cykly zase zvyšují riziko úspěšných útoků.

Když obnovujete certifikáty pomocí služby Microsoft CSP, můžete také obnovit pár klíčů daného certifikátu. Obecně platí, že čím déle je pár klíčů používán, tím vyšší je riziko prozrazení klíče. Měli byste určit nejdelší možnou životnost klíčů a obnovovat certifikáty novými páry klíčů před vypršením tohoto limitu.

Životní cyklus lze po jeho definování později změnit obnovením CA, certifikátů nebo klíčů v různých obdobích, která jste původně zadali. Přijdete-li například později na to, že životnost hlavního certifikačního úřadu představuje pro CA větší riziko, než jste původně předpokládali, můžete obnovit řetězec CA a životní cyklus upravit podle potřeby v zájmu snížení rizika.

Definování procesů zápisu a obnovení certifikátů

Definujte procesy zápisu a obnovení certifikátů, které budete ve své organizaci používat. Služba Microsoft Certificate Services podporuje následující metody zápisu a obnovení certifikátů:

- Interaktivní žádosti o certifikáty pomocí Průvodce podáním žádosti o certifikát (Certificate Request Wizard) (pouze pro uživatele, počítače a služby systému Windows 2000).
- Automatické žádosti o certifikáty pomocí Průvodce automatickým podáním žádosti o certifikát (Automatic Certificate Request Setup Wizard) (pouze pro certifikáty počítačů systému Windows 2000).
- Interaktivní žádosti o certifikáty pomocí webových stránek Microsoft Certificate Services (pro většinu klientských webových prohlížečů).
- Zápis karet Smart Card pomocí stanice Smart Card Enrollment Station.
- Vlastní aplikace zápisu a obnovení certifikátu pomocí nástroje Microsoft Enrollment Control.

Proces zápisu a obnovení certifikátů je určen uživateli a počítači, kterým chcete tyto služby poskytovat. Průvodce podáním žádosti o certifikát lze použít pouze v případě klientů systému Windows 2000. Webové služby zápisu a obnovení však lze použít v případě většiny klientů s webovými prohlížeči.

Webové stránky služby Microsoft Certificate Services lze používat tak, jak jsou k dispozici, stránky si však můžete také přizpůsobit. Tím je například možné omezit uživatelské volby nebo poskytnout dodatečné odkazy na online instrukce pro uživatele a další pomocné informace.

Definování zásad odvolávání certifikátů

Zásady odvolávání certifikátů vaší organizace zahrnují zásady odvolávání certifikátů a zásady používání seznamů odvolaných certifikátů (certificate revocation list - CRL).

Zásady odvolávání certifikátů

Zásady odvolávání certifikátů určují podmínky ospravedlňující odvolání certifikátu. Lze například určit, že certifikáty musí být odvolány v případě odchodu pracovníka nebo jeho převedení do jiného oddělení. Můžete také určit, že certifikáty musí být odvolány, pokud uživatelé zneužijí svá privilegia zabezpečení nebo dojde k prozrazení soukromých klíčů (například ke ztrátě karty Smart Card). V případě certifikátů počítačů lze specifikovat, že certifikáty musí být odvolány v případě náhrady počítače, ukončení jeho používání nebo při prozrazení klíče.

Zásady seznamů odvolaných certifikátů

Zásady CRL určují, kde budou seznamy CRL distribuovány a jaký je jejich publikační plán. Můžete například určit, že se některé seznamy CRL budou distribuovat do často používaných veřejných složek a webových stránek i do Active Directory. Lze zároveň zadat, že se určité seznamy CRL budou publikovat denně a nepoužije se u nich výchozí týdenní publikování.

Definování strategií údržby

Definujte své strategie údržby certifikačních úřadů a jejich obnovení po poškození. Mezi strategie údržby a obnovení po poškození patří tyto položky:

- Typy zálohování vykonávané pro certifikační úřady
- Časové plány zálohování certifikačních úřadů
- Zásady obnovování certifikačních úřadů po poškození
- Zásady agentů obnovení EFS
- Zásady obnovení zabezpečené elektronické pošty

Vývoj plánů obnovení po poškození

Můžete vyvinout plány, které pomohou s obnovou funkce certifikačních úřadů po jejich poruše nebo v případě kompromitace. Plány obnovení po poruše otestujte, aby byla zaručena jejich správná funkce, a proškolení správce v používání těchto plánů.

Plány obnovení po poruše zahrnují tyto věci:

- Procedury obnovení po poruše a seznamy úkolů, podle kterých budou správci postupovat
- Nástroje obnovení po poruše nebo odkazy na takové nástroje
- Kontingenční plány

Další informace o zálohování a obnovování v systému Windows 2000 najdete v této knize v kapitole „Určení strategií správy úložišť systému Windows 2000“.

Nefungující certifikační úřad

Certifikační úřad může mít poruchu z mnoha různých důvodů, například kvůli poruše pevného disku, poruše síťové karty nebo poruše na základní desce serveru. Některé poruchy lze rychle lokalizovat a opravit. Je například možné nahradit porouchanou síťovou kartu nebo základní desku, počítač restartovat a certifikační služby obnovit.

Došlo-li k poruše pevného disku, můžete jej vyměnit a obnovit server a certifikační úřad z poslední sady zálohování. Je-li poškozený certifikační úřad, můžete jej obnovit z poslední sady zálohování na serveru.

Musíte-li vyměnit server, nakonfigurujte nový server se stejným síťovým názvem a adresou IP, jako měl porouchaný server CA. K obnovení CA z nejnovější sady zálohování pak můžete použít nástroj Zálohování (Backup) nebo Průvodce obnovením certifikačních úřadů (Certification Authorities Restore wizard) systému Windows 2000.

Kompromitovaný certifikační úřad

Došlo-li ke kompromitaci certifikačního úřadu, musíte odvolat jeho certifikát. Odvoláním certifikátu CA se ruší platnost daného certifikačního úřadu a jeho podřízených úřadů, stejně jako všech certifikátů vystavených daným certifikačním úřadem a jemu podřízenými úřady. Odhalíte-li kompromitaci CA, co nejdříve vykonajte následující činnosti:

- Odvolejte certifikát kompromitovaného certifikačního úřadu. Jestliže došlo k obnovení CA, odvolejte všechny certifikáty CA, pouze pokud došlo ke kompromitaci všech souvisejících klíčů.
- Publikujte nový seznam CRL obsahující odvolaný certifikát CA. Uvědomte si, že klientské aplikace si mohou ukládat seznamy CRL až do vypršení jejich platnosti, takže se nově publikovaný seznam CRL neobjeví až do okamžiku, než vyprší platnost staršího seznamu.
- Odstraňte kompromitované certifikáty z úložiště důvěryhodných hlavních certifikačních úřadů a seznamů CTL.
- O kompromitaci uvědomte všechny uživatele a správce, kterých se to týká, a informujte je v tom smyslu, že všechny certifikáty vydané ovlivněnými certifikačními úřady se odvolávají.
- Zajistěte, aby nemohlo opakovaně dojít ke kompromitaci.

Chcete-li obnovit hierarchii CA, musíte zavést nové certifikační úřady nebo obnovit certifikát CA a vytvořit nový klíč, který nahradí kompromitovanou hierarchii. Pak musíte opakovaně vydat příslušné certifikáty uživatelům, počítačům a službám. V závislosti na tom, kde v hierarchii k odvolání došlo, to může znamenat vytvoření nové hierarchie CA nebo jen její části.

Vývoj vlastních aplikací

Pomocí standardních komponent a funkcí PKI systému Windows 2000 lze zavést velké množství řešení zabezpečení pomocí veřejných klíčů. S využitím rozhraní Microsoft CryptoAPI si však můžete vyvinout také své vlastní aplikace.

Pomocí CryptoAPI lze vyvíjet moduly vlastních zásad (custom policy modules) a vlastních modulů ukončení (custom exit modules) a integrovat tak certifikační služby s existujícími databázemi a adresářovými službami jiných výrobců. Můžete například vyvinout aplikaci, která ověří žádosti o certifikáty na základě informací o uživateli obsažených v nějaké již existující databázi nebo adresářové službě jiného výrobce.

Můžete také vyvinout vlastní aplikaci používající speciální typy certifikátů. Lze tak například vyvinout aplikaci, která vytvoří digitální otisk nějakého elektronického dokumentu a tento otisk pak uloží v certifikátu označeném časem a datem. Tyto certifikáty s otisky můžete uchovávat v registrační databázi dokumentů a zajistit tak integritu obsahu původních dokumentů. Porovnáním dokumentu s jeho digitálním otiskem v registrační databázi lze zjistit úpravy dokumentu od jeho zaregistrování. Tímto použitím

registru dokumentů zajistíte online sledování zajištění kvality svých výrobků a zaručíte tak integritu elektronických dokumentů testů a certifikací.

Navíc můžete vyvinout svou vlastní aplikaci zápisu a obnovení certifikátu pomocí technologie Active Server Pages. Lze například upravit standardní webové stránky certifikačních služeb (Microsoft Certificate Services) a přidat sem nebo naopak odstranit některé funkce. Můžete také vytvořit vlastní webové stránky integrující služby jiných výrobců či aplikací, které vyvíjíte.

Další informace o vývoji svých vlastních aplikací pro službu Microsoft Certificate Services najdete v odkaze na SDK pro platformu Microsoft na stránce webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Plánování prostředků

Měli byste odhadnout síťové, počítačové a další pomocné prostředky, které budou zapotřebí pro podporu certifikačních služeb, jež chcete ve své organizaci zavést. Celkový počet potřebných prostředků se může výrazně měnit v závislosti na velikosti vaší organizace a úrovni a rozsahu zaváděné infrastruktury PKI.

Při odhadování prostředků zvažte prostředky nutné k podpoře krátkodobých potřeb a plánovaného dlouhodobého růstu vaší organizace.

Mezi síťové a počítačové prostředky, potřebné pro zavedení PKI, patří:

- Servery, na nichž běží certifikační služby a vaše vlastní aplikace
- Kryptografický hardware, jako jsou například desky hardwarových šifrovacích akceleratorů
- Úložiště pro databázi certifikátů a vaše vlastní aplikace na pevném disku
- Prostředky úložišť nezbytné pro zálohování certifikačních úřadů a vašich aplikací
- Prostředky pro obnovení po poruše, jako jsou například sady obnovení nebo stále připravené náhradní servery

Výkonnost certifikačních služeb se může výrazně měnit v závislosti na těchto faktorech:

- **Délka klíče certifikačního úřadu používaného k podepisování certifikátů.** Čím delší je tento klíč, tím více výpočetního výkonu a času je zapotřebí pro podepsání certifikátu. Měli byste si uvědomit, že operace podpisu se vykonává (na serveru) jednou pro každý certifikát v okamžiku jeho vystavení, zatímco operace ověření se vykonává během života certifikátu mnohokrát (na klientovi či jiném serveru, podle protokolu). Uvědomte si, že podepisování certifikátu je nákladnější, než jeho ověřování.
- **Složitost logiky modulu zásad certifikačního úřadu (CA policy module) používané k ověřování žádostí o certifikáty.** Čím složitější je logika zásad, tím déle trvá zpracování a vystavení certifikátů. Většině použití by měl modul podnikových (enterprise policy module) a samostatných zásad (stand-alone policy module) systému Windows 2000 vyhovovat. Chcete-li vyvinout svůj vlastní modul zásad, náklady na složitost by měly být zváženy jak pro modul zásad tak i pro modul ukončení.
- **Vliv vlastních aplikací na výkonnost.** Vlastní aplikace ovlivňují celkovou výkonnost certifikačních aplikací. Například aplikace zápisu certifikátu využívající standardní skripty Common Gateway Interface (CGI) může představovat významná zdržení procesu zápisu.

Kapacita pevného disku potřebná k podpoře certifikačních databází závisí na těchto faktorech:

- **Kolik certifikátů vydá certifikační úřad.** Odhadněte, kolik certifikátů bude asi vystaveno během života daného certifikačního úřadu. Úřad CA, který bude vydávat větší počet certifikátů nebo bude mít delší životnost, bude také požadovat větší databázi certifikátů.
- **Velikost jednotlivých certifikátů.** Databáze certifikátů zahrnuje všechny informace v certifikátech, včetně veřejných klíčů. Certifikáty s delšími veřejnými klíči a obsahujícími další speciální informace budou po svém vystavení zabírat více prostoru na disku.

Některé databáze certifikátů mohou mít velikost několika gigabajtů nebo i více. U obvyklých databází se však nepředpokládá, že by jejich velikost přesáhla několik stovek megabajtů. Velikosti certifikátů byste měli zjistit v laboratoři a tyto výsledky pak použít k odhadu budoucí velikosti databáze podle počtu certifikátů, který daný certifikační úřad pravděpodobně během svého života vydá.

Zavedení infrastruktury veřejných klíčů

Máte-li již své strategie návrhu a zavedení veřejných klíčů ověřeny a vyzkoušeny v pilotních programech, můžete PKI zavést do svého výrobního prostředí. Následující seznam představuje základní proces, který lze použít k zavedení PKI.

Zavedení PKI zahrnuje tyto činnosti:

- Plánování zavedení po etapách.
- Zajištění školení a podpory pro uživatele.
- Instalace certifikačních úřadů.
- Instalace a konfigurace podpůrných systémů a aplikací.
- Konfigurace certifikátů, které budou vystavovány.
- Konfigurace publikace seznamů odvolaných certifikátů.
- Konfigurace zásad skupiny z hlediska veřejných klíčů.
- Konfigurace obnovení a zápisu certifikátů.
- Vydávání certifikátů uživatelům, počítačům a certifikačním úřadům

Plánování postupného zavedení

V případě větších průmyslových nasazení naplánujte zavádění infrastruktury veřejných klíčů po etapách. Různé části infrastruktury pak můžete vytvářet podle potřeb podpory cílů zabezpečení a výrobních potřeb.

Můžete například začít se systémem EFS a funkcemi protokolu IPSec, protože k využití výhod zabezpečení těchto funkcí není zapotřebí hierarchie certifikačních úřadů. Druhou nejvyšší prioritu můžete přiřadit zabezpečené poště a ověřování pomocí karet Smart Card. Můžete dát přednost zavedení infrastruktury zabezpečené pošty před zavedením infrastruktury karet Smart Card, nebo lze naplánuvat zajištění zabezpečené elektronické pošty jen pro jednu skupinu nebo síťové sídlo a zároveň vytvoření infrastruktury karet Smart Card v jiné skupině nebo síťovém sídle.

Chcete-li pomocí PKI dosáhnout zabezpečení elektronické pošty, můžete si pro jednotlivé etapy naplánuvat následující činnosti:

- V nadřazených doménách jednotlivých stromů ve vaší organizaci nainstalujte hlavní certifikační úřady sloužící k zajištění zabezpečené elektronické pošty (hlavní CA se používají k certifikování podřízených CA v dané doméně nebo poddoméně).
- Nainstalujte a nakonfigurujte systém a služby (podle potřeby) zabezpečené elektronické pošty.
- V doménách a poddoménách jednotlivých jednotek organizace nainstalujte podřízené certifikační úřady pro zajištění zabezpečené elektronické pošty (každá jednotka certifikuje a instaluje vystavující certifikační úřad pro své uživatelské skupiny).
- V doménách a poddoménách uživatelských skupin v jednotlivých sídlech nainstalujte a nakonfigurujte podle potřeby vystavující CA (certifikované jednotkami společností) a služby zápisu certifikátů.

Chcete-li vytvořit infrastrukturu PKI pro karty Smart Card, můžete si pro jednotlivé etapy naplánovat následující činnosti:

- V nadřazených doménách jednotlivých stromů ve vaší organizaci nainstalujte hlavní certifikační úřady sloužící pro zajištění provozu karet Smart Card (hlavní CA se používají k certifikování podřízených CA v dané doméně nebo poddoméně).
- Nainstalujte a nakonfigurujte čtečky karet Smart Card pro uživatele a správce karet Smart Card.
- V doménách a poddoménách jednotlivých jednotek organizace nainstalujte podřízené certifikační úřady pro karty Smart Card (každá jednotka certifikuje a instaluje vystavující certifikační úřad pro své uživatelské skupiny).
- V doménách a poddoménách uživatelských skupin v jednotlivých sídlech nainstalujte a nakonfigurujte podle potřeby vystavující CA (certifikované jednotkami společností) a stanice zápisu karet Smart Card.

Můžete si také naplánovat postupné zavádění PKI podpory dalších funkcí zabezpečení veřejných klíčů, jako jsou zabezpečené webové komunikace a zabezpečená webová sídla, podepisování softwarového kódu, ověřování IPsec a operace systému EFS a obnovení.

Instalace certifikačních úřadů

Pro zajištění požadovaných certifikačních služeb vaší organizace musíte nainstalovat potřebné hierarchie CA. Nejprve se instaluje hlavní (kořenový) certifikační úřad a pak jednotlivé podřízené úřady v hierarchii. Chcete-li například vytvořit hierarchii CA se třemi úrovněmi a řetězec důvěryhodností, nainstalujete certifikační úřady na serverové počítače v tomto pořadí:

1. Hlavní certifikační úřad
2. Podřízený certifikační úřad
3. Vystavující certifikační úřad

Certifikát hlavního certifikačního úřadu je podepsán sám sebou. Každý podřízený certifikační úřad je certifikován (jeho certifikát je vystaven) nadřazeným certifikačním úřadem v hierarchii. V případě hierarchie certifikátů se třemi úrovněmi certifikuje všechny podřízené CA hlavní CA a všechny vystavující CA jsou certifikovány podřízeným certifikačním úřadem v hierarchii.

Poznámka Podřízený certifikační úřad může být certifikován jiným podřízeným úřadem, čímž se vytváří hierarchie s více úrovněmi.

V zájmu vytvoření požadovaného řetězce důvěryhodnosti lze instalovat podnikové certifikační úřady, samostatné certifikační úřady nebo certifikační úřady od jiných výrobců. Chcete-li vytvořit CA systému Windows 2000 Server, použijte ovládací panel **Přidat nebo odebrat programy** a na jednotlivé servery CA přidejte služby Microsoft Certificate Services.

Během instalace podřízených certifikačních úřadů systému Windows 2000 Server můžete požadovat certifikát podřízeného úřadu od online CA nebo můžete žádost o certifikát uložit do souboru žádosti a vlastní akt požádání o certifikát pak realizovat offline. Vyberete-li offline žádost o certifikát, daný certifikační úřad není během instalace certifikován. Musíte použít modul snap-in Certifikační úřad (Certification Authority) konzoly MMC, ručně importovat certifikát CA a dokončit instalaci CA, jakmile nadřazený certifikační úřad vystavil certifikát instalovaného úřadu. Uvedený modul snap-in lze použít také k importu certifikátů podřízených CA vystavených nadřazenými CA od jiných výrobců.

Instalace a konfigurace podpůrných systémů a aplikací

Musíte také nainstalovat další systémy a aplikace potřebné k zajištění podpory PKI. Mezi podpůrné systémy a aplikace patří:

- Čtečky karet Smart Card na místních počítačích
- Systémy zabezpečení elektronické pošty a správy klíčů
- Vlastní moduly zásad a ukončení
- Vlastní aplikace zápisu a obnovení certifikátů
- Infrastruktura PKI a certifikační služby od jiných výrobců
- Hardwarové šifrovací karty pro akceleraci a ukládání klíčů na serverech

Konfigurace vystavovaných certifikátů

Standardně platí, že podnikové certifikační úřady systému Windows 2000 jsou po své instalaci připraveny vydávat několik typů certifikátů. Výchozí konfiguraci můžete upravit prostřednictvím modulu snap-in Certifikační úřad (Certification Authority) konzoly MMC a určit tak typy certifikátů vystavovaných jednotlivými CA. Můžete odstranit výchozí typy certifikátů, které nemusí daný certifikační úřad vystavovat. Můžete také zadat další typy certifikátů, které má daný certifikační úřad vystavovat.

Příklady konfigurací

Certifikační úřady lze nastavit tak, aby podporovaly více funkcí zabezpečení nebo třeba jen jedinou funkci. Zde jsou uvedeny některé možné způsoby konfigurace CA:

- V případě hlavního certifikačního úřadu nebo podřízeného certifikačního úřadu lze nakonfigurovat CA tak, aby mohl úřad vydávat pouze certifikáty podřízených certifikačních úřadů.
- V případě vystavujícího certifikačního úřadu, který podporuje služby zabezpečených webových komunikací, lze nakonfigurovat CA tak, aby úřad mohl vydávat pouze certifikáty ověřeného připojení, počítače a webového serveru.

- V případě vystavujícího certifikačního úřadu, který podporuje normální uživatele, lze úřad nakonfigurovat tak, aby vystavoval pouze certifikáty uživatelů. Podobně lze certifikační úřad určený pro správce nakonfigurovat tak, aby vystavoval výhradně certifikáty správců.
- V případě vystavujícího certifikačního úřadu, který podporuje zápis kartami Smart Card, lze úřad CA nakonfigurovat tak, aby vystavoval pouze certifikáty přihlášení kartou Smart Card a uživatele karty Smart Card.

Seznamy řízení zabezpečeného přístupu šablon certifikátů

Oprávnění požadovat různé typy certifikátů jsou určena seznamy řízení zabezpečeného přístupu jednotlivých šablon certifikátů. Podnikový certifikační úřad obsluhuje pouze žádosti o certifikáty uživatelů, počítačů nebo služeb, které mají v seznamu přístupových práv (access control list – ACL) dané šablony certifikátu vybráno oprávnění k zápisu (Enroll). ACL šablon certifikátů jsou přednastaveny tak, aby umožnily žádosti o odlišné typy certifikátů různým výchozím uživatelským účtům a skupinám se zabezpečením.

K úpravě ACL jednotlivých šablon certifikátů lze použít modul snap-in Síť a služby Active Directory (Active Directory Sites and Services) konzoly MMC.

▼ Chcete-li upravit seznamy přístupových práv (ACL) jednotlivých šablon certifikátů:

1. Zadejte příkaz **Zobrazit uzel služeb** (Show Services Node) nabídky **Zobrazit** (View).
2. Rozevřete uzel služeb (Services) a kontejnery služeb veřejných klíčů (Public Key Services) a šablon certifikátů (Certificate Templates).
3. V podokně podrobností vyberte šablonu certifikátu a zobrazte si kartu **Zabezpečení** (Security) jeho okna vlastností. Na této kartě najdete skupiny, které mají k dané šabloně přístup, a specifická oprávnění jednotlivých skupin.

Například standardně platí, že pouze členové skupiny se zabezpečením Domain Administrators mohou požádat o certifikáty a obdržet certifikáty agenta zápisu. Chcete-li zadat, že pouze určití členové vašeho bezpečnostního oddělení mohou požadovat a získat certifikát agenta zápisu (enrollment agent certificate), můžete změnit seznam řízení zabezpečeného přístupu šablony certifikátu agenta zápisu. Ze seznamu přístupových práv (ACL) můžete odstranit správce domény a přidat sem příslušné oprávněné uživatelské účty nebo skupiny.

V případě samostatných certifikačních úřadů (stand-alone CA) systému Windows 2000 musí být v žádosti o certifikát obsažen také jeho typ, protože samostatné certifikační úřady nepoužívají šablony certifikátů. Chcete-li u samostatných CA řídit typy vystavovaných certifikátů, můžete je používat ve spojení s vlastními moduly zásad a vlastními aplikacemi žádostí o certifikáty.

Konfigurace publikace seznamů odvolaných certifikátů

Podnikové certifikační úřady publikují seznamy CRL do Active Directory podle výchozího nastavení jednou za týden. Samostatné a podnikové certifikační úřady publikují seznamy CRL do adresáře na serveru CA podle výchozího nastavení jednou za týden. Okamžik distribuce CRL lze změnit v modulu snap-in Certifikační úřad (Certification Authority) konzoly MMC. Tento modul lze také používat k interaktivnímu publikování nového seznamu CRL nebo ke změně časového rozvrhu publikování.

Konfigurace zásad skupiny z hlediska veřejných klíčů

Ke konfiguraci zásad skupiny pro veřejné klíče síťových sídel, domén a organizačních jednotek se používá modul snap-in Zásady skupiny (Group Policy) konzoly MMC. Lze nastavit následující volitelné kategorie zásad veřejných klíčů:

Agenti obnovení EFS

Účtem obnovení EFS pro určitou doménu je standardně místní účet uživatele Administrator prvního řadiče domény instalovaného v doméně. Importem příslušných dalších certifikátů agentů obnovení EFS do zásad můžete zadat další agenty obnovení zašifrovaných dat systému EFS. Proto je zapotřebí nejprve vystavit certifikáty agentů obnovení EFS pro účty uživatelů na místních počítačích, kteří budou mít funkci náhradních agentů obnovení.

Automatický zápis certifikátů

Lze zadat automatický zápis a obnovení certifikátů počítačů. Je-li nakonfigurován automatický zápis, zadané typy certifikátů se vystaví všem počítačům v rámci zásad skupiny pro veřejné klíče. Certifikáty počítačů vystavené automatickým zápisem obnovuje vystavující certifikační úřad. Automatický zápis nefunguje, není-li alespoň jeden certifikační úřad online, aby mohl zpracovat žádosti o certifikáty.

U virtuálních privátních sítí (VPN) využívajících protokol IPSec s protokolem L2TP pamatujte, že je zapotřebí nastavit zásady skupiny tak, aby byl možný automatický zápis certifikátů IPSec. Protokol IPSec může využít libovolný z certifikátů podepsaný algoritmem Rivest-Shamir-Adleman (RSA) podle tabulky 12.2, který je vystavený počítači a uložený v účtu daného počítače. Další informace o certifikátech protokolu L2TP pro použití IPSec při připojení VPN najdete v nápovědě systému Windows 2000 Server.

Důvěryhodnost hlavního certifikátu

Po instalaci hlavního podnikového certifikačního úřadu se certifikát tohoto úřadu přidá mezi důvěryhodné hlavní certifikační úřady dané domény. Do kontejneru Důvěryhodné kořenové certifikační úřady (Trusted Root Certification Authorities) modulu snap-in Zásady skupiny (Group Policy) konzoly MMC můžete interaktivně přidat také certifikáty dalších hlavních CA. Přidané certifikáty hlavních CA se stanou důvěryhodnými hlavními CA v rámci zásad skupiny. Chcete-li v certifikační hierarchii použít samostatný certifikační úřad nebo CA jiného výrobce, budete muset certifikát tohoto certifikačního úřadu přidat do kontejneru důvěryhodných hlavních certifikačních úřadů zásad skupiny.

Seznam důvěryhodných certifikátů

Je možné vytvořit seznam důvěryhodných certifikátů a důvěřovat tak specifickým certifikačním úřadům a omezit použití certifikátů vystavených danými CA. Můžete například použít seznam důvěryhodných certifikátů a důvěřovat jen certifikátům vystaveným komerčním certifikačním úřadem a omezit tak možná využití těchto certifikátů. Pomocí seznamů důvěryhodných certifikátů můžete na extranetech také řídit důvěryhodnost certifikátů vydaných certifikačními úřady spravovanými vašimi obchodními partnery.

Vaše společnost může být například součástí jiné společnosti. Tato partnerská společnost vydává své vlastní certifikáty pro webový přístup, zabezpečenou elektronickou poštu, podepisování softwaru apod. Bude ve vašem zájmu mít možnost vyměňovat si zabezpečenou elektronickou poštu se zaměstnanci partnerské společnosti, nechcete však vydávat pro tento účel další certifikáty. Proto můžete přidat kořenový certifikační úřad této společnosti na nový seznam důvěryhodných certifikátů v kontejneru důvěry-

hodnosti vaší společnosti a určit, že certifikáty partnerské organizace budou důvěryhodné pouze při použití v rámci zabezpečené elektronické pošty.

Konfigurace obnovení a zápisu certifikátů

Služba Microsoft Certificate Services podporuje mnoho různých metod zápisu a obnovení, jako jsou žádosti o certifikáty prostřednictvím průvodce a webových stránek. Budete-li používat certifikační služby jiných výrobců nebo své vlastní aplikace zápisu a obnovení certifikátů, musíte zadat potřebnou konfiguraci těchto služeb a aplikací.

Začátek vystavování certifikátů

Když máte potřebné certifikační služby nainstalované a nakonfigurované, můžete začít vystavovat certifikáty pro uživatele, počítače a služby. Při začátku vystavování certifikátů pamatujte na následující body:

- Certifikáty se vystavují pro počítače v rámci nastavení automatických žádostí o certifikáty zásady skupin domény. Správci mohou také ručně požadovat certifikáty pro místní počítače pomocí Průvodce podáním žádosti o certifikát a webových stránek služby Microsoft Certificate Services. Zvažte naplánování ručního zápisu po etapách, aby došlo k rozložení administrativní zátěže při zápisech počítačů do delšího období.
- Správci karet Smart Card mohou začít vystavovat certifikáty karet Smart Card pomocí součásti Smart Card Enrollment Station webových stránek Microsoft Certificate Services. Zvažte naplánování zápisu karet Smart Card po etapách, aby došlo k rozložení administrativní zátěže při zápisech karet Smart Card do delšího období.
- V době přechodu na karty Smart Card je obvyklé umožnit ověření kartou Smart Card i zabezpečenou přihlašovací sekvencí Ctrl+Alt+Del. Protože se tím však omezuje zabezpečení sítě, jakmile jsou uživatelé karet Smart Card proškoleni a své karty používají, nakonfigurujte zásady uživatelských účtů tak, aby vyžadovaly interaktivní přihlášení pomocí karet Smart Card.

Po započetí vystavování certifikátů sledujte velmi pečlivě výkonnost certifikačních služeb a ujistěte se, že certifikační úřady zatížení zvládají. Nadměrné zatížení můžete vyřešit přidáním dalších certifikačních úřadů nebo naplánováním zápisu certifikátů po etapách. Také obnovování certifikátů může znamenat značný nárůst zatížení, a proto přidání dalších certifikačních úřadů a naplánování zápisu certifikátů po krátkých etapách pomůže pomoci rozložit špičková zatížení obnovování.

Seznam úkolů plánování infrastruktury veřejných klíčů

Tabulka 12.4 uvádí přehled úkolů, které musíte splnit v rámci plánování zavedení PKI.

Tabulka 12.4 Seznam úkolů plánování infrastruktury veřejných klíčů

Úkol	Kapitola
Určete požadavky na certifikáty.	Určení požadavků na certifikáty
Definujte procesy vystavování certifikátů.	Definování zásad certifikátů a postupů certifikačního úřadu
Definujte hierarchii důvěryhodnosti CA.	Definování strategie důvěryhodnosti certifikačních úřadů
Určete požadavky na zabezpečení CA.	Definování požadavků na zabezpečení certifikačních úřadů
Definujte životní cykly certifikátů.	Definování životních cyklů certifikátů
Určete procesy zápisu a obnovení certifikátů.	Definování procesů zápisu a obnovení certifikátů
Definujte zásady odvolávání certifikátů.	Definování zásad odvolávání certifikátů
Definujte zásady údržby.	Definování strategií údržby
Určete zásady obnovení po poruše.	Vývoj plánů obnovení po poškození
Vytvořte plán postupného zavedení po etapách.	Zavedení infrastruktury veřejných klíčů

ČÁST IV

Inovace a instalace systému Windows 2000



Možnost automatizovat inovaci a instalaci systému Windows 2000 může vaší organizaci ušetřit mnoho času. Část 4 proto vysvětluje různé metody automatizované instalace, poskytuje podrobný popis kroků, které vám s tímto procesem pomohou, a ukazuje, jak lze v systému Windows 2000 používat terminálové služby (Terminal Services).

V této části

Automatizování instalace a inovace serveru 381

Zavádění systému Windows 2000 pomocí serveru Systems Management Server 419

Inovace a instalace členských serverů 451

Zavádění terminálových služeb 471

KAPITOLA 13

Automatizování instalace a inovace serveru

Nyní jste připraveni vyvinout a provést automatizovanou instalaci systému Windows 2000 Server a přidružených aplikací. To je základní předpoklad k uskutečnění všech fází zavedení – testování, pilotních programů i vlastního zavádění do výrobního procesu. V této kapitole najdete popis dostupných metod automatizované instalace, včetně požadavků na přípravu a ukázkových konfigurací. Doporučujeme, aby se s touto kapitolou seznámili zejména síťoví technici, účastníci se návrhu procesu instalace, a správci systému, účastníci se instalace systému Windows 2000 a přidružených aplikací.

Instalace systému Windows 2000 může být buď čistá, na počítače, na nichž není instalována žádná verze operačního systému dřívějšího než Windows 2000, nebo inovace, na počítačích, na kterých v současné době běží systémy Microsoft Windows NT Server verze 3.51 nebo Microsoft Windows NT Server verze 4.0. Informace v této kapitole vám pomohou určit, zda je lepší uskutečnit čistou instalaci nebo inovaci.

V této kapitole

Rozhodování mezi inovací a čistou instalací 382

Příprava instalace 384

Automatizování instalace serverových aplikací 398

Automatizování instalace systému Windows 2000 Server 401

Příklad konfigurace instalace 414

Seznam úkolů plánování instalace 417

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Plán automatizované instalace.

Související informace v Resource Kitu

- Další informace o plánování naleznete v této knize v kapitole „Úvod do plánování zavedení systému“.
- Další informace o správě klientských počítačů najdete v této knize v kapitole „Definování standardů správy a konfigurace klientů“.
- Chcete-li získat dodatečné informace o automatizování instalací klientů, podívejte se do kapitoly „Automatizování instalace a inovace klientů“ v této knize.

- Další informace o parametrech bezobslužné instalace, na něž se tato kapitola odvolává, najdete v dokumentu „Microsoft Windows 2000 Guide to Unattended Setup“ (Unattend.doc) na CD operačního systému Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98, nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.
- Další informace o bezobslužné instalaci a ukázkové soubory odpovědí najdete v příloze „Příklady souborů odpovědí pro bezobslužnou instalaci“ v této knize.

Rozhodování mezi inovací a čistou instalací

V podnikovém prostředí není z hlediska nákladů výhodné instalovat systém Windows 2000 pomocí standardního interaktivního instalačního programu na každém jednotlivém počítači. Výrazného snížení celkových nákladů na vlastnictví (total cost of ownership – TCO) dosáhnete automatizovanými instalacemi systému Windows 2000 Server na více počítačů.



Důležité rozhodnutí Před zautomatizováním instalace systému Windows 2000 Professional musíte rozhodnout, zda půjde o inovaci ze systému Windows NT nebo o čistou instalaci.

Následující dvě položky vám pomohou určit, zda je lepší vykonat inovaci nebo čistou instalaci.

- Jestliže již vaše organizace implementovala nějaký operační systém Windows a vaše oddělení informačních technologií (IT) je spravováno centrálně, bude lepší vykonat inovaci. Plánujete-li vytvoření nějakého spravovaného prostředí, ale zatím takové ve své organizaci nemáte, pak bude lepší zadat čistou instalaci, aby bylo možné během instalace implementovat standardní konfigurace.
- Plánujete-li používat již existující hardware a softwarové aplikace, pak budete muset učinit inovaci. Jestliže však předpokládáte koupi nového hardwaru a instalaci nových softwarových aplikací, bude lepší zvolit čistou instalaci.

Řešení kritických problémů

Plánujete-li instalovat systém Windows 2000 Server na počítače, na nichž ještě není instalován žádný operační systém, je zřejmé, že půjde o čistou instalaci. Jestliže na počítačích již běží systém Windows 95, Windows 98, Windows NT Workstation 3.51 nebo Windows NT Workstation 4.0, budete se muset rozhodnout, zda je z hlediska nákladů výhodnější inovovat existující operační systém nebo provést čistou instalaci.

Tabulka 13.1 Problémy plánování, které musí být vyřešeny před inovací nebo instalací

Problém	Úkol
Cíle organizace	Určete hlavní cíle své organizace.
Regionální potřeby	Identifikujte specifické regionální potřeby a určete, zda jsou součástí vašeho podniku také zahraniční pobočky nebo společnosti.
Skupiny uživatelů	Analyzujte skupiny uživatelů včetně jejich specifických kategorií a potřeb, znalost problematiky počítačů a zkušenosti uživatelů, požadavky na zabezpečení a umístění uživatelů a jejich problémy se síťovým propojením včetně rychlosti propojení.
Potřeby aplikací	Určete předběžně, které produkty budou instalovány na všech počítačích, které produkty budou inzerovány jenom pro určité specifické typy serverů a které produkty se budou distribuovat do specifických kategorií typů serverů.
Hardware	Zinventarizujte existující hardware a stanovte potřeby nového hardwaru. Před inovací nebo instalací určete minimální požadavky na hardware. Naplánujte budoucí potřeby počítačů. Určete, jak se budou počítače pohybovat organizací. Zjistěte, zda všechny počítače obsahují mechaniku kompaktních disků s podporou spouštění.
Rizikové a problémové oblasti	Určete potenciální rizika včetně nekompatibility aplikací se systémem Windows 2000, problémy s časovým plánem, více síťovými lokacemi, decentralizovaným rozpočtem nebo dopad možných budoucích slučování.
Očekávání růstu	Určete očekávaný růst v období projektu po jednom roce, třech a pěti letech. Vezměte v úvahu také plánovaná sloučení, nová síťová sídla a plánovaný růst v jiných zemích.
Síťové záležitosti	Zjistěte, zda mají vzdálená síťová místa servery zavádění aplikací. Určete, jak se inovují servery mimo centrální sídlo.
Správa softwaru	Zjistěte, zda se již používá nějaký systém správy softwaru, například Microsoft Systems Management Server, v němž lze zavádění naplánovat.
Konektivita	Určete, zda je možné servery a propojení mezi nimi nastavit tak, aby mohly distribuovat velké balíčky všem uživatelům ve společnosti.

Volba metody instalace

Po vyřešení těchto problémů plánování si můžete vybrat metody použité k automatizování instalací. Tabulka 13.2 uvádí metody automatizovaných instalací a informace, zda je lze použít k inovaci, k čisté instalaci, nebo k obojímu.

Tabulka 13.2 Metody automatizované instalace

Metoda	Verze systému Windows 2000	Inovace	Čistá instalace
Syspart	Server a Professional	Ne	Ano
Sysprep	Server a Professional	Ne	Ano
SMS	Server a Professional	Ano	Ano
Spustitelné CD	Server a Professional	Ne	Ano
Vzdálená instalace operačního systému	Professional	Ne	Ano

Příprava instalace

Během přípravy na čistou instalaci systému Windows 2000 Server musíte provést následující:

- Vytvořit distribuční složku.
- Porozumět, jak použít soubor odpovědí.
- Pochopit příkazy instalačního programu systému Windows 2000.

Poznámka Principy vykonání automatizované instalace popsané v tomto oddílu platí pro čistou instalaci i inovaci. Nejobvyklejším postupem je vykonat čistou instalaci.

Na obrázku 13.1 je vývojový graf instalačního procesu.

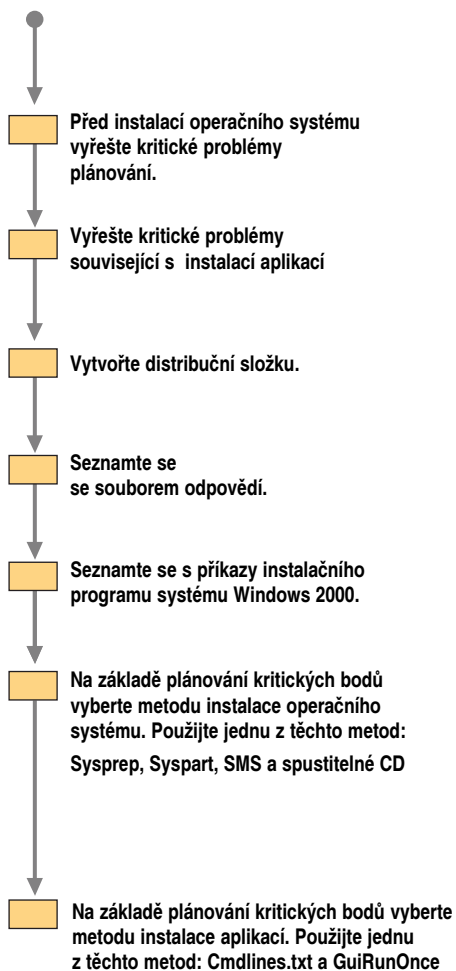
Vytváření distribučních složek

Chcete-li instalovat systém Windows 2000 Server na více počítačů v síti, musíte vytvořit alespoň jednu sadu distribučních složek. Distribuční složky se obvykle nacházejí na serveru, kam se počítače mohou připojit a odkud si mohou spuštěním souboru Winnt.exe nebo Winnt32.exe na cílovém počítači nainstalovat systém Windows 2000. Stejnou sadu distribučních složek s různými soubory odpovědí můžete použít k rozdílným implementacím systému. I když budete jako metodu instalace používat vytváření obrazů disku, distribuční složky zajistí konzistentní implementaci pro různé typy systému. Kromě toho můžete používat distribuční složky k aktualizaci budoucích obrazů změnou souborů v distribučních složkách nebo změnou souborů odpovědí a vytvořením nových obrazů a nemusíte tedy začínat znovu od začátku.

Chcete-li vyrovnat zatížení serverů a urychlit fázi kopírování instalačního programu systému Windows 2000 u počítačů se systémy Microsoft Windows 95, Windows 98, Windows NT nebo Windows 2000, vytvořte distribuční složky na více serverech. Soubor Winnt32.exe pak můžete spustit až s osmi umístěními zdrojových souborů. Další informace o příkazech instalačního programu najdete v oddílu „Přehled příkazů instalačního programu systému Windows 2000“ dále v této kapitole.

Poznámka V této kapitole označuje termín „Windows NT“ jak systém Microsoft Windows NT 3.51 tak i systém Microsoft Windows NT 4.0.

Začátek

**Obrázek 13.1** Vývojový graf automatizované instalace

Distribuční složky obsahují instalační soubory systému Windows 2000 Server nebo Microsoft Windows 2000 Advanced Server, ovladače zařízení a další soubory potřebné k instalaci.

S automatizováním procesu vytvoření distribuční složky vám pomůže Správce instalace (Setup Manager), nástroj nacházející se na CD systému Windows 2000 Server CD. Další informace o Správci instalace najdete v oddílu „Přehled souboru odpovědí“ dále v této kapitole.

Poznámka V této kapitole je „instalační program systému Windows 2000“ také zkráceně označován za „instalační program“.

▼ Chcete-li vytvořit distribuční složku, postupujte takto:

1. Připojte se k síťovému serveru, na němž chcete distribuční složku vytvořit.
2. Vytvořte ve sdílené oblasti síťového serveru složku \i386.

Chcete-li odlišit různé sdílené distribuce různých verzí systému Windows 2000 (Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server a Microsoft Windows 2000 Advanced Server), můžete vybrat jiný název této složky. Plánujete-li používat lokalizované jazykové verze systému Windows 2000 v zahraničních pobočkách, můžete vytvořit samostatné sdílené distribuce pro jednotlivé lokalizované verze.

3. Zkopírujte obsah složky \i386 z CD systému Windows 2000 Server do právě vytvořené složky.
4. V právě vytvořené složce vytvořte podsložku nazvanou \ \$OEM\$.

Podsložka \ \$OEM\$ zajišťuje potřebnou strukturu složek pro doplňkové soubory kopírované během instalace na cílový počítač. Mezi tyto soubory patří ovladače, nástroje, aplikace a všechny další soubory potřebné k zavedení systému Windows 2000 Server ve vaší organizaci.

Vytvoření struktury distribuční složky

Ukázka struktury distribuční složky je uvedena na obrázku 13.2.

\i386

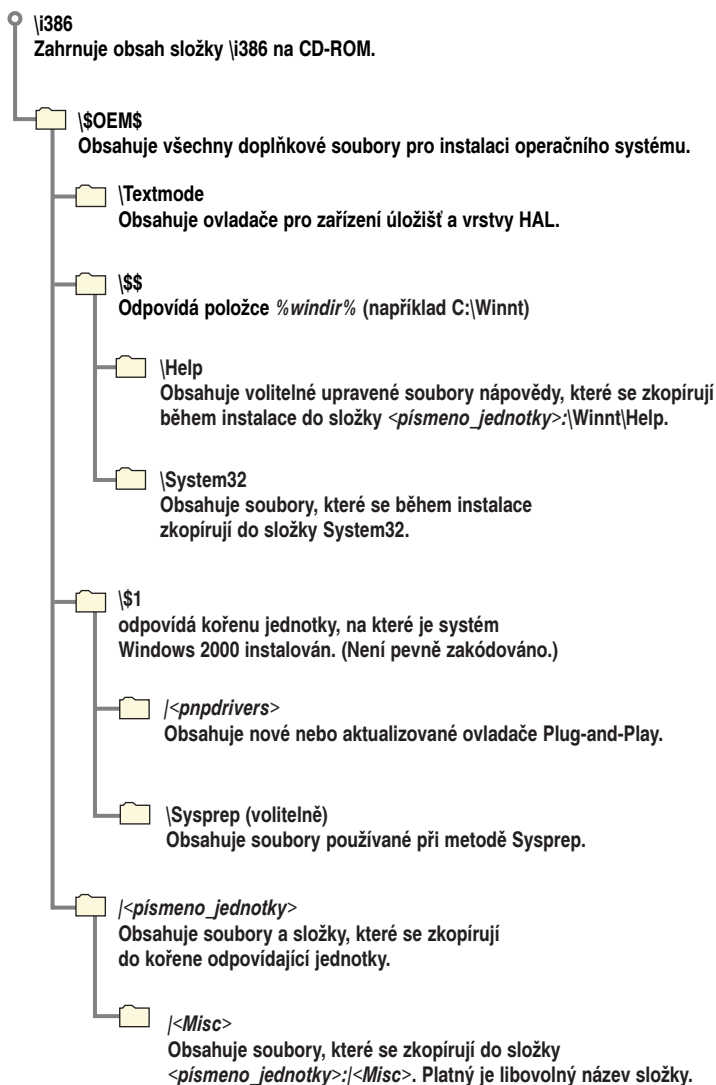
Toto je distribuční složka obsahující všechny soubory potřebné k instalaci systému Windows 2000. Tuto složku vytvořte v kořenu sdílené jednotky tak, že zkopírujete obsah složky \i386 na CD systému Windows 2000 Server CD do distribuční složky.

\ \$OEM\$

Podsložku \ \$OEM\$ vytvořte v distribuční složce přímo pod složkou \i386. Během instalace můžete do podsložky \ \$OEM\$ automaticky zkopírovat adresáře, standardní soubory ve formátu 8.3 a další nástroje vyžadované vaším procesem automatizované instalace.

Uvědomte si, že pokud v souboru odpovědí použijete klíč OEMFILES_PATH, můžete pak vytvořit podsložku \ \$OEM\$ i mimo distribuční složky. Soubor odpovědí je popsán v oddílu „Přehled souboru odpovědí“ dále v této kapitole. Dodatečné informace o parametrech a syntaxi souboru odpovědí najdete v dokumentu „Příručka bezobslužné instalace Microsoft Windows 2000“ (Unattend.doc) na CD operačního systému Microsoft Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

Složka \ \$OEM\$ může obsahovat volitelný soubor Cmdlines.txt, v němž je uveden seznam příkazů spuštěných během té části instalačního programu, která pracuje v grafickém uživatelském rozhraní (Graphical User Interface – GUI). Tyto příkazy lze použít k instalování dalších nástrojů, které mají být součástí vaší instalace. Další informace o souboru Cmdlines.txt najdete v oddílu „Použití souboru Cmdlines.txt“ dále v této kapitole.



Obrázek 13.2 Příklad struktury distribuční složky

Jestliže instalační program najde v kořenu distribučního bodu podsložku \OEM\$, zkopíruje všechny soubory v tomto adresáři do dočasného adresáře, který se vytváří v průběhu textové části instalačního programu.

Poznámka V této kapitole označujeme část instalačního programu s grafickým rozhraním za „grafický režim“ a část instalačního programu s textovým rozhraním za „textový režim“.

\\$OEM\\$\\Textmode

Podsložka \\\$OEM\$\\Textmode obsahuje nové nebo aktualizované soubory instalace ovladačů zařízení hromadného ukládání dat a vrstev abstrakce hardwaru (HAL). Tyto soubory mohou zahrnovat OEM vrstvy HAL, ovladače zařízení SCSI a soubor Txtsetup.oem, který řídí nahrávání a instalaci těchto komponent.

Nezapomeňte na soubor Txtsetup.oem. Všechny soubory umístěné v podsložce \\\$OEM\$\\Textmode (vrstvy HAL, ovladače a Txtsetup.oem) musí být uvedeny v oddílu [OEMBootFiles] souboru odpovědí.

\\$OEM\$\\\$

Podsložka \\\$OEM\$\\\$ odpovídá proměnným prostředí %systemroot% a %windir%. Tato podsložka obsahuje další soubory, které chcete zkopírovat do různých podsložek instalačního adresáře Windows 2000. Struktura této podsložky musí odpovídat standardní struktuře instalace systému Windows 2000, přičemž \\\$OEM\$\\\$ odpovídá %systemroot% nebo %windir% (například C:\\Winnt), \\\$OEM\$\\\$\\System32 odpovídá %windir%\\System32 atd. Každá podsložka musí obsahovat soubory, jež se zkopírují do odpovídající složky na cílovém počítači.

\\$OEM\$\\\$1

Podsložka \\\$OEM\$\\\$1 je v systému Windows 2000 novinkou a ukazuje na jednotku, kam se systém nainstaluje. Označení **\$1** odpovídá systémové proměnné %systemdrive%. Instalujete-li například systém Windows 2000 na jednotku D, \\\$OEM\$\\\$1 ukazuje na jednotku D.

\\$OEM\$\\\$1\\Pnpdrivers

Podsložka \\\$OEM\$\\\$1\\Pnpdrivers je v systému Windows 2000 novinkou a umožňuje vám do distribučních složek umístit nové nebo aktualizované ovladače zařízení Plug-and-Play. Tyto složky se zkopírují na místo %systemdrive%\\Pnpdrivers na cílovém počítači. Když do svého souboru odpovědí přidáte parametr OemPnPDriversPath, řeknete tak systému Windows, aby hledal (během instalace i po ní) nové a aktualizované ovladače zařízení Plug-and-Play nejen ve složkách původních součástí systému, ale také ve vámi vytvořených složkách. Parametr *Pnpdrivers* můžete nahradit názvem s osmi nebo méně znaky.

\\$OEM\$\\\$1\\Sysprep

Podsložka \\\$OEM\$\\\$1\\Sysprep je volitelná. Tato podsložka obsahuje soubory, které jsou zapotřebí ke spuštění nástroje Sysprep. Tyto soubory jsou popsány v oddílu „Duplikování disků pomocí nástroje Sysprep“ dále v této kapitole.

\\$OEM\$\\Písmeno_jednotky

V textovém režimu se struktura jednotlivých podsložek \\\$OEM\$\\Písmeno_jednotky zkopíruje do kořene odpovídající jednotky na cílovém počítači. Například soubory umístěné do podsložky \\\$OEM\$\\D se zkopírují do kořene jednotky D. Je také možné vytvářet podsložky v rámci těchto podsložek. Například po zadání \\\$OEM\$\\E\\Misc vytvoří instalační program na disku E podsložku \\Misc.

Soubory, které je zapotřebí přejmenovat, musí být uvedeny v souboru \$\$Rename.txt. Další informace o přejmenovávání souborů najdete v oddílu „Převedení délky názvu

souboru pomocí souboru `$$Rename.txt`“ dále v této kapitole. Pamatujte, že soubory v distribučních složkách musí mít krátké názvy (ve formátu 8.3).

Instalace zařízení hromadného ukládání dat

V systému Windows 2000 technologie Plug-and-Play detekuje a instaluje většinu hardwarových zařízení, které je možné později během instalace nahrát. Zařízení pro hromadné ukládání dat, například pevné disky, však musí být řádně nainstalovány, aby byla v grafickém režimu dostupná jejich plná podpora technologie Plug-and-Play.

Poznámka Zařízení nemusíte zadávat, pokud je systém Windows 2000 již podporuje.

Chcete-li nainstalovat zařízení SCSI v textovém režimu, tedy ještě před plným zpřístupněním technologie Plug-and-Play, musíte vytvořit soubor `Txtsetup.oem` popisující, jak má instalační program nainstalovat příslušné zařízení SCSI.

Důležité Před použitím aktualizovaných ovladačů proveďte, že jsou podepsány. Nejsou-li podepsány, instalační program nebude dokončen. Stav podepsání jednotlivých ovladačů zjistíte ve Správci zařízení (Device Manager). Můžete také spustit `Sigverif.exe` a vytvořit tak v podsložce `%windir%` soubor `Sigverif.txt`. Soubor `Sigverif.txt` uvádí stav podepsání všech ovladačů v systému.

▼ Chcete-li instalovat zařízení hromadného ukládání dat, postupujte takto:

1. V podsložce `\OEM` distribuční složky vytvořte podsložku `\Textmode`.
2. Do podsložky `\Textmode` zkopírujte následující soubory, které získáte od výrobce daného zařízení (nahraďte slovo *Ovladač* příslušným názvem ovladače):
 - `Ovladač.sys`
 - `Ovladač.dll`
 - `Ovladač.inf`
 - `Txtsetup.oem`

Poznámka Součástí některých ovladačů, například ovladačů miniportů, nemusí být soubor `.dll`.

3. V souboru odpovědí vytvořte oddíl `[MassStorageDrivers]` a do tohoto oddílu запиšte položky ovladačů, které chcete zahrnout. Příkladem možného zápisu v oddílu `[MassStorageDrivers]` může být:

„Adaptec 2940...“ = „0EM“

Informace o tomto oddílu najdete v souboru `Txtsetup.oem`, který vám dodá výrobce hardwaru.

Další informace o parametrech a syntaxi souboru odpovědí najdete v dokumentu „Příručka bezobslužné instalace Microsoft Windows 2000“ (`Unattend.doc`) na CD operačního systému Windows 2000. Soubor `Unattend.doc` je součástí souboru `Deploy.cab` ve složce `\Support\Tools`. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumník. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

4. V souboru odpovědí vytvořte oddíl [OEMBootFiles] a do tohoto oddílu zapište seznam souborů složky \$OEM\$\Textmode, například:

```
[OEMBootFiles]
<Ovladač>.sys
<Ovladač>.dll
<Ovladač>.inf
Txtsetup.oem
kde <Ovladač> je název ovladače.
```

5. Vyhovuje-li vaše zařízení hromadného ukládání dat standardu Plug-and-Play, bude mít v souboru Txtsetup.oem oddíl nazvaný [HardwareIds.Scsi.yyyyyy]. Není-li v souboru vašeho zařízení tento oddíl, budete jej muset vytvořit a pak do něj zapsat následující zadání:

```
id = „xxxxx“, „yyyyy“
```

kde xxxxx představuje identifikační číslo (id) zařízení a yyyyy představuje službu přiřazenou k zařízení.

Chcete-li tedy například instalovat ovladač Symc810, jehož identifikátor zařízení je PCI\VEN_1000&DEV_0001, zajistěte, aby soubor Txtsetup.oem obsahoval následující dodatečný oddíl:

```
[HardwareIds.scsi.symc810]
id = „PCI\VEN_1000&DEV_0001“, „symc810“
```

Instalace vrstev HAL (Hardware Abstraction Layer)

Chcete-li zadat instalaci vrstev HAL (hardware abstraction layer), potřebujete soubor Txtsetup.oem a soubory HAL, které vám dodá výrobce zařízení. Instalujete-li ovladače zařízení hromadného ukládání dat, musíte použít stejný soubor Txtsetup.oem. Použit může být jen jeden soubor Txtsetup.oem, pokud tedy potřebujete instalovat vrstvy HAL i ovladače zařízení hromadného ukládání dat, musíte všechna zadání zkombinovat do jednoho souboru.

Jestliže chcete využít ovladačů jiných výrobců, musíte příslušným způsobem upravit soubor odpovědí. Další informace o parametrech a syntaxi souboru odpovědí najdete v dokumentu „Příručka bezobslužné instalace Microsoft Windows 2000“ (Unattend.doc) na CD operačního systému Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

▼ Chcete-li instalovat HAL, postupujte takto:

1. Pokud jste tak ještě neučinili, vytvořte ve složce \$OEM\$ podsložku \Textmode.
2. Zkopírujte soubory, které jste získali od prodejce zařízení, do podsložky \Textmode.
3. V souboru odpovědí upravte oddíl [Unattend] vrstev HAL a přidejte sem ovladače, které chcete nainstalovat, například:

```
[Unattend]
Computertype = „<PopisHAL>“, OEM
```

Informace o položce <PopisHAL> získáte v oddílu [Computer] souboru Txtsetup.oem od poskytovatele ovladače.

4. V souboru odpovědí vytvořte oddíl [OEMBootFiles] a zadejte sem názvy souborů ve složce \$OEM\$\Textmode.

Instalace zařízení Plug-and-Play

Následující procedura ukazuje, jak se instalují zařízení Plug-and-Play, pokud se nejedná ani o zařízení hromadného ukládání ani o vrstvy HAL a zároveň nejsou obsažena na CD operačního systému Windows 2000.

▼ Chcete-li nainstalovat zařízení Plug-and-Play, postupujte takto:

1. V distribuční složce vytvořte podsložku pro speciální ovladače zařízení Plug-and-Play a jejich soubory .inf. Můžete například vytvořit složku nazvanou PnPDrvs:

```
$OEM$\$1\PnPDrvs
```

2. Přidáním následujícího řádku do souboru odpovědí přidáte potřebnou cestu na seznam prohledávaných jednotek:

```
OEMPnPDriversPath = „PnPDrvs“
```

Máte-li ve složce PnPDrvs podsložky, musíte zadat cestu ke každé podsložce. Tyto cesty musí být odděleny středníky.

Chcete-li jednoduše spravovat složky tak, aby do nich bylo možné ukládat ovladače zařízení i v budoucnosti, vytvořte složky pro všechny potenciální ovladače zařízení. Když tyto složky rozdělíte do podsložek, můžete ovladače zařízení uchovávat podle typu zařízení a nemusíte mít všechny ovladače zařízení v jediné složce. Doporučujeme vám vytvořit složky Audio, Modem, Síť, Tisk, Video a Ostatní. Složka Ostatní vám bude umožňovat ukládat ovladače nových hardwarových zařízení, která třeba ještě nejsou známá. Názvy složek v textu jsou uvedeny s diakritikou, vytvářejte je však bez diakritiky.

Například obsahuje-li složka PnPDrvs podsložky Audio, Modem a Síť, soubor odpovědí musí obsahovat následující řádek:

```
OEMPnPDriversPath = „PnPDrvs\Audio;PnPDrvs\Modem;PnPDrvs\Sit“
```

Převod délky názvu souboru pomocí souboru \$\$Rename.txt

Soubor \$\$Rename.txt určuje změnu krátkých názvů souborů na dlouhé názvy souborů během instalace. Soubor \$\$Rename.txt uvádí všechny soubory v určité složce, které je zapotřebí přejmenovat. Každá složka obsahující krátké názvy souborů, které je zapotřebí přejmenovat, musí obsahovat svou vlastní verzi souboru \$\$Rename.txt.

Chcete-li používat soubor \$\$Rename.txt, vložte tento soubor do složky obsahující soubory, které se musí převést. Syntaxe souboru \$\$Rename.txt je následující:

```
[název_oddílu_1]
krátký_název_1 = „dlouhý_název_1“
krátký_název_2 = „dlouhý_název_2“

krátký_název_x = „dlouhý_název_x“
```



```
[název_oddílu_2]
krátký_název_1 = „dlouhý_název_1“
krátký_název_2 = „dlouhý_název_2“

krátký_název_x = „dlouhý_název_x“
Parametry jsou definované takto:
```

- ***název_oddílu_x*** Cesta k podsložce obsahující dané soubory. Oddíl nemusí být pojmenovaný nebo může mít za název zpětné lomítko (\), což znamená, že oddíl obsahuje názvy souborů nebo podsložek v kořenu jednotky.
- ***krátký_název_x*** Název souboru nebo podsložky v dané podsložce, která se bude přejmenovávat. Tento název nesmí být uzavřen v uvozovkách.
- ***dlouhý_název_x*** Nový název souboru nebo podsložky. Obsahuje-li tento název mezery nebo čárky, musí být uzavřen v uvozovkách.

Tip Používáte-li ke spuštění instalace systém MS-DOS a vaše nástroje systému DOS nedokáží kopírovat složky s cestami delšími než 64 znaků, můžete složky pojmenovat krátkými názvy a později je prostřednictvím souboru \$\$Rename.txt přejmenovat.

Přehled souboru odpovědí

Soubor odpovědí je upravený skript, který odpovídá na otázky instalačního programu místo uživatele. CD systému Windows 2000 Server obsahuje ukázkový soubor odpovědí, který si můžete upravit a používat. Soubor odpovědí se obvykle nazývá *Unattend.txt*, můžete jej však přejmenovat. (Platnými názvy souboru odpovědí jsou například *Comp1.txt*, *Install.txt* a *Setup.txt* za předpokladu, že jsou tyto názvy správně použity v příkazu **setup**.) To vám umožňuje vytvořit a používat více souborů odpovědí, potřebujete-li v různých částech své organizace používat různé soubory odpovědí. Soubory odpovědí využívají také další programy, například *Sysprep*, který pracuje s volitelným souborem *Sysprep.inf*.

Soubor odpovědí říká instalačnímu programu, jak pracovat s distribučními složkami a soubory, které jste vytvořili. Například v oddílu *[Unattend]* souboru odpovědí je položka „*OEMPreinstall*“ říkající instalačnímu programu, aby zkopíroval podsložky *\$OEM\$* z distribučních složek na cílový počítač.

Soubor odpovědí obsahuje několik volitelných oddílů, které můžete upravit a zadat tak informace o požadavcích vaší instalace. Soubor odpovědí předá instalačnímu programu odpovědi na všechny otázky, které jsou vám kladeny během standardní interaktivní instalace systému Windows 2000. Dokument *Unattend.doc* obsahuje podrobné informace o klíších a hodnotách souboru odpovědí. Další informace o oddílech souboru odpovědí a jejich parametrech najdete v dokumentu „Příručka bezobslužné instalace Microsoft Windows 2000“ (*Unattend.doc*) na CD operačního systému Microsoft Windows 2000. Soubor *Unattend.doc* je součástí souboru *Deploy.cab* ve složce *\Support\Tools*. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

Chcete-li dosáhnout bezobslužné instalace systému Windows 2000 Server, musíte vytvořit soubor odpovědí a při spuštění instalačního programu metodou spustitelného CD nebo spuštěním souborů *Winnt.exe* či *Winnt32.exe* tento soubor určit. Příkladem spuštění instalace programem *Winnt.exe* může být:

Winnt /S:Z:\I386 /U:Z:\unattend.txt

Všimněte si přepínače **/U**: příkazového řádku, který při použití příkazu **Winnt** určuje bezobslužnou instalaci (v případě spuštění instalačního programu pomocí souboru **Winnt32** se pro zadání bezobslužné instalace používá parametr **/unattend**). Další informace o souborech Winnt.exe a Winnt32.exe najdete v oddílu „Přehled příkazů instalačního programu systému Windows 2000“ dále v této kapitole.

Vytvoření souboru odpovědí

Soubor odpovědí je upravený skript, jehož pomocí můžete spouštět bezobslužnou instalaci systému Windows 2000 Server. Soubor odpovědí lze vytvořit dvěma způsoby: pomocí Správce instalace (Setup Manager) nebo jeho ručním zápisem.

Vytvoření souboru odpovědí pomocí Správce instalace

S vytvářením a úpravou souboru odpovědí vám může pomoci aplikace Správce instalace (Setup Manager), kterou najdete doprovodném CD sady *Microsoft Windows 2000 Server Resource Kit* v souboru Deploy.cab ve složce \Support\Tools. Prostřednictvím Správce instalace můžete dodat procesu vytváření nebo aktualizace souboru odpovědí konzistentnost.

Správce instalace lze použít k následujícím činnostem (výsledky jsou pak vygenerovány jako parametry souboru odpovědí):

- Určení platformy souboru odpovědí (Microsoft Windows 2000 Professional, Windows 2000 Server, vzdálená instalace operačního systému nebo nástroj Sysprep).
- Určení úrovně automatizace bezobslužného režimu instalačního programu. (Tyto úrovně zahrnují „Provide Defaults“, „Fully Automated“, „Hide Pages“, „Read Only“ a „GUI-mode Setup“.)
- Určení výchozích informací o uživateli.
- Definování možností názvu počítače včetně vytvoření /UDF pro přístup k souboru platných názvů počítačů.
- Konfigurace nastavení sítě.
- Vytvoření distribučních složek.
- Přidání vlastních souborů loga a pozadí.
- Přidání souborů do distribučních složek.
- Přidání příkazů do oddílu [GuiRunOnce].
- Vytvoření souborů Cmdlines.txt.
- Určení kódových stránek.
- Specifikace regionálních nastavení.
- Specifikace časového pásma.
- Specifikace informací TAPI.

Správce instalace nedokáže vykonat tyto funkce:

- Určení systémových součástí, například Internet Information Services.
- Vytvoření souborů Txtsetup.oem.
- Vytvoření podsložek v distribuční složce.

Tabulka 13.3 popisuje některé obvyklejší specifikace souboru odpovědí vytvoření Správcem instalace.

Tabulka 13.3 Specifikace souboru odpovědí vytvořené Správcem instalace

Parametr	Smysl
Instalační cesta	Určuje požadovanou cestu na cílovém počítači, kam se nainstaluje systém Windows 2000 Server.
Možnost inovace	Určuje, zda půjde o inovaci ze systému Windows 95 či Windows 98, Windows NT nebo Windows 2000.
Název cílového počítače	Určuje název uživatele, název organizace a název počítače aplikovaný na cílový počítač.
Identifikátor produktu	Zadáva identifikační číslo produktu získané z dokumentace.
Skupina nebo doména	Určuje název skupiny nebo domény, do které počítač patří.
Časové pásmo	Zadáva počítači časové pásmo.
Informace o síťové konfiguraci	Zadáva typ síťového adaptéru (karty) a konfiguraci síťovými protokoly.

Poznámka Při instalaci systému Windows 2000 Server nemusíte hned vytvářet řadiče domény. Můžete vytvořit členské servery a pak je povýšit na řadiče domény později pomocí Průvodce instalací služby Active Directory (Active Directory Installation Wizard) (dcpromo.exe).

Ruční vytvoření souboru odpovědí

Chcete-li vytvořit soubor odpovědí ručně, použijte nějaký textový editor, například Poznámkový blok. Obecně lze říci, že se soubor odpovědí skládá ze záhlaví oddílů, parametrů a hodnot těchto parametrů. Většina záhlaví oddílů je sice předdefinovaná, můžete však nadefinovat další záhlaví oddílů. Jestliže vaše instalace nepotřebuje všechny parametry, nemusíte je zadávat.

Neplatné parametry mají za následek chyby nebo nekorektní chování po instalaci.

Formát souborů odpovědí je následující:

```
[oddíl1]
;
; Oddíl obsahuje klíče a odpovídající
; hodnoty daných klíčů/parametrů.
; Klíče a hodnoty jsou odděleny znaky ' = '.
; Hodnoty obsahující mezery obvykle musí být
; uzavřeny v uvozovkách „“.
```

;

klíč = hodnota

.

.

```
[oddíl2]
klíč = hodnota
```

.

.

Nastavení hesel pomocí souboru odpovědí

Použijete-li při instalaci soubor odpovědí, můžete nastavit parametry těchto příkazů hesel:

- AdminPassword
- UserPassword
- DefaultPassword
- DomainAdminPassword
- AdministratorPassword
- Password

Definice těchto příkazů najdete v dokumentu „Příručka bezobslužné instalace Microsoft Windows 2000“ (Unattend.doc) na CD operačního systému Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**. Navíc ukázkové soubory odpovědí používající některé z těchto parametrů najdete v příloze „Příklady souborů odpovědí pro bezobslužnou instalaci“ v této knize.

Poznámka Hesla jsou omezena na 127 znaků. Zadáte-li heslo obsahující více než 127 znaků, nebudete se moci do systému přihlásit, protože heslo bude neplatné.

Po dokončení instalace zůstane na počítači soubor odpovědí se všemi použitými nastaveními, všechny informace o heslech se z jeho místní kopie však odstraní, aby nebylo narušeno zabezpečení.

Upozornění Během instalace však soubor existuje na pevném disku. Je-li pro vás zabezpečení prvořadé, nepřidávejte do souboru odpovědí vytvořeného pro bezobslužnou instalaci informace o heslech.

Místní soubor odpovědí vám umožňuje automaticky nastavovat volitelné součásti spouštěním příkazů obsahujících parametry již zadané v původním souboru odpovědí použitým při instalaci. Tyto součásti mohou zahrnovat konfiguraci serveru jako řadiče domény, jako serveru klastru nebo povolovat službu Message Queuing.

Rozšiřování oddílů pevného disku

Instalaci můžete začít na malém oddílu disku (kolem 1 GB na větším disku) a zadat, aby se daný oddíl během procesu instalace systému Windows 2000 rozšířil. Toho docílíte použitím parametru ExtendOEMPartition v souboru odpovědí. Parametr ExtendOEMPartition funguje pouze na oddílech systému NTFS a lze jej použít jak ve standardním souboru odpovědí tak i v souboru odpovědí používaném při instalacích nástrojem Sysprep.

Další informace o nástroji Sysprep s souboru Sysprep.inf najdete v oddílu „Duplikování disků nástrojem Sysprep“ dále v této kapitole.

Poznámka Parametr ExtendOEMPartition funguje pouze na aktivním systémovém oddílu. Nefunguje na jiných oddílech stejného disku nebo na jiných discích počítače. Navíc použijete-li zadání ExtendOemPartition=1, oddíl se rozšíří o veškerý zbývající prostor na disku a poslední cylinder nechá prázdný. To slouží k tomu, abyste mohli používat dynamické svazky.

Použijete-li ExtendOEMPartition během instalace na oddílu systému File Allocation Table (FAT), musíte v oddílu [Unattended] souboru odpovědí ještě zadat File System=ConvertNTFS, aby se nejprve oddíl převedl na systém NTFS. Používáte-li parametr ExtendOEMPartition v případě instalace pomocí nástroje Sysprep, přečtěte si oddíl „Duplikování disků nástrojem Sysprep“ dále v této kapitole.

Další informace o použití ExtendOemPartition najdete v dokumentu „Příručka bezobslužné instalace Microsoft Windows 2000“ (Unattend.doc) na CD operačního systému Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

Použití souboru odpovědí v Průvodci instalací služby Active Directory

Po instalaci systému Windows 2000 Server můžete automatizovat proces vytvoření řadiče domény vykonaný Průvodcem instalací služby Active Directory (Active Directory Installation Wizard). Toho lze dosáhnout dvěma způsoby:

- Spuštěním následujícího příkazu v oddílu [GuiRunOnce] souboru odpovědí Unattend.txt:
dcpromo.exe
- Vytvořením speciálního souboru odpovědí pomocí příkazů definovaných v oddílu [DCInstall] podle přílohy „Příklady souborů odpovědí pro bezobslužnou instalaci“ a následným spuštěním tohoto příkazu:

dcpromo.exe /answer:*název_souboru_odpovědi*

Další informace o Průvodci instalací Active Directory najdete v kapitole „Určení strategií migrace domény“ v této knize.

Přehled příkazů instalačního programu systému Windows 2000

Chcete-li nainstalovat systém Windows 2000, musíte spustit příslušný instalační program, buď Winnt.exe nebo Winnt32.exe. V této kapitole označujeme oba soubory Winnt.exe a Winnt32.exe společným názvem „instalační program“. Typ instalačního programu, který musíte spustit, se určuje takto:

- V případě čisté instalace na počítače se systémem MS-DOS nebo Microsoft Windows 3.x spusťte soubor Winnt.exe z příkazového řádku systému MS-DOS.
- V případě čisté instalace nebo aktualizace systému Windows NT, Windows 95 nebo Windows 98 spusťte soubor Winnt32.exe.

Uvědomte si také, že můžete spustit standardní interaktivní instalaci ze spouštěcích disket, které jsou součástí CD systému Windows 2000 Server CD.

Upozornění Jestliže před instalací systému Windows 2000 inovujete nějaké aplikace na počítači, musíte jej před spuštěním instalačního programu nechat restartovat.

Další informace o metodách instalace najdete v oddílu „Automatizování instalace systému Windows 2000 Server“ dále v této kapitole.

Winnt.exe

Příkaz Winnt.exe má včetně parametrů automatizované instalace tento tvar:

winnt [/S[:cesta_zdroje]][/T[:dočasná_jednotka]]/U[:soubor_odpovědí]/R[x:složka]/E:příkaz]

Definici parametrů a syntaxi příkazu najdete v příloze „Příkazy instalačního programu“ v této knize.

V případě diskových jednotek s více oddíly nainstaluje instalační program Winnt.exe systém Windows 2000 do aktivního oddílu, pokud tento oddíl obsahuje dostatečné množství prostoru. Jinak instalační program vyhledá jiné oddíly, které obsahují dostatečné množství prostoru, a vyzve vás k zadání požadovaného oddílu. Při automatizovaných instalacích lze tuto výzvu odstranit spuštěním instalačního programu s parametrem /T, který automaticky ukáže na požadovaný oddíl, například:

```
winnt [/unattend] [:<cesta>\answer.txt] [/T[:d]]
```

Winnt32.exe

Příkaz Winnt32.exe má včetně parametrů automatizované instalace tento tvar:

```
winnt32 [/s:cesta_zdroje] [/tempdrive:písmeno_jednotky]
[/unattend[čísló][:soubor_odpovědí]] [/copydir:název_složky]
[/copysource:název_složky] [/cmd:příkazový_řádek]
[/debug[úroveň][:název_souboru]] [/udf:id[,soubor_UDB]]
[/syspart:písmeno_jednotky] [/noreboot] [/makelocalsource] [/checkupgradeonly]
[/m:název_složky]
```

Definici parametrů a syntaxi příkazu najdete v příloze B „Příkazy instalačního programu“ v této knize.

V případě diskových jednotek s více oddíly nainstaluje instalační program Winnt.exe systém Windows 2000 do aktivního oddílu, pokud tento oddíl obsahuje dostatečné množství prostoru. Jinak instalační program vyhledá jiné oddíly, které obsahují dostatečné množství prostoru, a vyzve vás k zadání požadovaného oddílu. Při automatizovaných instalacích lze tuto výzvu odstranit spuštěním instalačního programu s parametrem /tempdrive, který automaticky ukáže na požadovaný oddíl, například:

```
winnt32 [/unattend] [:<cesta>\answer.txt] [/tempdrive:d]
```

Systém Windows 2000 může použít až osm přepínačů /s ukazujících na další distribuční servery jako zdroje instalace na cílový počítač. Tato funkce pomáhá urychlit fázi kopírování souborů instalačního programu na cílový počítač a zajišťuje také další možnosti vyrovnávání zatížení distribučních serverů, z nichž lze instalační program spustit, například:

```
<cesta k distribuční složce 1>\winnt32 [/unattend] [:<cesta>\answer.txt]
[/s:<cesta k distribuční složce 2>] [/s:<cesta k distribuční složce 3>]
[/s:<cesta k distribuční složce 4>]
```

Tabulka 13.4 ukazuje příkazy instalačního programu a jejich použití v systému Windows 2000.

Tabulka 13.4 Použití příkazů instalačního programu

Příkaz instalačního programu	Verze systému Windows 2000	Inovace	Čistá instalace
Winnt.exe	Server a Professional	Ne	Ano
Winnt32.exe	Server a Professional	Ano	Ano

Automatizování instalace serverových aplikací

Po vyřešení kritických problémů plánování se můžete rozhodnout, jak budete automatizovat instalaci serverových aplikací. Ve většině případů bude výhodné použít funkce bezobslužné instalace dané aplikace.

Můžete si vybrat z těchto možností:

- Cmdlines.txt
- Spuštění instalačního programu aplikace nebo dávkového souboru z oddílu [GuiRunOnce] souboru odpovědí.

Použití souboru Cmdlines.txt

Soubor Cmdlines.txt obsahuje příkazy, které grafický režim vykoná při instalaci volitelných součástí, například aplikací, které se musí instalovat ihned po instalaci systému Windows 2000 Server. Plánujete-li použít soubor Cmdlines.txt, musíte jej umístit do podsložky \ \$OEM\$ distribuční složky. Používáte-li nástroj Sysprep, umístěte soubor Cmdlines.txt do podsložky \ \$OEM\$\ \$1\Sysprep.

Soubor Cmdlines.txt použijte v těchto situacích:

- Instalujete z podsložky \ \$OEM\$ distribuční složky.
 - Instalovaná aplikace má následující vlastnosti:
 - Nekonfiguruje se sama pro více uživatelů, například sada Microsoft Office 95.
- Nebo-
- Je vytvořena pro instalaci jedním uživatelem a replikování informací jednotlivých uživatelů.

Syntaxe souboru Cmdlines.txt je následující:

```
[Commands]
„příkaz_1“
„příkaz_2“
.
.
„příkaz_x“
```

Parametry jsou definované takto:

- „příkaz_1“, „příkaz_2“, ... „příkaz_x“ představují příkazy, které chcete spustit (a v jakém pořadí) v okamžiku, kdy grafický režim zavolá soubor Cmdlines.txt. Všimněte si, že všechny příkazy musí být v uvozovkách.

Při použití souboru Cmdlines.txt pamatujte na následující:

- Když jsou příkazy souboru Cmdlines.txt vykonávány během instalace, není k systému přihlášený žádný uživatel a není zaručeno síťové spojení. Proto se informace o jednotlivých uživateli zapisují do registru výchozího uživatele a všichni dále vytvoření uživatelé také obdrží tyto informace.
- Soubor Cmdlines.txt vyžaduje, abyste umístili soubory potřebné ke spuštění aplikace nebo nástroje do adresářů, ke kterým se během instalačního procesu přistupuje, což znamená, že tyto soubory musí být na pevném disku.

Použití oddílu [GuiRunOnce] souboru odpovědí

Oddíl [GuiRunOnce] souboru odpovědí obsahuje seznam příkazů, které se vykonají při prvním přihlášení uživatele na počítač po skončení instalačního programu. Chcete-li tedy například zajistit automatické spuštění instalace nějaké aplikace, můžete do oddílu [GuiRunOnce] zadat následující řádek:

```
[GuiRunOnce]
„%systemdrive%\<složka_aplikace>\<instalace_aplikace> -quiet“
```

Plánujete-li inicializaci instalace pomocí oddílu [GuiRunOnce], musíte vzít v úvahu ještě následující faktory:

Požaduje-li aplikace restartování, zjistěte, zda lze restartování nějakým způsobem potlačit.

To je velmi důležité, protože po každém restartu systému jsou ztracena všechna předchozí zadání v oddílu [GuiRunOnce]. Jestliže bude systém restartovat před dokončením zadání dříve určených v oddílu [GuiRunOnce], zbývající položky se nespustí. Neexistuje-li v aplikaci žádná možnost potlačení restartu, můžete se pokusit zabalit danou aplikaci do balíčku programu Windows Installer. Tuto funkci zajišťují nástroje jiných výrobců.

Součástí systému Windows 2000 je WinINSTALL LE (Limited Edition), nástroj přebalčkování pro Windows Installer. WinINSTALL LE vám umožňuje snadno přebalit aplikace vzniklé před zavedením nástroje Windows Installer do balíčků, které lze distribuovat pomocí nástroje Windows Installer. Další informace o programu WinINSTALL LE najdete ve složce \Valueadd\3rdparty\Mgmt\Winstle na CD systému Windows 2000 Server CD.

Další informace o balíčkování programu Windows Installer najdete v kapitole „Automatizování instalace a inovace klientů“ v této knize.

Důležité Jestliže instalujete nějakou aplikaci na vícejazykově lokalizovaných verzích systému Windows 2000, doporučujeme vám vyzkoušet přebalenou aplikaci na lokalizovaných verzích a ujistit se, že kopíruje soubory na správná místa a řádně zapisuje požadované položky registru.

Vyžaduje-li aplikace ke své instalaci prostředí Průzkumníka Windows, pak nebude oddíl [GuiRunOnce] fungovat, protože v době vykonání příkazů Run a RunOnce není ještě toto prostředí nainstalováno.

Kontaktujte výrobce aplikace a zjistěte, zda je k dispozici nějaká aktualizace nebo oprava, která může tyto situace instalace aplikace řešit. Není-li nic takového k dispozici, mů-

žete aplikaci přebalit do balíčku nástroje Windows Installer nebo použít jiné prostředky distribuce.

Aplikace používající stejný typ instalačního mechanismu nemusí fungovat správně, není-li použit příkaz /wait.

K tomu může dojít, když běžící instalace aplikace spustí další proces. Pokud ještě pracuje instalační rutina, pak může inicializace jiného procesu a zavření aktivního procesu způsobit spuštění další rutiny uvedené v položkách RunOnce registru. Protože běží více instancí instalačního mechanismu, druhá aplikace obvykle skončí chybou. Příklad řízení takové situace pomocí dávkového souboru najdete v oddílu „Řízení instalace více aplikací pomocí dávkového souboru“ dále v této kapitole.

Použití programů instalace aplikace

Upřednostňovanou metodou předběžné instalace aplikace je použití instalační rutiny, která je součástí dané aplikace. Toho můžete využít, pokud je instalovaná aplikace schopna po zadání přepínače **/q** nebo **/s** příkazového řádku běžet v tichém režimu (bez intervence uživatele). Seznam parametrů příkazového řádku podporovaných instalačním mechanismem najdete v nápovědě k aplikaci nebo v její dokumentaci.

Dále je uveden příklad řádku, který můžete vložit do oddílu [GuiRunOnce] a iniciovat tak bezobslužnou instalaci aplikace s využitím jejího vlastního instalačního programu.

```
<cesta k instalačnímu programu>\Setup.exe /q
```

Parametry instalačního programu se v jednotlivých aplikacích liší. Například parametr **/I** obsažený v některých aplikacích je užitečný, když chcete v zájmu sledování instalace vytvořit soubor protokolu. Některé aplikace mají příkazy, které jim zabrání v automatickém restartování. To vám pomůže řídit instalaci aplikací s minimálním počtem restartů.

Před zadáním předběžné instalace nějaké aplikace od jejího výrobce zajistěte všechny potřebné instrukce, nástroje a nejlepší postupy.

Důležité Bez ohledu na metodu instalování musíte splnit všechny licenční požadavky dané aplikace.

Řízení instalace více aplikací pomocí dávkového souboru

Chcete-li řídit způsob instalace více aplikací, můžete vytvořit dávkový soubor obsahující jednotlivé instalační příkazy a používající příkaz **Start** s přepínačem **/wait** příkazového řádku. Tato metoda zaručí, že se vaše aplikace nainstalují postupně a že jednotlivé aplikace bude plně nainstalovány, než dojde ke spuštění instalační rutiny následující aplikace. Dávkový soubor se pak spustí z oddílu [GuiRunOnce].

Následující procedura vysvětluje, jak vytvořit dávkový soubor, jak aplikaci nainstalovat a nakonec jak po dokončení instalace odstranit všechny odkazy na daný dávkový soubor.

▼ Chcete-li nainstalovat aplikaci pomocí dávkového souboru, postupujte takto:

1. Vytvořte dávkový soubor obsahující řádky podobající se následujícímu příkladu:

```
Start /wait <cesta k první aplikaci>\<Setup> <parametry příkazového řádku>
Start /wait <cesta k druhé aplikaci>\<Setup> <parametry příkazového řádku>
Exit
```

kde:

- <cesta> je cesta ke spustitelnému souboru spouštějícímu instalaci. Tato cesta musí být během instalace k dispozici.
 - <Setup> je název spustitelného souboru spouštějícího instalaci.
 - <parametry příkazového řádku> jsou nějaké dostupné parametry tichého režimu dané aplikace, kterou chcete instalovat.
4. Zkopírujte dávkový soubor do distribučních složek nebo na jiné místo přístupné během instalace.
 5. Je-li název dávkového souboru <filename>.bat, vložte do oddílu [GuiRunOnce] souboru odpovědí řádek, který daný soubor spustí, jak ukazuje následující příklad. Tento příklad předpokládá, že byl dávkový soubor zkopírován do složky Sysprep na místním pevném disku, i když může být umístěn na libovolném místě, kam má instalační program přístup.

```
[GuiRunOnce]
„%systemdrive%\sysprep\<filename>.bat“
„<cesta-1>\<příkaz-1>.exe“
„<cesta-n>\<příkaz-n>.exe“
„%systemdrive%\sysprep\sysprep.exe -quiet“
```

kde:

- <cesta-1>\<příkaz-1.exe> a <cesta-n>\<příkaz-n.exe> jsou plně zadané cesty k dalším instalačním či konfiguračním nástrojům jiných aplikací nebo nástrojů. Může jít také o cestu k jinému dávkovému souboru. Tyto cesty musí být během instalace dostupné.

Automatizování instalace systému Windows 2000 Server

V podnikovém prostředí není z hlediska nákladů efektivní instalovat systém Windows 2000 pomocí standardního interaktivního instalačního programu na každém jednotlivém počítači. Výrazného snížení celkových nákladů na vlastnictví (total cost of ownership – TCO) dosáhnete automatizovanými instalacemi systému Windows 2000 Server na více počítačů.

Automatizovat lze instalaci těchto součástí:

- Jádra operačního systému Windows 2000 Server.
- Všech aplikací, které nepracují jako služby.
- Podporu dalších jazyků v systému Windows 2000 Server pomocí instalace různých jazykových balíčků.
- Servisních balíčků pro systém Windows 2000 Server.

Automatizovaná instalace systému Windows 2000 Server zahrnuje spuštění instalačního programu se souborem odpovědí. Instalační program může proběhnout bezobslužně. Bezobslužná instalace zahrnuje tyto kroky:

- Vytvoření souboru odpovědí.
- Určení a implementace procesu konfigurace informací pro jednotlivé počítače.
- Určení a implementace procesu automatizace vybrané metody distribuce, například použití síťového distribučního bodu nebo duplikování pevného disku.

Nové možnosti automatizované instalace

Automatizovaná instalace systému Windows 2000 nabízí několik nových voleb souboru odpovědí řídících co a jak se má spustit. Další informace o parametrech a syntaxi souboru odpovědí najdete v dokumentu „Příručka bezobslužné instalace Microsoft Windows 2000“ (Unattend.doc) na CD operačního systému Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

Flexibilní práce v síti V systému Windows 2000 máte k dispozici flexibilní síťové konfigurace pro jednotlivé počítače včetně dodatečné podpory protokolů, služeb a klientů. Nyní je možné nastavit pořadí vážení, jednoduše zadat výchozí informace a instalovat více síťových karet v jednom systému. Aby byla instalace a konfigurace ještě jednodušší, systém Windows 2000 může automaticky nainstalovat a nakonfigurovat ovladače síťových zařízení. Systém Windows 2000 standardně instaluje pro všechny síťové adaptéry v systému výchozí komponenty, není-li tedy v souboru odpovědí řečeno jinak. Mezi výchozí síťové komponenty patří Klient sítě Microsoft (Client for Microsoft Networks), protokol TCP/IP, Sdílení souborů a tiskáren v sítích Microsoft (File and Printer Sharing for Microsoft Networks) a zavedení protokolu DHCP (Dynamic Host Configuration Protocol).

Možnost automatického přihlášení Soubor odpovědí si můžete upravit a umožnit počítači automatické přihlášení k účtu správce při prvním spuštění (nebo po zadaný počet spuštění) systému po dokončení instalace systému Windows 2000. Potřebujete-li, aby se systém Windows 2000 automaticky několikrát přihlásil, aby bylo možné vykonat úlohy zadané položkami RunOnce, budete muset vytvořit v souboru odpovědí neprázdné heslo správce (AdminPassword). Pomocí AutoAdminLogonCount pak lze zadat, kolikrát se má systém automaticky přihlásit v zájmu dokončení zadaných úloh. Použijete-li prázdné heslo, instalační program se bude moci přihlásit k systému jen jednou. Při dalších restartech bude nutné zadat oprávnění nějakým jiným způsobem. Smyslem tohoto opatření je snížit riziko narušení zabezpečení. Uvědomte si však, že zadání oprávnění správce do textového souboru vždy znamená ohrožení zabezpečení v případě, že uživatel získá k tomuto souboru přístup.

Automatické vykonávání příkazů Oddíl [GuiRunOnce] souboru odpovědí obsahuje seznam příkazů, které se mají postupně vykonat jako součást instalačního programu po dokončení grafického režimu. Pomocí [GuiRunOnce] lze specifikovat seznam instalovaných aplikací, nástrojů konfigurace systému a dalších nástrojů, jež se mají spustit při prvním přihlášení k instalovanému počítači.

Zjednodušené zadávání časové zóny V souboru odpovědí lze jednodušeji a s menším počtem chyb než v systému Windows NT zadat časové pásmo počítače. Protože jsou tu uvedeny možné časové zóny, chyby jsou méně časté, jelikož nyní již nemusíte zadávat celý řetězec časové zóny.

Vylepšená místní a jazyková nastavení V souboru odpovědí lze zadat místní nastavení systému a uživatelů, metodu klávesnice a vstupů a instalovanou podporu jazyků. Správce instalace (Setup Manager) tento proces ještě více zjednodušuje, protože vám nastavení instalace systému nabízí v grafickém rozhraní průvodce.

Jednodušší předběžná instalace zařízení Protože se zavádí podpora technologie Plug-and-Play, klíče OemPnPDriversPath a nová struktura sdílení distribučních bodů,

předběžné instalování zařízení nyní spočívá v jednoduchém přidání ovladačů do složky na sdíleném distribučním místě a určení klíče `OemPnPDriversPath`.

Metody automatizované instalace

Automatizovanou instalaci systému Windows 2000 Server lze spustit několika metodami. Vybraná metoda závisí na výsledku vašeho kritického plánování, které bylo popsáno dříve v této kapitole.

Mezi metody automatizované instalace na serverech patří:

- Použití nástroje Syspart na počítačích s rozdílným hardwarem.
- Použití nástroje Sysprep k duplikování disků.
- Použití serveru Systems Management Server.
- Použití spustitelného CD.

Tabulka 13. popisuje situace, kdy se používají různé metody automatizované instalace.

Tabulka 13.5 kdy se používají metody automatizované instalace

Metoda	Použití
Syspart	Nástroj Syspart se používá pro čistou instalaci na počítače s rozdílným hardwarem.
Sysprep	Nástroj Sysprep se používá, mají-li hlavní a cílový počítač stejný hardware, což zahrnuje také ovladače HAL a zařízení hromadného ukládání dat.
Systems Management Server	Systems Management Server se používá ke spravovaným inovacím programu Windows 2000 Server na více systémech, zejména jsou-li geograficky rozptýleny.
Spustitelné CD	Metoda spustitelného CD se používá u počítačů, jejichž systém základních vstupů a výstupů (BIOS) umožňuje spuštění z CD.

Použití nástroje Syspart na počítačích s rozdílným hardwarem

Nástroj Syspart se spouští volitelným parametrem programu `Winnt32.exe`. Metodu Syspart můžete použít, když nemají hlavní počítač a počítač, na který instalujete systém Windows 2000 Server podobný hardware. Tato metoda omezuje čas zavedení odstraněním kroku kopírování souborů instalačního programu.

Syspart vyžaduje použití dvou fyzických disků, přičemž na cílovém pevném disku musí být primární oddíl.

Požadujete-li podobnou instalaci a konfiguraci operačního systému na typech hardwaru, kde se liší ovladače HAL nebo zařízení hromadného ukládání dat, můžete pomocí nástroje Syspart vytvořit hlavní sadu souborů s potřebnými konfiguračními informacemi a podporou ovladačů, které pak lze zkopírovat. Tyto obrazy lze následně použít na nepodobných systémech, kde se řádně detekuje hardware a konzistentně nakonfiguruje operační systém. Obsahuje-li vaše prostředí více typů systémů závislých na hardwaru, můžete použít nástroj Syspart k vytvoření hlavního obrazu jednotlivých typů. Na instalujete systém Windows 2000 na jeden z počítačů každého typu a pomocí nástroje Sysprep pak vytvoříte obrazy použité na zbývajících počítačích stejného typu. Další in-

formace o nástroji Sysprep najdete v oddílu „Duplikování disků nástrojem Sysprep“ dále v této kapitole.

Ještě než začnete, vyberte počítač, který bude považován za referenční. Na referenčním počítači musí být instalován systém Windows NT nebo Windows 2000.

▼ Chcete-li nainstalovat systém Windows 2000 Server pomocí nástroje Syspart, postupujte takto:

1. Spustíte referenční počítač a připojíte se k distribuční složce.
2. Spustíte instalační program.

Stiskněte tlačítko Start, zadejte příkaz Spustit (Run) a pak запиšte:

```
winnt32 /unattend:unattend.txt /s:zdroj_instalace /syspart:druhá_jednotka
/tempdrive:druhá_jednotka /noreboot
```

Důležité Úspěšná instalace nástrojem Syspart je podmíněna použitím parametru */tempdrive*. Při použití přepínače */tempdrive* příkazového řádku se ujistěte, že máte na svém druhém oddílu dostatek volného diskového prostoru k instalaci systému Windows 2000 Server i aplikací. Geometrie disku, který plánujete použít jako cíl nástroje Syspart, musí být stejná jako geometrie disku na počítači, na který budete duplikovat.

Parametry */syspart* a */tempdrive* musí ukazovat na stejný oddíl druhého pevného disku. K instalaci systému Windows 2000 Server musí dojít na primárním oddílu druhého pevného disku.

Upozornění Syspart automaticky označí jednotku za aktivní a výchozí spouštěcí zařízení. Proto před opakovaným zapnutím počítače jednotku vyjměte.

Mezi související definice patří:

Unattend.txt Soubor odpovědí používaný při bezobslužné instalaci, který poskytuje odpovědi na některé nebo všechny výzvy, na něž uživatel obvykle během instalace reaguje. Použití souboru odpovědí je při vytváření hlavního obrazu volitelné.

zdroj_instalace Umístění souborů systému Windows 2000 Server. Chcete-li instalovat z více zdrojů současně, zadejte více přepínačů */s* příkazového řádku.

druhá_jednotka Volitelná druhá jednotka, na kterou předběžně nainstalujete systém Windows 2000 a aplikace.

Duplikování disků pomocí nástroje Sysprep

Duplikování disků je dobrou volbou, potřebujete-li nainstalovat identickou konfiguraci na více počítačů. Na hlavní počítač nainstalujete systém Windows 2000 a aplikace, které chcete mít instalované na všech cílových počítačích. Pak spustíte Sysprep a nástroj kopírování disku od jiné společnosti. Sysprep připraví pevný disk na hlavním počítači, aby mohl nástroj kopírování disků přenést obraz disku na ostatní počítače. Tato metoda dramaticky zkracuje čas zavedení v porovnání se standardními nebo skriptovými instalacemi.

Chcete-li použít Sysprep, váš hlavní a cílové počítače musí mít identické ovladače vrstvy HAL, podpory ACPI a zařízení hromadného ukládání dat. Systém Windows 2000 automaticky detekuje zařízení Plug-and-Play a Sysprep opakovaně detekuje a vyhod-

nocuje zařízení na systému v okamžiku startu počítače po proběhnutí nástroje Sysprep. To znamená, že zařízení Plug-and-Play, jako jsou síťové karty, modemy, grafické karty a zvukové karty nemusejí být na cílových počítačích stejné jako na hlavním počítači. Hlavní výhodou instalace pomocí nástroje Sysprep je rychlost. Obraz disku lze zabalíčkovat a zkomprimovat a jako součást obrazu se vytvoří jen soubory potřebné pro danou konfiguraci. Na dalších systémech se vytvoří další potřebné ovladače Plug-and-Play. Obraz disku lze zkopírovat také na CD a tímto způsobem jej distribuovat do sídel s pomalým připojením.

Poznámka Protože hlavní a cílové počítače musí mít stejné ovladače HAL, podpory ACPI a zařízení hromadného ukládání dat, někdy může být nutné mít ve svém prostředí několik obrazů.

Nástroj Sysprep vám umožňuje nakonfigurovat hlavní obraz obsahující potřebné komponenty členského serveru a server později nakonfigurovat a volitelně jej povýšit na řadič domény. To lze učinit ručně nebo spuštěním příkazů v oddílu [GuiRunOnce] souboru Sysprep.inf. Další informace o souboru Sysprep.inf najdete v dále v tomto oddílu.

Důležité Během duplikování disku se u výrobce svého softwaru ujistěte, že neporušujete licenční dohodu instalace softwaru, který chcete duplikovat.

Přehled procesu Sysprep

Tento oddíl popisuje proces vytvoření zdrojového počítače, který se použije pro duplikování disku.

1. Nainstalujte systém Windows 2000. Systém Windows 2000 Server nainstalujte na počítač, který má hardware podobný cílovým počítačům. Při tvorbě tohoto počítače se nesmíte připojit k doméně a heslo místní správy musí zůstat prázdné.
2. Nakonfigurujte počítač. Přihlaste se jako správce a pak nainstalujte a nastavte aplikace systému Windows 2000 Server a další aplikace. Můžete použít Internet Information Services (IIS) nebo zadat jiné služby.
3. Zkontrolujte obraz. Pomocí auditování podle svých kritérií ověřte, že konfigurace obrazu je správná. Odstraňte nadbytečné informace včetně zbytků protokolů auditování a událostí.
4. Připravte obraz na duplikaci. Jakmile jste si jisti, že je počítač nakonfigurován přesně podle vašich požadavků, můžete spustit přípravu systému na duplikování. Toho dosáhnete spuštěním nástroje Sysprep s volitelným souborem Sysprep.inf, který je popsán dále v této kapitole. Po dokončení funkce nástroje Sysprep se počítač automaticky vypne nebo oznámí, že je možné jej bezpečně vypnout.
5. Provedte duplikaci. V tomto okamžiku je pevný disk počítače nastaven tak, že při dalším startu počítače se spustí detekce Plug-and-Play, vytvoření nových identifikátorů zabezpečení (SID) a spuštění minimální verze průvodce instalací. Nyní jste připraveni systém duplikovat pomocí nějakého hardwarového nebo softwarového řešení. Při dalším spuštění systému Windows 2000 Server z tohoto disku nebo z jiného disku vytvořeného duplikováním daného obrazu bude systém detekovat a vyhodnocovat zařízení Plug-and-Play, čímž se dokončí instalace a konfigurace na cílovém počítači.

Důležité Komponenty, které závisí na službě Active Directory, nelze duplikovat.

Soubory nástroje Sysprep

Chcete-li použít nástroj Sysprep, ručně spusťte soubor Sysprep.exe nebo pomocí oddílu [GuiRunOnce] souboru odpovědí instalačního programu zajistíte, aby se Sysprep.exe spustil automaticky. Chcete-li použít nástroj Sysprep, musí se ve složce Sysprep v kořenu systémové jednotky (%systemdrive%\Sysprep\)) nacházet soubory Sysprep.exe a Setupcl.exe. Jestliže si přejete umístit tyto soubory na správné místo během automatizované instalace, musíte je přidat do svých distribučních složek do podsložky \$OEM\$\\$1\Sysprep\. Další informace o této podsložce najdete v oddílu „Vytvoření struktury distribuční složky“ dříve v této kapitole.

Tyto soubory připraví operační systém na duplikování a spustí minimální verzi průvodce instalací. Ve složce Sysprep můžete také použít volitelný soubor odpovědí Sysprep.inf. Soubor Sysprep.inf obsahuje výchozí parametry, jejichž pomocí můžete zajistit konzistentní reakce na případné výzvy. Tím se omezuje požadavek na zadání uživatele a následně i možné chyby uživatelů. Soubor Sysprep.inf můžete umístit také na disketu, která musí být po zobrazení obrazovky spuštění systému Windows vložena do disketové jednotky. Tím je zajištěna možnost dalších úprav nastavení na cílovém počítači. Disketová jednotka čte data v okamžiku, kdy se objeví obrazovka „Prosím čekejte“ průvodce instalací. Jakmile průvodce úspěšně dokončí svou činnost, systém ještě naposledy restartuje, odstraní se složka Sysprep a celý její obsah a systém je připraven na přihlášení uživatele.

Sysprep.exe

Program Sysprep.exe má tři volitelné parametry:

- *quiet* – spustí Sysprep bez zobrazování hlášení.
- *nosidgen* – spustí Sysprep bez obnovení čísel SID, která již na systému existují. To je užitečné v případech, že nemáte v úmyslu duplikovat počítač, na němž je nástroj Sysprep spuštěný.
- *reboot* – automaticky restartuje počítač poté, co jej Sysprep vypne. Není tedy nutné počítač znovu ručně zapínat.

Sysprep.inf

Soubor Sysprep.inf je soubor odpovědí, který se používá k automatizaci procesu minimální verze průvodce instalací. Používá stejnou syntaxi souborů .ini a názvy klíčů (podporovaných) jako soubor odpovědí instalačního programu. Soubor Sysprep.inf je zapotřebí umístit do složky %systemdrive%\Sysprep nebo na disketu. Použijete-li disketu, musíte ji použít po zobrazení obrazovky spouštění systému Windows. Disketa se přečte v okamžiku, kdy se objeví obrazovka „Prosím čekejte“ průvodce instalací. Uvědomte si, že pokud soubor Sysprep.inf během spuštění nástroje Sysprep nevyužijete, průvodce zobrazí všechna dialogová okna uvedená dále v tomto oddílu.

Poznámka Jestliže jste vytvořili soubor Sysprep.inf na hlavním počítači a potřebujete jej měnit podle jednotlivých počítačů, můžete použít dříve popsanou metodu disket.

Následující kód je příklad souboru Sysprep.inf:

```
[Unattended]
;Vyzvat uživatele k přijetí licenčních podmínek (EULA).
OemSkipEula=No
;Použít výchozí nastavení Sysprep a znovu vytvořit stránkovací soubor
;systému, aby se vyrovnaly možné rozdíly ve velikosti dostupné RAM.
KeepPageFile=0
;Zadat umístění dodatečných jazykových souborů, které mohou být
;zapotřebí v případě globální organizace.
InstallFilePath=%systemdrive%\Sysprep\i386

[GuiUnattended]
;Zadat neprázdné heslo správce.
;Zadané heslo bude použito, pouze pokud bylo na původním zdroji obrazu
;(hlavním počítači) zadáno neprázdné heslo. Jinak bude heslo zadané
;na hlavním počítači heslem použitým i na tomto počítači. Lze jej
;zaměnit přihlášením se jako místní správce a ruční změnou hesla.
AdminPassword="..
;Nastavit časovou zónu.
TimeZone=20
;Přeskočit uvítací obrazovku při spouštění systému.
OemSkipWelcome=1
;Nepřeskočit dialogové okno místních nastavení, aby mohl uživatel
;zadat, která místní nastavení se použijí.
OemSkipRegional=0

[UserData]
;Znovu zadat informace o uživateli pro systém.
FullName="Autorizovaný uživatel"
OrgName="Název organizace"
ComputerName=XYZ_Pocitac1

[GUIRunOnce]
;Povýšit při startu tento počítač na řadič domény.
DCPromo/answer:<umístění souboru odpovědi povýšení>

[Identification]
;Připojit počítač do domény ITDOMAIN
JoinDomain=ITDOMAIN

[Networking]
;Svázat výchozí protokoly a služby k síťové kartě (kartám) použité
;v daném počítači.
InstallDefaultComponents=Yes
```

Poznámka Heslo správce lze pomocí souboru Sysprep.inf změnit, pouze pokud je existující heslo správce prázdné. To platí také v případě, kdy chcete změnit heslo správce pomocí grafického rozhraní nástroje Sysprep.

Další informace o oddílech souboru odpovědí a příkazech souvisejících se souborem Sysprep.inf najdete v příloze „Příklady souborů odpovědí pro bezobslužnou instalaci“ v této knize.

Setupcl.exe

Soubor Setupcl.exe vykonává toto:

- Vytváří nový identifikátor zabezpečení počítače.
- Spouští minimální verzi instalačního programu.

Minimální verze instalačního programu

Minimální verze instalačního programu se rozběhne při prvním spuštění počítače z disku duplikovaného metodou Sysprep. Tento průvodce získá všechny informace potřebné k dalšímu nastavení cílového počítače. Nepoužíváte-li soubor Sysprep.inf nebo necháte-li některé jeho oddíly prázdné, minimální verze instalačního programu zobrazí ta okna, jejichž otázky nebyly zodpovězeny v souboru Sysprep.inf. Možnými obrazovkami jsou:

- Licenční dohoda pro koncového uživatele (EULA)
- Místní volby
- Název uživatele a společnosti
- Název počítače a heslo správce
- Nastavení sítě
- Nastavení TAPI (zobrazí se pouze existuje-li na počítači modem nebo nové modemové zařízení)
- Licence serveru (pouze u serveru)
- Volba časové zóny
- Dokončení/restart

Chcete-li přeskočit tyto obrazovky, musíte zadat určité parametry v souboru Sysprep.inf. Tyto parametry jsou uvedeny v tabulce 13.6.

Poznámka Protože instalační program zjišťuje optimální nastavení grafických zařízení, nezobrazí se již při probíhání instalačního programu nebo jeho minimální verze obrazovka „Nastavení zobrazení“. Nastavení [Display] lze zadat buď v souboru odpovědí použitém pro váš hlavní počítač nebo v souboru Sysprep.inf použitém pro cílový počítač. Jsou-li v souboru odpovědí určeném pro hlavní počítač zadána nastavení [Display], Sysprep tato nastavení zachová, pokud nebude Sysprep.inf obsahovat jiná nastavení nebo nebude grafická karta či monitor požadovat nastavení, která se odlišují od nastavení na hlavním počítači.

Tabulka 13.6 Parametry přeskočení obrazovek minimální verze průvodce v souboru Sysprep.inf

Parametr	Hodnota
Místní volby	oddíl [RegionalSettings] [GuiUnattended] OemSkipRegional=1
Název uživatele a společnosti	[UserData] FullName="Název uživatele" OrgName="Název organizace"
Název počítače a heslo správce	[UserData] ComputerName=W2B32054 [GuiUnattended] AdminPassword=„
Nastavení sítě	[Networking] InstallDefaultComponents=Yes
Nastavení TAPI	[TapiLocation] AreaCode=425
Výběr časové zóny	[GuiUnattended] TimeZone=<index požadované časové zóny>
Dokončení/restart	NA

Ruční spuštění nástroje Sysprep

Po instalaci systému Windows 2000 Server můžete připravit systém na přenos na jiné podobně konfigurované počítače pomocí nástroje Sysprep. Chcete-li Sysprep spustit ručně, musíte nejprve nainstalovat systém Windows 2000 Server, nakonfigurovat jej a nainstalovat aplikace. Pak spusíte Sysprep bez přepínače *-reboot* příkazového řádku. Jakmile se systém vypne, duplikujte obraz jednotky na podobně nakonfigurované počítače.

Když uživatelé poprvé spustí své duplikované počítače, spustí se minimální verze instalace nástroje Sysprep, která umožní uživatelům nastavení jejich systémů. Pomocí souboru Sysprep.inf můžete také přednastavit některé nebo všechny konfigurační parametry nástroje Sysprep. Složka Sysprep (která obsahuje soubory Sysprep.exe a Setupcl.exe) se po dokončení minimální verze průvodce nástroje Sysprep automaticky odstraní.

▼ Chcete-li připravit instalaci systému Windows 2000 Server na duplikování, postupujte takto:

1. Stiskněte tlačítko Start, zadejte příkaz Spustit (Run) a pak запиšte:

```
cmd
```

2. V příkazovém řádku se přepněte do kořenové složky jednotky C a pak zadejte:

```
md sysprep
```

3. Vložte do mechaniky CD systému Windows 2000 Server CD. Otevřete si soubor Deploy.cab ve složce \Support\Tools.
4. Zkopírujte soubory Sysprep.exe a Setupcl.exe do složky Sysprep.

Používáte-li soubor Sysprep.inf, také jej zkopírujte do složky Sysprep. Uvědomte si, že pro zajištění správné funkce nástroje Sysprep se musí soubory Sysprep.exe, Setupcl.exe a Sysprep.inf nacházet ve stejné složce.

5. V příkazovém řádku se přepněte do složky Sysprep:

```
cd sysprep
```

6. Podle potřeby zadejte jeden z následujících příkazů:

```
Sysprep
Sysprep -reboot
Sysprep /<volitelný parametr>
Sysprep /<volitelný parametr> -reboot
Sysprep /<volitelný parametr 1>.../<volitelný parametr X>
Sysprep /<volitelný parametr 1>.../<volitelný parametr X> -reboot
```

7. Jestliže nezádáte přepínač *-reboot* příkazového řádku, vykonajte následující:

Jakmile se objeví zpráva o tom, že máte vypnout počítač, zadejte příkaz **Vypnout** (Shut Down) nabídky **Start**. Nyní můžete použít nástroj kopírování disků jiného výrobce a vytvořit obraz instalace.

8. Jestliže jste zadali přepínač *-reboot* příkazového řádku pouze pro účely auditování, pak se počítač restartuje a spustí se minimální verze průvodce instalací. V takovém případě vykonajte následující:

- Zkontrolujte, že minimální verze instalace zobrazuje požadované výzvy. V tomto okamžiku můžete také auditovat systém a další aplikace. Jakmile je auditování ukončeno, znovu spusíte Sysprep bez přepínače *-reboot* příkazového řádku.
- Jakmile se objeví zpráva o tom, že máte vypnout počítač, zadejte příkaz **Vypnout** (Shut Down) nabídky **Start**. Nyní můžete použít nástroj kopírování disků jiného výrobce a vytvořit obraz instalace.

Poznámka Do složky Sysprep můžete také přidat soubor Cmdlines.txt, který instalační program následně zpracuje. Tento soubor spustí příkazy po dokončení instalace včetně těch požadovaných pro instalaci aplikací.

Automatické spuštění nástroje Sysprep po dokončení instalačního programu

Oddíl [GuiRunOnce] souboru odpovědí obsahuje příkazy vykonané po dokončení instalačního programu. Oddíl [GuiRunOnce] můžete použít k vytvoření instalace, která dokončí instalační program, automaticky se přihlásí k počítači, spustí nástroj Sysprep v režimu **-quiet** a nakonec počítač vypne. Aby k tomu všemu došlo, musíte zajistit následující:

1. Potřebné soubory nástroje Sysprep umístěte do distribuční složky \$OEM\$\\$1\Sysprep\, aby se zkopírovaly na správné místo na systémové jednotce.
2. Do oddílu [GuiRunOnce] souboru odpovědí zadejte následující poslední příkaz, který se spustí na počítači:

```
%systemdrive%\Sysprep\Sysprep.exe -quiet
```

Je-li zapotřebí více restartů, zadejte tento příkaz tak, aby byl spuštěn jako poslední při posledním použití oddílu [GuiRunOnce].

Rozšiřování diskových oddílů pomocí nástroje Sysprep

Grafický instalační program systému Windows 2000 a jeho minimální verzi lze použít k rozšíření oddílů NTFS prostřednictvím souborů odpovědí. Tento nový prvek má tyto funkce:

- Umožňuje vám vytvářet obrazy, které lze rozšířit na větší diskové oddíly a plně tak využít pevné disky, které mají více prostoru než původní pevný disk na hlavním počítači.
- Umožňuje vytvářet obrazy na menších discích.

Abyste určili nejlepší možnosti integrace této funkce do svého prostředí, musíte projít následující kroky a na základě nástrojů používaných k vytváření obrazů operačního systému vybrat metodu, která bude ve vašem případě fungovat nejlépe.

Upozornění Jestliže vám vaše nástroje obrazů umožňují obraz upravovat, můžete odstranit soubory Pagefile.sys, Setupapi.log a Hyberfil.sys (jestliže existují), protože tyto soubory na cílovém počítači minimální verze instalace znovu vytvoří. Tyto soubory nesmíte odstranit na aktivním systému, protože to může znamenat chybnou funkci systému. Tyto soubory však lze v případě potřeby odstranit z obrazu.

▼ Chcete-li rozšířit oddíl pevného disku při použití nástroje vytváření obrazů od jiného výrobce nebo hardwarového zařízení vytváření obrazů, které podporuje systém NTFS používaný Windows 2000, postupujte takto:

1. Nakonfigurujte oddíl na pevném disku hlavního počítače tak, aby měl minimální velikost nutnou pro instalaci systému Windows 2000 a všech jeho komponent a aplikací, které chcete předběžně instalovat. Tím se omezí požadavky na celkovou velikost obrazu.
2. Do oddílu [Unattended] souboru odpovědí, který se používá k vytvoření hlavního obrazu, vložte příkaz `FileSystem=ConvertNTFS`. Nemusíte sem zadávat parametr `ExtendOemPartition`, protože chcete udržet co nejmenší možnou velikost obrazu.

Poznámka Příkaz `ConvertNTFS` v souboru `Sysprep.inf` nefunguje, protože se jedná výhradně o funkci textového režimu a nástroj Sysprep textovým režimem neprochází.

3. Do oddílu [Unattended] souboru `Sysprep.inf` vložte příkaz:

```
ExtendOemPartition = 1
```

(nebo jinou velikost v megabajtech, o kterou se má oddíl rozšířit)

4. Nainstalujte systém Windows 2000 na hlavní počítač. Nástroj Sysprep systém automaticky vypne.
5. Vytvořte obraz jednotky.
6. Umístěte obraz na cílový počítač, kde má cílový počítač stejnou velikost systémového oddílu jako hlavní počítač.
7. Restartujte cílový počítač.

Spustí se minimální verze instalačního programu a téměř okamžitě dojde k rozšíření oddílu.

▼ **Chcete-li rozšířit oddíl pevného disku při použití nástroje vytváření obrazů, který nepodporuje systém NTFS používaný Windows 2000**

1. Nakonfigurujte oddíl na pevném disku hlavního počítače tak, aby měl minimální velikost nutnou pro instalaci systému Windows 2000 a všech jeho komponent a aplikací, které chcete předběžně instalovat. Tím se omezí požadavky na celkovou velikost obrazu.
2. Převedte systém souborů pomocí nástroje Convert.exe, který je součástí systému Windows 2000, na NTFS.
3. Do oddílu [GuiRunOnce] souboru odpovědí, který se používá k vytvoření hlavního obrazu, vložte jako poslední dvě položky následující příkazy:

```
[GuiRunOnce]
<Příkaz1> = „<příkazový řádek>“
<Příkaz2> = „<příkazový řádek>“
...
<Příkazn-1> = „Convert c:\ /fs:ntfs“
<Příkazn> = „%systemdrive%\sysprep\sysprep.exe -quiet“
```

kde:

- <příkazový řádek> zahrnuje všechny příkazy, které je zapotřebí spustit v zájmu instalace aplikací nebo konfigurace operačního systému před vytvořením jeho obrazu.
- <Příkazn-1> je předposlední příkaz, který se vykoná v oddílu [GuiRunOnce] souboru odpovědí. Tím se spustí program **convert**. Protože program **convert** namůže převést aktivní systém na NTFS v době, kdy běží operační systém, operací systém se nastaví tak, aby k tomu došlo při dalším restartu. Jelikož následující spouštěnou položkou je Sysprep, systém se v tomto procesu nepřevede na NTFS.
- <Příkazn> je poslední příkaz spuštěný na počítači. To musí být Sysprep.exe. Po svém spuštění připraví Sysprep počítač na vytváření obrazů a pak počítač vypne.

Poznámka Do souboru odpovědí nemůžete v tomto kroku zahrnout parametr ExtendOemPartition, protože oddíl, na kterém je obraz vytvořen, není NTFS. Také bude vhodné mít co nejmenší obraz.

4. Do oddílu [Unattended] souboru Sysprep.inf vložte příkaz:

```
ExtendOemPartition = 1
```

(nebo jinou velikost v megabajtech, o kterou se má oddíl rozšířit)

5. Nainstalujte systém Windows 2000 na hlavní počítač. Nástroj Sysprep systém automaticky vypne.

Důležité Počítač nerestartujte.

6. Vytvořte obraz jednotky.
7. Umístěte obraz na cílový počítač, kde má cílový počítač stejnou velikost systémového oddílu jako hlavní počítač.
8. Restartujte cílový počítač.

Program nejprve převede systémový oddíl cílového počítače na NTFS.

Počítač se pak automaticky restartuje.

Spustí se minimální verze instalačního programu a téměř okamžitě dojde k rozšíření oddílu.

Použití serveru Systems Management Server

K provedení spravovaných inovací programu Windows 2000 Server na více systémech, zejména jsou-li geograficky roztroušené, můžete použít SMS. Uvědomte si, že SMS se používá pouze při instalaci na počítače s již dříve nainstalovaným operačním systémem. Před inovací pomocí SMS je důležité vyhodnotit stávající síťovou infrastrukturu včetně šířky přenosového pásma, hardwaru a geografických omezení. Hlavní výhodnou inovace pomocí SMS je, že můžete udržovat centralizované řízení procesu inovace. Můžete například řídit, kdy k inovaci dojde (například během školení nebo po něm, po ověření hardwaru a po zálohování uživatelských dat), které počítače se budou inovovat a jak se budou aplikovat síťová omezení. Další informace o zavedení SMS najdete v kapitole „Zavádění systému Windows 2000 pomocí serveru Systems Management Server“ v této knize.

Použití spustitelného kompaktního disku

Metodu instalace systému Windows 2000 pomocí spustitelného CD lze použít na počítači, jehož BIOS umožňuje spouštění systému počítače z CD. Tato metoda je velmi užitečná u počítačů ve vzdálených sídlech s pomalým připojením a bez místního oddělení IT. Metoda spustitelného CD používá Winnt32.exe, což umožňuje rychlou instalaci.

Poznámka Metodu spustitelného CD lze použít pro čisté instalace. Chcete-li vykonat inovaci, musíte spustit Winnt32.exe z existujícího operačního systému.

Pro zajištění maximální flexibility nastavte následující pořadí spouštění v systému BIOS:

- Síťová karta
- CD
- Pevný disk
- Disketa

Chcete-li použít spustitelné CD, musí být splněna následující kritéria:

- Váš počítač musí podporovat spustitelná CD standardu El Torito bez emulace.
- Soubor odpovědí musí obsahovat oddíl [Data] s potřebnými klíči.
- Soubor odpovědí musí být pojmenován Winnt.sif a musí být umístěn na disketě.

Další informace o parametrech a syntaxi souboru odpovědí najdete v dokumentu „Příručka bezobslužné instalace Microsoft Windows 2000“ (Unattend.doc) na CD operačního systému Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

▼ **Chcete-li nainstalovat systém Windows 2000 Server pomocí spustitelného kompaktního disku, postupujte takto:**

1. Spusťte systém z CD Windows 2000 Server.
2. Jakmile se objeví modrá obrazovka „Instalace systému Windows 2000“ v textovém režimu, vložte do disketové jednotky disketu obsahující soubor Winnt.sif.
3. Když počítač přečte z diskety potřebné informace, disketu z mechaniky odstraňte. Nyní se spustí instalace z CD, jak je zadáno v souboru Winnt.sif.

Poznámka Metoda spustitelného CD vyžaduje, aby byly všechny potřebné soubory na CD. Ve spojení s touto metodou nelze použít soubory Uniqueness Database Files (UDB).

Příklad konfigurace instalace

Následující příklady obsahují procedury instalace systému Windows 2000 Server na počítačích s již existující serverovou konfigurací i bez ní.

Existující servery

Příklady v tomto oddílu jsou pro počítače s následujícími již existujícími serverovými konfiguracemi:

- Počítače se systémem Windows NT Server se serverovými aplikacemi kompatibilními s programem Windows 2000 Server.
- Počítače se systémem Microsoft Windows NT Server verze 3.5 či dřívější nebo servery s operačními systémy nepocházejícími od společnosti Microsoft.

Příklad 1: Windows NT Server se serverovými aplikacemi kompatibilními se systémem Windows 2000

Tento příklad ukazuje dvě metody instalace systému Windows 2000 Server na počítače se systémem Windows NT Server s kompatibilním hardwarem a bez něj.

▼ **Chcete-li instalovat systém Windows 2000 Server na počítače s kompatibilním hardwarem, postupujte takto:**

1. Zálohujte celý systém.
2. Inovujte systém jednou z následujících metod:
 - Iniciujte nevyžádanou instalaci. To znamená, že se program nebo aplikace automaticky odešle z nadřazeného počítače na cílový počítač. Tato metoda nevyžaduje k inicializaci nějakou aktivitu uživatele nebo správce.
 - Iniciujte místní instalaci spuštěním souboru Winnt32.exe z příkazového řádku s vybranými parametry.
 - Vykonejte ruční instalaci (bez souboru odpovědí) a zodpovězte všechny výzvy.
 - Vykonejte automatickou nebo poloautomatickou instalaci. Při plně automatické instalaci poskytne soubor odpovědí odpovědi na všechny otázky. Poloautomatická instalace vám umožňuje určit stupeň automatizace a umožnit určitá zadání uživatele případně vámi vybraných aplikací.

▼ **Chcete-li instalovat systém Windows 2000 Server na počítač s nekompatibilním hardwarem, u kterého není zapotřebí vyměnit pevný disk, postupujte takto:**

1. Vyměňte potřebný hardware s výjimkou pevného disku.
2. Provéřte, že všechny nový hardware řádně funguje.
3. Zálohujte celý systém.
4. Inovujte systém jednou z následujících metod:
 - Iniciujte nevyžádanou (plně automatickou) instalaci.
 - Iniciujte místní instalaci spuštěním souboru Winnt32.exe z příkazového řádku s vybranými parametry.
 - Vykonejte ruční instalaci (bez souboru odpovědí) a zodpovězte všechny výzvy.
 - Vykonejte automatickou nebo poloautomatickou instalaci.

▼ **Chcete-li instalovat systém Windows 2000 Server na počítač s nekompatibilním hardwarem, u kterého je zapotřebí vyměnit pevný disk, postupujte takto:**

1. Inovujte alespoň jednu z následujících položek:
 - Paměť RAM
 - Procesor
2. Provéřte, že všechny nový hardware řádně funguje.
3. Zálohujte celý systém.
4. Vyměňte pevný disk. Zkopírujte na něj zálohovaný obraz.
5. Jestliže inovujete, proveďte inovaci jednou z následujících metod. To může být užitečné zejména v situacích, kdy je na serveru jedinečná nebo téměř jedinečná konfigurace:
 - Iniciujte nevyžádanou (plně automatickou) instalaci.
 - Iniciujte místní instalaci spuštěním souboru Winnt32.exe z příkazového řádku s vybranými parametry.
 - Vykonejte ruční instalaci (bez souboru odpovědí) a zodpovězte všechny výzvy.
 - Vykonejte automatickou nebo poloautomatickou instalaci.
6. Vykonáváte-li čistou instalaci, použijte jednu z následujících metod:
 - Pomocí nástroje Syspart umístěte všechny potřebné soubory na disk ještě před jeho náhradou použitím hardwaru nebo softwaru pro duplikování disků. Jakmile se systém spustí, automaticky se objeví instalační program. Znovu nainstalujte všechny potřebné serverové aplikace.
 - Iniciujte nevyžádanou (plně automatickou) instalaci.
 - Iniciujte místní instalaci spuštěním souboru Winnt32.exe z příkazového řádku s vybranými parametry.
 - Vykonejte ruční instalaci (bez souboru odpovědí) a zodpovězte všechny výzvy.
 - Vykonejte automatickou nebo poloautomatickou instalaci.

Příklad 2: Počítače se systémem Windows NT Server 3.5 či dřívějším nebo servery s operačními systémy nepocházejícími od společnosti Microsoft

Mezi serverové operační systémy, které nelze přímo aktualizovat na systém Windows 2000 Server patří NT 3.5 a dřívější verze, Novell, Banyan Vines, UNIX a OS/2. Chcete-li se připravit na čistou instalaci, obstarajte si klientský počítač sestavený partnerem OEM nebo poskytovatelem řešení.

▼ Chcete-li instalovat systém Windows 2000 na počítač se systémem Windows NT 3.5 či dřívějším nebo s operačním systémem nepocházejícím od společnosti Microsoft, postupujte takto:

1. Systém zálohujte.
2. Jednou z následujících metod spusťte soubor Winnt.exe z příkazového řádku s požadovanými parametry:
 - Vykonejte ruční instalaci (bez souboru odpovědí) a zodpovězte všechny výzvy.
 - Vykonejte automatickou nebo poloautomatickou instalaci. Použijte jednu z těchto metod:
 - Metodu spustitelného CD.
 - Metodu Syspart. To je užitečné při instalaci nových pevných disků do počítačů.
 - Metodu Sysprep. Používá se při instalaci na identické počítače (ovladače HAL a zařízení hromadného ukládání dat musí být shodné).

Poznámka V případě potřeby je možné vykonat čistou instalaci na existující počítač, není to však doporučený postup. Máte-li servery, které nelze inovovat, nahraďte jednotlivé servery novými servery obsahujícími čistou instalaci systému Windows 2000 Server. Výsledkem bude dostatek času na ověření stability systému, omezení možného dopadu na uživatele a zajištění času pro migraci potřebných odkazů a nastavení na nový server.

3. Nainstalujte aplikace kompatibilní se systémem Windows 2000 Server.
4. Podle potřeby ověřte funkce systému.
5. Před vypnutím existujícího systému migrujte uživatele a odkazy tak, aby ukazovaly na nový systém.

Nové servery

Počítače bez operačního systému dřívější verze než Windows 2000 vyžadují čistou instalaci systému Windows 2000 Server.

Na instalaci se připravte získáním klientského počítače od partnera OEM nebo poskytovatele řešení.

▼ Chcete-li instalovat systém Windows 2000 Server na počítač, na kterém není instalován žádný dřívější operační systém, postupujte takto:

1. Vykonejte ruční instalaci (bez souboru odpovědí) a zodpovězte všechny výzvy.
-Nebo-
2. Vykonejte automatickou nebo poloautomatickou instalaci. Použijte jednu z těchto metod:

- Metodu spustitelného CD.
- Metodu Syspart. To je užitečné při instalaci nových pevných disků do počítačů.
- Metodu Sysprep. Používá se při instalaci na identické počítače (ovladače HAL a zařízení hromadného ukládání dat musí být shodné).
- Metodu spouštěcí diskety a spuštění instalačního programu se souborem odpovědí.

Seznam úkolů plánování instalace

Tabulka 13.7 představuje souhrn hlavních úkolů souvisejících s instalací systému Windows 2000 Server a požadovaných aplikací.

Tabulka 13.7 Přehled úkolů instalace

Úkol	Umístění v kapitole
Vyřešte kritické problémy plánování.	Řešení kritických problémů
Vytvořte distribuční složku.	Příprava instalace
Seznamte se se souborem odpovědí.	Přehled souboru odpovědí
Seznamte se s příkazy instalačního programu systému Windows 2000.	Přehled příkazů instalačního programu systému Windows 2000
Na základě kritického plánování zvolte metodu instalace aplikace.	Automatizování instalace serverových aplikací
Na základě kritického plánování zvolte metodu instalace operačního systému.	Automatizování instalace systému Windows 2000 Server

KAPITOLA 14

Zavádění systému Windows 2000 pomocí serveru Systems Management Server

Server Systems Management Server (SMS) společnosti Microsoft poskytuje různé nástroje, které vám pomohou se zavedením systémů Microsoft Windows 2000 Server a Microsoft Windows 2000 Professional v podnikovém prostředí. S doporučenými konfiguracemi a procedurami popsány v této kapitole by se měli seznámit vedoucí projektu a analytici, techničtí analytici systému Windows 2000 a správci SMS, kteří se účastní celého procesu. Tato doporučení lze sice aplikovat i na menší organizace, zaměříme se však především na organizace s nejméně 2500 osobních počítačů.

Abyste porozuměli informacím v této kapitole, nemusíte být seznámeni se serverem Systems Management Server verze 2.0. K zavedení systému Windows 2000 však budete potřebovat někoho se zkušenostmi se SMS. Předpokládá se, že již máte vytvořenou infrastrukturu SMS nebo že ji vytvoříte ještě před zaváděním systému Windows 2000. V této kapitole také najdete popis důležitých rozdílů mezi SMS 2.0 a serverem Systems Management Server verze 1.2.

V této kapitole

Distribuce softwaru pomocí serveru Systems Management Server 420

Vytvoření balíčku systému Windows 2000 pro server Systems Management Server 425

Distribuce balíčků systému Windows 2000 432

Inzerování balíčků systému Windows 2000 439

Zjednodušení konsolidace a migrace domén
pomocí serveru Systems Management Server 448

Rozdíly mezi servery Systems Management Server 1.2
a Systems Management Server 2.0 448

Seznam úkolů plánování použití serveru
Systems Management Server k zavedení systému Windows 2000 449

Další zdroje 450

Cíle kapitoly

Tato kapitola vám pomůže s vývojem těchto plánovacích dokumentů:

- Plán distribuce softwaru systému Windows 2000
- Definice balíčku SMS systému Windows 2000

Související informace v sadě Resource Kit

Další informace o automatizaci inovací systému Windows 2000 najdete v této knize v kapitolách „Automatizování instalace a inovace serveru“ a „Automatizování instalace a inovace klientů“.

Další informace o automatizování konsolidace a migrace domén najdete v kapitole „Určení strategií migrace domén“ v této knize.

Distribuce softwaru pomocí serveru Systems Management Server

Zavádění systému Windows 2000 je mnohem jednodušší, používáte-li automatizovanou instalaci. Avšak i aplikování automatizovaných procedur na více serverových a klient-ských počítačů ve vaší organizaci představuje mnoho dalších úkolů. Mezi ně patří:

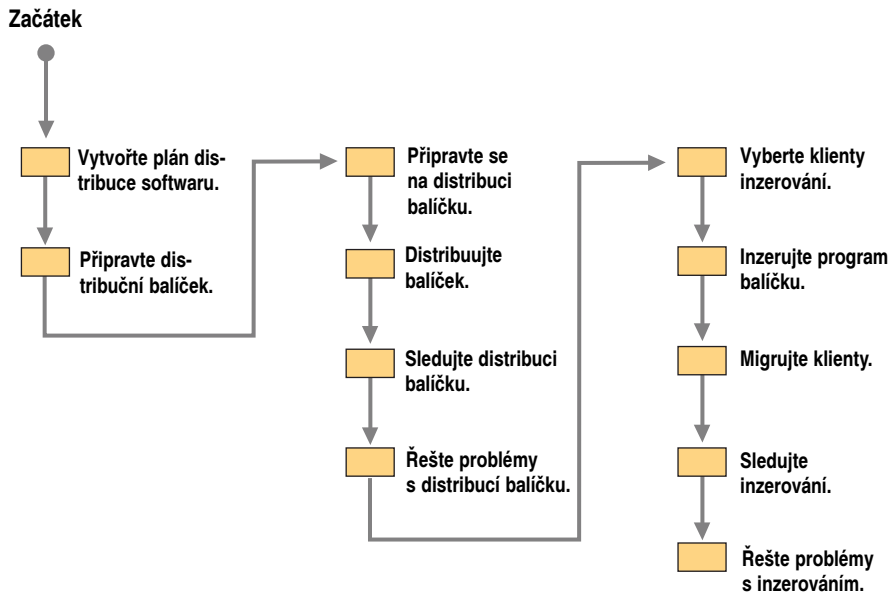
- Výběr počítačů vybavených pro systém Windows 2000 a na jejichž podporu jste připraveni.
- Distribuce zdrojových souborů systému Windows 2000 na všechna síťová sídla včetně vzdálených sídel a sídel bez osob technické podpory.
- Sledování distribuce na všechna sídla.
- Zabezpečené zajištění dostatečných oprávnění operačního systému pro inovaci.
- Automatické iniciování instalace softwarového balíčku s možností předání řízení načasování uživateli.
- Vyřešení problémů souvisejících s distribucí a instalací.
- Hlášení poměru a úspěchu zavedení.

Systems Management Server vám pomůže se všemi uvedenými úkoly. Základní úkoly, které jsou součástí zavedení systému Windows 2000 pomocí SMS, jsou znázorněny na obrázku 14.1.

SMS poskytuje nástroje pro inovaci vašich stávajících počítačů, nikoli však pro instalaci nových počítačů, které ještě nemají instalovaný operační systém. Chcete-li použít distribuci softwaru pomocí SMS, musíte na cílové počítače nainstalovat klientské komponenty SMS. Tyto komponenty SMS vyžadují počítač s řádně nakonfigurovaným operačním systémem.

Poznámka Označení „klient SMS“ představuje všechny cílové počítače bez ohledu na jejich funkci.

Současné klienty SMS však lze použít k inicializaci instalace systému Windows 2000 do nové hierarchie adresářů nebo na nový diskový oddíl. V takovém případě jde spíše o čistou instalaci systému Windows 2000 a nikoli o inovaci.



Obrázek 14.1 Zavedení systému Windows 2000 pomocí SMS

Poznámka SMS vám také může pomoci s jinými činnostmi zavádění systému Windows 2000. Další informace o použití SMS při zavádění systému Windows 2000 najdete v kapitole „Analýza infrastruktury sítě pomocí serveru Systems Management Server“ v této knize.

Distribuce softwaru pomocí serveru Systems Management Server 2.0

Distribuce softwaru pomocí serveru Systems Management Server vychází z více komponent a úloh, které vám umožňují celý proces plně řídit.

Balíčky SMS

Distribuce softwaru pomocí SMS začíná *balíčkem* SMS. Balíček je základní jednotka distribuce softwaru a obsahuje zdrojové soubory programu a podrobnosti, které řídí proces distribuce softwaru.

Každý balíček obsahuje nejméně jeden *program*, což je příkazový řádek, který se spustí na každém cílovém počítači a řídí vykonávání balíčku. Programy mohou řídit instalaci softwaru nebo obsahovat jiný příkazový řádek, který se má spustit na všech cílových počítačích. Většina balíčků také obsahuje *zdrojové soubory balíčku*, například instalační soubory softwaru, které program po svém spuštění používá.

Některé softwarové aplikace nabízejí rozsáhlé možnosti instalace. Jiné balíčky a nástroje nic takového nenabízejí. Neposkytuje-li program, který chcete distribuovat, příslušné možnosti instalace, například bezobslužný běh, můžete svůj program připravit na instalaci pomocí nástroje SMS Installer. SMS Installer dokáže vytvořit instalační skripty obslužné nebo bezobslužné instalace, které si můžete dále upravit. Tento druh využití

skriptů se nehodí pro inovaci systému Windows 2000. Může však být užitečný v případě balíčků odesílaných před inovací na systém Windows 2000, které počítač připravují, nebo u balíčků odesílaných po inovaci, aby dokončily konfiguraci počítače. Další informace o nástroji SMS Installer najdete v kapitole „Creating Self-Extracting Files with SMS Installer 2.0“ v knize *Microsoft Systems Management Server Administrator's Guide*.

Balíček lze vytvořit pomocí položky **Packages** (balíčky) v konzole **SMS Administrator** (správce SMS) nebo můžete vytvořit či obdržet *soubor definice balíčku* a použít průvodce vytvořením balíčku z definice (**Create Package from Definition**). Soubor definice balíčku představuje alternativní neinteraktivní možnost vytvoření balíčku. Jde o formátovaný soubor, který obsahuje všechny informace potřebné pro vytvoření balíčku. Soubor definice balíčku pro systém Windows 2000 je součástí SMS 2.0. K vytvoření balíčků ze souborů definice balíčků bez zásahu uživatele můžete použít nástroje a průvodce SMS. Jakmile je balíček vytvořen, vyberte distribuční body pomocí průvodce správou distribučních bodů (**Manage Distribution Points**) SMS.

Distribuce

Balíčky také obsahují informace o distribuci softwaru, například adresář zdrojových souborů balíčku. *Distribuční body* jsou sdílená místa na systémech síťových sídel, kam se zdrojové soubory balíčku zkopírují a kam k nim budou mít klientské počítače přístup. Balíčky také obsahují informace o tom, jak a kdy se mají distribuční body aktualizovat. V zájmu jednodušší správy je možné distribuční body seskupovat do skupin distribučních.

Je-li zapotřebí balíčky rozšířit do jiných sídel, SMS tyto soubory zkomprimuje, aby je bylo možné přenášet mezi sídly. Zkomprimovanou kopii zdrojových souborů balíčku můžete vytvořit a používat také v rámci původního sídla.

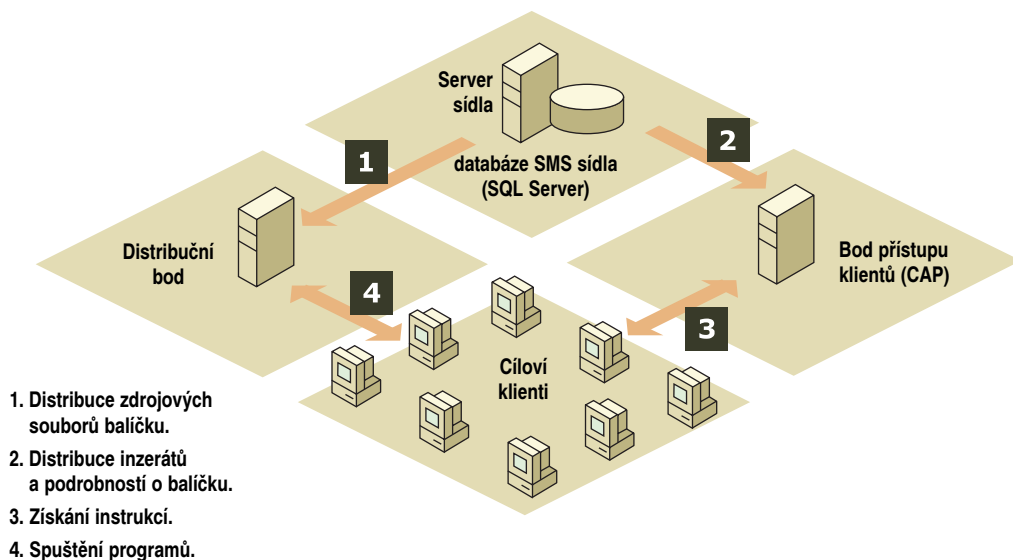
Distribuci balíčku lze řídit pomocí položky **Distribution Points** (distribuční body), která se nachází pod definicí balíčku v položce **Packages** v konzole SMS Administrator.

Inzerování

Jakmile vytvoříte balíček systému Windows 2000, můžete vytvořením inzerátu pro uživatele inzerovat jeden nebo více programů balíčku. Inzerát specifikuje, jaký program je k dispozici klientským počítačům, jaké počítače inzerát obdrží a na kdy bude naplánována instalace programu. Na obrázku 14.2 je zachycen proces distribuce softwaru.

I když klient SMS přijme inzerát, uživatel může mít částečnou kontrolu nad časovým naplánováním balíčku. Inzerát lze spustit ve speciálním privilegovaném režimu, takže uživatelům žádná zvláštní práva přiřazovat nemusíte. Inzerát lze spustit také tak, aby nevyžadoval žádné zadání od uživatele.

Inzerát je možné vytvořit pomocí položky **Advertisements** (inzeráty) konzoly SMS Administrator.



Obrázek 14.2 Proces distribuce softwaru pomocí SMS 2.0

Další informace o distribuci softwaru pomocí SMS najdete v knize *Systems Management Server Administrator's Guide*.

Doporučené postupy distribuce softwaru pomocí SMS

V případě velkých distribucí softwaru, jako je tomu u systému Windows 2000, je důležité uvědomit si obě fáze distribuce softwaru pomocí serveru Systems Management Server 2.0: distribuci a inzerování. Distribuce přenese software do blízkosti počítačů, které se mají inovovat. Inzerování proces inovace spustí. U balíčků tak velkých, jako představuje systém Windows 2000, spotřebuje distribuční fáze velké množství prostředků a mohou se objevovat problémy způsobené nedostatkem diskového prostoru. Proto musíte distribuční fázi pozorně naplánovat a sledovat. Po úspěšném dokončení distribuční fáze začnete s fází inzerování.

Svou distribuci otestujte nejprve distribucí systému Windows 2000 na jediné sídlo. Úvodní inzerování balíčku také musíte poslat pouze klientům daného sídla. To vám umožní v omezeném měřítku otestovat infrastrukturu a procedury SMS. Jakmile získáte důvěru v celý proces, můžete podle možností kapacit distribuovat balíček na více sídel a rozšířit také rozsah inzerování, který bude nyní zahrnovat více klientů a sídel až postupně bude zahrnovat celou vaši organizaci.

Další doporučené postupy najdete v následujícím pojednání o procesu distribuce softwaru.

Jak vám server SMS pomůže se zavedením systému Windows 2000

Systems Management Server může být velmi užitečný při zavádění systému Windows 2000 následujícími způsoby:

Odeslání zdrojových souborů Windows 2000 na všechna sídla

SMS má *odesilatele*, kteří mohou odesílat soubory různými síťovými protokoly a přes prakticky libovolné síťové připojení. Odesílatelé mají oproti tradičním metodám přenosu souborů několik výhod, jimiž jsou:

- Použití jen části šířky pásma sítě, čímž je umožněna současná funkce dalších úkolů.
- Předávání balíčků jen během zadaných hodin, například v době, kdy téměř nikdo propojení nevyužívá.
- Kontrola souborů při přenosu, takže dojde-li k poruše síťového spojení, přenos se obnoví v bodě poslední kontroly a nebude probíhat celý znovu od začátku.
- Volba alternativní cesty k cíli.
- Pro přenos balíčků použijte raději hierarchii SMS, než abyste rozesílali balíčky na všechna sídla z původního sídla.

Využití odesílatelů je výhodné, jsou-li od sebe vaše sídla vzdálená, zejména nemají-li žádné osoby technické podpory. V takových případech můžete spolehlivě distribuovat software systému Windows na všechna sídla, aniž by to mělo vliv na další funkce probíhající ve vaší společnosti.

Sledování distribuce na všechna sídla

SMS automaticky odesílá po dokončení každého kroku zprávu o stavu. Pomocí pod-systému stavu SMS můžete tyto zprávy jednoduše sledovat.

Výběr počítačů

Protože zavádění inovací systému Windows 2000 je rozsáhlý, složitý a náročný proces, musíte jej rozdělit do etap. Tím se rozprostře jak aktivita v síti tak i požadovaná podpora. Také nemusí být všechny počítače připraveny na přijetí balíčku ve stejný čas; některé počítače například nemusí mít dostatečnou paměť nebo diskový prostor. SMS sbírá inventurní informace o vašich počítačích a umožňuje vám vytvářet dotazy vybírající odpovídající počítače. Rozsah výběrů můžete zvyšovat, jakmile získáte důvěru v celý proces.

Kolekce podrobností inventáře mohou automaticky zahrnovat všechny další počítače, které nyní splňují kritéria výběru. Představte si například kolekci definovanou tak, že zahrnuje počítače s 64 MB paměti nebo více. Přidáte-li klientskému počítači SMS, který měl paměť 32 MB, dalších 32 MB, pak bude schopen přijmout inovaci systému Windows 2000 a automaticky se přidá do dané kolekce.

Zabezpečené zajištění dostatečných práv operačního systému

Inovace operačního systému ovlivňuje všechny aspekty počítače, a proto vyžaduje, aby měli koncoví uživatelé rozsáhlá přístupová práva. Možná však váháte s udělením takových rozsáhlých oprávnění uživatelům, kteří nemají hluboké znalosti počítačů nebo důležitých zásad a procedur vaší společnosti. SMS má speciální privilegia a inovace může probíhat v jejich kontextu.

Automatická inicializace instalace

Inovace lze inicializovat automaticky nebo je mohou inicializovat uživatelé. Celý proces můžete nastavit tak, že i když bude zahrnovat uživatele, nebudou nuceni zadávat složité volby. Můžete dát uživatelům možnost řídit načasování, takže k inovaci může dojít v okamžiku, kdy svůj počítač nevyužívají.

Řešení problémů

Jestliže inovace na systém Windows 2000 způsobí problémy na nějakém počítači, můžete je vyřešit pomocí určitých funkcí SMS. Stavové a inventární informace zajišťované SMS vám mohou poskytnout mnoho podrobných údajů o daném počítači z centrálního dobře využitelného zdroje – konzoly SMS Administrator. Prostřednictvím nástrojů vzdálené správy SMS můžete vzdáleně řídit daný počítač, přenášet soubory a pracovat s počítačem jinými způsoby (pokud je jeho klient SMS funkční). Má-li uživatel nekompatibilní aplikaci nebo aplikaci, kterou by bylo lepší opakovaně nainstalovat, můžete ji automaticky inovovat nebo odstranit pomocí distribuce softwaru SMS.

Hlášení stavu

Stavové zprávy SMS se negenerují jen při distribuci balíčku, ale také při inzerování a instalaci na počítače uživatelů. Tato stavová hlášení můžete použít ke zjištění poměru a úspěchu zavádění.

Kroky potřebné k využití těchto funkcí SMS jsou popsány v následujících procedurách. Podrobné informace o aktivování odpovídajících podsystémů SMS a jejich efektivním využívání najdete v dokumentaci SMS.

Vytvoření balíčku systému Windows 2000 pro server Systems Management Server

Chcete-li použít k zavedení systému Windows 2000 server Systems Management Server, musíte vložit soubory Windows 2000 do balíčku SMS. Musíte vytvořit samostatné balíčky pro systémy Windows 2000 Server a Windows 2000 Professional. SMS 2.0 obsahuje předdefinované balíčky pro verze Windows 2000 Server a Professional. Ty lze použít jako výchozí při vytváření vašich vlastních balíčků systému Windows 2000.

SMS získává soubory všech balíčků z distribuční složky. Další informace o vytváření struktury distribučních složek najdete v kapitole „Automatizování instalace a inovace serveru“ v této knize. Musíte vytvořit takovou strukturu distribučních složek, jaká je popsána v uvedené kapitole, a zahrnout do ní všechny pomocné soubory potřebné k dokončení inovace, jako jsou například ovladače zařízení Plug-and-Play a soubory odpovědí. Můžete sem dokonce zahrnout standardní aplikace, jazykové doplňky a servisní balíčky.

Každý předdefinovaný balíček SMS systému Windows 2000 obsahuje také programy SMS. Každý program je různou kombinací voleb, které zadáváte pro instalaci balíčku Windows 2000. Například vašim výchozím programem může být instalace systému Windows 2000 bez účasti uživatele. Chcete-li umožnit zkušeným uživatelům některé volby, potřebují další program. Všechny takové programy SMS musí být kompatibilní se sadou souborů balíčku dostupných v distribuční složce.

Příprava balíčku inovace na systém Windows 2000 Server

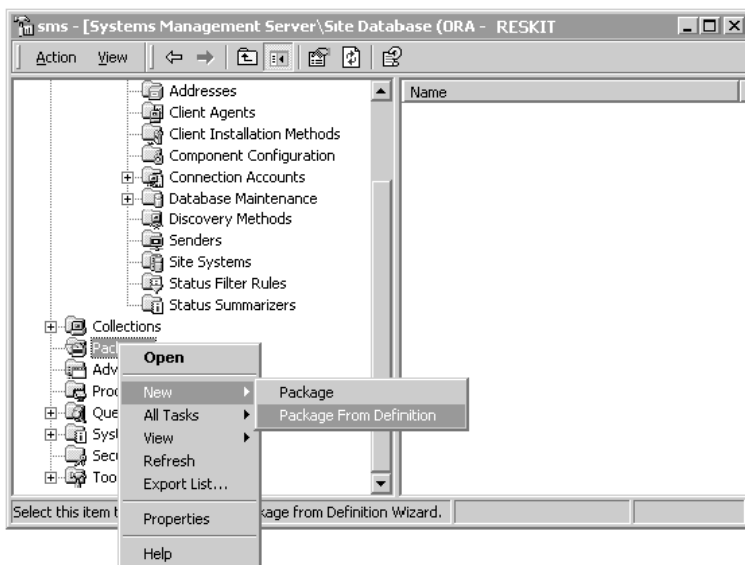
Následující procedura popisuje vytvoření typického balíčku inovace na systém Windows 2000 Server. Prvním krokem je nastavení umístění zdrojových souborů balíčku a předdefinovaného balíčku SMS určeného k distribuci systému Windows 2000 Server.

▼ **Chcete-li vytvořit balíček SMS systému Windows 2000 Server, postupujte takto:**

1. Nastavte umístění zdrojových souborů balíčku.

Tento proces je popsán v kapitole „Automatizování instalace a inovace serveru“ v této knize. Proces zahrnuje soubory systému Windows 2000, soubor odpovědí a další potřebné soubory.

2. V konzole SMS Administrator vyberte položku **Packages**. V nabídce **Akce** (Action) vyberte příkaz **Nový** (New) a pak zadejte **Package From Definition** (balíček z definice), jak ukazuje obrázek 14.3.



Obrázek 14.3 Spuštění průvodce Package from Definition SMS

3. V úvodním okně stiskněte tlačítko **Další** (Next). V seznamu **Package definition** (definice balíčku) vyberte položku **Windows 2000 Server**.
4. Na stránce **Source Files** (zdrojové soubory) vyberte **Create a compressed version of the source** (vytvořit komprimovanou verzi zdroje) a pak stiskněte tlačítko **Další** (Next). Do pole **Source directory** (zdrojový adresář) zadejte cestu ke zdrojovým souborům balíčku (viz krok 1). Stiskněte tlačítko **Další** (Next) a pak tlačítko **Dokončit** (Finish).

Je-li na serveru sídla velmi málo diskového prostoru, můžete na stránce **Source Files** (zdrojové soubory) zvolit položku **Always obtains files from a source directory** (vždy převzít soubory ze zdrojového adresáře). Tím se však zpomalují budoucí distribuce softwaru a navíc musíte zajistit, aby byl zdrojový adresář vždy k dispozici.

5. Po dokončení průvodce vyberte pod novým balíčkem položku **Programs** (programy). V podokně výsledků (na pravé straně konzoly) poklepejte na položku **Automated upgrade from NTS 3.51/4.0 (x86)** (automatizovaná instalace z NTS 3.51/4.0 (x86)). Pak ověřte, že předdefinovaný příkaz v poli **Command line** (pří-

kazový řádek) je správným instalačním příkazem, který potřebujete. Krok 5 zopakujte pro další používané programy.

Chcete-li prověřit, že předdefinované zadání v poli **Command line** (příkazový řádek) odpovídá vašim potřebám, přečtěte si oddíl „Prohlídka definice balíčku systému Windows 2000 Server“ dále v této kapitole.

Zvažte také zadání souboru odpovědí v příkazovém řádku, protože pak je možné zadat velké množství konfiguračních voleb. Další informace o souborech odpovědí najdete v kapitole „Automatizování instalace a inovace serveru“ v této knize.

6. Do pole **Comment** (komentář) zadejte komentář jednotlivých používaných programů.

Uživatelé vaše komentáře uvidí, takže buďte popisní. Předejte uživatelům kontaktní informace, například jméno, telefonní číslo nebo adresu elektronické pošty nějaké osoby, kterou mohou kontaktovat v případě, že budou potřebovat další informace.

7. Na kartě **Requirements** (požadavky) jednotlivých programů upravte (v případě potřeby) hodnoty **Estimated disk space** (odhadovaný diskový prostor) a **Estimated run time** (odhadovaný čas běhu) tak, aby odpovídaly vaší inovaci. Tyto hodnoty jsou informacemi pro uživatele.

8. Na kartě **Environment** (prostředí) jednotlivých programů prověřte, že položka **Program can run** (program může pracovat) je nastavena na **Whether or not a user is logged on** (je-li i není-li přihlášen uživatel).

Toto nastavení zajistí spuštění programu s právy správce, která jsou nezbytná pro inovace systému Microsoft Windows NT Server.

9. Dialogové okno vlastností programu zavřete stiskem tlačítka **OK**.

10. Vyberte balíček Windows 2000 Server a zadejte příkaz **Vlastnosti** (Properties) nabídky **Akce** (Action). Na kartě **Reporting** (hlášení) zadejte do pole **Version** (verze) hodnotu **5.0**. Zkontrolujte, že hodnota pole **Name** (název) je Windows NT a hodnota pole **Publisher** (vydavatel) je Microsoft.

Důležité Nastavení těchto hodnot je důležité pro zachování přesnosti stavových informací inzerování. Jinak se každé vykonání balíčku SMS označí za úspěšné, i když bude přerušeno nebo skončí chybou.

11. Dialogové okno vlastností balíčku zavřete stiskem tlačítka **OK**.
12. Chcete-li se ujistit, že uživatelé nebudou moci inovovat své počítače až do okamžiku, než budete na zavedení systému Windows 2000 připraveni, vyberte položku **Access Accounts** (účty přístupu) pod novým balíčkem a v podokně výsledků odstráňte účty přístupu **Guests** a **Users**.

Uvědomte si, že SMS neskrývá sdílené body distribuce softwaru a že uživatelé budou na svém počítači potřebovat práva správce (nebo na počítačích musí být systém Microsoft Windows 95 či Microsoft Windows 98), aby mohli těchto sdílených bodů využít.

Přístup uživatelům, kteří jsou oprávněni k inovaci na systém Windows 2000, budete muset zajistit později.

V této fázi také neupravujte distribuční body ani nevytvářejte inzerát.

Upozornění Chcete-li pomocí zabezpečení řídit, kdo může balíček upravit nebo zavést, přečtěte si kapitolu „Distribuce softwaru“ v knize *Systems Management Server 2.0 Administrator's Guide*.

Potřebujete-li různé varianty svých inovací zajistit použitím více souborů odpovědí inovací na systém Windows 2000, musíte v konzole SMS Administrator vytvořit další programy balíčku. Každý z takových programů bude mít přepínačem **/unattend** aplikace **winnt32** zadán jiný soubor odpovědí. Samostatné soubory odpovědí umožňují inovovat různé skupiny počítačů různými způsoby, přičemž se zároveň používá jen jeden balíček.

Systems Management Server 2.0 zahrnuje mnoho pokročilých voleb pro balíčky a jejich programy. Je například možné zadat, aby byly soubory systému Windows 2000 přístupné pod určitým názvem sdílení v distribučních bodech. Pak je mohou jednoduše používat lidé vykonávající ruční inovaci i server SMS. Dokumentace serveru SMS obsahuje podrobné informace o těchto volbách.

Umožnění zadání uživatelů během inovace

Většina správců SMS považuje za nejlepší neumožnit uživatelům žádná zadání během instalací balíčků. Když si uživatelé sami koupí a instalují nějaký software, instalační program od nich obvykle požaduje nějaké údaje, například na který disk se má instalovat nebo jaké jeho funkce se mají instalovat. Každé zadání uživatele představuje možnost chybné volby, která může způsobit problémy. Uživatelé nemusí vždy plně rozumět důsledkům zadávaných voleb. I když chybu udělá třeba jen malé procento uživatelů, v době inovací tisíců počítačů mohou požadavky na řešení problémů daleko převyšovat vaše možnosti.

Další důvod eliminace zadání uživatelů během inovace spočívá v umožnění instalace v okamžiku, kdy u počítače nikdo není, čímž se minimalizují nepříjemné důsledky pro uživatele.

Jestliže zadáte všechny odpovědi v souboru odpovědí, zajistíte tak udržení standardní konfigurace. Budete-li tyto standardy dodržovat, zjednodušíte budoucí údržbu a podporu počítačů, protože se omezí počet proměnných, které se mohou k nějakému problému vztahovat.

Vytvoříte-li soubor odpovědí se všemi podrobnostmi potřebnými k inovaci, instalační program systému Windows 2000 pak nebude požadovat žádné zadání od uživatelů. Jestliže nějaké podrobnosti nezadáte (a řádek **UnattendMode** v souboru odpovědí to umožňuje) nebo jestliže nepoužijete přepínač **/unattend** příkazového řádku, program se na tyto podrobnosti zeptá uživatele. Soubor odpovědí inovace serveru se může podobat tomu následujícímu (musíte změnit řádek **JoinDomain**):

```
[Unattended]
FileSystem = LeaveAlone
UnattendMode=FullUnattended
NTUpgrade=Yes
[Networking]
InstallDefaultComponents = Yes
[Identification]
JoinDomain = RED1DOM
```

Poznámka Soubor odpovědí musíte zadat použitím příkazu **winnt32 /unattend:soubor.odpovědí**. Příkaz **winnt32 /unattend** vykoná bezobslužnou inovaci, potřebné informace však získá z aktuální konfigurace.

Prohlídka definice balíčku systému Windows 2000 Server

Definice balíčku Windows 2000 Server, která je součástí serveru Systems Management Server 2.0, zahrnuje předdefinované programy. Chcete-li porozumět vykonávání inovací, seznamte se s těmito programy.

Inovace na systém Windows 2000 Server ze systému Windows NT Server zahrnuje přepínače **/unattend30** a **/batch**. Přepínač **/unattend30** znamená, že budete vykonávat bezobslužnou inovaci a že se všechny požadované informace převezmou ze stávající instalace. Počítač bude restartovat 30 sekund po dokončení první fáze instalačního programu, což znamená po skončení kopírování souborů na počítač. Soubor odpovědí se nepoužívá.

Přepínač **/batch** zadává, aby instalační program nezobrazoval chybová hlášení. Tento přepínač je užitečný, když posíláte balíček uživatelům, kteří se instalace nemusí účastnit, nebo spouštíte-li inovaci v okamžiku, kdy u daného počítače nikdo není. Pokud se však při instalaci vyskytnou nějaké problémy, například nedostatek volného prostoru na disku nebo nesprávný adresář **Start in**, pak to nebude hned zjevné, jelikož se nezobrazí žádná chybová hlášení.

Můžete ovšem také použít informace o chybách ze stavových zpráv SMS, které se vytvoří jako výsledek této operace. Jestliže se během testování setkáte s nějakými problémy a stavové zprávy vám nepostačují, odstraňte přepínač **/batch** a umožněte během testování balíčku zobrazování chyb. Také platí, že jestliže uživatel během první fáze instalačního programu systému Windows 2000 stiskne tlačítko **Storno** (Cancel), systém se jej už nebude ptát, zda chce instalační program ukončit.

Standardně je adresář **Start in** (kde začít) balíčku zadán jako **i386**. To je určeno pro případy, kdy zdroj balíčku obsahuje adresář i386 a zrcadlí tak CD-ROM systému Windows 2000. Jestliže však zdroj balíčku obsahuje jen soubory v adresáři i386 na CD-ROM a pod ním, není nutné zadávat adresář **Start in**.

Odhadované hodnoty diskového prostoru a času běhu zobrazené balíčky SMS verze 2.0 jsou skutečně jen odhady, které nemusí být ve vašem prostředí realistické. V některých případech budete muset tyto hodnoty zvýšit. Tyto hodnoty jsou pouze informační a slouží uživateli.

Na kartě **Environment** (prostředí) si všimněte, že se program spouští s právy správce zabezpečeně zajištěnými serverem SMS. To je důležitá výhoda při inovacích klientů se systémy Microsoft Windows NT Workstation na systémy Windows 2000 Professional. Tato funkce znamená, že nemusíte koncovému uživateli přiřazovat oprávnění správce. Může být také důležitá v případě, kdy servery vlastní organizační jednotky a kdy mají centrální správci potřebné práva na těchto serverech jen prostřednictvím SMS.

Jestliže do příkazového řádku programu balíčku vložíte soubor odpovědí, můžete pak zadat mnoho voleb inovace. Je pak například možné určit, na který disk se systém Windows 2000 nainstaluje nebo zda je zapotřebí vykonat inovaci či novou instalaci.

Příprava balíčku inovace na systém Windows 2000 Professional

Chcete-li inovovat počítače na systém Windows 2000 Professional pomocí SMS, musíte nejprve vytvořit balíček Windows 2000 Professional. Tento balíček se připravuje a používá podobným způsobem jako balíček systému Windows 2000 Server. Následující proceduru začněte, jako byste vytvářeli balíček Windows 2000 Server, nezapomeňte však zadat, že se jedná o balíček Windows 2000 Professional. Protože inovace systémů Windows 95 a Windows 98 na systém Windows 2000 přináší určité specifické problémy, musíte vytvořit nový program, jak je uvedeno v následujícím oddílu.

Poznámka Chcete-li pomocí SMS distribuovat také systém Windows 2000 Advanced Server, musíte vytvořit další samostatný balíček. Mnoho souborů a podrobností nastavení v tomto programu sice odpovídá prvkům systému Windows 2000 Server, existují tu však také rozdíly vyžadující, aby obě verze měly samostatné balíčky. Při vytváření balíčků distribuce jiných verzí systému Windows 2000 Server můžete použít jako startovací bod balíček verze pro systém Windows 2000 Server.

Inovace systému Windows 95 a Windows 98

Kromě odlišností ve zdrojových souborech je dalším významným rozdílem mezi inovacemi na systémy Windows 2000 Server a Windows 2000 Professional soubor odpovědí při inovaci klientů Windows 95 nebo Windows 98 na systém Windows 2000 Professional. Počítače se systémy Windows 95 nebo Windows 98 nebyly členy domény (i když se uživatelé s nimi pracující třeba přihlašovali k doméně) a neměly místní účty (i když třeba obsahovaly soubory místních profilů a seznamů hesel). Proto je zapotřebí v souboru odpovědí zadat určité podrobnosti, mezi které patří i následující body (musíte změnit hodnoty **JoinDomain**, **DomainAdmin** a **DomainAdminPassword**):

```
[Unattended]
FileSystem = LeaveAlone
UnattendMode=FullUnattended
Win9xUpgrade=Yes
[Networking]
InstallDefaultComponents = Yes
[GUIUnattended]
AdminPassword=Test123
[Identification]
JoinDomain = RED1
DomainAdmin = AddComputers
DomainAdminPassword = Restricted
```

Počítač, inovovaný na systém Windows 2000 ze systému Windows 95 nebo Windows 98, obdrží místní účet Administrator. Tento účet vyžaduje heslo, které je možné zadat v oddílu **GUIUnattended** souboru odpovědí nebo lze vyzvat k jeho zadání uživatele na konci inovace. Toto heslo si může v souboru odpovědí přechytit kdokoli s přístupem do bodu sdílení balíčku SMS, což je obvykle většina uživatelů. Není to významné ohrožení zabezpečení, protože počítače se systémy Windows 95 a Windows 98 nebyly před inovací vůbec zabezpečené, což je dáno povahou těchto operačních systémů.

Možná budete chtít nastavit heslo správce na nějakou zabezpečenou hodnotu a začít se zaváděním omezených privilegií správce. To můžete učinit po inovaci spuštěním programu, který nastavuje heslo na hodnotu sdílenou pouze mezi autorizovanými osobami. Heslo se v programu zkompileje a neoprávněným osobám není přístupné. Tako-

vé programy můžete jednoduše vytvořit pomocí obvyklých programovacích nebo skriptových nástrojů, jako je například SMS Installer. Program pak můžete distribuovat pomocí SMS nebo jej můžete vyvolat na konci inovace systému Windows 2000 zadáním odpovídajících údajů do souboru odpovědí.

Třebaže počítače se systémy Windows 95 a Windows 98 nejsou členy domén, počítače se systémem Windows 2000 musí být členy domén. Proto musíte do souboru odpovědí zahrnout řádek **JoinDomain** a určit tak, k jaké doméně se má počítač připojit spolu s účtem a heslem správy s oprávněním připojit počítače do dané domény.

Upozornění Soubory odpovědí mohou číst i neoprávněné osoby, proto při jejich vytváření musíte vzít v potaz také otázky zabezpečení. Je však nepravděpodobné, že by lidé přistupovali k souborům balíčku distribučního dobo SMS, protože distribuční body jsou skryté a lidé musí vědět, kde tyto podrobnosti hledat. Vhodným opatřením je však použít účet správy, jehož jediným právem je přidávat pracovní stanice do domény (**Add workstations to domain**). Dalším opatřením je přidat počítače inovované tímto způsobem k dedikované doméně prostředků. Pak musí mít účet správy práva pouze v dané doméně, a proto nemůže způsobit problémy v jiných doménách, v nichž máte třeba ovladače domén účtů nebo jiné citlivé počítače.

Soubor odpovědí musí také určovat, že chcete inovovat počítače se systémy Windows 95 nebo Windows 98. Toho docílíte vložením následujícího řádku do souboru odpovědí:

```
Win9xUpgrade=Yes
```

Bez tohoto řádku vykonáte čistou instalaci a nikoli inovaci systému na Windows 2000. Během inovace systému Windows 95 nebo Windows 98 na systém Windows 2000 odstraňuje instalační program Windows 2000 programy, u nichž má podezření na nekompatibilitu s Windows 2000. K tomu dochází i u některých klientských komponent SMS 2.0. Systém Windows 2000 nabízí nástroj nazvaný knihovny DLL migrací, který migraci takových programů zjednodušuje. Další informace o knihovnách DLL migrací najdete v odkazu Microsoft Systems Management Server na stránce webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Inovace systému Windows NT Workstation

Inovace systému Windows NT Workstation na systém Windows 2000 je v porovnání s inovací systémů Windows 95 a Windows 98 mnohem jednodušší. To je dáno tím, že systémy Windows NT Workstation a Windows 2000 Professional mají mnohem více společného. Z toho důvodu je možné vykonat inovaci systému Windows NT Workstation bez použití souboru odpovědí nebo jen s jeho minimální verzí.

Je důležité podívat se na nastavení vlastností **Environment** (prostředí) daného programu SMS, aby bylo zaručeno jeho spuštění s právy správce. To není nutné, budou-li v okamžiku inicializace balíčku na klientských počítačích přihlášení uživatelé s právy správce.

Distribuce balíčků systému Windows 2000

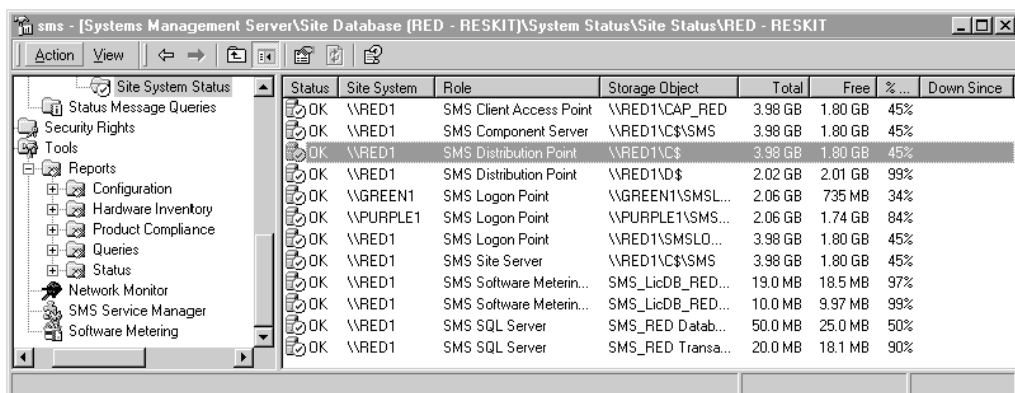
Soubory balíčku SMS systému Windows 2000 musíte distribuovat na všechna sídla, kde očekáváte inovaci nějakých počítačů. Distribuce je zapotřebí, i když jde třeba jen o jedno sídlo. Distribuce se skládá z odeslání souborů balíčku na dané sídlo a následném přesunu souborů SMS do distribučních bodů v rámci daného sídla.

Příprava na distribuci balíčků

Před distribuováním balíčků systému Windows 2000 musíte vykonat několik úkolů, jejichž prostřednictvím zajistíte, že je vaše hierarchie SMS připravena na jejich přijetí.

Kontrola stavu serverů sídel a distribučních bodů

Systém Windows 2000 je poměrně velký a vyžaduje značné místo na disku. Kopie systému Windows 2000 nejsou zapotřebí jen pro inovované počítače, ale SMS potřebuje kopie také v okamžiku přesouvání balíčků mezi servery. Proto musíte prověřit své servery sídel a distribuční body a zajistit, aby měly dostatek diskového prostoru. Nejsnáze toho dosáhnete prostřednictvím položky **System Status** (stav systému) konzoly SMS Administrator, výběrem položky **Site Status** (stav sídla) a následným klepnutím na položku **Site System Status** (stav systému sídla) jednotlivých sídel (viz obr. 14.4). Podokno výsledků zobrazuje distribuční body a jejich volný diskový prostor.



Status	Site System	Role	Storage Object	Total	Free	%...	Down Since
OK	\\RED1	SMS Client Access Point	\\RED1\\CAP_RED	3.98 GB	1.80 GB	45%	
OK	\\RED1	SMS Component Server	\\RED1\\C\$\\SMS	3.98 GB	1.80 GB	45%	
OK	\\RED1	SMS Distribution Point	\\RED1\\C\$	3.98 GB	1.80 GB	45%	
OK	\\RED1	SMS Distribution Point	\\RED1\\D\$	2.02 GB	2.01 GB	99%	
OK	\\GREEN1	SMS Logon Point	\\GREEN1\\SMSL...	2.06 GB	735 MB	34%	
OK	\\PURPLE1	SMS Logon Point	\\PURPLE1\\SMS...	2.06 GB	1.74 GB	84%	
OK	\\RED1	SMS Logon Point	\\RED1\\SMSLO...	3.98 GB	1.80 GB	45%	
OK	\\RED1	SMS Site Server	\\RED1\\C\$\\SMS	3.98 GB	1.80 GB	45%	
OK	\\RED1	SMS Software Meterin...	SMS_LicDB_RED...	19.0 MB	18.5 MB	97%	
OK	\\RED1	SMS Software Meterin...	SMS_LicDB_RED...	10.0 MB	9.97 MB	99%	
OK	\\RED1	SMS SQL Server	SMS_RED Datab...	50.0 MB	25.0 MB	50%	
OK	\\RED1	SMS SQL Server	SMS_RED Transa...	20.0 MB	18.1 MB	90%	

Obrázek 14.4 Stav sídel s distribučními body a jejich volným diskovým prostorem

Kontrola odpovídajícího počtu distribučních bodů na jednotlivých sídlech

Můžete také omezit počet inovací systému Windows 2000, které chcete současně vykonávat v jednom sídle. Inovace mohou představovat vysoké zatížení místní sítě a distribučních bodů. Ještě před inovací je tedy zapotřebí experimentovat v laboratoři nebo spustit pilotní program. Během testování použijte servery, které jsou pro vaše distribuční body typické, a pracujte také v typické síti. Pak můžete odhadnout, kolik klientů je možné bez problémů inovovat najednou.

Zjistíte-li, že nejužším místem inovací není vaše síť ale distribuční body, zvažte přidání dalších distribučních bodů na sídlo. Další informace o přidávání distribučních bodů najdete v kapitole „Distributing Software“ v knize *Systems Management Server Administrator's Guide*.

Použijte skupiny distribučních bodů

Protože balíček systému Windows 2000 je poměrně rozsáhlý a bude se hodně využívat, zajistěte vyhrazení distribučních bodů pro tento balíček. Na tyto distribuční body se pak můžete odkazovat jako na skupinu. Chcete-li snížit množství úkonů správy, můžete pro distribuční body systému Windows 2000 vytvořit skupinu distribučních bodů.

Skupiny distribučních bodů lze vytvářet (nebo přidávat či odstraňovat distribuční body ze skupiny) v okamžiku, kdy vytváříte nebo upravujete distribuční body. Během distribuce pak můžete do stejných míst, jako zadáváte distribuční body, zadat také skupiny distribučních bodů.

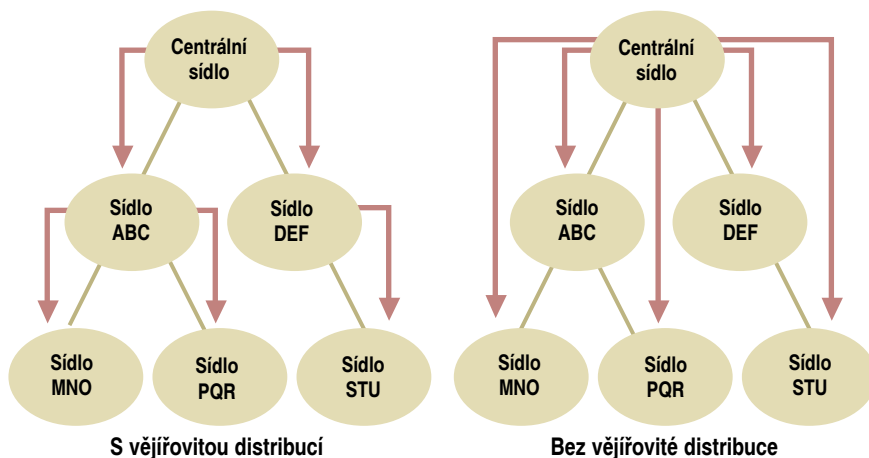
Zajistěte správné ovládací prvky odesilatele

Odesíláte-li balíček Windows 2000 na nějaké sídlo, na němž nejsou instalovány odpovídající ovládací prvky odesilatele, může dojít k přetížení síťového propojení v okamžiku, kdy to nepříjemně ovlivní další normální funkce sítě. Proto zkontrolujte ovládací prvky odesilatele a ujistěte se o jejich správném nastavení.

Konzola SMS Administrator obsahuje definice adres SMS jednotlivých sídel. Adresy SMS zahrnují název serveru SMS sídla, podrobnosti zabezpečení přístupu k danému sídlu a podrobnosti o síťovém přenosu (je-li to zapotřebí). Adresy také obsahují plán určující, kdy lze vykonat přenosy vysoké, střední a nízké důležitosti a jaká část síťového propojení může být během dne použita.

Zajistěte správnou funkci vějířovité distribuce

Systems Management Server 2.0 má funkci nazvanou vějířovitá distribuce, která umožňuje podřazeným sídlům distribuovat software na nižší úroveň sídel. Tím se snižuje zatížení sídla, z něhož distribuce softwaru pochází, protože software se pak nemusí distribuovat z původního sídla na všechna ostatní sídla. Tím se také omezuje zatížení síťových propojení mezi inicializačním sídlem a ostatními sídly, což je často největší problém. Distribuuje-li software na mnoho sídel, pak několikanásobné kopírování systému Windows 2000 přes síť z libovolného sídla může představovat neúnosně vysoké zatížení. Obrázek 14.5 ukazuje rozdíly mezi distribucí softwaru vějířovitou metodou a tradičním způsobem.



Obrázek 14.5 Dva typy distribuce softwaru

Vějířovitá distribuce se uskutečňuje automaticky, nemá-li inicializační sídlo adresu SMS cílového sídla. Proto musíte použít konzolu SMS Administrator, zkontrolovat adresy SMS a ujistit se, že jediný server SMS s adresou určitého sídla je jeho nadřazeným sídlem.

Vyberte testovací sídlo

Chcete-li se ujistit, že je váš plán kompletní, distribuujte balíček systému Windows 2000 na testovací sídlo nebo menší počet sídel. Teprve později jej odešlete do celé organizace. To vám umožní rychle opravit problémy a minimalizovat jejich dopad.

Testovací sídlo nebo sídla by měla být co nejtypičtější, alespoň jedno sídlo by však mělo představovat vysoce riskantní scénář. Příklady takového scénáře jsou zavádění se serverem sídla nebo distribučními body, které mají k dispozici jen velmi málo diskového prostoru nebo mají výjimečně pomalé či nespolehlivé síťové propojení.

Nejlepší je na této úrovni testování začít s malými sídly, jejichž požadavky nejsou složité. Ideální testovací sídlo má specialisty technické podpory, kteří jsou stále připraveni, a uživatele, kteří s vašimi cíli souhlasí. Na takových sídlech můžete určit řešení všech problémů, které jste třeba do svých kontingenčních plánů během plánování zavádění nezahrnuli. Jakmile získáte větší důvěru v celý proces, přeneste své testování na sídla, která jsou větší, složitější, nebo jejichž podpora je obtížnější.

Během fáze distribuce musí být vaše zavádění systému Windows 2000 pro uživatele transparentní, protože jste na jejich počítačích ještě inovaci nespustili. Proto musíte být opatrní nyní a zejména v pozdějších fázích procesu zavádění.

Další informace o úkolech naznačených v tomto oddílu najdete v knize *Systems Management Server Administrator's Guide*.

Distribuce balíčků na sídla a distribuční body

Základní procedura distribuce balíčků je uvedena dále. Při vykonávání tohoto úkolu budou na seznamu uvedeny všechny distribuční body na všech sídlech, takže můžete vybrat všechny zamýšlené distribuční body najednou. Zajistěte však nejprve distribuci

balíčku na malý počet sídel, abyste mohli otestovat svou infrastrukturu a procedury SMS. Jakmile získáte větší důvěru v celý proces, můžete zahrnout další distribuční body na jiných sídlech. Další informace o této proceduře najdete v kapitole „Distributing Software“ v knize *Systems Management Server Administrator's Guide*.

▼ **Chcete-li distribuovat balíček SMS systému Windows 2000 Server, postupujte takto:**

1. V konzole SMS Administrator vyberte položku **Packages** (balíčky) a daný balíček Windows 2000. Pak vyberte položku **Distribution Points** (distribuční body).
2. Z nabídky **Akce** (Action) zadejte **Nový** (New) a pak vyberte příkaz **Distribuční body** (Distribution Points).
3. Objeví se průvodce novými distribučními body (**New Distribution Points**).
4. Úvodní obrazovku přeskočte stiskem tlačítka **Další** (Next) a pak vyberte distribuční body, které chcete použít.

Pokud se jedná o testovací distribuci, vyberte určené distribuční body. Používáte-li skupiny distribučních bodů, vyberte. Všimněte si, že jsou tu uvedeny všechny distribuční body všech sídel. Nyní tedy máte možnost vybrat všechny zamýšlené distribuční body. Můžete také vybrat jen omezený počet distribučních bodů a mít tak lepší kontrolu nad provozem v síti.

5. Distribuci spusťte stiskem tlačítka **Dokončit** (Finish).

Upozornění Distribuční proces začne po stisku tlačítka **Dokončit** (Finish) v kroku 4. Možná si všimnete určitého zpoždění, které je dané zpracováváním v systému, prioritami balíčků či plány odesílatele, buďte však připraveni na okamžitou aktivitu SMS.

Další informace o toku balíčku po iniciování distribuce najdete v kapitole „Software Distribution Flowcharts“ v knize *Microsoft Systems Management Server 2.0 Resource Guide* (která je součástí sady *Microsoft BackOffice 4.5 Resource Kit*). Soubory systému Windows 2000 se zkomprimují do jediného souboru, který se pak odešle podřízeným sídlům. V jednotlivých sídlech může být balíček odeslán dalším podřízeným sídlům, mají-li distribuční body daného balíčku.

Testování distribuce

Po započetí distribuce balíčků systému Windows 2000 zkontrolujte, že se správně zavádějí do distribučních bodů. Následující oddíl „Sledování distribuce“ popisuje, jak můžete prověřit, zda všechny balíčky dorazily na všechny distribuční body, a jak lze rychle identifikovat problémy. Distribuce však ještě musíte prověřit a ujistit se, že jsou úplné a že jsou správně vytvořené adresářové stromy. V tomto okamžiku sice nemusíte kontrolovat všechny distribuční body, alespoň v několika z nich však prověřte, že distribuce funguje podle vašich záměrů.

Rozšíření distribuce

Jakmile je úspěšně dokončena první distribuce balíčku, můžete balíček distribuovat na další sídla a distribuční body. Procedura je úplně stejná, můžete však odesílat balíček častěji na více distribučních bodů najednou a nemusíte celý proces tak důkladně kontrolovat. Rozhodně však musíte balíčky distribuovat na daná sídla ještě před inzerováním balíčku uživatelům na těchto sídlech. Server SMS nezpřístupní inzerování klientům do okamžiku, než je distribuční bod přístupný.

Distribuce pomocí fyzického dopravce

Síťová propojení na některá z vašich sídel mohou být pomalá nebo nespolehlivá, popřípadě již plně vytížená jiným síťovým provozem. Z těchto důvodů nemusí být odesílání tak velkého balíčku jako je systém Windows 2000 přes taková síťová propojení přijatelné. Server SMS 2.0 zahrnuje alternativního odesílatele, označovaného jako Courier Sender, který zajistí všechny výhody distribuce softwaru prostřednictvím SMS, ale bez nadměrného síťového provozu, který je obvyklou součástí přenosu balíčků na sídla.

Nástroj Courier Sender zkopíruje balíček SMS na CD-ROM nebo jiné podobné médium, které se pak odešle poštou nebo přepravcem na vaše sídla. Na sídlech někdo vloží doručený disk CD-ROM do serveru sídla a spustí jednoduchý program. Od tohoto okamžiku probíhá distribuce softwaru jako obvykle. Inzeráty, stavové informace a další informace budou proudit sítí v zadaných časech, tento provoz je však vzhledem k provozu potřebnému k přenosu samotného balíčku velmi malý.

Sledování distribuce

Kompletní distribuce systému Windows 2000 v organizaci s mnoha síťovými sídly může trvat poměrně dlouho. U některých sídel bude distribuce trvat déle, protože mají třeba pomalejší připojení do rozsáhlých sítí (WAN), jejich spolehlivost je nižší, je jinak nastaveno časové plánování odesílatele atd. Existuje také možnost, že i přes dobrou přípravu může být na některých sídlech nebo distribučních bodech v okamžiku příchodu balíčku nedostatek diskového prostoru. Z těchto důvodů je důležité dát distribuci systému Windows 2000 dostatek času na úplné dokončení. Distribuci pozorně sledujte a dávejte pozor na problémy vyžadující nějaké řešení. Ještě se přesvědčte, že distribuce byla dokončena na všech sídlech.

Podsystém System Status

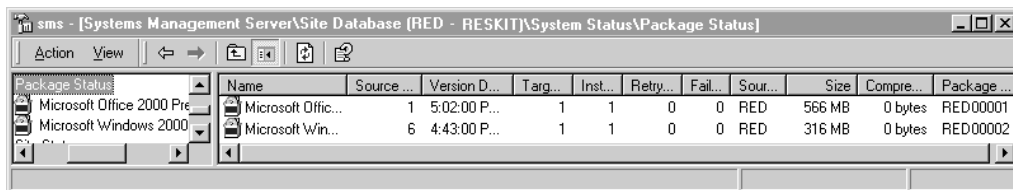
SMS 2.0 obsahuje výkonný podsystém stavu systému System Status, který slouží ke sledování distribuce. Konzola SMS Administrator obsahuje uzel System Status (stav systému), kde najdete celkové i podrobné výsledky podsystému System Status. Stav distribuce balíčku lze získat také v poduzlu Package Status (stav balíčku).

Poznámka Při vytvoření balíčku se definice daného balíčku okamžitě distribuuje na všechna podřízená sídla. V tomto okamžiku se však nedistribují vlastní soubory balíčku, pokud nějaké vůbec existují. Stejná definice balíčku se opakovaně odešle při aktualizaci definice balíčku. Pak jsou k dispozici stavové informace o distribuci definice balíčku. Proto při prohlížení stavu balíčku rozlišujte mezi distribucí definice balíčku a souborů balíčku.

Stav distribuce softwaru se shrnuje na několika dále uvedených úrovních:

Package Status pro všechny balíčky

Vyberete-li položku **Stav balíčku** (Package Status) pod **Stav systému** (System Statusu), uvidíte (viz obr. 14.6), kolik distribučních bodů je cílem jednotlivých balíčků a kolik z nich již bylo instalováno, kolik se o instalaci opakovaně pokouší a kolik neuspělo. Tato úroveň je užitečná k určení, kolik distribučních bodů, pokud nějaké, potřebuje intervenci z vaší strany. Všimněte si rozdílů velikostí původního a zkomprimovaného balíčku. K určitým účelům, například pro řešení problémů, může být také užitečné identifikační číslo balíčku.

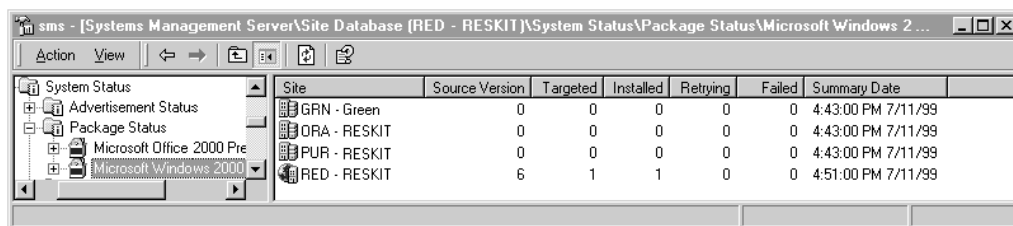


Obrázek 14.6 Stav všech balíčků

Na této úrovni nejsou žádné stavové zprávy, na které byste se mohli dotazovat.

Package Status pro určitý balíček

Pod položkou **Stav balíčku** (Package Status) pro všechny balíčky můžete vybírat jednotlivé balíčky. Na této úrovni vidíte (viz obr. 14.7), která sídla už balíček mají nebo nemají a která potřebují nějakou intervenci. Pomocí sloupce **Verze zdroje** (Source Version) si také můžete ověřit, že všechna sídla mají stejnou verzi balíčku.

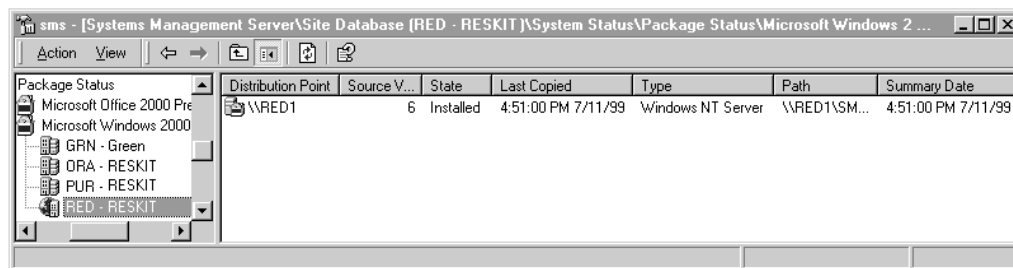


Obrázek 14.7 Stav balíčku systému Windows 2000 na všech sídlech

Na této úrovni si můžete rozevřít nabídku **Akce** (Action) a zadat Show Messages, **zobrazit zprávy, všechny** (Show Messages, All). Uvidíte všechny stavové zprávy daného balíčku ze všech sídel a distribučních bodů. To může představovat velké množství zpráv, a proto je lepší dívat se na zprávy po jednotlivých sídlech.

Package Status na sídlech

Pod položkou **Package Status** (stav balíčku) pro určitý balíček si můžete zobrazit jednotlivá sídla. Tato úroveň kontroly stavu vám umožňuje zobrazit si (viz obr. 14.8), které specifické distribuční body v síťovém sídle mají problémy s distribucí.



Obrázek 14.8 Stav balíčku systému Windows 2000 na určitém sídle

Na této úrovni si můžete rozevřít nabídku **Akce** (Action) a zadat **Zobrazit zprávy, všechny** (Show Messages, All). Uvidíte všechny stavové zprávy daného balíčku z daného sídla a jeho distribučních bodů. Následující sekvence zpráv je typická (zprávy z daných distribučních bodů jsou uvedeny v dalším oddílu):

- 30000 nebo 300001 – balíček byl vytvořen nebo upraven
- 30003 – program byl vytvořen
- 2300, 2310 a 2311 – správce distribuce připravuje balíček
- 2339 – správce distribuce inicializuje časový plán a odesílatele, aby mohl odeslat informace o balíčku (nikoli soubory balíčku)
- 30009 – distribuční bod byl přiřazen
- 2333 – příprava na odeslání zkomprimovaného obrazu balíčku
- 2335 – správce distribuce inicializoval časový plán a odesílatele, aby mohl odeslat soubory balíčku na sídla
- 2315 – správce distribuce odstranil komprimovaný obraz balíčku

Při kontrole stavových zpráv si všimněte, že jednotlivé sekvence činností správce distribuce (Distribution Manager) končí zprávou 2301, která indikuje úspěšné vykonání sekvence. Tato zpráva se objeví, kdykoli správce distribuce dokončí nějaké činnosti. Správce distribuce je komponenta SMS, která distribuuje balíčky ze serveru sídla na distribuční body SMS a inicializuje odesílání balíčku na další sídla.

Package Status na distribučních bodech

Pod položkou **Stav balíčku** (Package Status) pro určité sídlo si můžete zobrazit jednotlivé distribuční body. Na této úrovni si můžete rozevřít nabídku **Akce** (Action) a zadat **Zobrazit zprávy, všechny** (Show Messages, All). Uvidíte všechny stavové zprávy daného balíčku z daného distribučního bodu. Následující sekvence zpráv je typická:

- 2317 – správce distribuce obnovuje balíček na distribučním bodě (nezobrazuje se při prvním odeslání balíčku na distribuční bod)
- 2342 – správce distribuce začíná distribuovat balíček na distribuční bod
- 2322 – správce distribuce dekomprimoval balíček do dočasného adresáře (v některých případech)
- 2329 – správce distribuce zkopíroval balíček z dočasného adresáře nebo zdroje distribuce na distribuční bod
- 2330 – správce distribuce úspěšně distribuoval balíček na distribuční bod

Poznámka V knize *Systems Management Server Resource Guide* se nachází kapitola „Status Messages“, která uvádí všechny stavové zprávy a jejich úplný text.

Hlášení stavu distribuce balíčku

Třeba byste rádi vytvořili hlášení o stavu distribuce balíčku, ať už pro svou pohodlnou orientaci nebo v zájmu naplnění jiných svých požadavků. Můžete zadávat dotazy na třídy stavu distribuce balíčku a výsledky ukládat do nějakého nástroje sestav, podobně jako je tomu i u dalších nástrojů sestav SMS. Tabulka 14.1 uvádí odpovídající třídy a kategorie stavových informací, které v jednotlivých třídách najdete.

Tabulka 14.1 Třídy stavu distribuce balíčku

Třída	Stavová informace
SMS_PackageStatus	Celkové informace přehledu o stavu balíčků na distribučních bodech.
SMS_PackageStatus RootSummarizer	Informace o stavu daného balíčku. Připojuje se k položce Package Status v konzole SMS Administrator.
SMS_PackageStatus DetailsSummarizer	Podrobné informace o stavu daného balíčku podle kódu sídla. Připojuje se ke stromu konzoly balíčku pod položkou Package Status v konzole SMS Administrator.
SMS_PackageStatus DistPointsSummarizer	Podrobné informace o stavu daného balíčku na daném sídle. Připojuje se ke kódu sídla pod stromem konzoly balíčku pod položkou Package Status v konzole SMS Administrator.

Řešení problémů s distribucemi

Sledování distribuce softwaru vám naznačí, zda došlo v nějakém okamžiku k problémům s distribucí. Obvykle je to způsobeno nedostatkem diskového prostoru, potížemi se síťovým připojením nebo problémy se serverem. Takové problémy označuje text stavové zprávy.

Určení problému je vždy prvním krokem při řešení všech technických problémů. Jakmile víte, v jaké komponentě došlo k chybě, můžete se zaměřit na další odpovídající problémy. Pomocí výše popsaných sledovacích technik můžete problém lokalizovat. Součástí kapitoly „Software Distribution Flowcharts“ knihy *Systems Management Server Resource Guide* jsou vývojové diagramy znázorňující typický tok procesu distribuce softwaru. Zjistíte-li, že se vaše distribuce softwaru k nějakému bodu nedostala, je velmi pravděpodobné, že k chybě došlo v předchozím bodu vývojového grafu.

Jakmile přijdete na určitou komponentu, pomůže vám ke zjištění důvodů jejího selhání porozumění její funkci. S tím vám také pomůže vývojový graf. Navíc vám soubory protokolů mohou naznačit, co se s komponentou děje na velmi nízké úrovni, a tedy i co nefunguje. Protokolování se povoluje pomocí nástroje SMS Service Manager.

Také kapitola „Software Distribution Flowcharts“ knihy *Systems Management Server 2.0 Resource Guide* obsahuje typy řešení problémů při distribuci softwaru.

Inzerování balíčků systému Windows 2000

Uživatelé mohou inovovat počítače na systém Windows 2000 v okamžiku, kdy obdrží inzerát. Inzeráty obsahují popisné informace o balíčku pro koncové uživatele a zahrnují také podrobnosti nezbytné k tomu, aby server SMS mohl spouštět programy. Inzeráty lze dokonce nastavit tak, aby se spustily v určitém čase, aby uživatel nemohl zablokovat inovaci nebo aby mohlo k inovaci dojít v okamžiku, kdy uživatel u počítače není.

Výběr inovovaných počítačů

Inzerát říká serveru SMS, aby zpřístupnil kolekci SMS určitý program v balíčku. Kolekce je velmi flexibilní definice počítačů, uživatelů a skupin uživatelů. V případě distribuce softwaru Windows 2000, použijete nejprve kolekce obsahující malý počet počítačů určených pro účely testování. Později budete pracovat s kolekcemi představujícími všechny počítače připravené na systém Windows 2000. Kolekci lze dále rozdělit podle síťových sídel nebo organizačních jednotek.

Další výhodou kolekcí je, že jsou dynamické. V průběhu času můžete do kolekce přidávat počítače a všechny inzeráty dostupné dané kolekci se automaticky zpřístupní i nově přidaným počítačům. Vychází-li kolekce například z paměťové kapacity počítačů, počítače se do kolekce přidávají v okamžiku, kdy jejich hardware odpovídá požadavkům systému Windows 2000. Nainstalujete-li do počítače další paměť, inventář hardwaru SMS to zjistí a zaznamená v rámci SMS. Takový počítač se pak automaticky přidá do určité kolekce, a proto mu bude přístupná inovace na systém Windows 2000. Kromě části fyzického přidání paměti do počítače je celý proces automatický.

Další informace o určení, které počítače ve vaší organizaci jsou připraveny na inovaci, najdete v kapitole „Analýza infrastruktury sítě pomocí serveru Systems Management Server“ v této knize. To zahrnuje definování dotazů výběru počítačů z inventáře spravovaného serverem SMS. Takové dotazy lze používat k vytváření kolekcí, jak popisuje následující procedura. SMS také nabízí ukázkovou sestavu „Windows 2000 Upgrade Candidates by Site and Roles“, která vám může s tímto procesem pomoci.

▼ Chcete-li vytvořit kolekci počítačů připravených na inovaci na systém Windows 2000, postupujte takto:

1. V konzole SMS Administrator vyberte položku Kolekce (**Collections**).
2. V nabídce **Akce** (Action) ukažte na příkaz **Nový** (New) a potom zvolte **Collection**.
3. V dialogovém okně **Vlastnosti kolekce** (Collection Properties) zadejte název kolekce.
4. Na kartě **Pravidla členství** (Membership Rules) stiskněte tlačítko **New Query Rule** (nové pravidlo dotazu).
5. V okně **Vlastnosti pravidla dotazu** (Query Rule Properties) stiskněte tlačítko **Browse** (procházet) a vyberte příslušný dotaz.

Můžete použít například předem vytvořený dotaz sloužící k vytvoření sestavy počítačů, které lze inovovat na systém Windows 2000. (Pomoc s vývojem takového dotazu najdete v kapitole „Analýza infrastruktury sítě pomocí serveru Systems Management Server“.) Můžete samozřejmě použít i jiné dotazy, například pro výběr všech systémů Windows 95 (**All Windows 95 Systems**) nebo dotazy, které jste nadefinovali tak, aby zahrnuly všechny počítače na daných síťových sídlech.

6. Podle potřeby přidejte pravidla dotazu a pravidla přímého členství.

Alternativně můžete v kroku 4 stisknout tlačítko **New Direct Rule** (nové pravidlo přímého členství) a počítače, které chcete inovovat, pak zadat pomocí průvodce vytvoření pravidla přímého členství (Create Direct Membership Rule). Tato volba je nejlepší během testování, zejména máte-li jen malý počet přesně vybraných počítačů, na nichž chcete balíček spustit.

Musíte také zvážit skutečnost, že SMS 2.0 umožňuje, aby kolekce obsahovaly počítače, uživatele a skupiny uživatelů. Použití uživatelů nebo skupin uživatelů v případě systému Windows 2000 však nemusí být vhodné, protože uživatelé se často mohou přihla-

šovat na různé počítače. Pak by bylo možné inovovat každý počítač, na který se daný uživatel přihlásí, zejména je-li inzerát nastaven tak, že se spustí až to uživatel chce nebo nechce. Počítače, na které se takoví uživatelé přihlašují, však nemusí být připraveny na inovaci nebo jejich obvyklí uživatelé nemusí být proškoleni v obsluze systému Windows 2000.

Upozornění Další informace zabezpečeném řízení toho, kdo může inzerát upravit nebo používat, najdete v kapitole „Distributing Software“ v knize *Systems Management Server Administrator's Guide*.

Příprava klientů na příjem inzerátů

Počítače, na které budete inzerát směřovat, musí být na inzerát připraveny. Během inovace na systém Windows 2000 bude počítač muset několikrát restartovat. Může-li k tomu dojít automaticky, celou inovaci lze vykonat bez zadání od uživatelů.

Někteří uživatelé své počítače chrání spouštěcím heslem. Toto heslo požaduje samotný počítač, a proto jej software nemůže obejít. Počítač se spuštěním počká až na zadání tohoto hesla a inovace systému Windows 2000 proto nemůže pokračovat. Proto uživatelům oznamte, aby dočasně zrušili svá hesla spuštěním počítače. Není-li to možné, někdo bude muset být během inovace u počítače přítomen. Tentýž problém nastává v případech, kdy počítač požaduje potvrzení restartu, kvůli změnám konfigurace hardwaru a jiným záležitostem.

Uživatelé však inovaci na upozorněte, aby stačili zavřít všechny dokumenty. Budou-li uživatelé vědět, že inovace proběhne zanedlouho, spíše se také zúčastní školení o novém systému, vykonají zálohování svých dat a připraví si programy, za které zodpovídají.

Inzerujete-li balíček s takovým přiřazením, aby k inovaci došlo v noci nebo o víkendu, musí být na klientských počítačích se systémy Windows 95 a Windows 98 přihlášen nějaký uživatel. Jen tak může dojít k automatickému spuštění inzerátu. Tito uživatelé mohou také používat zabezpečený spořič obrazovky zabráňující jiným osobám v použití počítače v jejich nepřítomnosti. Na klientských počítačích systému Windows NT nemusí být přihlášen žádný uživatel a inzerát se přesto spustí.

Inzerování balíčků počítačům

Nyní máte připraven balíček systému Windows 2000 na distribuci, máte vybrané správné počítače, a počítače jsou připravené na inovaci. Dalším krokem je iniciování procesu. To učiníte vytvořením inzerátu, jak ukazuje následující postup.

▼ Chcete-li vytvořit inzerát systému Windows 2000, postupujte takto:

1. V konzole SMS Administrator vyberte položku **Advertisements** (inzeráty).
2. V nabídce **Akce** (Action) ukažte na příkaz **Nový** (New) a potom zvolte **Inzerát** (Advertisement)..
3. V seznamu **Balíček** (Package) vyberte položku **Microsoft Windows 2000 Server English**.
4. V seznamu **Program** vyberte položku **Automated upgrade from NTS 3.51/4.0 (x86)** (automatizovaná inovace ze systému NTS 3.51/4.0 (x86)).

5. Stiskněte tlačítko **Procházet** (Browse) a pak vyberte kolekci, které budete program inzerovat.
6. Chcete-li nastavit spuštění inzerátu na určitý čas, zobrazte si kartu **Časový plán** (Schedule). Časové plány inzerování se přidávají stiskem tlačítka **Nový** (New).

Upozornění Přiřazené inzeráty se na každém počítači, na kterém jsou inzerovány, spouští pouze jednou. Pokud je inzerát na klientském počítači neúspěšný, klient se nepokusí o jeho automatické opakované spuštění. Tím je zajištěno, že se počítače neocitnou v nekonečné smyčce pokusu o spuštění přiřazeného inzerátu, chyby, restartu a opakovaného pokusu. Proto můžete v kroku 6 také zvolit **Allow users to run the program independently of assignments** (umožnit uživatelům spustit program nezávisle na přiřazení). Tím umožníte uživatelům spustit program před plánem nebo jej spustit později, když program při prvním pokusu skončí chybou. Je také možné vytvořit později nový inzerát pro počítače, u nichž inovace skončila chybou.

Stejně jako u předchozí fáze distribuce softwaru systému Windows 2000 začněte s inzerováním v omezeném měřítku, a ukáže-li se být úspěšným, rozšířte je. V tomto okamžiku je to velmi důležité, protože distribuce softwaru v každém případě ovlivní uživatele. Inzerování lze rozšířit vytvořením dalších inzerátů, přičemž každý bude zaměřen na jiné kolekce, nebo úpravou kolekce, ze které aktuální inzerát vychází, aby tak obsahovala stále více počítačů. Samostatné inzeráty jsou zapotřebí v případě inzerování různých programů v jednotlivých kolekcích. Například inovační program systému Windows 95 smí být inzerován pouze na počítačích v kolekci Windows 95.

Rozšíření zabezpečení na distribučních bodech

Jestliže jste při vytváření balíčku omezili přístup k balíčku na distribučních bodech, nyní musíte přístup umožnit. Učinite tak následující procedurou. Spouštíte-li program pomocí SMS s privilegii správy, jako účty přístupu k balíčku zadejte účty klientských síťových připojení používané na sídle SMS.

▼ Chcete-li otevřít zabezpečení balíčku systému Windows 2000, postupujte takto:

1. V konzole SMS Administrator vyberte položku **Packages** (balíčky).
2. Vyberte balíček systému Windows 2000 a pak položku **Access Accounts** (účty přístupu).
3. V nabídce **Akce** (Action) ukažte na příkaz **Nový** (New) a potom zvolte **Windows NT Access Account** (účet přístupu systému Windows NT).
4. V dialogovém okně **Access Account Properties** (vlastnosti účtu přístupu) stiskněte tlačítko **Set** (nastavit).
5. V dialogovém okně **Windows NT Account** (účet systému Windows NT) zadejte doménu a uživatele nebo skupinu a určete typ účtu (**Account Type**). Dialogové okno zavřete stiskem tlačítka **OK**.
6. V dialogovém okně **Access Account Properties** ověřte nastavení položky **Permissions** (oprávnění) na hodnotu **Read** (čtení).

Touto procedurou podle potřeby přidejte další uživatele nebo skupiny.

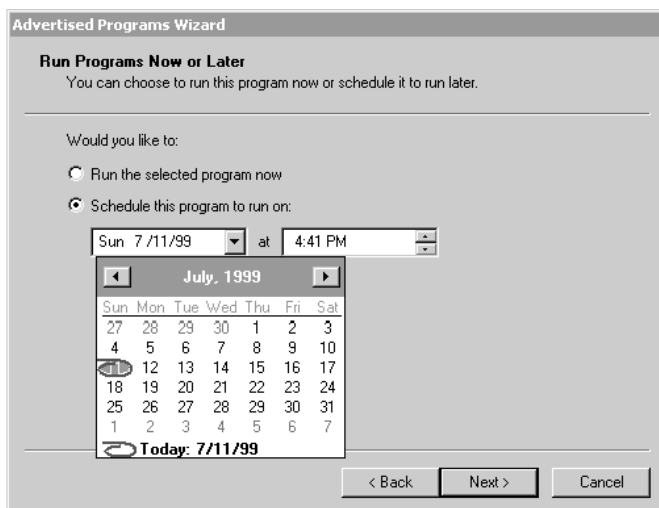
Inovace počítačů

Jakmile máte systém Windows 2000 na distribučním bodě ve stejném sídle, jako jsou inovované počítače, a na těchto počítačích se nachází příslušný inzerát, můžete:

- Naplánovat inovaci na dobu vyhovující uživateli.
- Hlásit stav inovace.

Vykonání inzerátu na jednotlivých počítačích

K distribuci všem uživatelům může pomocí SMS dojít v době, která je podle vás nejvhodnější. Můžete však dát uživatelům možnost nastavit datum a čas (viz obr. 14.9), kdy svůj počítač nebudou používat. Je také možné zadat povinnou inovaci do určitého data a času, aby uživatelé nemohli inovaci neustále odkládat.



Obrázek 14.9 Uživatelé si mohou inovaci naplánovat na nějakou vhodnou dobu

Distribuce uživatelům bude také obsahovat příslušné parametry příkazového řádku určující, který soubor odpovědí se má použít, a další volby zajišťující vykonání instalace podle vámi určených standardů.

Mnoho organizací nedává koncovým uživatelům na klientských počítačích plná privilegia. Tím se minimalizují problémy způsobené neodbornými nebo nechtěnými zásahy do konfigurace počítače ze strany uživatelů. Tento nedostatek privilegií v normální situaci zabrání uživatelům v zadání inovace svého počítače na systém Windows 2000. SMS se tomuto problému vyhýbá tak, že spouští inovaci na systém Windows 2000 v kontextu speciálního účtu zabezpečení SMS.

Stav inovace na jednotlivých počítačích

Po dokončení prvních a posledních fází inovace na systém Windows 2000 na počítači vytvoří Systems Management Server stavový soubor, který se šíří hierarchií SMS. Tyto informace lze použít k vytvoření hlášení celkového postupu projektu inovace nebo ke zjištění stavu jednotlivého počítače, jak popisuje následující oddíl.

V případě potřeby je možné vytvářet své vlastní stavové soubory indikující určité detaily související se stavem inovace. Programy vytvářející tyto stavové soubory se vyvolávají jako součást vykonání balíčku, a proto musí být součástí jeho definice. Takové stavové soubory můžete používat, když například instalační program systému Windows 2000 spouští nějaké úkoly ještě po inovaci systému.

Sledování inzerátů

Stavové zprávy SMS, které hlásí postup inovace na jednotlivých počítačích, lze použít také ke sledování postupu zavádění systému Windows 2000 jako celku. Lze tak zjišťovat počet počítačů připravených na inovaci, počet úspěšně inovovaných počítačů a umístění chyb. Pak můžete zasáhnout na místech, kde nastaly nějaké problémy.

Podsystém System Status

SMS 2.0 obsahuje výkonný podsystém stavu systému System Status, který slouží ke sledování distribuce. Konzola SMS Administrator obsahuje uzel **Stav systému** (System Status), kde najdete celkové i podrobné výsledky podsystému System Status. Stav inzerátů lze získat také v podozlu **Stav inzerátu** (Advertisement Status).

Stav pro všechny inzeráty

Vyberete-li položku **Stav inzerátu** (Advertisement Status) pod **Stav systému** (System Status) v konzole SMS Administrator, uvidíte následující informace:

- Kolik systémů obdrželo inzerát
- Na kolika systémech došlo při zpracování inzerátu k obecným chybám
- Kolikrát byl inzerovaný program spuštěn
- Kolikrát program doběhl až do konce nebo skončil chybou
- Různé podrobnosti o inzerátu

Příklad těchto informací je uveden na obrázku 14.10. Na této úrovni se nelze dotazovat na žádné stavové zprávy.

Name	Received	Failed	Programs St...	Program Er...	Program Succ...	Package	Program
Microsoft O...	3	0	3	2	2	Microsoft Offic...	Typical
Office2000...	3	0	2	0	1	Microsoft Offic...	User input
Windows 2...	1	0	5	0	4	Microsoft Win...	Batch File
Windows 2...	1	0	3	0	3	Microsoft Win...	NT4WS U...

Obrázek 14.10 Stav všech inzerátů

Stav určitého inzerátu

Pod stavem všech inzerátů můžete vybrat jednotlivé inzeráty. Na této úrovni uvidíte tyto údaje:

- Která sídla mají klienty, jež daný inzerát přijali
- Která sídla obsahují klienty, u nichž došlo během zpracování inzerátu k obecné chybě
- Kolikrát se na jednotlivých sídlech inzerovaný program spustil
- Kolikrát program proběhl úspěšně nebo skončil chybou

Obrázek 14.11 ukazuje tento typ stavových informací. Na této úrovni se nelze dotazovat na žádné stavové zprávy.

The screenshot shows the SMS console window titled 'sms - [Systems Management Server\Site Database (RED - RESKIT)\System Status\Advertisement Status\Windows 2000 P...'. The left pane shows a tree view with 'System Status' expanded, then 'Advertisement Sta...', then 'Microsoft Offic...', then 'Office2000her...', and finally 'Windows 200...'. The right pane displays a table with the following data:

Site	Received	Failures	Programs Started	Program Errors	Program Success	Summary Date
RED - RESKIT	1	0	5	0	4	5:01:00 PM 7/5/99
PUR - RESKIT	0	0	0	0	0	6:00:00 PM 7/11/99
ORA - RESKIT	0	0	0	0	0	6:00:00 PM 7/11/99

Obrázek 14.11 Stav inzerátu systému Windows 2000

Stav sídla

Na úrovni stavu inzerátu lze vybírat jednotlivá sídla. V nabídce **Akce** (Action) ukažte na příkaz **Zobrazit zprávy** (Show Messages) a pak si volbou **Všechny** (All) zobrazte všechny stavové zprávy určitého inzerátu na daném síťovém sídle. Následující pořadí zpráv je typické:

- 30006 – inzerát byl vytvořen
- 3900 – inzerát byl v sídle zpracován (distribován na klientské přístupové body atd.)
- 10002 – inzerát byl přijat klientem
- 10005 – program byl spuštěn
- 10007 – program skončil chybou

Tato zpráva indikuje, proč k tomu došlo. Obvyklými důvody jsou zrušení či jiné nucené zastavení programu uživatelem nebo nedostatek diskového prostoru na klientském počítači.

- 10009 – program byl úspěšně dokončen

V tomto okamžiku je dokončena část SMS inovace. To odpovídá konci první fáze instalačního programu systému Windows 2000 (fázi inovace souborů).

- 13126 – inovace byla dokončena (bude hlášeno jako 10009, pokud používáte SMS 2.0 SP2 nebo vyšší)

V tomto okamžiku je dokončen instalační program systému Windows 2000. Poslední dvě fáze (textová a grafická) skončily a počítač je připraven na přihlášení uživatele.

Hlášení stavu inzerátu

Třeba byste rádi vytvořili hlášení o stavu inzerátu, ať už pro svou pohodlnou orientaci nebo v zájmu naplnění jiných svých požadavků. Můžete zadávat dotazy na podsystém stavu inzerátů SMS a výsledky ukládat do nějakého nástroje sestav, podobně jako je tomu i u dalších nástrojů sestav SMS. Tabulka 14.2 uvádí odpovídající třídu a kategorii stavových informací, které v této třídě najdete.

Tabulka 14.2 Třída stavu inzerátu

Třída	Stavová informace
SMS_AdvertisementStatusSummarizer	Zobrazuje podrobné informace o stavu inzerátu uspořádané do skupin podle kódu. Připojuje se k položkám inzerátů pod Advertisement Status (stav inzerátu) v konzole SMS Administrator.

Další informace o zápisu sestav založených na datech sbíraných serverem SMS najdete v odkazu Microsoft Systems Management Server Technical Details na stránce webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

V případě hlášení stavu inzerátu systému Windows 2000 budete potřebovat sestavy podobné následujícím:

Inzerované počítače, které inzerát neobdržely

Tato sestava je porovnáním počítačů, které jsou součástí odpovídající kolekce, ale nemají stavovou zprávu 10002. Pokud byl program inzerován před vytvořením sestavy, tato sestava bude ukazovat počítače, které nebyly v poslední době používány nebo které nejsou řádně připojeny do sítě či infrastruktury SMS.

Počítače, které inzerát obdržely, ale program nespustily

Tato sestava je porovnáním počítačů, které mají stavovou zprávu 10002, ale nemají stavovou zprávu 10005. Pokud byl program přiřazen ke spuštění před vytvořením sestavy, tato sestava bude uvádět počítače, které nebyly od okamžiku prvního inzerování daného inzerátu spuštěny nebo které se odpojily od sítě či infrastruktury SMS. Nebyl-li program zatím přiřazen, tato sestava bude zahrnovat také počítače, jejichž uživatelé inovaci zatím nespustili.

Počítače, na kterých se program spustil, ale neskončil úspěšně

Tato sestava je porovnáním počítačů, které mají stavovou zprávu 10005, ale nemají stavovou zprávu 10009. Pravděpodobně jde o počítače, na nichž uživatel přerušil inovaci nebo neměly dostatek diskového prostoru. Podrobnosti získáte podrobnějším prozkoumáním popisu zprávy 10007. Jsou-li oba problémy obvyklé, pak bude asi vhodné vytvořit sestavu těchto specifických počítačů.

Existuje také určitá možnost, že k chybě na některých počítačích dojde tak, že nebude obdržena ani stavová zpráva 10007 ani stavová zpráva 10009. Chcete-li vzít v úvahu i tuto možnost, můžete vytvořit sestavu počítačů se stavovými zprávami 10005, ale bez stavových zpráv 10008 či 10009. V případě uživatelů, kteří inovaci zrušili, může k vyřešení problému postačovat zpráva elektronické pošty zdůrazňující důležitost inovace. Je také možné program nastavit tak, že k jeho vykonání musí v určitém čase dojít. V případě jiných problémů může být zapotřebí ruční zásah (může postačovat použití vzdálených nástrojů SMS).

Počítače, na kterých program úspěšně skončil, ale nebyla přijata konečná inovace

Tato sestava je porovnáním počítačů se stavovými zprávami 10009, ale bez stavových zpráv 13126. Pravděpodobně jde o počítače, na nichž se inovace spustila, ale z nějakého důvodu se zastavila. Spustíte-li sestavu v období rozsáhlých inovací, například přes víkend, může vám tato sestava pomoci identifikovat problémy, které můžete ručně opravit ještě než si toho uživatelé všimnou. Obvykle však trvá inovaci nejméně hodinu nebo i více postoupit od okamžiku vytvoření zprávy 10009 do bodu, ve kterém se vytváří zpráva 13126.

Poznámka SMS 2.0 SP2 obsahuje opravu systému hlášení stavu balíčku, která nahrazuje zprávu 13126 zprávou 10009 představující správné chování. Zprávy se také vytvářejí spolehlivěji a zpráva 10009 má smysluplný text, zatímco zpráva 13126 nemá žádný text. Proto vám před zaváděním systému Windows 2000 doporučujeme zavést SMS 2.0 SP2. Po zavedení SP2 musí logika sestav prostřednictvím textu zprávy rozlišovat mezi dvěma zprávami 10009.

Počítače inovované denně

Tato sestava je součtem stavových zpráv 13126 rozložených v čase. Může být užitečná při sledování celkového stavu projektu.

Řešení problémů s inzeráty

Proces sledování inzerátů vám pomáhá zjistit problémy ještě dříve, než vás na ně upozorní uživatelé. Mezi typické problémy patří nedostatek diskového prostoru, zásah uživatele a chyby v definici balíčku. Takové problémy vám naznačí text stavových zpráv. Také proveďte, že je balíček k dispozici alespoň na jednom distribučním bodě v daném síťovém sídle.

Určení problému je vždy prvním krokem při řešení všech technických problémů. Jakmile víte, v jaké komponentě došlo k chybě, můžete se zaměřit na další odpovídající problémy. Pomocí výše popsaných sledovacích technik můžete problém lokalizovat. Součástí kapitoly „Software Distribution Flowcharts“ knihy *Systems Management Server Resource Guide* jsou vývojové grafy znázorňující typický tok procesu distribuce softwaru. Také kapitola „Software Distribution Flowcharts“ knihy *Systems Management Server Resource Guide* obsahuje obrázky znázorňující činnosti na straně klienta. Zjistíte-li, že se vaše distribuce softwaru k nějakému bodu nedostala, je velmi pravděpodobné, že k chybě došlo v předchozím bodu vývojového grafu.

Jakmile přijdete na určitou komponentu, pomůže vám ke zjištění důvodů jejího selhání porozumění její funkci. S tím vám také pomůže vývojový graf. Navíc vám soubory protokolů mohou naznačit, co se s komponentou děje na velmi nízké úrovni, a tedy i co nefunguje. Protokolování na serveru se povoluje pomocí nástroje SMS Service Manager, protokolování na straně klientů je povoleno stále.

SMS obsahuje několik funkcí, které vám mohou pomoci se zjištěním problémů na klientských počítačích. Mezi ně patří:

- Vzdálené řízení klientského počítače.
- Přenos souborů na počítač a náhrada souborů vyžadujících aktualizaci.
- Restartování počítače.

- Získání podrobností o počítači buď na základě rutinního inventáře nebo z nástrojů vzdáleného řízení v reálném čase. (Rutinní inventář však máte k dispozici i v okamžiku, kdy se klient nachází v režimu offline.)
- Inovace softwaru nekompatibilních aplikací.

Mohou také nastat situace vyžadující ruční zásah, například když inovace nedokáže restartovat počítač či jej připojit k síti nebo když klientské komponenty SMS přestanou fungovat.

Zjednodušení konsolidace a migrace domén pomocí serveru Systems Management Server

V minulosti měly velké organizace mnoho domén. Se systémem Windows 2000 důvody pro udržování tak velkého počtu domén s velkou pravděpodobností zmizí, a proto jejich konsolidace zjednoduší správu počítačů. Migrace na nativní domény systému Windows 2000 umožní vaši organizaci plně využít funkcí systému Windows 2000.

Problémy konsolidace a migrace domén popisuje podrobně kapitola „Určení strategií migrace domén“ v této knize. Tato kapitola také uvádí strategie a techniky, které proces konsolidace a migrace zjednoduší. S celým procesem vám výrazně pomůže SMS, a proto by mělo být zváženo zavádění systému Windows 2000 pomocí SMS společně s konsolidací a migrací domén. Pomocí SMS můžete například zadat skriptová vykonávání části DCPromo inovačního procesu řadičů domén.

Největší výhoda použití SMS ke konsolidaci a migraci domén se objevuje během zavádění inovací na systém Windows 2000. Po upravení hodnoty **JoinDomain** v souboru odpovědí lze počítače umístit do nové, konsolidované domény.

Rozdíly mezi servery Systems Management Server 1.2 a Systems Management Server 2.0

Systems Management Server 2.0 se od svého předchůdce, serveru Systems Management Server 1.2, výrazně liší. Obě verze mají podobnou sadu funkcí, ale každá verze dosahuje těchto funkcí zásadně odlišnými technikami. Plánujete-li k zavedení systému Windows 2000 nebo ke konsolidaci domén použít SMS 1.2, musíte si být vědomi toho, že se distribuce softwaru v SMS 1.2 odlišuje od SMS 2.0 následujícími způsoby:

- Jako cíle distribuce softwaru lze použít pouze počítače a toto určení není dynamické (pro nové počítače splňující požadavky na inovaci musí být vytvořeny nové úlohy).
- Počítače se systémem Windows NT, na kterých nemá přihlášený uživatel privilegia správy, musí mít instalován Package Command Manager jako nástroj Service. Za tento doplněk k SMS 1.2, se nic neplatí, tento nástroj však musíte zavést před začátkem zavádění systému Windows 2000.
- Se stavovým podsystémem úloh se obtížněji pracuje.
- Na původním sídle balíčku musí stále existovat komprimovaná kopie balíčku.
- Programy nemohou před svým vykonáním přinutit jiné programy ke spuštění a nelze je centrálně zakázat.

- Počítače se systémem Windows 2000 nemusí SMS 1.2 jako klienty podporovat. Proto po inovaci na systém Windows 2000 mohou přestat fungovat jako klienti SMS 1.2 nebo již nemusí být podporováni. Další informace o podpoře SMS 1.2 počítačů se systémem Windows 2000 najdete v odkazu Microsoft Systems Management Server na stránce webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

V obou verzích SMS se liší ještě další funkce, které mohou být pro vaše zavádění systému Windows 2000 užitečné. Další informace o těchto funkcích a rozdílech najdete v kapitole „Analýza infrastruktury sítě pomocí serveru Systems Management Server“ v této knize.

Seznam úkolů plánování použití serveru Systems Management Server k zavedení systému Windows 2000

Tabulka 14.3 uvádí hlavní úkoly zavádění systému Windows 2000 pomocí serveru SMS uvedené v této kapitole.

Tabulka 14.3 Seznam úkolů zavádění systému Windows 2000 pomocí serveru SMS

Úkol	Umístění v kapitole
Seznamte se s koncepty souvisejícími s distribucí softwaru pomocí SMS.	Distribuce softwaru pomocí serveru Systems Management Server a Rozdíly mezi servery Systems Management Server 1.2 a Systems Management Server 2.0
Přípravte balíčky.	Vytvoření balíčku systému Windows 2000 pro server Systems Management Server
Distribuuje balíčky.	Distribuce balíčků systému Windows 2000
Distribuce otestujte.	Distribuce balíčků systému Windows 2000
Distribuci sledujte.	Distribuce balíčků systému Windows 2000
Vyřešte problémy s distribucí.	Distribuce balíčků systému Windows 2000
Vytvářejte hlášení o distribuci.	Distribuce balíčků systému Windows 2000
Inzerujte balíčky.	Inzerování balíčků systému Windows 2000
Otestujte inzeráty a balíčky.	Inzerování balíčků systému Windows 2000
Inovujte počítače.	Inzerování balíčků systému Windows 2000
Sledujte inzeráty.	Inzerování balíčků systému Windows 2000
Vyřešte problémy s inzeráty.	Inzerování balíčků systému Windows 2000
Vytvářejte hlášení o inzerátech.	Inzerování balíčků systému Windows 2000
Pomocí SMS zjednodušte konsolidaci a migraci domén.	Zjednodušení konsolidace a migrace domén pomocí serveru Systems Management Server

Další zdroje

- Další informace o použití serveru Systems Management Server najdete v knize *Microsoft Systems Management Server Administrator's Guide*.
- Podrobné informace o použití serveru Systems Management Server najdete v knize *Microsoft Systems Management Server 2.0 Resource Guide*, která je součástí sady *Microsoft BackOffice 4.5 Resource Kit*.

KAPITOLA 15

Inovace a instalace členských serverů

Členské servery zajišťují souborové, tiskové, webové, aplikační a komunikační služby. Členské servery nejsou řadiče domén, každý členský server má však v doméně účet. V první fázi zavádění systému Windows 2000 Server můžete inovovat své stávající členské servery nebo instalovat nové členské servery. To vám umožní využívat funkce systému Windows 2000 Server ještě před zavedením adresářové služby Active Directory. Tato kapitola uvádí úvahy související s plánováním i procedury, které jsou užitečné pro správce při instalování nebo inovování členských serverů na systém Windows 2000 Server.

Doporučujeme, abyste měli pracovní znalosti systému Microsoft Windows NT verze 4.0, znalosti o sítích a práci v nich a abyste rozuměli síťovým sídlům systému Microsoft Windows 2000. To vám pomůže určit požadavky na instalaci a inovaci na systém Windows 2000 Server v prostředí vaší podnikové sítě.

V této kapitole

Plánování inovace a instalace členských serverů 452

Příprava členských serverů na inovaci nebo novou instalaci 454

Vykonání inovace nebo instalace 457

Určení rolí serverů jednotlivých systémů Windows 2000 Server 459

Vykonání úloh po inovaci a instalaci 467

Seznam úkolů plánování členských serverů 469

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Plán instalace a inovace členských serverů
- Inventář existujícího hardwaru a softwaru

Související informace v sadě Resource Kit

- Další informace o síťových sídlech systému Windows 2000 najdete v kapitole „Návrh struktury služby Active Directory“ v této knize.
- Další informace o vytváření plánů testování najdete v kapitole „Vytváření testovací laboratoře systému Windows 2000“ v této knize.

Plánování inovace a instalace členských serverů

Jednou z největších výhod instalování a inovování na systém Windows 2000 Server je dostupnost adresářových služeb Active Directory. I když však instalování služby Active Directory zatím odložíte, můžete přesto inovovat členské servery na systém Windows 2000 Server. Pak budete moci přistupovat k novým a vylepšeným funkcím součástí a službám, jako jsou služby směrování a vzdáleného přístupu (Routing and Remote Access) a terminálové služby (Terminal Services).

Servery v doméně systému Windows 2000 mohou mít jednu ze dvou rolí: mohou být doménovými řadiči nebo mohou být *členskými servery*. Členský server je server se systémem společnosti Microsoft, který může mít účty v doméně Microsoft Windows NT verze 3.51, Windows NT 4.0 nebo Windows 2000. Je-li však členem domény systému Windows 2000, neobsahuje žádné objekty Active Directory. Členské servery sdílejí společné funkce zabezpečení, jako jsou zásady domény a uživatelská práva.

Členské servery mohou fungovat jako:

- Souborové servery
- Tiskové servery
- Webové servery
- Proxy-servery
- Servery služby směrování a vzdáleného přístupu (Routing and Remote Access)
- Aplikační servery, které zahrnují:
 - Servery komponent
 - Servery terminálů
 - Servery certifikátů
 - Servery databází
 - Servery elektronické pošty

Proces instalace nebo inovace systému Windows 2000

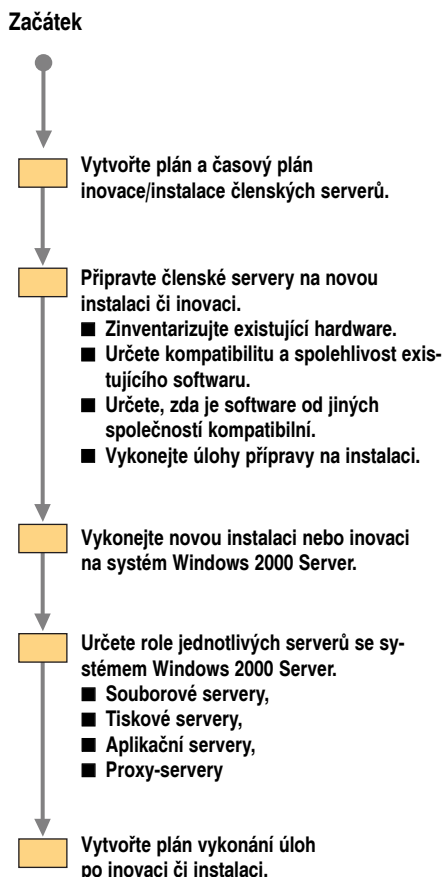
Proces plánování instalace nebo inovace členských serverů vám může zabrat hodně času. Předběžné plánování minimalizuje problémy, ke kterým může dojít při inovacích sítě. Obrázek 15.1 ukazuje doporučený proces, který byste měli dodržet při návrhu strategie inovace odpovídající vaší síti.

Vytvoření plánu inovace a instalace

Dokonalé naplánování zajistí hladké zavedení systému Windows 2000. Kromě vývojového grafu uvedeného v předchozím oddílu vám s vytvořením plánu inovace či instalace členských serverů pomohou ještě následující body:

- Je-li to nutné, upravte existující dokumenty návrhu sítě tak, aby odpovídaly vašemu aktuálnímu síťovému prostředí.

Nemáte-li aktualizovaný síťový diagram, před pokračováním inovace sítě jej raději vytvořte.
- Prověřte aktuální infrastrukturu sítě z hlediska:
 - Kompatibility softwaru
 - Potřeb interoperability
 - Hardwarových potřeb



Obrázek 15.1 Proces instalace a inovace členských serverů

- Věnujte se také těmto otázkám:
 - Kolik nových členských serverů je zapotřebí?
 - Které členské servery by měly být inovovány?
 - Které členské servery by měly být před inovací nahrazeny novým hardwarem?
- Dokumentujte změny ve vašem aktuálním síťovém prostředí a určete související otázky plánování.
- V případě potřeby vytvořte testovací prostředí, abyste mohli členské servery s nekompatibilním softwarem před jejich nasazením otestovat.

Vytvoření časového plánu

Během inovace serverů obvykle dochází k přerušení síťových služeb. Abyste toto riziko minimalizovali, vytvořte časový plán inovace, který zajistí omezení doby výpadků během pracovních hodin. Při vytváření časového plánu inovace zvažte také následující body:

Doba věnovaná instalaci nebo inovaci na jednom serveru

Doba potřebná k inovaci serveru se mění v závislosti na rychlosti hardwaru a počtu a typu aplikací a služeb, které chcete po instalaci operačního systému nainstalovat. Zkušený správci dokáží nainstalovat či inovovat operační systém na jednom serveru přibližně za jednu hodinu. Vyhodnocení instalace a testování serveru před jeho skutečným nasazením na síť však může trvat několik hodin i dnů.

Implementace nových služeb a funkcí systému Windows 2000 Server

Po instalaci nebo inovaci serveru na něm lze nakonfigurovat nové služby a funkce. Před instalací serveru na síť je zapotřebí server otestovat v prostředí testovací laboratoře.

Scénář: Minimalizování doby výpadku sítě při inovaci serveru

Jedním z nejvýhodnějších způsobů minimalizace doby výpadku je instalovat nebo inovovat členské servery po etapách. Představme si, že na síti s celkovým počtem 70 serverů běží systém Microsoft Windows NT Server verze 4.0 a že síť má různé typy členských serverů. Správce si prostuduje analýzu růstu sítě a rozhodne, že kromě existujících členských serverů je zapotřebí ke zvládnutí růstu sítě v příštím roce dalších pět serverů. Aby měly ostatní servery a klienti stále zaručen přístup na Internet, k souborům a k aplikacím, nemůže správce inovovat všechny servery najednou. Naše ukázková síť obsahuje následující typy a počty jednotlivých skupin členských serverů:

- Pět souborových serverů (bude přidán jeden nový souborový server)
- Deset aplikačních serverů (bude přidán jeden nový aplikační server)
- Deset serverů IIS
- Pět faxových serverů
- Pět proxy-serverů
- Deset směrovačů (bude přidán jeden nový směrovač)
- Pět serverů služby směrování a vzdáleného přístupu (bude přidán jeden nový server služby směrování a vzdáleného přístupu)
- Patnáct tiskových serverů (bude přidán jeden nový tiskový server)
- Pět serverů databáze SQL

Nejprve správce určí, jak dlouho bude trvat inovace jednotlivých skupin členských serverů. Správce se rozhodne převést jeden server z každého typu do režimu offline, inovovat jej a vyzkoušet během normálních pracovních hodin, přičemž ostatní servery ponechá v režimu online a funkční. Proběhne-li inovace a testování v pořádku, ostatní servery budou inovovány v noci po skončení pracovní doby, přičemž o síťové služby se budou starat již inovované servery. Instalace dodatečných serverů se uskuteční až po inovaci všech stávajících serverů. Tím se získá čas potřebný ke konfiguraci služeb a komponent nových serverů.

Příprava členských serverů na inovaci nebo novou instalaci

Instalace nebo inovace členských serverů na systém Windows 2000 Server vyžaduje, aby byly počítače kompatibilní s novým operačním systémem. Chcete-li připravit

úspěšnou inovaci nebo instalaci členských serverů, musíte vykonat různé činnosti a získat určité informace.

Inventarizace existujícího hardwaru

V rámci přípravy členských serverů musíte nejprve inventarizovat existující hardware. Toho dosáhnete zdokumentováním následujících informací o každém serveru:

- Výrobce a model inovovaného počítače.
- Velikost instalované fyzické paměti.
- Typ instalované síťové karty.
- Všechna zařízení Plug-and-Play.
- Zdroj nepřerušitelného napájení (UPS) připojený k serveru.
- Typ externích pevných disků připojených k počítači.
- Rozdělení pevného disku a dostupný volný prostor.
- Používané hardwarové nebo softwarové redundantní pole nezávislých disků (RAID).
- Typ instalované jednotky CD-ROM.

Určení požadavků systému

Požadavky systému Windows 2000 Server jsou větší, než byly u systému Windows NT Server 4.0. Každý server na síti musí splňovat alespoň minimální požadavky, aby systém Windows 2000 Server fungoval výkonně. Minimálním hardwarové požadavky jsou:

- Procesor Pentium 166 MHz nebo vyšší

Nová instalace systému Windows 2000 Server podporuje počítače s až čtyřmi procesory. Inovujete-li počítač se systémem Windows NT Server, který podporoval více než čtyři procesory, musíte jej inovovat na systém Windows 2000 Advanced Server, protože ten podporuje až osm procesorů.

- Alespoň 64 megabajtů (MB) paměti s náhodným přístupem (RAM), doporučeno je však 128 MB, přičemž 4 gigabajty (GB) jsou maximum.
- Oddíl pevného disku s dostatečným prostorem pro instalační proces

Potřebný prostor vypočtete tak, že začnete s hodnotou 850 MB a přidáte 2 MB za každý megabajt paměti na vašem počítači. V závislosti na následujících bodech může být zapotřebí více paměti:

- Instalované komponenty a služby.
- Používaný systém souborů.

Systém souborů s alokační tabulkou (FAT) vyžaduje dalších 100 až 200 MB diskového prostoru.

- Metoda použité instalace.

Chcete-li instalovat přes síť, budete potřebovat při porovnání s instalací z CD operačního systému dalších 100 až 200 MB diskového prostoru pro dodatečné soubory ovladačů, které musí být během celého procesu k dispozici.

Navíc může inovace vyžadovat mnohem více diskového prostoru než nová instalace. Po přidání funkcí služby Active Directory se může existující databáze uživatelských účtů zvětšit až desetkrát.

Poznámka Po dokončení instalačního programu je skutečný diskový prostor potřebný pro operační systém (vyjma uživatelských účtů) obvykle menší než volný prostor požadovaný instalačním programem. To závisí na konkrétním počítači, na který se komponenty instalují.

Další požadavky najdete v adresáři \Support na CD operačního systému Windows 2000 Server.

Určení kompatibility a spolehlivosti existujícího softwaru

Je velmi důležité, abyste se před inovací ujistili o kompatibilitě softwaru, který musíte používat, se systémem Windows 2000. To můžete učinit kontaktováním výrobce softwaru nebo vytvořením testovací sítě, na které bude aplikace pracovat.

Při určování kompatibility a spolehlivosti existujícího softwaru si zodpovězte také následující otázky:

- Jaké systémy souborů (FAT nebo NTFS) se používají?
- Jaké operační systémy a servisní balíčky se v současné době používají?
- Pro jaký operační systém byl daný program napsán (Microsoft Windows NT, Microsoft Windows 98, Microsoft Windows 95, Microsoft Windows 3.x nebo Microsoft MS-DOS)?
- Byl program vytvořen pro funkci v určitém síťovém prostředí? Pro jakou verzi takové sítě?
- Jsou program a konfigurační soubory programu uloženy na serveru nebo na klientech?
- Jsou datové soubory uloženy na serveru nebo na klientech?

Po zodpovězení těchto otázek budete vědět, zda je existující software ve vašem prostředí kompatibilní se systémem Windows 2000 Server.

Určení kompatibility softwaru jiných výrobců

Software pro systém Windows 2000 Server označený speciálním logem kompatibility (software vytvořený přímo pro Windows 2000 Server) využívá funkcí systému Windows 2000 Server, jako je služba Active Directory. V systému Windows 2000 Server by měl bez problémů pracovat libovolný software napsaný pro systémy Windows 2000, Windows NT, Windows 95 nebo Windows 98. Software napsaný pro 16bitové systémy Windows (Windows 3.x) nebo systém MS-DOS by měl fungovat v prostředí systému Windows 2000 Server, ale vztahují se na něj další podmínky:

- Software může vyžadovat speciální konfigurační soubory, například Autoexec.nt a Config.nt.
- 16bitový software může mít nebo vyžadovat speciální ovladače zařízení, které již nejsou k dispozici nebo jsou nekompatibilní se systémem Windows 2000 Server. V takovém případě kontaktujte výrobce softwaru a zjistěte, zda má k dispozici nebo vyvíjí ovladač zařízení, který potřebujete.

Ve všech případech byste měli důkladně otestovat veškerý software na platformě Windows 2000 v laboratorním prostředí a neriskovat tak výpadek sítě nebo ztrátu dat v prostředí výroby. Další informace o nastavení testovacího prostředí najdete v kapitolách „Vytvoření testovací laboratoře systému Windows 2000“, „Pilotní zavádění systému

Windows 2000“ a „Testování kompatibility aplikací se systémem Windows 2000“ v této knize.

Vykonání úkolů před instalací

Chcete-li zajistit bezpečnost systémových souborů a hladný průběh instalace, doporučujeme vám vykonat určité úkoly:

Přečtěte si dokumenty popisující přípravu na instalaci

Existují tři důležité dokumenty, které by si měli správci sítě před vykonáním inovace prostudovat.

- **Seznam kompatibilního hardwaru (Hardware Compatibility List)**

Seznam kompatibilního hardwaru (Hardware Compatibility List – HCL) obsahuje informace o kompatibilitě hardwaru, které vám pomohou určit, zda je váš aktuální hardware kompatibilní se systémem Windows 2000 Server. Tento seznam je obsáhlý, společnost Microsoft však informace neustále aktualizuje. Chcete-li zjistit, zda je hardware ve vaší společnosti certifikován na seznamu HCL, prozkoumejte odkaz Hardware Compatibility List stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

- **Read1st.txt**

Soubor Read1st.txt obsahuje nejnovější a nejdůležitější informace, které byste si měli přečíst před instalací či inovací a které doplňují dokumentaci systému Windows 2000 Server.

- **Relnotes.txt**

Tento dokument obsahuje poznámky týkající se dalších informací o systému Windows 2000 Server a je také doplňkem dokumentace. Soubor obsahuje podrobné technické popisy doplňků operačního systému. Po jeho přečtení budete schopni činit informovaná rozhodnutí o zavádění členských serverů ve vaší síti.

Zaznamenejte si systémové informace

Je důležité, abyste si před začátkem inovace zaznamenali všechny systémové informace související s jednotlivými servery. Tím získáte důležitý referenční dokument, který budete potřebovat v případě, že bude nezbytné vrátit členský server do jeho původního stavu.

Chcete-li si zobrazit informace o serveru v systému Windows NT Server 4.0, pak v nabídce **Nástroje správy** (Administrative Tools) klepněte na položku **Diagnostika systému Windows NT Server** (Windows NT Server Diagnostics). Chcete-li si tyto informace vytisknout, klepněte na příkazy **Soubor** (File) a **Tisk sestavy** (Print Report) ve Správci diagnostiky systému Windows NT Server (Windows NT Server Diagnostics Manager).

Vykonání inovace nebo instalace

Rozhodnutí, zda vykonat inovaci nebo novou instalaci systému Windows 2000 Server na členský server, závisí na tom, jestli již existují členské servery s operačními systémy Windows NT, nebo zda budou do infrastruktury zavedeny nové servery.

Seznam úkolů před instalací

Před spuštěním instalačního programu systému Windows 2000 Server si projděte následující body a splňte položky platící pro členské servery ve vaší infrastruktuře sítě.

Zkontrolujte chyby v protokolech událostí.

V systému Windows NT 4.0 zkontrolujte v **Prohlížeči událostí** (Event Viewer) protokoly událostí systému, aplikací a zabezpečení a ujistěte se, že tu aktuálně nejsou zaznamenány žádné chyby. Najdete-li nějaké chyby, před inovací na systém Windows 2000 Server je odstraňte.

Zálohujte systémové a důležité soubory.

Zálohujte všechny jednotky na daném počítači. Před inovací si uložte všechny potřebné informace o nastavení pevného disku.

V systému Windows NT 4.0 můžete k uložení tabulky oddílů pevného disku na disketu použít nástroj **Správce disku** (Disk Administrator – **windisk.exe**). V panelu nabídek zvolte **Oddíl** (Partition) a pak zadejte příkazy **Konfigurace** (Configuration) a **Uložit** (Save).

Jsou-li jednotky naformátovány na systém souborů NTFS, nemusíte v rámci přípravy disků zadávat žádné akce. Instalační program systému Windows 2000 Server je převede na systém NTFS používaný v systému Windows 2000 Server. Také zakažte zrcadlení disků. Zrcadlený svazek totiž snižuje riziko neobnovitelné chyby, protože máte na jiné jednotce duplikovanou sadu dat. Je-li zrcadlení aktivní během inovace a data na primární jednotce se poškodí, může to mít za následek ztrátu všech dat na zrcadlené jednotce.

Všechny své důležité soubory také zálohujte na pásku nebo na sdílené síťové místo. V zájmu ochrany dat je velmi důležité dokončit nejprve tento krok pro případ, že by se během inovace projevila nějaká chyba.

Používáte-li program Zálohování (Backup), kontrolou protokolu zálohování, který se nachází v adresáři \Winnt\Backup.log, ověřte po dokončení procesu zálohování, že nedošlo k žádným chybám.

Pomocí programu Regback.exe na doprovodném CD sady *Microsoft Windows NT Server Resource Kit* můžete také zálohovat registr. Tento nástroj zálohuje klíče registru do souborů bez použití pásky. Systém Windows 2000 Server však bude zálohovat registr v okamžiku zálohování dat stavu systému (System State).

Odstraňte nekompatibilní software a nástroje.

Odstraňte všechny antivirové programy, síťové služby jiných společností a klientský software. V souboru s poznámkami k vydání produktu (na CD operačního systému Windows 2000 Server) si přečtěte informace o známých problémech s určitými aplikacemi.

Odpojte zařízení UPS.

Odpojte sériový kabel připojující zařízení UPS. Systém Windows 2000 Server se pokouší automaticky detekovat zařízení připojená k sériovým portům, což může v případě zařízení UPS způsobovat v instalačním procesu problémy.

Je-li to možné, nastavte systém BIOS počítače tak, aby rezervoval všechny požadavky na přerušení (IRQ) právě používané zařízeními ISA nevyhovujícími standardu Plug-and-Play. Pokud tak neučiníte, může instalace skončit následující zprávou:

INACCESSIBLE_BOOT_DEVICE

Dojde-li k tomu, nebude možné instalaci dokončit.

Také nezapomeňte aktualizovat svou disketu nouzového obnovení a nouzového spuštění.

Inovace členských serverů

Existuje jediná, z větší části automatizovaná procedura inovace členských serverů. Během inovace migruje systém Windows 2000 Server aktuální nastavení operačního systému a zapotřebí je jen minimum zadání správce.

Chcete-li inovovat počítač, vložte do mechaniky CD operačního systému Windows 2000 Server. Všechny kroky vás provede instalační program. Po výzvě zadejte **Inovovat na systém Windows 2000** (Upgrade to Windows 2000). V posledním kroku dojde k restartu instalačního programu Windows 2000 Server, přičemž se převezmou informace a použijí existující nastavení předchozího operačního systému.

Vykonání nové instalace

Existují tři způsoby instalace systému Windows 2000 Server na počítač bez operačního systému:

- Podporuje-li počítač jako spouštěcí zařízení jednotku CD-ROM, instalační program se spustí automaticky po vložení CD operačního systému. Ujistěte se, že je systém BIOS nakonfigurován tak, aby se CD spustilo automaticky.

Poznámka Na mnoha počítačích není možnost spouštění z CD standardně nastavena. Lze ji však zadat ručně.

- Jestliže počítač nepodporuje jednotku CD-ROM jako spouštěcí zařízení, musíte systém Windows 2000 Server instalovat pomocí čtyř instalačních disket.
- Zvolíte-li nahrání operačního systému ze sítě, budete potřebovat diskety síťového klienta, který rozpozná síťovou kartu právě instalovanou v počítači. To vám umožní přihlásit se k vaší příslušné doméně.

Poznámka Nahrajete-li systém Windows 2000 Server ze sítě, potřebujete příslušný počet klientských licencí odpovídající počtu instalovaných serverů.

V případě počáteční instalace nových členských serverů neexistují na počítačích žádné služby nebo aplikace. V takovém případě máte počítač kompatibilní se systémem Windows 2000 Server a splňující všechny systémové požadavky uvedené dříve v této kapitole. Takový počítač musí být na místní síti (LAN) nebo mít podporovanou jednotku CD-ROM a naformátovaný pevný disk.

Určení rolí serverů jednotlivých systémů Windows 2000 Server

Členské servery mohou mít na síti různé funkce, což umožňuje správcům zavést různý rozsah služeb a zformovat střední vrstvu infrastruktury sítě. Následující oddíly popisují každou z možných rolí a v případě potřeby poskytují podrobnosti týkající se instalace a inovace jednotlivých typů serverů.

Souborové servery

Souborové servery zajišťují na úrovni oddělení a pracovní skupiny přístup k souborům. V předchozích operačních systémech Windows byla místa sdílení souborů umístěna v rámci daného síťového sídla – uživatel se musel připojit k jednotlivým souborovým serverům a pak přistoupit k souborům, které potřeboval. Jestliže souborový server nebyl dostupný, uživatel musel přistoupit k jinému souborovému serveru, který obsahoval stejný soubor. Systém Windows 2000 Server přístup ke sdíleným místům prakticky odstraňuje.

Sdílené položky na souborovém serveru systému Windows 2000 Server lze prostřednictvím distribuovaného systému souborů (DFS) systému Windows 2000 Server distribuovat v celém sídle nebo doméně. Pomocí infrastruktury DFS se může skupina souborových serverů zobrazovat jako jedna entita. Pro příklad si představme následující názvy souborových serverů systému Windows NT 4.0:

- \\souborový_server\soubor1
- \\souborový_server\soubor2
- \\souborový_server\soubor3
- \\souborový_server\soubor4

Pomocí DFS systému Windows 2000 Server můžete přidat všechny čtyři souborové servery do stromu DFS a používat jen jedno sdílené místo nazvané \\souborový_server. Tím umožníte všem klientům přístup k libovolným souborům na všech čtyřech souborových serverech. Dosahuje se tím redundance a vyrovnávání zatížení, protože služba Active Directory se nejprve pokusí najít souborový server, který se nachází nejbližší ke klientovi požadujícímu danou informaci. Není-li tento server dostupný, DFS k získání potřebných informací použije další souborový server.

Plánujete-li používat k distribuci souborových serverů v doméně systém DFS, doporučujeme vám naplánovat si před inovací, jaké servery budou distribuovat určitá sdílená místa. Je například vhodné umístit všechny souborové servery s uloženými aplikacemi do jedné skupiny pojmenované \\souborový_server\aplikace. Jiná sada souborových serverů, na které se ukládají zálohovaná data, může být pojmenována \\souborový_server\záloha. Tím bude zajištěno, aby se už uživatelé nemuseli rozhodovat, které sdílené místo mají použít.

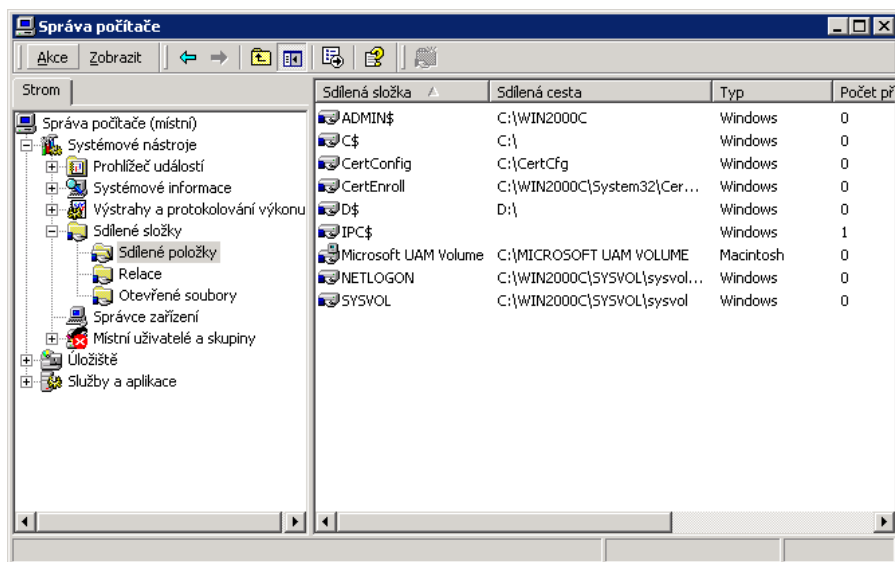
Další informace o plánování, instalaci, konfiguraci a použití systému DFS najdete v kapitole „Distributed File System“ v knize *Microsoft Windows 2000 Server Distribuované systémy* a v kapitole „Určení strategií správy úložišť systému Windows 2000“ v této knize.

Poznámka Doménové systémy DFS vyžadují spuštěnou službu Active Directory.

Svazky systému Macintosh

Při inovaci souborových serverů Windows NT 4.0 se svazky systému Macintosh zajišťujete inovací služeb pro systém Macintosh (Services for Macintosh) nebo je znovu nainstalujete, pokud jste je před inovací odstranili. Než budete pokračovat, také zálohujte všechny soubory systému Macintosh. Pak můžete inovovat server na systém Windows 2000 Server podle instrukcí uvedených dříve v této kapitole.

Po dokončení inovace si můžete zobrazit migrovaný svazek systému Macintosh pomocí funkce **Správa počítače** (Computer Management), jak ukazuje obrázek 15.2.



Obrázek 15.2 Správa počítače zobrazující migrovaný souborový svazek systému Macintosh

V systému Windows 2000 Server lze přistupovat ke svazku Macintosh buď prostřednictvím protokolu AppleTalk nebo pomocí protokolu TCP/IP. Máte-li na síti klienty používající pouze AppleTalk, můžete tento protokol nahrát prostřednictvím ovládacího panelu vlastností místní sítě.

Instalujete-li nový souborový server hostící svazky systému Macintosh, nejprve musíte ověřit, že váš hardware splňuje určité minimální požadavky. Podívejte se do seznamu hardwaru uvedeného dříve v této kapitole a do seznamu HCL na CD operačního systému Windows 2000 Server. Pak nainstalujte systém Windows 2000 Server podle instrukcí uvedených dříve v této kapitole.

Po dokončení instalace převedte nový server na souborový server systému Windows 2000 pomocí **Průvodce konfigurací serveru** (Configure Your Server) a volbou položky **Souborový server** (File Server) nebo zobrazením položky **Správa počítače** (Computer Management) nabídky **Nástroje pro správu** (Administrative Tools) a klepnutím na položku **Sdílené složky** (Shared Folders).

Svazky systému Novell NetWare

Počítači se systémem Windows 2000 Server umožňuje poskytovat souborové a tiskové služby přímo klientům systému NetWare a kompatibilním doplňkový nástroj File and Print Services for NetWare (souborové a tiskové služby pro systém NetWare) společnosti Microsoft. Server se pak klientům NetWare jeví jako jakýkoli jiný server NetWare a klienti mohou přistupovat ke svazkům, souborům a tiskárnám na serveru. Software klienta systému NetWare nevyžaduje žádné doplňky ani změny.

Tento nástroj je součástí produktu společnosti Microsoft, Microsoft Services for NetWare v. 5: Add-on Utilities for Microsoft Windows 2000 Server and Microsoft Windows NT Server 4.0.

Testování míst sdílení souborů

Po inovaci členského serveru na systém Windows 2000 Server se přesvědčte následujícími kroky, že stále můžete přistupovat ke sdíleným položkám:

- Na serveru si otevřete Průzkumníka Windows. Klepněte na dvě nebo tři místa sdílení souborů a pak zadejte příkaz **Vlastnosti** (Properties) nabídky **Soubor** (File) a podívejte se na stav jejich sdílení.
- Přihlaste se na jednoho nebo více klientů, připojte se k jednotkám několika známých sdílených bodů a ověřte, že sdílení na serveru se systémem Windows 2000 funguje.

Jestliže jste na serverech zajistili podporu systému DFS, přesvědčte se postupným vypínáním jednotlivých souborů a následným vykonáním výše uvedených kroků, že lze dosáhnout všech souborových serverů.

Tiskové servery

Organizace všech velikostí chtějí zajistit uživatelům v rámci sídla nebo domény možnost tisku. Tiskové služby jsou většinou nastaveny v rámci skupin organizační jednotky, aby byly snadno přístupné všem uživatelům ve skupině. Tiskárny lze nastavit jako veřejné tiskárny, na které je přístup globální, nebo soukromé tiskárny, na které má přístup jen nějaký tým nebo určití uživatelé skupiny. Počet uživatelů s přístupem k určité skupině tiskáren vyžaduje pozorné plánování.

Nastavení tiskového serveru

Požadavky na nastavení tiskových serverů se systémem Windows 2000 Server jsou následující:

- Na serveru musí být systém Windows 2000 Server.
- Server musí mít dostatečnou paměť RAM pro zpracování dokumentů.

Spravuje-li tiskový server velké množství tiskáren, může vyžadovat větší paměť, než potřebuje systém Windows 2000 Server pro jiné úlohy. Neodpovídá-li velikost paměti RAM tiskového serveru jeho zatížení, může to znamenat nízkou výkonnost tisku.

- Server musí mít dostatečný diskový prostor pro zařazování dokumentů do okamžiku jejich skutečného tisku.

To je důležité v případě rozsáhlých dokumentů nebo jejich kumulování. Například pokusí-li se o tisk deset uživatelů najednou, tiskový server musí mít dostatek diskového prostoru pro uložení všech dokumentů až do jejich odeslání na tiskové zařízení. Dokumenty, které se již do paměti serveru nevejdou, zůstanou na klientech až do okamžiku, kdy bude mít server dostatek prostoru. Tento proces způsobuje snížení výkonnosti klienta.

- Musí být instalované vhodné ovladače tiskáren.

Vhodné ovladače tiskáren jsou ty, které byly napsány pro systém Windows 2000 Server. Takové ovladače najdete na CD operačního systému Windows 2000 Server nebo je můžete získat od výrobce vaší tiskárny. Ovladače tiskáren pro různé hardwarové platformy nelze zaměňovat.

Klienti, na kterých neběží operační systém společnosti Microsoft, mají s ohledem na tisk na síťové tiskárny další požadavky. Na tiskové servery musíte nainstalovat další služby a na klienty musíte nainstalovat příslušné ovladače tiskáren. Těmito službami jsou:

- Systém Macintosh – Services for Macintosh
- Systém NetWare – Client and Gateway Services for NetWare
- Tisk protokolem TCP/IP na systém UNIX – také se označuje za službu Line Printer Daemon (LPD)

Potřebné ovladače získáte u výrobce tiskárny.

Instrukce pro nastavení prostředí síťového tisku

Jestliže ještě nemáte vytvořeno prostředí síťového tisku, použijte k vývoji síťového tisku následující instrukce:

- Určete počet uživatelů, kteří budou tisknout, a jimi generované tiskové zatížení.
- Určete potřeby tisku. Potřebují-li například uživatelé ve skupině prodeje tisknout barevné brožury, musíte jim zajistit barevné tiskové zařízení.
- Určete, kde budou tiskárny umístěny. Uživatelé by měli mít možnost si své vytištěné dokumenty jednoduše vyzvednout.
- Určete počet tiskových serverů potřebných ke zpracování množství a typů tiskáren na síti.
- Zamyslete se také nad následujícími body:
 - Sdílené tiskárny umožňují více uživatelům tisknout na jedno zařízení.
 - Skupiny tiskáren umožňují více tiskárnám sdílet tiskovou frontu. Tisková zařízení musí být stejná a umístěna u sebe, pokud tedy nesdílejí společný emulační režim.
 - Priority tiskáren umožňují tiskovým frontám zpracovat určité tiskové úlohy přednostně na základě priorit přiřazených uživatelům nebo skupinám uživatelů (oproti zpracování v chronologickém pořadí).

Integrace služby Active Directory s tiskovými službami systému Windows 2000

Síťový tisk lze zdokonalit použitím služby Active Directory. Je však důležité uvědomit si, že vylepšení výkonnosti a funkčnosti tiskových služeb systému Windows 2000 Server lze používat i bez zavedení služby Active Directory.

Po zavedení služby Active Directory bude daný server Windows 2000 představovat standardní tiskový objekt. Pomocí tohoto objektu můžete službou Active Directory publikovat tiskárny, které se mají sdílet v celé síti. Tím nabídnete uživatelům jednoduchý způsob hledání tiskáren ve struktuře Active Directory. Uživatelé pak budou schopni najít atributy tisku, jako jsou například možnosti tisku (PostScript, barva, papír velikosti A3 atd.) a umístění tiskárny včetně možnosti připojit se k dané tiskárně a odeslat na ni dokumenty (podle oprávnění přístupu k tiskárně).

Testování míst sdílení tiskáren

Po instalaci nebo inovaci tiskových serverů na systém Windows 2000 Server se pomocí následujících kroků ujistíte, že všechna místa sdílení tiskáren fungují:

▼ **Chcete-li otestovat instalaci tiskového serveru, postupujte takto:**

1. V ovládacích panelech si otevřete složku **Tiskárny** (Printers).
2. Zadejte příkaz **Vlastnosti** (Properties) nabídky **Soubor** (File). Objeví se dialogové okno vlastností tiskárny.
3. V okně vlastností stiskněte tlačítko **Vytisknou zkušební stránku** (Print Test Page).
4. Ujistěte se o správné funkci míst sdílení tiskáren pod systémem Windows 2000 Server.

Po vytištění zkušební stránky na jednotlivých tiskárnách serveru zopakujte uvedený test z více klientů a prověřte, že se mohou připojit k místu sdílení tiskáren a předat jim tiskové úlohy.

Aplikační servery

Aplikační servery představují centrální umístění programů používaných více uživateli. Aplikaci tak nemusíte nahrávat na 1000 klientů, ale můžete jim umožnit přístup k aplikaci přes sdílené místo. V závislosti na diskovém prostoru potřebném pro běh programu může takový server vyžadovat větší úroveň prostředků. Například aplikační server databázového programu bude potřebovat více paměti a diskového prostoru než server hostící program zpracování textu.

Při vykonávání nové instalace systému Windows 2000 Server nebo inovace systému Windows NT 4.0 nejprve zálohujte všechna data související s aplikacemi pracujícími se systémem Windows 2000 Server. Po zálohování aplikací a dat inovujte aplikační server v testovacím prostředí a ujistěte se o jeho kompatibilitě.

Aplikační členský server může hostit různé programy a služby. Popis některých služeb najdete v tabulce 15.1.

Tabulka 15.1 Programy a služby na aplikačním členském serveru

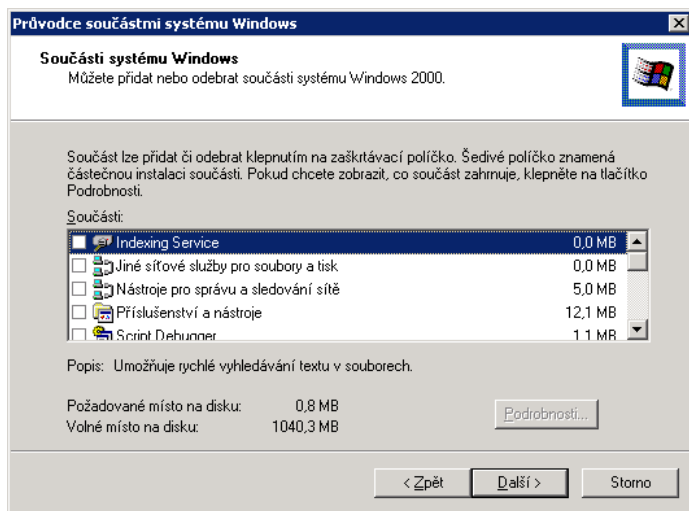
Služba	Popis
Služby součástí systému	Spravuje serverové součásti jako je vyrovňování zatížení aplikací (Application Load Balancing), transakční služby (Transaction Services), správu aplikací (Application Management) a řazení zpráv (Message Queuing).
Terminálové služby	Softwarové služby umožňující klientským aplikacím spuštění na serveru. Klienti pak fungují jako terminály a nikoli jako nezávislé systémy.
Databáze	Poskytuje platformu pro operaci a správu databázových programů, jako je například Microsoft SQL Server.
Elektronická pošta	Poskytuje platformu pro operaci a správu serverů elektronické pošty, jako je například Microsoft Exchange Server.

Poznámka V případě serverů databází a elektronické pošty musí být nad systémem Windows 2000 instalovány ještě další aplikace. Tyto služby samotný systém Windows 2000 nepodporuje.

S výjimkou programů Microsoft Exchange Server a Microsoft SQL Server lze nakonfigurovat všechny uvedené služby pomocí **Průvodce konfigurací serveru** (Configure Your Server) po instalaci systému Windows 2000 Server.

Služby součástí systému

Aplikační členské servery poskytují platformu pro spouštění služeb součástí jako je vyrovnávání zatížení, transakční služby správa aplikací a řazení zpráv. Tyto služby lze používat prostřednictvím ovládacího panelu **Přidat nebo odebrat programy** (Add/Remove Programs) a **Průvodce součástmi systému Windows**, který je uveden na obrázku 15.3.



Obrázek 15.3 Průvodce součástmi systému Windows

Jestliže inovujete ze systému Windows NT Server 4.0, kontrolou konfigurace po inovaci proveďte řádnou migraci služeb z předchozího operačního systému.

Terminálové služby

Terminálové služby umožňují spouštět klientské aplikace na serveru, takže klienti pak fungují jako terminály a nikoli jako nezávislé systémy. Server poskytuje prostředí více úloh a běží na něm programy systému Windows používané klienty. Terminálové služby lze také zavést pomocí **Průvodce součástmi systému Windows** (Windows Components Wizard). Další informace o terminálových službách najdete v kapitole „Zavádění terminálových služeb“ této knihy.

Databázový server

Aplikační členské servery systému Windows 2000 poskytují stabilní platformu pro spouštění a správu databázového softwaru, jako je například SQL Server. Po instalaci systému Windows 2000 Server není pro spuštění databázové služby zapotřebí žádná další konfigurace operačního systému.

Inovujete-li na systém Windows 2000 Server ze systému Windows NT verze 4.0 nebo dřívějšího, nezapomeňte před spuštěním inovace zálohovat všechny databáze na členském serveru. Používáte-li jinou databázovou aplikaci než SQL Server, ujistěte se také,

že je kompatibilní se systémem Windows 2000 Server. Další informace o aplikaci SQL Server najdete v knize *Microsoft SQL Server Resource Guide*, která je součástí sady *Microsoft BackOffice 4.5 Resource Kit*.

Webové servery

Webový server je počítač vybavený softwarem serveru, který v reakci na požadavky webových klientů na síti TCP/IP používá internetové protokoly, jako jsou protokol přenosu hypertextu (Hypertext Transfer Protocol – HTTP) a protokol přenosu souborů (File Transfer Protocol – FTP).

Dále jsou uvedeny obecné požadavky nastavení webových členských serverů systému Windows 2000:

- Přečtěte si seznam HCL a ujistěte se o kompatibilitě hardwaru.
- Určete, jaké nové či dodatečné součásti se objeví na webovém serveru.
- Zálohujte si data pro případ problémů během instalace nebo inovace.
- Po inovaci na systém Windows 2000 Server webové členské servery otestujte.

Součástí systému Windows 2000 Server je webová služba Internet Information Services (IIS). Pomocí IIS můžete zřídit webové sídlo nebo sídlo přenosu souborů na intranetu vaší společnosti, vytvářet sídla pro Internet nebo vyvíjet aplikace skládající se z komponent.

Systém Windows 2000 Server obsahuje modul snap-in Správce služeb sítě Internet (Internet Services Manager) konzoly Microsoft Management Console (MMC). Tento modul snap-in je výkonný nástroj správy sídla poskytující přístup ke všem nastavením serveru. Budete-li používat IIS, pomocí tohoto modulu snap-in budete spravovat složitá sídla na intranetu své společnosti nebo publikovat informace na Internet.

Doporučujeme vám webové servery po inovaci na systém Windows 2000 Server otestovat. Chcete-li ověřit spojení z nějakého členského serveru systému Windows 2000 na jiná webová sídla, vykonajte následující zkoušku:

- Na serveru si otevřete modul snap-in Správce služeb sítě Internet (Internet Services Manager) konzoly MMC a zkontrolujte, že všechna webová sídla (která existovala před inovací) byla úspěšně inovována na webovou službu na členském serveru Windows 2000. Provéřte, že služba běží.
- Na klientovi si otevřete webový prohlížeč a zkontrolujte spojení na webová sídla na daném členském serveru systému Windows 2000.

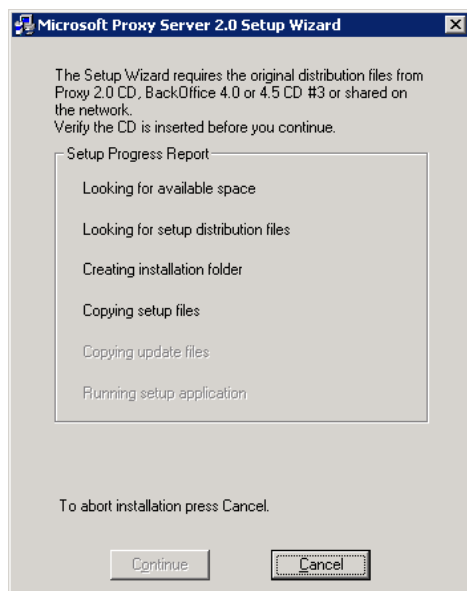
Další informace o IIS najdete v knize *Microsoft Internet Information Services 5.0 Resource Kit*.

Proxy-servery

Program Microsoft Proxy Server umožňuje klientům a serverům přístup na Internet a přitom chrání váš intranet před narušiteli. Členské servery se spuštěným programem Proxy Server 2.0 lze bez problémů inovovat, aby však systém Proxy Server fungoval i po instalaci, je zapotřebí jej aktualizovat.

Systém Windows 2000 Server vyžaduje nahrání průvodce instalací programem Proxy Server 2.0 na členském serveru. Chcete-li nainstalovat Proxy Server, nahrajte si průvodce instalací (viz obr. 15.4) na svůj místní pevný disk nebo disketu a postupujte podle jeho instrukcí. Další informace o nahrání kopie průvodce najdete v odkazu Microsoft

Proxy Server stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.



Obrázek 15.4 Průvodce instalací serveru Proxy Server 2.0

Vykonání úloh po inovaci a instalaci

Je důležité, abyste před integrací členského serveru do výrobního prostředí server otestovali a ujistili se, že inovace nebo instalace proběhla úspěšně. Před zapojením systému Windows 2000 Server do výrobního prostředí musí být zřejmé, že server poskytuje lepší služby a zvýšenou funkčnost a že nedojde k neplánovaným výpadkům.

Testování síťového připojení

Po inovaci nebo instalaci členského serveru musíte zkontrolovat jeho připojení k síti. Ztratíte-li připojení k síti v prostředí sítě TCP/IP, použijte k vyřešení problému následující seznam.

- Pomocí nástroje IPCONFIG ověřte konfigurační parametry protokolu TCP/IP na nově inovovaném systému Windows 2000 Server. Mezi tyto parametry patří adresa IP, maska podsítě a výchozí brána.
- Po kontrole konfigurace nástrojem IPCONFIG použijte k vyzkoušení síťového připojení nástroj PING. Je to diagnostický nástroj, který testuje konfiguraci TCP/IP a zjišťuje chyby připojení. Otevřete si okno příkazového řádku a zkontrolujte tyto položky:
 - Odešlete PING na adresu 127.0.0.1 (adresa zpětné smyčky). Tím se zkontroluje správná instalace a nahrání protokolu TCP/IP.
 - Odešlete PING na adresu IP místního hostitele. Tím se ověří jeho správné přidání.

- Odešlete PING na adresu IP výchozí brány. Tím se zkontroluje správná funkce výchozí brány.
- Odešlete PING na adresu IP vzdáleného hostitele. Tím se ověří možnost komunikace přes směrovač.

Ladění síťových serverů

Některé z členských serverů se systémem Windows 2000 na místní síti mohou vyžadovat ještě doladění výkonnosti. Ani ta nejdokonaleji naplánovaná inovace serverů nemusí být schopna eliminovat všechny problémy, které se mohou objevit, jako jsou například úzká místa v systému. Dojde-li k nějakému problému v systému, můžete jej odhalit pomocí prvků v modulu snap-in Sledování systému (System Monitor) systému Windows 2000 Server v rámci nástroje Výkon (Performance). Data lze sbírat sledováním procesoru, disku a síťových aktivit. Pomocí těchto dat odhalíte úzká místa v požadavcích na určité prostředky, které tak vyžadují další vyladění.

Úzká místa systému mohou být způsobena:

- Nedostatečnými prostředky jako jsou procesory, paměť nebo pevné disky.
To lze vyřešit zinventarizováním síťového hardwaru a určením, které servery potřebují inovaci hardwaru.
- Nevyrovnaná zatížení, která servery zatěžují nerovnoměrně.

K vyřešení tohoto problému slouží v systému Microsoft Windows 2000 Advanced Server nástroj Network Load Balancing (vyrovnávání zatížení sítí), který zajišťuje rovnoměrné rozložení zatížení prostředků. Další informace o nástroji Network Load Balancing a systému Microsoft Advanced Server najdete v kapitole „Zajištění dostupnosti aplikací a služeb“ v této knize.

Během ladění síťových serverů ještě pamatujte na následující:

- Zadávejte jen jednu změnu najednou, protože problém, který se jeví jako otázka nastavení nebo komponenty jediného prostředku, může ve skutečnosti představovat více prostředků. Také je jednodušší vrátit zpět jediné nastavení než skupinu nastavení a změna příliš mnoha nastavení najednou může ve skutečnosti vaši situaci zhoršit. Zaznamenávejte si zadané změny a jejich vliv na systém.
- Po každé změně sledujte systém a určete, zda měla na serveru pozitivní účinek.
- Podívejte se, zda nejsou v **Prohlížeči událostí** (Event Log Viewer) v sadě **Nástroje pro správu** (Administrative Tools) nějaké protokoly událostí vytvořené díky problémům s výkonností.

Nástroje pro správu systému

Většina úkolů správy systému Windows 2000 Server se zadává pomocí konzoly Microsoft Management Console (MMC) a přidružených modulů snap-in.

Tabulka 15.2 uvádí obvyklé nástroje pro správu souborových, tiskových a webových služeb.

Tabulka 15.2 Obvyklé úkoly správy

Úkol	Nástroj systému Windows 2000 Server
Správa míst sdílení souborů	Modul snap-in Správa počítače (Computer Management) konzoly MMC Průzkumník Windows
Správa míst sdílení tiskáren	Složka Tiskárny (Printer) v ovládacích panelech (Control Panel) nebo pod položkou Nastavení (Settings) v nabídce Start
Správa webových sídel	Modul snap-in Správce služeb sítě Internet (Internet Services Manager) konzoly MMC

Součástí systému Windows 2000 Server jsou také nástroje pro vzdálenou správu. Ty umožňují vzdálenou správu serveru z libovolného počítače se spuštěným systémem Windows 2000 Server.

Další informace o použití vzdálené správy najdete v nápovědě systému Windows 2000 Server.

Seznam úkolů plánování členských serverů

Tabulka 15.3 uvádí úkoly, které je zapotřebí vykonat při plánování inovace nebo instalace členských serverů.

Tabulka 15.3 Seznam úkolů plánování členských serverů

Úkol	Umístění v kapitole
Vytvořte plán a časový plán inovace/instalace členských serverů.	Plánování inovace a instalace členských serverů
Zinventarizujte existující hardware.	Příprava členských serverů na inovaci nebo novou instalaci
Určete požadavky systému.	Příprava členských serverů na inovaci nebo novou instalaci
Určete spolehlivost a kompatibilitu existujícího softwaru.	Příprava členských serverů na inovaci nebo novou instalaci
Určete kompatibilitu softwaru jiných výrobců.	Příprava členských serverů na inovaci nebo novou instalaci
Inovujte existující server.	Vykonání inovace nebo instalace
Vykonejte novou instalaci.	Vykonání inovace nebo instalace
Určete role serverů: – souborové servery – tiskové servery – aplikační servery – webové servery – proxy-servery	Určení rolí serverů jednotlivých systémů Windows 2000 Server
Otestujte připojení k síti.	Vykonání úloh po inovaci a instalaci
Vyladte síťové servery.	Vykonání úloh po inovaci a instalaci

KAPITOLA 16

Zavádění terminálových služeb

Terminálové služby (Terminal Services) poskytují klientským počítačům přístup k systému Microsoft Windows 2000 a nejnovějším aplikacím pro systém Windows. Zajišťují také z libovolného podporovaného klienta přístup na váš počítač a k instalovaným aplikacím. S touto zabudovanou funkcí systému Microsoft Windows 2000 by se měli seznámit manažeři IT a správci systémů, kteří chtějí zvýšit svou flexibilitu při zavádění aplikací, lépe řídit náklady na správu počítačů a vzdáleně spravovat síťové prostředky. Před studiem této kapitoly vám doporučujeme přečíst si kapitoly „Úvod do plánování zavedení systému Windows 2000“ a „Plánování zavedení“ v této knize.

V této kapitole

Přehled terminálových služeb 471

Vytváření plánu zavedení terminálových služeb 476

Vytváření návrhu zavedení terminálových služeb 483

Konfigurování serverů na zavedení terminálových služeb 495

Příprava na zavedení klientů 496

Plánování testování a pilotních programů 502

Použití skupiny odborné pomoci a nástrojů správy 504

Seznam úkolů plánování zavádění terminálových služeb 505

Cíle kapitoly

Tato kapitola vám pomůže vytvořit následující dokument plánování:

- Plán zavedení terminálových služeb

Přehled terminálových služeb

Terminálové služby (Terminal Services) spuštěné na systému Windows 2000 Server umožňují, aby k vykonávání klientských aplikací, zpracování dat a ukládání dat docházelo na serveru. Prostřednictvím softwaru *emulace terminálu* umožňují přístup na pracovní plochu serveru. Software emulace terminálu může pracovat na různých klientských hardwarových zařízeních, jako jsou osobní počítače, Handheld PC (HPC) se systémem Windows CE nebo terminály. Termín *terminál systému Windows* (Windows-based Terminal – WBT) obecně popisuje určitou třídu terminálových zařízení tenkých klientů, která mohou získat přístup na servery se spuštěným operačním systémem Windows pro více uživatelů, jako jsou například terminálové služby.

Pomocí terminálových služeb odesílá software emulace terminálu stisknuté klávesy a pohyby myši na server. Terminálový server zpracuje místně veškerá data a předá kli-

entovi zpět aktuální zobrazení. Tento postup umožňuje vzdálenou správu serverů a centralizovanou správu aplikací a navíc minimalizuje požadavky na šířku přenosového pásma mezi serverem a klientem.

Uživatelé mohou získat přístup k terminálovým službám přes libovolné spojení protokolem Transmission Control Protocol/Internet Protocol (TCP/IP) včetně vzdáleného přístupu (Remote Access), Ethernetu, Internetu, bezdrátového připojení, rozlehlé sítě (WAN) nebo virtuální privátní sítě (VPN). Uživatelé jsou pak omezeni pouze charakteristikami nejslabšího článku spojení a zabezpečení spojení je určeno zavedením protokolu TCP/IP v datovém středisku.

Terminálové služby umožňují vzdálenou správu síťových prostředků, jednotné prostředí pro všechny uživatele v pobočkách ve vzdálených lokacích a grafické prostředí k obchodním aplikacím na textových počítačích. Mezi výhody terminálových služeb patří:

- Je umožněno používání 32bitových aplikací pro systém Windows na zařízeních, která nemusí být založena na systému Windows, jako například:
 - Systém Windows for Workgroups 3.11 nebo novější
 - Terminály systému Windows (zařízení Windows CE)
 - Klienti se systémem MS-DOS
 - Terminály systému UNIX
 - Systém Macintosh
- Klienti bez systému Windows vyžadují použití doplňku jiného výrobce.
- Klienti terminálových služeb potřebují jen minimální prostor na disku, paměť a konfiguraci.
- Zjednodušuje se podpora vzdálených počítačů a prostředí poboček.
- Je zajištěno centralizované zabezpečení a řízení.
- Nijak nejsou omezeny aplikace a existující infrastruktura sítě.

Terminálové služby jsou zabudovanou funkcí systému Windows 2000. Terminálové služby lze spustit v jednom ze dvou režimů:

Vzdálená správa

Funkce vzdálené správy představuje pro správce systému významnou metodu vzdálené správy jednotlivých serverů se systémem Windows 2000 přes libovolné připojení TCP/IP. Lze spravovat sdílení souborů a tiskáren, upravovat registr z jiného počítače na síti a vykonávat jiné úkoly, jako byste seděli přímo u konzoly. Režim vzdálené správy lze použít ke správě serverů, které nejsou normálně kompatibilní s režimem vzdálené správy terminálových služeb, jako jsou například servery se spuštěnými klastrovými službami. Další informace o použití klastrů v systému Windows najdete v kapitole „Zajištění dostupnosti aplikací a služeb“ v této knize.

Režim vzdálené správy instaluje pouze komponenty vzdáleného přístupu terminálových služeb. Neinstaluje komponenty sdílení aplikací. To znamená, že vzdálenou správu lze použít s minimální ztrátou výkonu i na nejdůležitějších serverech, jejichž provoz musí být vždy zajištěn. Terminálové služby umožňují nejvýše dvě současná připojení vzdálené správy. Pro tato připojení nejsou zapotřebí žádné další licence a nepotřebujete ani licenční server.

Aplikační server

V režimu aplikačního serveru lze aplikace zavádět a spravovat z centrálního místa, čímž se šetří čas správců potřebný pro vývoj a zavádění, stejně jako čas a námaha související s údržbou a inovováním. Po zavedení aplikace v terminálových službách ji může používat mnoho klientů – přes připojení vzdáleného přístupu, místní síť (LAN) a rozsáhlou síť (WAN) a z mnoha různých typů klientů.

Aplikace lze instalovat přímo na terminálový server, nebo můžete použít vzdálenou instalaci. K publikování balíčků aplikací nástroje Windows Installer na terminálový server nebo na skupinu terminálových serverů lze například použít zásady skupiny a Active Directory. Aplikace lze na jednotlivých serverech instalovat pouze prostřednictvím účtu Administrator a navíc pouze pokud je zavedeno potřebné nastavení zásad skupiny.

Terminálové služby nedokáží předat aplikaci adresy internetového protokolu (Internet Protocol – IP) jednotlivých klientských počítačů. Protože právě to vyžaduje klastrová služba systému Windows, nelze provozovat klastrovou službu v režimu aplikačního serveru.

Při zavádění terminálového serveru jako aplikačního serveru je vyžadováno licencování klienta. Každý klientský počítač bez ohledu na protokol používaný pro připojení k terminálovému serveru musí mít licenci klientského přístupu terminálových služeb a licenci klientského přístupu systému Windows 2000.

Licenční komponenty terminálových služeb

Terminálové služby mají svou vlastní metodu licencování klientů, kteří se připojují k terminálovým serverům, jež se od metody licencování klientů pro systém Windows 2000 Server liší. Licencování terminálových služeb zahrnuje následující součásti: Microsoft Clearinghouse, licenční server, terminálový server a klientské licence.

Microsoft Clearinghouse

Microsoft Clearinghouse je databáze udržovaná společností Microsoft, jejímž smyslem je aktivovat licenční servery a vystavovat sadu Key Pack licence klienta pro licenční servery, které je požadují. Databáze Clearinghouse obsahuje informace o všech aktivovaných licenčních serverech a vystavených sadách Key Pack licencí klientů. K databázi Clearinghouse je možné přistoupit prostřednictvím průvodce licencováním, který je součástí funkce licencování terminálových služeb.

Licenční server

Na licenčním serveru jsou uloženy všechny klientské licence terminálových služeb nainstalované pro určitý terminálový server a licenční server také sleduje licence vystavené klientským počítačům nebo terminálům. Terminálový server musí být schopen připojit se k aktivovanému licenčnímu serveru, aby bylo možné vystavovat licence klientům. Jeden aktivovaný licenční server může obsluhovat několik terminálových serverů najednou.

Terminálový server

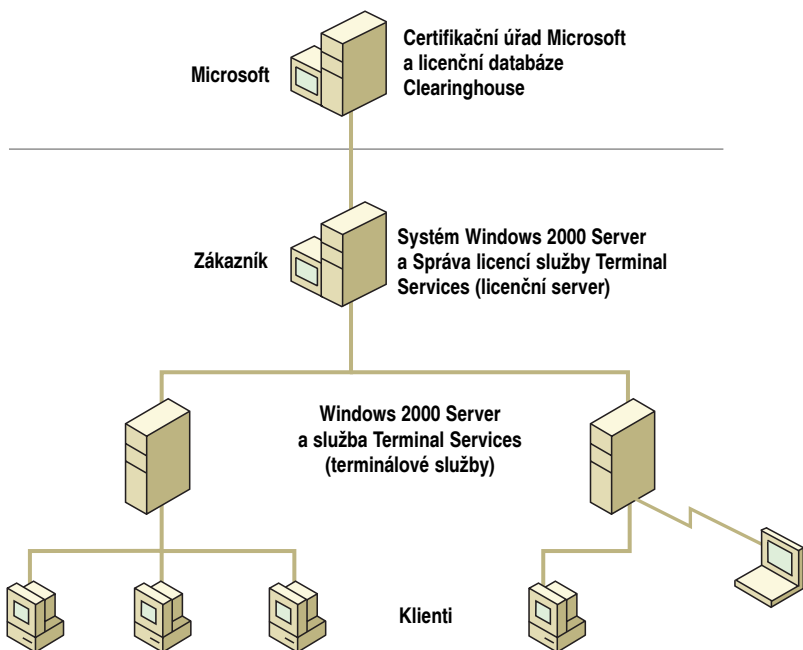
Terminálový server je počítač, na kterém jsou povoleny terminálové služby. Poskytuje klientům přístup k aplikacím systému Windows, které pracují výhradně na serveru, a podporuje více relací klientů na server. Během přihlašování klientů na terminálový

server ověří server klientské licence. Nemá-li klient licenci, terminálový server ji bude pro klienta požadovat od licenčního serveru.

Klientské licence

Každý klientský počítač nebo terminál, který se připojuje k terminálovému serveru, musí mít platnou klientskou licenci. Klientská licence je uložena místně a předá se terminálovému serveru po každém připojení klienta k serveru. Server ověří licenci a pak umožní klientovi připojení.

Obrázek 16.1 zobrazuje licenční komponenty terminálových služeb.



Obrázek 16.1 Licenční součásti terminálových služeb

Další informace o nastavení licenčních součástí terminálových služeb najdete v oddílu „Nastavení licenčního serveru“ dále v této kapitole.

Požadované licence

Zavedení terminálových služeb a klientů terminálových služeb na síti vyžaduje následující licence:

Licence systému Windows 2000 Server Tato licence je součástí tohoto zakoupeného produktu.

Licence klientského přístupu k systému Windows 2000 Server Tuto licenci musí mít každé zařízení, které se připojuje k systému Windows 2000 Server. Licence klientského přístupu umožňují klientům používat souborové, tiskové a další síťové služby poskytované systémem Windows 2000 Server. Součástí terminálových služeb systému Windows 2000 Server vyžaduje licencování jednotlivých počítačů, pokud si tedy nekoupí-

te licenci Internet Connector terminálových služeb systému Windows 2000. licence Internet Connector je popsána dále v této kapitole.

Každý klientský počítač nebo terminál vyžaduje následující licence:

Licence klientského přístupu k systému Windows 2000 Server nebo licence systému Windows 2000

Licence klientského přístupu dává každému klientskému počítači nebo terminálu se systémem Windows právo přistupovat k terminálovým službám na systému Windows 2000 Server. Tato licence je například zapotřebí k uskutečnění terminálové relace a spuštění aplikací systému Windows na serveru. Licence systému Windows 2000 umožňuje kromě práva přistupovat k terminálovým službám na systému Windows 2000 Server také právo nainstalovat si operační systém Windows 2000. Licence klientského přístupu k terminálovému serveru není zapotřebí u klientů, kteří se připojují k terminálovým serverům výhradně v režimu vzdálené správy.

Volitelné licence terminálových služeb

Kromě požadovaných licencí terminálových služeb existují ještě dvě volitelné licence: licence Internet Connector terminálových služeb systému Windows 2000 a licence Work at Home klientského přístupu k terminálovým službám systému Windows 2000.

Licence Internet Connector terminálových služeb systému Windows 2000

Místo licencí klientského přístupu si můžete koupit licenci Internet Connector terminálových služeb systému Windows 2000. Tato licence se prodává samostatně jako doplňková licence k systému Windows 2000 Server. Umožňuje maximálnímu počtu 200 uživatelů současně anonymní připojení k terminálovému serveru přes Internet. To je užitečné pro organizace, které chtějí představit software pro Windows uživatelům Internetu, aniž by museli aplikace pro Windows přepisovat na aplikace pro Web. Žádní z uživatelů, kteří chtějí přistupovat k terminálovému serveru s touto licencí, nesmějí být zaměstnanci dané společnosti.

Použijete-li licenci Internet Connector ve spojení s určitým systémem Windows 2000 Server, terminálové služby umožňují pouze přístup anonymním klientům. Licenci Internet Connector nelze používat ve spojení s jinými typy licencí klientského přístupu k terminálovým službám na stejném systému Windows 2000 Server.

Licence Work at Home klientského přístupu k terminálovým službám systému Windows 2000

Licence Work at Home klientského přístupu k terminálovým službám, jež je dostupná prostřednictvím licenčních programů Microsoft Volume, je určena pro organizace, které chtějí používat terminálové služby k zajištění přístupu na kancelářské počítače systému Windows 2000 a k 32bitovým aplikacím pro systém Windows svým zaměstnancům. Ke každé zakoupené licenci systému Windows 2000 Professional nebo licenci klientského přístupu k terminálovým službám si můžete koupit ještě licenci Work at Home klientského přístupu k terminálovým službám systému Windows 2000.

Rozšíření od jiných výrobců

Nástroj MetaFrame je doplněk terminálových služeb systému Windows 2000 od společnosti Citrix Systems. Obsahuje protokol Citrix Independent Computing Architecture (ICA) a zajišťuje rozšířené možnosti pro:

- Klientská zařízení
- Síťová připojení
- Místní systémové prostředky

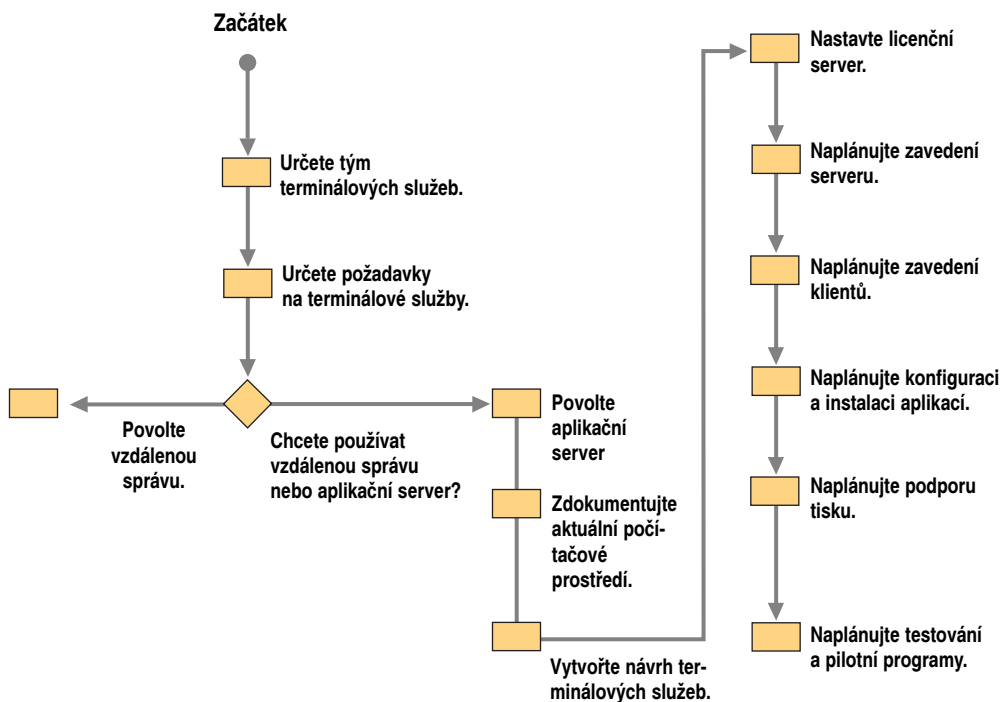
MetaFrame také zahrnuje různé nástroje pro správu, které se používají s terminálovými službami systému Windows 2000. Další informace o nástroji MetaFrame zjistíte u společnosti Citrix Systems.

Vytváření plánu zavedení terminálových služeb

Když nyní znáte možnosti terminálových služeb a požadavky na licencování, můžete vstoupit do fáze plánování zavedení terminálových služeb. Tento oddíl vám pomůže se získáním informací potřebných k vytvoření plánu zavedení terminálových služeb ve vaší organizaci.

Proces zavedení terminálových služeb

Než začnete s fází plánování zavedení terminálových služeb, zamyslete se nad využitím postupu zobrazeného na obrázku 16.2.



Obrázek 16.2 Proces zavádění terminálových služeb

Všechny uvedené činnosti jsou popsány v následujících oddílech.

Určení týmu terminálových služeb

Týmová práce je zásadní otázkou plánování a zavádění terminálových služeb. Plánování musí zahrnovat správce systémů, kteří budou mít na starosti síťové problémy, správ-

ce, kteří se budou starat o aplikace terminálových služeb, a další osoby zodpovědné za vaše obchodní či výrobní jednotky.

Jádro plánovacího týmu musí určit obchodní potřeby, které budou terminálové služby zajišťovat, a navrhnout zavedení terminálových služeb.

Určení požadavků terminálových služeb

Po sestavení týmu bude jeho prvním úkolem určit, jaké obchodní či výrobní scénáře budou terminálové služby řešit. Scénáře v tomto oddílu vám pomohou určit, jak lze terminálové služby ve vaší organizaci co nejlépe využít. S požadavky jednotlivých scénářů se seznámte, ještě než začnete plánovat zavádění.

Scénář 1: Vzdálená správa pomocí terminálových služeb

Vzdálená správa pomocí terminálových služeb umožňuje správcům systému s potřebnými oprávněními vzdáleně spravovat jednotlivé servery se systémem Windows 2000 přes připojení TCP/IP.

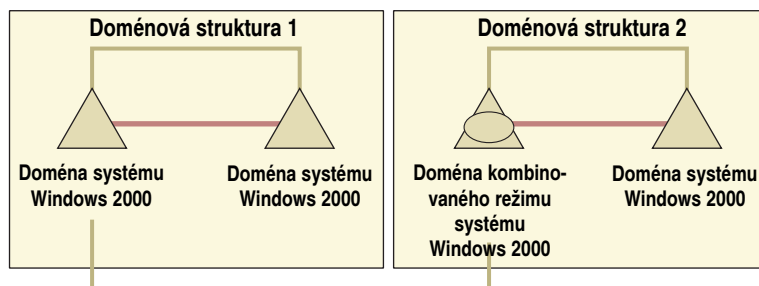
V tomto scénáři používá správce systému ke vzdálené správě serverů v jejich vlastní adresářové doméně určité funkce, například modul Domain Manager konzoly Microsoft Management Console (MMC), a správu adresářové služby.

Povolením terminálových služeb v režimu vzdálené správy se správa serveru rozšíří do doménových struktur a domén kombinovaného režimu, kde jsou počítače se systémy Windows 2000 i Microsoft Windows NT. Pomocí služby Windows Clustering lze správu serverů rozšířit i na klastrové servery. Je-li na všech serverech spuštěn systém Windows 2000, vzdálenou správu lze zavést na všech serverech v podniku, což umožní přímé připojení a správu.

Protože povolení terminálových služeb má na server jen malý dopad, doporučuje se povolení terminálových služeb na všech serverech v doménové struktuře. Pokud v takové situaci vypadne jeden ze serverů, jiný ho nahradí. V případě kombinovaných prostředků nebo v situacích, kdy musí být řízení omezeno, lze zavést vzdálenou správu pouze na omezeném počtu serverů, například na řadičích domén. Ostatní servery lze spravovat přes doménu standardními nástroji správy. V obou případech platí, že správu lze spustit z libovolné platformy podporující klienta terminálových služeb; nemusí se jednat o systém Windows 2000.

V režimu vzdálené správy mají terminálové služby dvě zabudovaná připojení na server (per-server), která nevyžadují žádnou speciální instalaci ani zvláštní licencování.

Obrázek 16.3 ukazuje správu serveru pomocí vzdálené správy přes doménové struktury a do domény fungující v kombinovaném režimu.



Obrázek 16.3 Vzdálená správa rozšiřuje správu serveru

Scénář 2: Vzdálený přístup

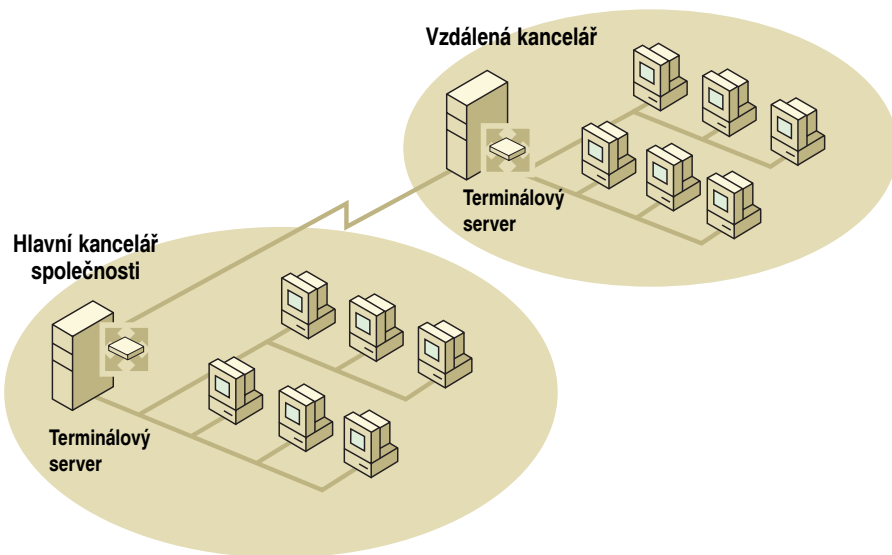
Vzdálený přístup rozšiřuje možnosti terminálových služeb přes externí připojení TCP/IP. Možnosti uživatele jsou omezeny pouze charakterem nejslabšího článku v propojení.

V tomto scénáři mohou uživatelé ve vzdálené kanceláři s klientským softwarem terminálových služeb na počítačích přistupovat k účetní aplikaci na terminálovém serveru v centrální kanceláři. K základním datům společnosti tak lze přistupovat pomocí připojení vzdáleného přístupu uskutečněného modemem. Protože mezi serverem a klientem se přenáší jen základní informace z klávesnice a informace zobrazení, požadavky na šířku pásma jsou velmi nízké a plná funkčnost je umožněna i uživatelům s pomalým modemovým připojením. Bez zvyšování potřeby šířky pásma lze přidávat více aplikací, pokud tedy intenzivně nepracují s grafikou.

Než někdo v pobočkové kanceláři může přistoupit k vašim síťovým prostředkům, musí uvést svá oprávnění a musí být plně ověřen. Při směrování přístupu k síťovým prostředkům přes terminálový server můžete použít další vrstvu zabezpečení.

Podobný princip lze použít pro umožnění přístupu k aplikacím, které se používají jen zřídka či již byly odstraněny, nebo k aplikacím, které se teprve vyvíjejí.

Obrázek 16.4 ukazuje způsob, jakým se zaměstnanci ve vzdálené kanceláři mohou připojit k hlavní kanceláři společnosti pomocí spojení TCP/IP.



Obrázek 16.4 Vzdálená kancelář a hlavní kancelář propojené spojením TCP/IP

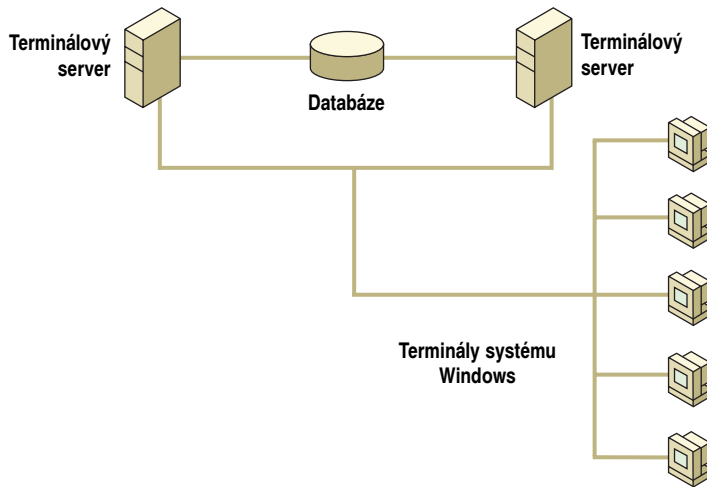
Scénář 3: Obchodní aplikace

Režim aplikačního serveru terminálových služeb se ideálně hodí k zavedení obchodních aplikací, zejména takových, které se obtížně instalují nebo se musí často inovovat. V tomto scénáři přistupují operátoři zadávání dat k obchodním aplikacím a tak zadávají informace o výrobku do nějaké databáze. Protože daná aplikace běží na terminálo-

vém serveru, operátoři zadávání dat pracují na terminálech systému Windows a nikoli na klientských počítačích. Dojde-li k výpadku serveru, klientská zařízení se mohou připojit k jinému serveru. Tento režim podporuje ukládání dat odděleně od terminálových serverů a pomocí vyrovnávání zatížení sítě ve skupině terminálových serverů umožňuje řízení přepnutí při chybě. Dojde-li k výpadku nějakého terminálu, lze jej nahradit s minimálním vyrušením operátora zadávání dat.

V celé organizaci jsou oddělení uspořádána a zabezpečení je vytvořeno tak, aby byl zajištěn potřebný přístup k informacím a síťovým prostředkům, které jsou zapotřebí pro úkoly jednotlivých uživatelů.

Obrázek 16.5 ilustruje způsob, jakým mohou operátoři zadávání dat zadávat informace o výrobku do databáze pomocí obchodní aplikace umístěné na terminálovém serveru.



Obrázek 16.5 Řada obchodních aplikací na terminálových serverech

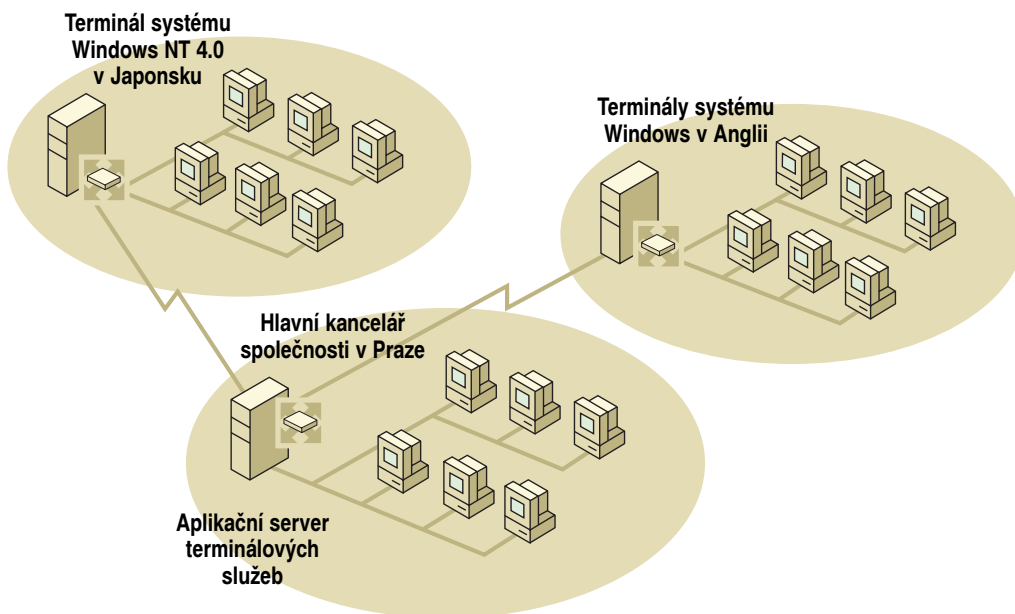
Scénář 4: Centrální zavádění kancelářských počítačů

Centrálního zavádění kancelářských počítačů se dosahuje nahráním desktopových aplikací na server systému Windows 2000 se spuštěnými terminálovými službami v režimu aplikačního serveru. Každý klientský počítač má jedinou malou aplikaci emulující desktop systému Windows jednotlivých uživatelů. Vlastní programy ve skutečnosti běží na serveru.

V tomto scénáři zajistí velká společnost zaměstnancům po celém světě spolehlivý přístup k výrobním a starším aplikacím i k nástrojům produktivity práce v kanceláři. Jsou-li na serveru se systémem Windows 2000 aktivovány terminálové služby, klienti mohou spouštět řízenou, standardizovanou sadu aplikací, a to i když se nacházejí na vzdálených místech nebo pracují na starším hardwaru. Příslušná přístupová práva klientů zajistí zabezpečení systému.

Protože počítač s Windows je tak dostupný všem uživatelům, vývojáři mohou pomocí nástrojů, jako je například Microsoft Visual Basic, ve svých aplikacích používat standardní uživatelské rozhraní systému Windows.

Obrázek 16.6 ukazuje způsob, jakým může organizace zajistit pomocí terminálových služeb celosvětový přístup k určitým aplikacím a nástrojům.



Obrázek 16.6 Centrální zavádění aplikací a nástrojů pomocí terminálových služeb

Požadavky na zavedení

Předchozí scénáře terminálových služeb se často překrývaly. Například uživatelé, kteří přistupují ke svému počítači přes centrální počítač, někdy tak zároveň činí prostřednictvím vzdáleného přístupu využívajícího modem. Před zavedením terminálových služeb ve vaší organizaci si pečlivě prostudujte požadavky jednotlivých scénářů uvedené v tabulce 16.1.

Tabulka 16.1 Požadavky na zavedení

	Vzdálená správa	Vzdálený přístup	Řada obchodních aplikací	Zavedení centrálního počítače
Licencování		X	X	X
Licenční server		X	X	X
Doménová struktura	X		X	X
Vyrovňování zatížení		X	X	X
Cestovní profily	X			
Místní tisk	X	X	X	X
Zabezpečení	X	X	X	X

Příprava počítačového prostředí

Před vytvořením návrhu zavedení terminálových služeb se musíte dokonale seznámit s aktuálním počítačovým prostředím. Další informace o dokumentování vašeho počítačového prostředí najdete v kapitole „Plánování zavedení“ v této knize. Další informace související se zaváděním terminálových služeb, najdete v následujících úvahách.

Instalace licenčního serveru na řadič domény

V doménách systému Windows 2000 musí být licenční server instalován na řadiči domény. V pracovních skupinách a doménách systému Windows NT 4.0 lze instalovat licenční server na libovolný server se systémem Windows 2000. Plánujete-li však migraci z pracovní skupiny nebo domény systému Windows NT na doménu systému Windows 2000, rozhodně vám doporučujeme nainstalovat licenční server na řadič domény nebo na počítač, který lze na řadič domény povýšit.

Přístup přes rozsáhlou síť

Zjistěte, zda nebyly na směrovačích nebo firewallech zavedeny filtry, které by mohly zabránit klientům v získání vzdáleného přístupu k terminálovému serveru. Také zkontrolujte, že není na firewallu blokovaný port protokolu Remote Desktop Protocol (RDP) (port 3389) a že přístup k určitým segmentům společnosti není omezen na síťové adresy protokolů Internet Protocol (IP) nebo Internetwork Packet Exchange (IPX). Je-li nastaveno toto blokování vzdálených připojení, tým je musí během zavádění nějakým způsobem vyřešit.

Přístup k síťovým službám

Možná budete chtít zákazníkům nebo dodavatelům umožnit přístup k určitým aplikacím či datům. Můžete také zjistit, že nejjednodušší způsob, jakým mohou uživatelé získat přístup k terminálovým službám, je Internet. Plánujete-li zpřístupnění serverů přes Internet, zamyslete se nad bezpečnostními dopady.

Jestliže vaše organizace používá firewall, zjistěte, zda jde o firewall pracující na úrovni paketů nebo aplikací. Firewally pracující na úrovni paketů lze snáze nakonfigurovat na nové protokoly. Pokud vaše organizace používá firewall pracující na úrovni aplikací, zjistěte, zda jeho výrobce definoval filtr pro protokol RDP. Není-li tomu tak, výrobce kontaktujte a požádejte jej o vytvoření potřebného filtru.

Zdokumentujte metodu, kterou síť používá k připojení k Internetu. To vám pomůže určit, jaká šířka pásma zbývá pro terminálové služby. Má síť trvalé připojení? Popište počet a typ linek používaných k připojení, jako jsou linky T1 nebo linky Integrated Services Digital Network (ISDN).

Připojení klienta a serveru terminálových služeb

Protokol RDP podporuje připojení TCP/IP mezi klientem a serverem terminálových služeb. Takové připojení může být vytvořeno pomocí síťových a telefonických připojení, nativně na místní síti LAN nebo připojením VPN přes rozsáhlou síť. Terminálové služby by použily libovolné připojení IP. Je však důležité zvážit, zda typ poskytnutého připojení odpovídá vykonávané práci a zda jím zajištěné zabezpečení odpovídá přenášeným datům. Jediný uživatel může dobrého výkonu dosáhnout i prostřednictvím analogového modemu, rozhodně však nebude možné sdílet linku 28,8 kb/s v celé kanceláři se 100 uživateli.

Přístup k aktuálnímu prostředí

Vytvořte podrobné vyhodnocení aktuálního prostředí včetně terminálů systému Windows, klientských počítačů, terminálů se zelenými obrazovkami, počítačů Macintosh, pracovních stanic UNIX, terminálů UNIX X a větších přenosných zařízení. Nepokoušejte se zdokumentovat jednotlivé počítače. Postačí odhadnout počty a popsat standardy v celé divizi nebo organizaci. Mezi úlohy tohoto vyhodnocení patří:

- Zajistěte přehled celkového počtu aktuálně používaných klientských počítačů.
- Popište aktuální konfiguraci počítačů, na kterých budou pracovat klienti terminálových služeb ve smyslu procesorů, operačních systémů, dostupného diskového prostoru, paměti RAM a grafiky. Zaznamenejte si všechny oficiální i neoficiální standardy, které existují ve vaší divizi nebo v celé organizaci, a označte počítače, které jsou pod tímto standardem. Všechny klientské počítače, které nesplňují minimální standardy, je zapotřebí inovovat nebo nahradit. Podívejte se na počet jednotlivých tříd svých klientů a určete standard, který bude maximalizovat váš konkrétní poměr mezi náklady a získanými výhodami.
- Zdokumentujte, kolik terminálů existuje ve vašem prostředí a jakého jsou typu, což zahrnuje také všechny existující terminály systému Windows, které budou používány v rámci terminálových služeb, a všechny terminály se zelenými obrazovkami a terminály UNIX X, které budou muset být nahrazeny.

Terminály se zelenými obrazovkami nelze používat jako klienty terminálového serveru; v některých případech si je můžete ponechat pro přístup ke starším mainframovým systémům nebo je můžete inovovat na terminály systému Windows a získat tak přístup k terminálovým službám i k mainframovému počítači.

- Zdokumentujte všechny systémy, se kterými musí klienti terminálových služeb komunikovat. Jestliže aktuální klientské počítače získávají přístup k těmto systémům přes bránu jiného systému než Windows 2000, možná bude zapotřebí instalovat novou bránu. Určete, zda má vaše společnost příslušné licence potřebné pro získání přístupu k těmto systémům z prostředí systému Windows.

Úvahy o zavádění aplikací

Zdokumentujte aplikace, které zamýšlíte zavést na klientské počítače pomocí terminálových služeb. Některé aplikace mají funkce, jež jim znemožňují pracovat v rámci terminálových služeb nebo způsobují jejich slabou výkonnost. Z tohoto důvodu je lepší říci uživatelům, aby si takové aplikace nainstalovali místně, kde je to proveditelné. Zjména musíte zjistit následující údaje:

- Aplikace požadující ke své funkci speciální hardware, jako jsou čtečky čárových kódů nebo čtečky karet. Tato zařízení lze používat ve spojení s klientem terminálových služeb, pouze pokud se připojují ke klientskému počítači nebo terminálu takovým způsobem, že počítač rozpozná periferní zařízení jako zařízení typu klávesnice. Periferní zařízení, která se připojují k místnímu počítači paralelním či sériovým portem nebo speciální kartou, v současné době klient terminálového serveru protokolu RDP nerozpozná.
- Multimediální aplikace nebo aplikace s velmi velkým grafickým výstupem nepracují pod terminálovými službami uspokojivě. Do této kategorie spadá mnoho her a také aplikace s datovými toky různých médií.

V jiných případech aplikace fungují, ale vyžadují speciální instalační nebo vykonávací skripty. Obvykle takové skripty řeší problémy programu, jako je špatné používání registru nebo chybějící podpora ukládání souborů pro více uživatelů. Po skriptech terminálových služeb se ptejte u výrobce dané aplikace. Další informace o tomto tématu najdete v odkazu Terminal Services Application Information stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Pokud jste své vlastní aplikace nenapsali jako víceuživatelské, mohou také vyžadovat úpravy nebo podpůrné skripty. Další informace o vytváření skriptů najdete v odkazu Terminal Services Creating Installation and Execution Scripts na stránce webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Poznámka Uživatelé, kteří nejsou správci, nemohou používat k instalaci aplikací na terminálový server technologii Windows Installer.

Vytváření návrhu zavedení terminálových služeb

Po identifikaci svých obchodních a výrobních potřeb a inventarizaci počítačového prostředí můžete začít plánovat zavedení terminálových služeb. Tento oddíl vám pomůže se získáním informací potřebných pro vytvoření plánu zavedení terminálových služeb ve vaší organizaci.

Nastavení licenčního serveru

Jestliže budou terminálové služby pracovat v režimu aplikačního serveru, je zapotřebí licenční server. Licenční služba terminálových služeb má jen minimální nároky – ukládá klientské licence, které byly vystaveny pro určitý terminálový server, a sleduje licence, které byly vystaveny klientským počítačům nebo terminálům.

Licenční server musí být aktivován pomocí databáze Microsoft Clearinghouse a z této databáze do něj musí být nahrány licence přístupu klientů, které se budou dále distribuovat. Terminálové servery přistupují k licenčnímu serveru, pouze pokud potřebují vystavit nové licence, a licenční server je zapotřebí spravovat výhradně ve smyslu získání licencí z databáze Clearinghouse.

Povolení licenčního serveru

Licenční služby terminálových služeb lze na počítači aktivovat během instalace systému Windows 2000 Server. Doporučujeme vám aktivaci terminálových služeb na nějakém členském serveru nebo samostatném serveru a instalování licenčního serveru na jiný počítač.

Existují dva typy licenčních serverů, licenční server domény a licenční server podniku. Před instalací licenčního serveru zvažte, který z těchto dvou typů licenčních serverů budete potřebovat:

- Doménový licenční server je vhodný, chcete-li mít v každé doméně samostatný licenční server. Máte-li pracovní skupiny nebo domény systému Windows NT 4.0, můžete nainstalovat jen doménový licenční server. Terminálové servery mohou přistupovat k doménovým licenčním serverům, pouze pokud se nacházejí ve stejné doméně jako licenční server. Licenční server se standardně instaluje jako doménový licenční server.

- Podnikový licenční server může obsluhovat terminálové servery ve všech doménách v rámci síťového sídla, musí však jít o domény systému Windows 2000. Dokáže obsluhovat pouze terminálové servery ve stejném síťovém sídle. Tento typ licenčního serveru je vhodný, máte-li mnoho domén. Podnikové licenční servery lze instalovat pouze pomocí ovládacího panelu Přidat nebo odebrat programy (Add/Remove Programs) a nikoli během instalace systému Windows 2000.

Při určování, kam se má na fyzickou síť licenční server zavést, uvažte, jak terminálový server licenční server objeví a bude s ním komunikovat. Při aktivaci terminálových služeb pro systém Windows 2000, začne terminálový server hledat v doméně a Active Directory systému Windows 2000 nějaký licenční server (v prostředí pracovních skupin bude terminálový server vysílat všem serverům v pracovní skupině na stejné podsíti).

Terminálový server hledá doménový licenční server každých 15 minut a existenci podnikového licenčního serveru v adresářové službě kontroluje každou hodinu. Najde-li terminálový server doménový licenční server, bude jej následně kontrolovat každé dvě hodiny. Nedokáže-li terminálový server najít doménový licenční server, pak jej začne vyhledávat každých 15 minut. Je-li nalezen podnikový licenční server, terminálový server kontroluje adresářovou službu každou hodinu. Tyto kontroly představují zanedbatelný síťový provoz.

Poznámka V doménách systému Windows 2000 musí být doménový licenční server nainstalován na řadiči domény. V pracovních skupinách a doménách systému Windows NT 4.0 může být doménový licenční server nainstalován na libovolném serveru. Plánujete-li migraci z pracovní skupiny nebo domény systému Windows NT 4.0 na domény systému Windows 2000, bude vhodné instalovat licenční server na počítač, který bude povýšen na řadič domény systému Windows 2000.

Chcete-li rychle aktivovat licenční server a přistoupit k databázi Microsoft Clearinghouse přes Internet, nainstalujte server na počítač s přístupem k Internetu.

Licenční server systému Windows 2000 musíte zavést do 90 dnů od povolení terminálového serveru systému Windows 2000. Nepovolíte-li licenční službu na serveru se systémem Windows 2000 do skončení tohoto období, terminálové služby systému Windows 2000 nebudou fungovat.

Aktivování licenčního serveru

Aby byl server identifikován a mohl vystavovat klientské licence pro terminálové servery, musí být licenční server aktivován. Licenční server se aktivuje pomocí Průvodce správou licencí.

Existují čtyři metody aktivování licenčního serveru:

- Přes Internet
- Pomocí Webu
- Faxem
- Telefonicky

Je-li počítač, na kterém je spuštěn nástroj licencování terminálových služeb, připojen k Internetu, je metoda aktivace přes Internet nejjednodušší a nejrychlejší. Průvodce správou licencí vás nasměruje na zabezpečené webové sídlo společnosti Microsoft, kde se aktivují licenční servery. Jakmile aktivujete licenční server, společnost Microsoft jej vybaví digitálním certifikátem, který zaručuje vlastnictví a identitu serveru. Pomocí to-

hoto certifikátu může licenční server následně vykonávat transakce se společností Microsoft a přijímat licence přístupu klientů pro vaše terminálové servery.

Není-li váš licenční server připojen k Internetu, ale vy máte možnost přistupovat k síti World Wide Web prostřednictvím prohlížeče na jiném počítači, můžete aktivovat svůj licenční server metodou webové aktivace. Průvodce správou licencí vás nasměruje na zabezpečené webové sídlo společnosti Microsoft, kde obdržíte certifikát licenčního serveru.

Alternativní metody aktivování licenčního serveru zahrnují faxování informací nebo volání nejbližšího centra zákaznické podpory (Customer Support Center – CSC). S tím vám také pomůže Průvodce správou licencí, s jehož pomocí zjistíte i příslušné telefonní nebo faxové číslo. Použijete-li metodu aktivování faxem, potvrzená žádost se vám vrátí od společnosti Microsoft. Použijete-li metodu aktivace přes telefon, váš požadavek vyřídí představitel služby zákazníkům telefonicky.

Licenční server je zapotřebí aktivovat jen jednou. Při čekání na dokončení aktivčního procesu může váš licenční server vystavovat pro klienty dočasné licence, které jim umožní používat terminálové servery po dobu až 90 dnů.

Digitální certifikát, který jednoznačně identifikuje váš licenční server, je uložen ve formě identifikátoru (ID) licenčního serveru. Kopii tohoto čísla si uložte na bezpečné místo. Chcete-li si toto číslo zobrazit po aktivování licenčního serveru, vyberte licenční server a z nabídky **Zobrazit** (View) zadejte příkaz **Vlastnosti** (Properties). Nastavte metodu komunikace na server WWW a stiskněte tlačítko **OK**. Pak vyberte příkaz **Nainstalovat licence** (Install Licenses) nabídky **Akce** (Action) a stiskněte tlačítko **Další** (Next). Uprostřed obrazovky Průvodce správou licencí je uvedeno identifikační číslo licenčního serveru.

Instalace licencí

Aby bylo povoleno nastavení Internet Connector a aby mohli klienti jiného systému než Windows 2000 trvale přistupovat k terminálovému serveru systému Windows 2000, musí být na licenčním serveru instalovány licence terminálové služby. Licence klientského přístupu k terminálovým službám systému Windows 2000 a licence Internet Connector si můžete koupit standardní metodou. Po koupi je instalujete pomocí Průvodce správou licencí.

Stejně jako existují čtyři metody aktivace licenčního serveru, existují také čtyři metody instalace licencí terminálových služeb. Po instalaci licencí vás program požádá o potvrzení týkající se koupě licencí. Jde o tyto informace:

- Jestliže jste licence zakoupili prostřednictvím smlouvy Microsoft Select nebo Enterprise, program po vás bude požadovat číslo souhlasu se zápisem (Enrollment Agreement Number).
- Pokud jste licence získali prostřednictvím Microsoft Open License, program bude požadovat číslo ověření a licenční číslo.
- Jestliže jste licence zakoupili pomocí sady Microsoft LicensePak, program bude potřebovat 25znakový licenční kód, který je uveden v balíčku Microsoft LicensePak.

Po instalaci licencí může váš licenční server začít vystavovat licence. Klienti s 90denními dočasnými licencemi budou při svém dalším přihlášení inovováni na licence klientského přístupu k terminálovým službám (pokud počet instalovaných licencí klientského přístupu nepřekročí počet nezpracovaných dočasných licencí).

Použití nástroje správy licencí terminálových služeb

Součástí Správa licencí služby Terminal Services (Terminal Services Licensing) je nástroj správy vytvořený tak, aby vám pomáhal s aktivováním licenčních serverů, instalací licencí klientského přístupu a sledování využití terminálových serverů klienty. Tím licencování terminálových služeb pomáhá správcům systému přesně vést a zavádět licence klientského přístupu k terminálovým službám a licence Internet Connector.

Pomocí nástroje správy licencí terminálových služeb lze po připojení k licenčnímu serveru vykonávat následující úlohy:

- Aktivovat licenční server.
- Instalovat klientské licence.
- Opakovaně aktivovat licenční server.
- Deaktivovat licenční server.
- Opakovat instalaci klientských licencí.

Všechny tyto úkony se uskutečňují prostřednictvím Průvodce správou licencí.

Kromě těchto úkolů můžete správu licencí terminálových služeb použít také pro připojení k libovolnému licenčnímu serveru na síti a následnému zobrazování informací o licencích na daném serveru. Můžete si zobrazit následující užitečné licenční informace:

- Seznam instalovaných sad Key Pack klientských licencí.
- Celkový počet licencí v jednotlivých sadách Key Pack klientských licencí a počet dostupných a vystavených licencí v každé sadě Key Pack.
- Název počítače a datum vystavení jednotlivých licencí.
- Název počítače a data vypršení platnosti jednotlivých dočasně vystavených licencí.

Jakmile počet klientů požadujících licence od licenčního serveru překročí počet licencí, které jste aktivovali, systém vás upozorní na nutnost instalovat nové licence. Toto upozornění se objeví jako událost v protokolu událostí systému Prohlížeče událostí (Event Viewer). Počet licencí klientského přístupu, které budete potřebovat, lze zjistit z počtu nevyřízených dočasných licencí.

Zálohování licenčního serveru

Je důležité, abyste licenční server zálohovali a zajistili tak snadnou obnovitelnost licenčních informací v případě poruchy systému. Zálohování je zapotřebí provádět pravidelně a musí zahrnovat alespoň stav systému (System State) a adresář Lserver. Standardně se jedná o adresář %windir%\system32\Lserver.

Při obnovování počítače musí běžet licenční služba. Obnovení databáze a stavu systému na původní licenční server (ten se stejným identifikátorem) má za následek obnovení všech historických i aktuálně platných licenčních informací. Obnovíte-li zálohovanou licenční databázi na jiný licenční server, daný licenční server obnoví pouze historické informace o vystavených licencích. Licence, které nebyly vydány, se neobnoví. Informace o nevydaných licencích se však odešlou do systémového protokolu událostí, který si lze zobrazit v Prohlížeči událostí (Event Viewer). Informace v systémovém protokolu událostí budou zahrnovat počet a typ nevydaných licencí, které nebyly obnoveny. Chcete-li obnovit nevydané licence, nainstalujte je metodou telefonické instalace. Představitel podpory zákazníků může opakovaně vydat licence, které jste ztratili.

Návrh sítě pro přístup k terminálovému serveru

Při zavádění terminálových služeb musíte vzít v úvahu infrastrukturu sítě. Z větší části se jedná o obvyklé problémy návrhu sítě, avšak terminálové služby vyžadují ještě několik zvláštních ohledů.

Terminálové služby nemohou předávat aplikacím adresy IP jednotlivých klientů. Víceuživatelské aplikace vyžadující, aby uživatel měli jednoznačné adresy IP, v prostředí terminálových služeb nepracují správně, protože každý uživatel se objevuje pod adresou IP samotného serveru. Například určité firewally a starší hostitelé používají adresu IP klienta k učení zabezpečení a fyzického umístění. Plány může být zapotřebí upravit tak, aby terminálové služby podporovaly takové aplikace.

Stejně tak je důležité uvědomit si, že všichni uživatelé budou sdílet stejné připojení IP z daného terminálového serveru. Aplikace či služby, které ničí, zamykají nebo si monopolizují daný prostředek, mohou mít vliv na celkovou funkci serveru.

Vyrovňování zatížení sítě and terminálové služby

Vyrovňování zatížení sítě (Network Load Balancing) se používá k rozdělení zatížení na dva nebo více serverů. Vyrovňování zatížení sítě představuje skupinu serverů jako jedinou virtuální adresu IP a zajišťuje mechanismus dynamického rozdělení zatížení. To je užitečné v prostředích, kde se velký počet uživatelů připojuje k serveru kvůli obchodním aplikacím nebo k databázi, kde není ochrana relace důležitá. Protože terminálové služby nejsou vhodné pro klastrování, vyrovňování zatížení může často představovat dobré řešení obsluhy velké skupiny uživatelů.

Tradiční řešení vyrovňování zatížení nemohou vždy zaručit, že uživatel bude znovu připojen ke stejnému serveru. V případech, jako je scénář obchodních aplikací, neexistují prakticky žádná data vztahující se k aktuální relaci, která by bylo zapotřebí brát v úvahu. V případě složitějších zavádění počítačů nebo vzdáleného přístupu může podnik říci, že ukončené relace nebude vůbec nijak podporovat, aby se snížily požadavky kladené na prostředky a zvýšilo zabezpečení. Může být také možné pomocí atributů určitých typů vyrovňování zatížení připojovat se předvídatelně ke stejnému terminálovému serveru a tak zachovávat relace.

Zachování relace není analogií zachování uživatelských dat. Je dobře možné spravovat dva nebo více terminálových serverů takovým způsobem, že uživatel se bude moci připojit k libovolnému serveru a získat příslušný přístup. Stačí jen uložit uživatelská data a uživatelské profily mimo terminálové servery. Servery pak uživatelské profily a úložiště najdou na příslušném místě. Uživatelům se následně prostředí jeví úplně stejně bez ohledu na server, ke kterému se skutečně připojili.

Vyrovňování zatížení sítě představuje dobrá řešení mnoha terminálových serverů. Vyrovňování zatížení sítě využívá afinitu (příbuznost) IP, která umožňuje uživateli se stejnou adresou IP opakovaně se připojit v případě ukončení relace ke stejnému počítači. To znamená, že vyrovňování zatížení sítě lze používat také k obnovování relací, pokud uživatel nepřešel na jiný počítač. Dokonce i když je používán protokol Dynamic Host Configuration Protocol (DHCP), adresa IP uživatele zůstane stejná, pokud se mezi tím od sítě neodhlásí.

Systém doménových názvů (Domain Name System – DNS) představuje alternativní strategii vyrovnávání zatížení. Pomocí techniky round robin DNS lze jediný název přeložit na více různých adres IP, přičemž každá má vlastní klonovaný server. Používáte-li systém DNS, zakažte odpojení relace (**Session Disconnect**) na serverech se spuštěnými terminálovými službami. Protože klient se může připojit k libovolnému ze serverů, může se připojit k jinému serveru, než na kterém zůstala spuštěná odpojená relace.

Další informace o vyrovnávání zatížení sítě najdete v kapitole „Zajištění dostupnosti aplikací a služeb“ v této knize.

Návrh a vytvoření struktury domén

Vývoj návrhu sítě zahrnuje také plánování umístění terminálových služeb v předpokládané infrastruktuře systému Windows 2000. Existují tři základní možnosti struktury domén, které se vztahují k instalaci terminálových služeb:

Nepoužívá se žádná doménová struktura. Bez doménové architektury musí mít uživatelé samostatné účty na všech serverech systému Windows 2000 se spuštěnými terminálovými službami. To omezuje škálovatelnost a ztěžuje správu skupin a uživatelů.

Implementování terminálových služeb systému Windows 2000 v existujícím prostředí domén systému Windows NT 4.0. To vám umožňuje využít nových funkcí terminálových služeb systému Windows 2000, aniž by to mělo vliv na výrobní prostředí. Pamatujte však, že existující omezení správce účtů se zabezpečením (Security Account Manager – SAM) modelu domén systému Windows NT 4.0 platí i pro tento přístup. Správci mají možnost přidávat atributy terminálových služeb k uživatelským účtům. Tím se do zadání uživatele v doménové databázi SAM přidá malé množství informací, obvykle 1 KB nebo méně.

Využití infrastruktury Active Directory systému Windows 2000. Tato volba plně využije službu Active Directory a umožňuje hostit v databázi tisíce uživatelů. Zároveň máte možnost řídit prostředí uživatelů připojených k terminálovým službám pomocí zásad skupiny.

Při definování struktury Active Directory vám doporučujeme umístit terminálové servery do samostatné organizační jednotky (OU), odděleně od ostatních počítačů a bez uživatelů. OU terminálových služeb musí obsahovat pouze počítače terminálových služeb a žádné jiné objekty uživatelů a počítačů bez terminálových služeb. Stejně jako budete přenosné počítače pravděpodobně spravovat jinak než klientské počítače, budete také jinak spravovat terminálové servery.

Použití uživatelských profilů a cestovních uživatelských profilů systému Windows 2000

Profil popisuje konfiguraci systému Windows 2000 pro určitého uživatele včetně nastavení uživatelského prostředí a dalších voleb. Profily obvykle obsahují informace uživatelů, jako jsou instalované aplikace, ikony na pracovní ploše a volby barev. Pomocí profilů, které se nacházejí na kartě **Profil služby Terminal Services** (Terminal Services Profile) dialogového okna **vlastností uživatele** (User Properties), můžete určitému uživateli nakonfigurovat profily specifické pro terminálové služby.

V některých případech již mohou mít uživatelé přiřazeny profily systému Windows 2000. Může však být vhodné přiřadit profily terminálových služeb uživatelům v následujících případech:

- Kdykoli uživatel získává přístup k terminálovým službám přes rozsáhlou síť (WAN).
- Jestliže chce správce nabídnout uživateli relaci, která se liší od vlastního prostředí uživatele.

Když se uživatel přihlásí k serveru se spuštěnými terminálovými službami, server se pokusí nahrát profily v tomto pořadí:

- Profil terminálových služeb uživatele
- Cestovní profil systému Windows 2000 uživatele
- Profil systému Windows 2000 uživatele

Cestovní uživatelské profily

Cestovní uživatelské profily umožňují uživatelům přesunovat se mezi různými počítači a přitom si zachovávat stejné prostředí a nastavení preferencí. Informace o profilu je uložena v mezipaměti na místním pevném disku terminálového serveru. V určitých případech se doporučuje, aby byly po odhlášení uživatele tyto informace odstraněny. Patří sem tyto situace:

- Přístup k terminálovým službám je zajištěn skupinou hostitelů terminálových služeb.
- Přístup k terminálovým službám je jen občasný a chcete minimalizovat množství použitého diskového prostoru.

Nejvýhodnějším způsobem odstranění profilů z mezipaměti je umístit všechny hostitele terminálových služeb do kontejneru Active Directory systému Windows 2000 a aplikovat na ně speciální zásady, které zajistí odstranění všech uložených profilů při odhlášení.

Chcete-li používat cestovní uživatelské profily, předem si naplánujte a určete, kde budou uloženy a jak budou spravovány. Nejprve určete umístění na souborovém nebo tiskovém serveru s dostatkem prostoru pro ukládání profilů, který je zároveň vždy dostupný uživatelům terminálových služeb. Pak vytvořte sdílenou položku systému Windows 2000, k níž mohou uživatelé získat přístup s oprávněními ke čtení a zápisu. Profily je zapotřebí uložit na jiná síťová místa, než jsou domovské adresáře uživatelů.

Aby bylo možné používat cestovní profily ve skupině počítačů terminálových služeb, musí být počítače terminálových služeb identické z hlediska konfigurace aplikací a operačního systému, jako je například umístění složky %systemroot% a instalační místa všech aplikací. V jiném případě seskupte různé konfigurace do samostatných skupin a spravujte je odděleně.

Zásady skupiny

Zásady skupiny představují efektivní mechanismus správy a řízení chování terminálových služeb ve vašem prostředí. Zásady skupiny (Group Policy) se používají ke správě sady hodnot registru a oprávnění souborů, jež společně definují prostředky počítače dostupné síťovému sídlu Active Directory, doméně nebo organizační jednotce (OU).

Zásady skupiny vycházejí z funkce hodnot uložených v registru obsahujících nastavení zabezpečení, instalaci softwaru, skripty přihlášení/odhlášení a spuštění/vypnutí, zavádění souborů a omezené speciální složky. Zásady skupiny se aktivují pomocí Active Directory a ovlivňují počítače i uživatele v následujících skupinách: místní počítač, síťová sídla (sítě), domény a organizační jednotky.

Pokud ve vaší organizaci používají stejní uživatelé jak terminálové služby tak i systém Windows 2000 Professional, používejte zásady opatrně. Stejně zásady platí pro relace

uživatelů terminálových služeb i na systému Windows 2000 Professional (s výjimkou správy aplikací jednotlivých uživatelů, která je na aplikačním serveru terminálových služeb zakázána). V takovém případě musíte aplikovat na servery se spuštěnými terminálovými službami jinou sadu zásad počítačů tím, že počítač umístíte do samostatné OU.

Uživatelé na terminálovém serveru v režimu aplikačního serveru nemohou použít nástroj Windows Installer a přidat chybějící komponenty aplikace. Proto je důležité všechny potřebné komponenty nainstalovat místně při první instalaci programu. K tomu můžete využít transformační soubor (.mst). Soubory transformací jsou modifikacemi balíčků .msi a říkají nástroji Windows Installer, které komponenty se mají nainstalovat místně.

Přístup k aplikacím

Správci mohou řídit přístup uživatelů k aplikacím terminálových služeb následujícími způsoby:

Povinné profily

Profily mohou určovat, které aplikace jsou pro daného uživatele viditelné.

Systémové zásady

Zásady mohou uživatelům zabránit v otevření aplikací pomocí Průzkumníku Windows a příkazu Spustit (Run). Zásady vycházejí z domén, takže mohou ovlivnit vlastní počítače uživatelů i jejich relace terminálových služeb.

Zásady skupiny nejprve aplikují zásady uživatelů domény a pak je buď sloučí se zásadami počítačů nebo je jimi nahradí. To umožňuje terminálovému serveru měnit a omezovat možnosti poskytované uživatelům.

Špatně zapsané zásady mohou uživatelům zabránit v přístupu k programům na všech počítačích v doméně a nikoli jen v získání přístupu k terminálovým službám. Jestliže správce implementuje zásady vycházející z identifikátoru (ID) uživatele nebo skupiny systému Windows 2000, pak se všechny specifikace těchto zásad aplikují na daného uživatele nebo skupinu bez ohledu na to, jaký systém používají. Například zásady zabráňující uživatelům z účtárny spustit Microsoft Word ovlivní všechny uživatele z účtárny v celé doméně, ať už používají terminálové služby nebo jen své místní počítače.

Používání domovských adresářů

Je důležité naplánovat použití domovských adresářů v prostředí terminálových služeb, protože většina aplikací musí instalovat informace specifické pro daného uživatele nebo zkopírovat konfigurační soubory pro jednotlivé uživatele. Chcete-li udržet rozumnou velikost uživatelských profilů (méně než 2 MB), doporučujeme vám, aby měli všichni uživatelé terminálových služeb své síťové domovské adresáře a síťový adresář Dokumenty (My Documents), do kterého se budou ukládat informace určitých aplikací.

Systém Windows 2000 standardně definuje domovský adresář pro každého uživatele. Výchozí adresář uživatele se nachází pod adresářem dokumentů a nastavení (Documents and Settings). Tento adresář obsahuje dokumenty i nastavení uživatele. Dokumenty uživatele se ukládají do domovského adresáře uživatele nebo do složky Dokumenty (My Documents). Terminálové služby zapisují soubory aplikací pro určitého uživatele, například soubory .ini, do adresáře systému Windows uživatele a standardně odkazují všechny aplikace hledající systémový adresář Windows do adresáře Windows uživatele.

Uživatelé obvykle používají domovské adresáře k ukládání svých osobních souborů. To může být problém v případě používání cestovních profilů, když se zároveň domovský adresář nachází v adresáři profilu uživatele. Systém Windows 2000 po každém přihlášení uživatele zkopíruje vše v adresáři profilu uživatele do mezipaměti profilu. To může představovat značný čas a spotřebu prostředků, zejména je-li cestovní profil uložen na jiném místě sítě.

Doporučujeme vám používat domovské adresáře specifické terminálovým službám, které jsou automaticky dostupné přes modul snap-in konzoly MMC. Jedním přístupem může být vytvoření adresáře na souborovém serveru nazvaného třeba Domovadr a nastavení oprávnění ke změně na hodnotu Everyone. Pak lze zadat umístění domovského adresáře terminálových služeb jako p:\Domovadr\%username%. Terminálové služby automaticky vytvoří podadresář uživatelského jména a přiřadí mu příslušná oprávnění. Standardně má každý uživatel plný přístup ke svému domovskému adresáři a správci mohou do daného adresáře soubory kopírovat, nemohou je zde však ani čist ani odstraňovat.

Je užitečné, aby měli všichni uživatelé stejné písmeno virtuální jednotky bodu přesměrování do jejich domovského adresáře. Bude pak možné používat skripty kompatibility aplikace. Při prvním spuštění skriptu kompatibility aplikace na serveru vás skript vyzve k zadání písmena jednotky, které se odkazuje na kořen domovského adresáře uživatele. Toto písmeno se použije i ve všech dalších skriptech kompatibility aplikace. Je důležité, aby se na všech terminálových serverech v seskupení serverů používalo stejné písmeno jednotky.

Přesměrování složky (Folder Redirection) je zvláštní funkce systému Windows 2000 umožňující uživatelům a správcům přesměrovat cestu nějaké složky na jiné místo. Tím novým místem může být složka na místním počítači nebo adresář na sdíleném místě. Uživatelé mají možnost pracovat se sdílenými dokumenty na zabezpečeném serveru stejně, jako by se nacházely na místní jednotce. Pomocí této funkce může správce přesměrovat složku Dokumenty (My Documents) uživatele na soukromé sdílené místo serveru, ke kterému lze přistupovat jak z klientského počítače se systémem Windows 2000 Professional, tak i v rámci připojení k terminálovým službám. Tato funkce se spravuje pomocí zásad skupiny (Group Policy).

Plánování zabezpečení

Zabezpečení je zásadní součástí plánu zavedení terminálových služeb. Kromě problémů zabezpečení řešených ve vašem plánu zavedení systému Windows 2000 se na terminálové služby vztahují další úvahy odpovídající víceuživatelskému prostředí.

Tento oddíl popisuje problémy zabezpečení související s terminálovými službami včetně verze systému souborů NTFS použité ve Windows 2000, práv uživatelů a správce, procedur automatického přihlašování, šifrování a dalších otázek zabezpečení.

Další informace o zabezpečení systému Windows 2000 najdete v kapitole „Plánování distribuovaného zabezpečení“ v této knize.

System souborů NTFS

Vzhledem k víceuživatelské podstatě terminálových služeb vám rozhodně doporučujeme používat systém souborů NTFS verze systému Windows 2000 jako jediný systém souborů na serveru a vyhýbat se systému s alokační tabulkou souborů (FAT). Systém FAT neposkytuje žádné zabezpečení uživatelů a adresářů, zatímco pomocí systému NTFS lze omezit podadresáře jen pro určité uživatele nebo skupiny uživatelů. Právě to

je velmi důležité ve víceuživatelském systému, jako jsou terminálové služby. Bez zabezpečení poskytovaného systémem NTFS může každý uživatel přistupovat ke všem adresářům a souborům na terminálovém serveru.

Práva uživatelů

Terminálové služby se distribuují s výchozí sadou uživatelských práv, které lze v zájmu dosažení vyššího zabezpečení upravit. Aby se mohl uživatel přihlásit k terminálovému serveru, musí mít na daném počítači místní přihlašovací práva. Terminálový server v režimu vzdálené správy standardně zajišťuje práva pouze členům skupiny Administrators na daném počítači a v režimu sdílení aplikací zajišťuje práva všem členům skupiny Users. Protože systém Windows 2000 standardně zahrnuje do skupiny Users na počítači, který není řadičem domény, všechny uživatele domény, všichni uživatelé domény se mohou přihlásit k terminálovému serveru, zajišťujícímu sdílení aplikací. Skupiny a uživatelé, kteří se mohou přihlásit, a jim předané možnosti řízení lze změnit pomocí nástroje Konfigurace služby Terminal Services.

Uživatelé, kterým je povolen přístup například přes protokol RDP a kteří se interaktivně přihlašují na server s terminálovými službami, se automaticky přidají do zabudované místní skupiny Terminal Services Users. Uživatel patří do této skupiny jen během interaktivního přihlášení k terminálovému serveru. Tato zabudovaná skupina dává správcům možnost řídit prostředky, ke kterým mohou uživatelé terminálových služeb přistupovat. Tato skupina se podobá zabudované skupině Interactive.

Vyhýbejte se konfigurování terminálových služeb jako řadiče domény, protože všechny zásady práv uživatelů aplikované na takový server se budou aplikovat na všechny řadiče domény v dané doméně. Představme si, aby mohli uživatelé ve vašem případě používat terminálové služby, musí být oprávnění k místnímu přihlášení. Je-li server se spuštěnými terminálovými službami řadičem domény, uživatelé se budou moci místně přihlásit ke všem řadičům domény v doméně terminálových služeb.

Práva správce

Členové skupiny Administrators na terminálovém serveru mohou řídit, kteří uživatelé mohou k serveru přistupovat, jaká mají práva a jaké aplikace mohou spouštět. Většina tohoto řízení je součástí obvyklých práv správce serveru systému Windows 2000. Tato práva jsou v rámci terminálových služeb rozšířena a zahrnují:

- Správa serveru – K nastavení oprávnění uživatelů a aktivity připojení a k odpojení akcí a možností připojení používejte nástroj Konfigurace služby Terminal Services.
- Řízení uživatelů – Oprávnění uživatelů vzhledem k terminálovým službám nastavte pomocí nástroje Konfigurace služby Terminal Services. Specifické informace profilu terminálových služeb vytvořte pomocí rozšíření User Manager.
- Řízení připojení – Ke sledování aktivních uživatelů, relací a procesů použijte funkci Správce služby Terminal Services. Můžete také stínovat relace a vynucovat odpojení.
- Instalace aplikací – Pracuje-li terminálový server v režimu sdílení aplikací, může na něj instalovat aplikace pouze správce. Toto omezení neplatí pro režim vzdálené správy.

Procedury automatického přihlašování

Podle toho, jak budou lidé používat terminálové služby, jim můžete zajistit přístup k systému souborů. Uživatelé, kteří potřebují jen přístup k jedné aplikaci, například k databázi, lze po spuštění umístit přímo do dané aplikace. Toho lze docílit tak, že se kli-

ent terminálového serveru pomocí nástroje Správce připojení klienta (Client Connection Manager) nastaví na automatické spuštění určité aplikace pro uživatele. Předem nakonfigurovaného klienta terminálového serveru lze distribuovat nějaké skupině uživatelů a předat jim tak stejnou přímou aplikaci. Jestliže bude terminálový server poskytovat všem uživatelům, kteří se k němu mohou připojit, stejnou aplikaci, server může být nakonfigurován tak, aby při přihlášení automaticky inicializoval danou aplikaci. To se zadává prostřednictvím konfigurace terminálových služeb.

Uživatelům můžete také povolit připojení bez zadání uživatelského jména a hesla. Toho lze také dosáhnout po jednotlivých uživateli pomocí nástroje Správce připojení klienta (Client Connection Manager) nebo po jednotlivých serverech prostřednictvím konfigurace terminálových služeb či rozšíření Správce uživatelů (User Manager). Obecně platí, že byste měli naplánovat použití této metody připojení, pouze pokud se uživatelé přihlašují přímo k obchodním aplikacím, zejména když samotná aplikace vyžadují zadání přístupového hesla. Tuto serverovou funkci používejte opatrně, protože k serveru se pak bude moci přihlásit kdokoli s klientem terminálových služeb.

Systém Windows 2000 nabízí ještě možnost druhotného přihlášení. Tato funkce se používá zejména proto, aby mohli uživatelé zadávat vykonání aplikací v jiném kontextu zabezpečení. V prostředí terminálových služeb, kde se klientské počítače automaticky přihlašují pomocí základního uživatelského účtu, je velmi cenná, protože aktuální uživatel může chtít vykonat nějakou aplikaci vyžadující vyšší úroveň zabezpečení. V této situaci můžete ke spuštění aplikace v jiném kontextu, aniž by přitom bylo nutné uživatele odhlašovat, použít příkaz **runas**.

Příkaz **runas** můžete zadat z příkazového řádku nebo jej lze vložit do zástupce aplikace. Po vytvoření zástupce určité aplikace lze do zástupce funkci příkazu **runas** snadno zahrnout. Stačí v okně vlastností zástupce zaškrtnout položku **Spustit jako jiný uživatel** (Run as different user). Před vykonáním aplikace se pak systém zeptá uživatele na doménový uživatelský účet systému Windows 2000 a heslo.

Úprava specifických informací uživatele

Když se uživatel přihlásí k systému, terminálové služby vykonají dávkový soubor `UsrLogon.cmd` v adresáři `System32`. Tento soubor zadá potřebné úpravy uživatelského prostředí a zajistí, že uživatelé budou moci řádně spouštět své aplikace. Jsou-li potřebné nějaké úpravy uživatelského prostředí terminálových služeb, můžete je zadat editací tohoto souboru. Uvědomte si však, že úpravou tohoto souboru můžete způsobit problém se skripty kompatibility aplikace, které tento dávkový soubor spouští.

Změna procesu přihlašování

Zvažte kontrolu existence proměnných prostředí `%CLIENTNAME%` nebo `%SESSIONNAME%` v přihlašovacích skriptech. Tyto proměnné prostředí jsou specifické pro terminálové služby a v uživatelském prostředí se objevují až po přihlášení k terminálovému serveru v režimu vzdálené správy nebo aplikačního serveru. Když pak například skript zjistí, že antivirový program je na terminálových službách již spuštěn, můžete přeskočit jeho opakované spuštění.

Šifrování

Přenosům dat mezi klientem a serverem terminálových služeb můžete přiřadit jednu ze tří úrovní šifrování. Vysoká úroveň šifrování je k dispozici pouze v Severní Americe.

Nízká úroveň šifrování

Při nízké úrovni šifrování se provoz od klienta k serveru šifruje pomocí algoritmu RC4 a 56bitového klíče (40bitového klíče v případě klientů RDP 4.0), zatímco provoz od serveru ke klientovi není šifrovaný. Nízká úroveň šifrování chrání citlivá data, jako jsou zadání hesel, a data aplikací. Data odesílaná ze serveru klientovi představují jen změny na obrazovce a jako taková se i v nezašifrovaném stavu jen obtížně odhalují.

Střední úroveň šifrování

Při střední úrovni šifrování je provoz v obou směrech zašifrován pomocí algoritmu RC4 a 56bitového klíče (40bitového klíče v případě klientů RDP 4.0).

Vysoká úroveň šifrování

Provoz v obou směrech je pouze v severoamerických verzích terminálových služeb šifrován pomocí algoritmu RC4 a 128bitového klíče. V exportních verzích terminálových služeb používá vysoká úroveň zabezpečení algoritmus RC4 a 56bitový klíč (40bitový klíč v případě klientů RDP 4.0).

Další úvahy o zabezpečení

Při plánování zabezpečení terminálových služeb se ještě zamyslete nad následujícími body:

Karty Smart Card Interaktivní přihlašování k systému Windows 2000 umožňuje ověřit uživatele sítě Active Directory pomocí certifikátu X.509 verze 3, který je uložen na kartě Smart Card společně se soukromým klíčem. Tato funkce však není k dispozici uživatelům, kteří se ověřují prostřednictvím terminálových služeb. Totéž platí i pro jiná hardwarová ověřovací zařízení.

Zabezpečení sítě a komunikací Vzdálený přístup neomezuje přístup uživatelů terminálových služeb, takže když jeden z uživatelů vytvoří modemové připojení nebo připojení VPN k Internetu či jinému systému, všichni uživatelé terminálových služeb mají k připojení přístup.

Služba Information Services na terminálových službách Musíte zakázat anonymní používání protokolu přenosu souborů (File Transfer Protocol – FTP) a zabránit tak nezabezpečenému přístupu do systému souborů.

Odstranění nepoužívaných služeb Odstraněním podsystémů IBM OS/2 a POSIX zabráníte uživatelům ve vykonávání aplikací systémů OS/2 a POSIX, které obcházejí regulační opatření zabezpečení. Další informace o zajištění zabezpečení vašeho systému najdete v kapitole „Plánování distribuovaného zabezpečení“ v této knize.

Vzdálený přístup

Terminálové služby mohou vzdáleným uživatelům poskytovat přístup k aplikacím, které jsou kvůli slabé výkonnosti telefonických nebo pomalých síťových připojení nevyužitelné. Informace o obrazovce, myši a klávesnici odesílané terminálovými službami obvykle využívají menší šířku pásma než aplikace, která se musí přenést na místní počítač uživatele a tam se teprve spustit.

Terminálové služby přes Internet

K získání přístupu k terminálovým službám přes Internet mohou uživatelé využít také protokol Layer-2 Tunneling Protocol (L2TP) nebo protokol Point-to-Point Tunneling Protocol (PPTP). Pomocí šifrování oba tunelovací protokoly zajišťují zabezpečený pří-

stup k soukromým sítím pro uživatele pracující přes veřejné médium. Tyto protokoly jsou doporučeny vzhledem k jimi zajišťovanému zabezpečení, k terminálovým službám však lze přistupovat také libovolnou implementací protokolu TCP/IP.

Firewally

Používá-li vaše organizace pro zabezpečení firewall, nezapomeňte nechat pro spojení RDP mezi klientem a serverem otevřený port 3389. Nejlepších výsledků dosáhnete použitím firewallu zajišťujícím ověřování podle uživatelů. Firewall umožňující přístup na základě adresy IP pustí uživatele dál, pokud byl zajištěn přístup adrese IP serveru se spuštěnými terminálovými službami.

Konfigurování serverů na zavedení terminálových služeb

Doporučujeme vám kupovat serverové počítače pro terminálové služby u stejného výrobce a stejně je také nakonfigurovat. To usnadní správu terminálových služeb. Zavádíte-li terminálové služby, které mají obsluhovat různé potřeby, zvažte rozdělení serverů do skupin podle jejich funkce a snažte se, aby si byly všechny počítače v jednotlivých skupinách co nejpodobnější.

Používá-li vaše organizace nějaké standardy vybavení, při plánování koupě nového hardwaru pro zajištění terminálových služeb se těchto standardů držte. V případě potřeby zvyšte aktuální standard, aby byla správa a údržba softwaru i hardwaru co nejjednodušší.

Při plánování zavedení serverů zvažte potřeby paměti, stránkovacího souboru a souboru výpisu, procesorů a registru. *Soubor výpisu* slouží k výpisu paměti v případě chyby. K těmto položkám se vztahují následující úvahy:

Paměť

Dobrým principem je 128 MB paměti RAM pro základní služby operačního systému a další paměť pro jednotlivé uživatele. Toto dodatečné množství paměti se mění a mělo by být v rozsahu 16 MB a 20 MB na relaci. Chcete-li vypočítat dodatečné množství paměti, naplánujte přibližně 13 MB pro počítač uživatele a pak přidejte množství potřebné ke spouštění aplikací. Uvědomte si, že pokud jednu aplikaci spustí více uživatelů, kód dané aplikace se v paměti nezdvíjí (vykonatelný kód je sdílen ve všech instancích dané aplikace). 16bitové aplikace vyžadují asi o 25 procent více paměti než 32bitové aplikace.

Jestliže budou uživatelé spouštět paměťově náročné aplikace, jako jsou aplikace typu klient/server s velkými paměťovými nároky, musíte zvýšit množství paměti alokované jednotlivým uživatelům. Každý server musí mít tolik fyzické paměti, aby bylo zajištěno, že se stránkovací soubor prakticky nikdy nebude používat.

Stránkovací soubory a soubory výpisu

Množství diskového prostoru vyhrazené každému stránkovacímu souboru serveru musí být přinejmenším polovinou celkového množství fyzické paměti RAM počítače.

Je vhodné umístit operační systém terminálového serveru na jednu fyzickou jednotku a stránkovací soubor uložit jinde. Má-li server velké množství fyzické paměti, musíte zvážit, zda je na jednotce pevného disku dostatek prostoru k zaznamenání souboru výpisu na systémový oddíl. Zvažte takové faktory, jako je celková paměť, velikost strán-

kovacího souboru, instalované aplikace a celková velikost jednotky pevného disku. Lepší výkonnost zajistíte, když bude stránkovací soubor na odděleném fyzickém disku. Na systémech s velkými objemy paměti RAM (obvykle 128 MB a více) zvažte zákaz používání souborů výpisu, pokud tedy není jednotka C dostatečně velká, aby dokázala soubor výpisu pojmout.

Procesory

Terminálový server musí splňovat požadavky systému Windows 2000 Server. Množství výkonu procesoru na uživatele závisí na typech spouštěných aplikací a nejlépe se ověřit pokusným zavedením. Další informace o škálování najdete v odkazu Terminal Services Scaling stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Registr

Velikost registru se dynamicky nastavuje během instalace a vychází z velikosti stránkovacího souboru. Kvóta registru vychází z velikosti paměti. Velikost registru lze také nastavit prostřednictvím ovládacího panelu. Poklepejte na panel **Systém** (System) a pak si zobrazte kartu **Upřesnit** (Advanced). Na kartě **Upřesnit** (Advanced) stiskněte tlačítko **Možnosti výkonu** (Performance Options) a pak stiskněte tlačítko **Změnit** (Change). Zadejte velikost registru.

Příprava na zavedení klientů

Klientské počítače nebo terminály se připojují k terminálovému serveru pomocí malého klientského programu instalovaného na disku nebo prostřednictvím firmwaru. Volba použité klientské platformy závisí na aktuální instalaci a individuálních potřebách uživatele. Přinejmenším se musíte ujistit, že všechny klientské počítače nebo terminály, které se mají připojovat k terminálovému serveru, jsou fyzicky schopny hostit klientský software a připojovat se přes síť.

Zavádění na terminály se systémem Windows CE

Terminály se systémem Windows CE se obvykle ze všech terminálů, které lze použít pro získání přístupu k terminálovým službám, „nejvíce podobají“ systému Windows. Tyto terminály se nastavují a konfigurují pomocí průvodců pracujících ve známém uživatelském rozhraní Microsoft Win32, které je součástí systému Microsoft Windows 95 a novějších operačních systémů Windows.

Zvažte zakoupení terminálů od prodejců, kteří vám poskytnou nástroj umožňující správcům vzdálené vykonávání inovací terminálů, konfiguraci terminálů a správu položek.

Terminály se systémem Windows lze obvykle konfigurovat místně. Patří sem:

- Použití protokolu DHCP
- Připojení prostřednictvím LAN, protokol PPP, adresa IP, maska podsítě a připojení brány
- Umožnění DNS v zájmu vyhledávání názvu terminálového serveru při vytváření připojení

Většinu terminálů se systémem Windows lze použít k získání přístupu k terminálovým službám přes telefonické připojení při použití protokolu PPP. Některé terminály se systémem Windows nepodporují šifrování během přihlašovacího procesu. V takovém případě musíte nakonfigurovat zařízení používané k zajištění připojení k sítím na zpracování hesel v prostém textu, jinak nedojde k vytvoření připojení. Přihlašování relace terminálového serveru lze vždy šifrovat.

Terminály se systémem Windows CE mohou jako součást firmwaru obsahovat emulátory jiných typů terminálů. Uživatelé takových terminálů mohou vytvořit simultánní připojení k různým typům serverů a přepínat se mezi různými emulátory terminálového zařízení.

Na terminálu se systémem Windows CE se lze mezi relacemi přepínat pomocí následujících klávesových zkratk:

- **Ctrl+Alt+End** Přenese prostředí uživatelského rozhraní terminálu se systémem Windows CE do popředí.
- **Ctrl+Alt+šipka nahoru** Přepne se do předchozích aktivních relací, aniž by se na popředí objevilo uživatelské prostředí.
- **Ctrl+Alt+šipka dolů** Přepne se do následujících aktivních relací, aniž by se na popředí objevilo uživatelské prostředí.
- **Ctrl+Alt+Home** Přepne se do výchozího připojení, pokud pracuje. Jestliže nepracuje, prostředí toto spojení spustí.
- **F2** Vyvolá uživatelské rozhraní konfigurace vlastností terminálu.

Další informace o prodejcích nabízejících terminály se systémem Windows CE najdete v odkazu [Terminal Services Vendors](http://windows.microsoft.com/windows2000/reskit/webresources) stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Zavádění na klientské počítače

Klientské počítače se systémem Windows, které se budou připojovat k terminálovým službám, by měly mít alespoň mikroprocesor řady 80386 běžící na 33 MHz (doporučuje se však procesor 486/66), 16bitovou grafickou kartu VGA a zásobník Microsoft TCP/IP. Klient terminálových služeb běží na systémech Windows 2000, Windows for Workgroups 3.11, Windows 95, Windows 98 a Windows NT 3.51 a novější.

Klient terminálových služeb zabírá pouze asi 500 KB diskového prostoru a při svém spuštění si obvykle vyhrazuje asi 4 MB paměti RAM. Je-li umožněno ukládání klientských bitových map do mezipaměti, může být využito dalších 10 MB diskového prostoru. Nejlepšího výkonu dosáhnete, když bude počítač se spuštěným klientem terminálových služeb obsahovat celkem 8 MB nebo více fyzické paměti RAM v systémech Windows for Workgroups 3.11 či Windows 95, 24 MB nebo více v systému Windows 98 a 32 MB nebo více v systému Windows 2000.

Klientský software RDP se nyní instaluje standardně jako podsoučást terminálových služeb. Ve výchozím stavu se různí klienti instalují do adresáře:

```
%systemroot%\system32\clients\tsclient
```

Zavedení klienta je možné dvěma způsoby:

- Vytvořením místa sdílení souborů a vykonáním instalace přes síť.
- Zadáním příkazu **Vytváření klientů služby Terminal Services** (Terminal Services Client Creation) nabídky **Nástroje pro správu** (Administrative Tools) a vytvořením obrazu klienta, který lze nainstalovat pomocí diskety.

Poznámka Klient terminálových služeb vyžaduje pro připojení k serveru protokol TCP/IP, avšak samotné terminálové služby mohou v případě potřeby přistupovat k serverům systému Novell pomocí protokolu IPX.

Inovace na terminálové služby

Přístup k inovaci na terminálové služby závisí na existujícím nastavení terminálových služeb:

WinFrame s nebo bez MetaFrame Z WinFrame na terminálové služby neexistuje žádná přímá cesta inovace. V tomto případě nejprve musíte inovovat na Microsoft Terminal Server 4.0 a pak inovovat na systém Windows 2000.

Terminal Server 4.0 bez MetaFrame Máte-li instalovaný Terminal Server 4.0, můžete využít přímou cestu inovace na terminálové služby. Při instalaci systému Windows 2000, server rozpozná program Terminal Server 4.0, automaticky vykoná jeho inovaci a automaticky umožní terminálové služby v režimu aplikačního serveru. Jestliže povolíte terminálové služby v režimu aplikačního serveru, může být nezbytné znovu nainstalovat existující aplikace.

Terminal Server 4.0 s MetaFrame Inovace ze serveru Terminal Server 4.0 s MetaFrame se podobá inovaci ze serveru Terminal Server 4.0, nejprve však musíte inovovat MetaFrame na verzi pro systém Windows 2000. Jakmile je nástroj MetaFrame inovován, můžete postupovat stejně jako při inovaci serveru Terminal Server 4.0 bez MetaFrame.

Windows NT bez terminálových služeb Při instalaci systému Windows 2000 umožníte používání terminálových služeb volbou terminálových služeb v režimu vzdálené správy nebo aplikačního serveru.

Instalace a konfigurace aplikací

Server se systémem Windows 2000, který je nakonfigurován na spouštění terminálových služeb v režimu aplikačního serveru, poskytuje v jeden okamžik připojení více uživatelům k libovolnému počtu aplikací.

Doporučujeme vám přidávat a odstraňovat aplikace pomocí ovládacího panelu Přidat nebo odebrat programy (Add/Remove Programs). Tím se automaticky spravují instalační požadavky terminálových služeb. Je také možné instalovat aplikace přímo za předpokladu, že se server převede do režimu instalace pomocí příkazového řádku **change user /install**. Server lze převést zpět z instalačního režimu příkazem **change user /execute**.

Tyto příkazy nejsou při použití panelu Přidat nebo odebrat programy (Add/Remove Programs) zapotřebí. Protože při práci s příkazovými řádky je vždy možné zadat něco chybně nebo na něco zapomenout, upřednostňuje se instalace pomocí uvedeného ovládacího panelu. Jestliže byla nějaká aplikace nainstalována bez pomoci ovládacího panelu Přidat nebo odebrat programy či bez nastavení serveru do režimu instalace pomocí příkazového řádku, aplikaci je zapotřebí odstranit a řádně znovu nainstalovat.

Na aplikační server terminálových služeb mohou instalovat aplikace pouze správci.

Zavádění aplikací pomocí zásad skupiny

Zavádění aplikací pomocí Active Directory a zásad skupiny (Group Policy) za použití nástroje Windows Installer je velmi flexibilní metoda, protože umožňuje instalaci

a správu aplikací mnoha různými způsoby. Třemi hlavními způsoby zavedení aplikací nástrojem Windows Installer jsou:

- Instalace na místním počítači uživatelem.
- Přiřazení správcem systému z řadiče domény uživateli nebo počítači.
- Publikování správcem systému z řadiče domény uživateli.

Před instalací aplikace pomocí nástroje Windows Installer musí pro danou aplikaci existovat instalační balíček .msi.

Zavádění aplikací z řadiče domény

Chcete-li zavést nějakou aplikaci z řadiče domény, správce systému musí přiřadit aplikaci .msi počítači. Aplikacíni servery nemohou aplikace přiřazovat nebo publikovat uživatelům.

Transformační soubory jsou zapotřebí, pokud původní instalační balíček aplikace nenainstaloval všechny potřebné komponenty aplikace na místní disk. Transformační soubory vám umožňují vybrat, jaké součásti, pokud vůbec nějaké, je zapotřebí během instalace nahrát.

Správce systému může také nainstalovat aplikaci ze vzdáleného připojení nebo z konzoly aplikačního serveru. Typická instalace se inicializuje pomocí následujícího příkazu:

```
Msixec/I NázevAplikace.MSITRANSFORMS=NázevTransformačníhoSouboru.MST  
ALLUSERS=1
```

Instalace aplikace ve víceuživatelském prostředí se výrazně odlišuje od instalace jednotlivému uživateli. Instalace softwaru aplikačního serveru nesmí ohrozit spuštěný systém a navíc musí být instalace nakonfigurována tak, aby umožnila současně relace více uživatelů. Z těchto důvodů mohou aplikace instalovat pouze správci – uživatelé nemohou nic instalovat.

Je zodpovědností správce systému ještě před umožněním připojení vzdálených uživatelů určit, které aplikace jsou zapotřebí, a zajistit jejich místní instalaci a dostupnost.

Podpora vícejazyčných a mezinárodních uživatelů

Terminálové služby jsou dostupné také ve vícejazyčné verzi systému Windows 2000. Vícejazyčná verze systému Windows 2000 vám umožňuje na počítač nainstalovat a nakonfigurovat více jazyků uživatelského rozhraní. To zjednodušuje proces zavedení a omezuje hardwarové náklady pro nadnárodní organizace. Například švýcarská korporace, která musí podle zákona zajistit uživatelské prostředí v angličtině, francouzštině a němčině, může všechny tři jazyky použít na jediném serveru.

Před povolením terminálových služeb ve vícejazyčné verzi systému Windows 2000 určete, jaké jazyky uživatelského prostředí budete potřebovat. Jestliže budou počítače s terminálovými službami obsluhovat uživatele v různých zemích světa, ale všichni mezinárodní uživatelé umějí anglicky, můžete zavést pouze mezinárodní anglickou verzi terminálových služeb.

Správci mohou nastavit jazyk uživatelského rozhraní pomocí zásad skupiny. Uživatelé si volí jazyk na kartě **Obecné** (General) ovládacího panelu **Místní nastavení** (Options). Má-li uživatel cestovní profil specifikující jazyk, který není instalován, systém použije výchozí jazyk angličtinu.

Terminálové služby sledují čas v souladu s časovou zónou, pro kterou byly nakonfigurovány. Nefungují tedy podle jednotlivých uživatelů. Uživatelé, kteří se nacházejí v jiné časové zóně než server, si musí být vědomi časových rozdílů.

Tisk z terminálových služeb

Tisk z terminálových služeb se podobá tisku z jiných verzí systému Windows 2000. Uživatelé a správci si však musí být vědomi určitých důležitých rozdílů.

Síťový tisk lze v prostředí terminálových služeb spravovat různými způsoby. V rámci malé jednotky nějaké organizace či oddělení může správce nakonfigurovat tiskárny místně na serveru se spuštěnými terminálovými službami. Tiskárny mohou být místně připojeny přes paralelní port nebo síťové rozhraní. Tyto tiskárny jsou automaticky dostupné všem uživatelům na systému.

Uživatel, který chce tisknout místně na tiskárnu připojenou k jeho vlastnímu počítači, může buď použít schopnost klienta terminálových služeb přeměrovat tiskovou úlohu na místní zařízení, nebo použít síť typu peer-to-peer.

Tisk na místní tiskárnu pomocí protokolu RDP

Terminálové služby nabízejí přesměrování tiskáren, které směřuje tiskové úlohy z terminálového serveru na tiskárnu připojenou ke klientovi. Existují dva způsoby zajištění klientského přístupu k místní tiskárně pomocí RDP: automatické přesměrování tiskárny a ruční přesměrování tiskárny.

Automatické přesměrování tiskárny je podporováno na všech klientských platformách Win32, včetně systémů Windows 95, Windows 98 a Windows NT. Když se klient přihlásí k terminálovým službám, automaticky se detekují místní tiskárny připojené k portům LPT, COM a USB a v relaci uživatele se vytvoří odpovídající fronty. Jakmile se klient odpojí nebo ukončí relaci, tisková fronta se odstraní a všechny čekající tiskové úlohy se ukončí.

Ruční přesměrování tiskárny musí být použito v klientech systému Windows for Workgroups 3.11 a na terminálech WBT. V takovém případě se tiskárna ručně přidává pomocí průvodce přidáním tiskárny v ovládacích panelech. K výběru portu tiskárny ze seznamu dostupných portů se použije název klientského počítače. Přesměrování tisku lze v rámci jednotlivých připojení zakázat pomocí nástroje Konfigurace služby Terminal Services (Terminal Services Configuration) nebo podle jednotlivých uživatelů pomocí nástroje Uživatelé a služby Active Directory (Active Directory Users and Computers) nebo Místní uživatelé a počítače (Local Users and Computers). Další informace o přesměrování tiskáren najdete v nápovědě systému Windows 2000 Server.

Síťové sdílení tiskárny

Stejně jako místní diskové jednotky i **síťové sdílení** umožňuje uživatelům získat přístup k tiskárně vzdáleně ze serveru. Nainstaluje-li uživatel do místní tiskárny síťovou kartu, stane se síťovou tiskárnou a sdílení souborů nemusí být na počítači uživatele povoleno.

Tiskárny se definují podle jednotlivých uživatelů. Proto je tiskárna po svém definování pro určitého uživatele dostupná pouze danému uživateli během jeho relace. Jestliže uživatel použije Správce tisku (Print Manager), uvidí pouze tiskárny, na které má povolení tisknout. Když se uživatel odpojí, server zruší přesměrování tiskárny. Přesměrování tiskáren navíc není dostupné aplikacím pro systém MS-DOS.

Metoda **síťového sdílení** je určena pro tiskárny připojené místně k osobním počítačům se spuštěnými systémy Windows for Workgroups 3.11 a novějšími. Uživatelé terminálů WBT se spuštěným protokolem RDP nemohou v současné době tisknout na místní tiskárny touto metodou.

Tisk přes síť WAN nebo telefonické připojení

Budou-li uživatelé získávat přístup k terminálovým službám přes síť WAN nebo telefonické připojení, pokuste se přesně odhadnout požadavky na šířku pásma všech tiskových úloh, které přes tato média budou řazeny.

Jestliže bude uživatel tisknout na místní tiskárnu, která se sice nachází na síti LAN uživatele, ale přes pomalé připojení od samotného serveru se spuštěnými terminálovými službami, tisková úloha se řadí k tiskárně přes toto pomalé připojení. Náklady na tento přenos se pak přidávají k obvyklým požadavkům na šířku pásma terminálových služeb, protože síť musí kromě tiskové úlohy zpracovávat také údaje o klávesnici, události myši a aktualizace zobrazení.

Také vám doporučujeme, abyste minimalizovali potřeby tisku velkých nebo barevných obrázků přes tato pomalá připojení, protože představují velkou spotřebu šířky pásma.

Doporučené postupy konfigurace klientů

Nejlepší výkonnost terminálových služeb zajistíte uživatelům dodržáním těchto doporučení:

- Minimalizujte použití graficky náročných prvků včetně animovaných obrázků, spořičů obrazovek, blikajících kurzorů a animovaného Pomocníka sady Microsoft Office.
- Zakažte použití systému Active Desktop.
- Zakažte plynulé posouvání.
- Minimalizujte použití grafiky a animací, jako jsou rozbalovací nabídky na pracovní ploše, zejména v nabídce Start. Potřebné zástupce umístěte na pracovní plochu a podnabídku Programy udržujte co nejmenší. Nepoužívejte bitové mapy jako tapetu – ve vlastnostech zobrazení nastavte na kartě **Pozadí** (Background) položku tapety na hodnotu **žádný** (None) a na kartě **Vzhled** (Appearance) vyberte jedinou barvu.
- Povolte sdílení souborů na klientských počítačích, přičemž sdílené jednotky nějak jednoduše pojmenujte, například „jednotka“. Věnujte pozornost souvisejícím problémům zabezpečení.
- Kdykoli je to možné, vyhýbejte se použití systému MS-DOS nebo aplikací Win16 (16bitových).
- Nakonfigurujte terminálový server tak, aby vracel aplikacím, které používají funkci systému NetBIOS volající název počítače, přihlašovací jméno uživatele a nikoli název počítače.
- Vyškolte uživatele v používání sekvencí klávesových zkratk terminálových služeb. Mezi sekvencemi klávesových zkratk používaných v klientské relaci terminálových služeb a relací systému Windows 2000 existují důležité rozdíly.

Plánování testování a pilotních programů

Možné problémy se zaváděním terminálových služeb se nejlépe odhalují během testování a pilotních programů. Při tomto ladění systému a řešení chyb se mohou objevit problémy infrastruktury, konfigurace systému nebo softwaru.

Úvahy o testovací laboratoři

Ideálním prostředím pro vyzkoušení zavedení terminálového serveru je testovací laboratoř, která byla vytvořena tak, aby co nejlépe simulovala vlastní prostředí zavedení. Testovací laboratoř bude fungovat jako miniaturní verze samotné vaší organizace a bude umožňovat sledování provozu terminálových služeb ještě před jejich zavedením.

Při vytváření testovací laboratoře terminálových služeb se zamyslete nad těmito body:

- Použijte serverový počítač od stejného výrobce a se stejnou konfigurací, jako budou mít servery používané ve vlastním nasazení, a vytvořte reprezentanty klientských počítačů, které budou ve vaší organizaci používat terminálové služby.
- Duplikujte síťovou konfiguraci ve vaší organizaci. Používá-li síť technologie Ethernet i Token Ring, musíte mít v testovací laboratoři oba systémy. Je-li to možné, vytvořte v laboratoři samostatnou doménu systému Windows 2000 Server, abyste mohli sledovat výkonnost řadičů domény bez vlivu dalších síťových aktivit. Plánujete-li zavést terminálové služby na síti WAN, vybavte testovací laboratoř směrovači a pomocí simulátoru linky simulujte čekací doby sítě.
- Budou-li terminálové služby používat různá oddělení podobnými, nikoli však stejnými způsoby, bude pravděpodobně možné emulovat všechna oddělení v jediné testovací laboratoři. Je-li rozdíl významnější, měli byste zvážit vytvoření samostatných laboratoří pro jednotlivá oddělení nebo sady úkolů.
- Na testovacím serveru vytvořte typickou sadu aplikací. Tento krok je velmi důležitý k odhalení možných problémů v situacích, kdy uživatelé spouštějí současně různé aplikace.

Sledování výkonu

Sledování výkonu je velmi důležitou součástí testování i každodenních operací v prostředí terminálových služeb. V počátečních fázích pilotního programu je zapotřebí určit základní požadavky. Během zavádění se pak tyto základní požadavky porovnávají se skutečným výkonem. To vám pomůže rychle odhalit a odstranit úzká místa v systému. Informace v tomto oddílu popisují základní čítače nástroje Sledování systému (System Monitor) potřebné k analýze výkonu terminálových služeb. Třemi základními součástmi systému, které mají vliv na výkonnost tohoto prostředí, jsou procesor, paměť a síť.

Vyhodnocení výkonu procesoru

Určení slabého výkonu procesoru na serveru terminálových služeb se podobá zjištění slabého výkonu procesoru na serveru se systémem Windows 2000, mohou se však lišit základní hodnoty čítačů. Nejdůležitějšími čítači určování úzkých míst systému jsou:

Procentuální část času procesoru (Procesor) Toto je čítač aktivity na všech procesorech systému. Ve víceprocesorovém systému je tento čítač roven celkovému množství aktivity procesoru vydělenému počtem procesorů. Tento čítač je užitečný zejména po prověření, že všechny procesory v systému zpracovávají toky rovnoměrně.

Délka fronty procesoru (Systém) Toto je okamžitá délka fronty procesoru v jednotkách toků. Všechny procesory používají jedinou frontu, ve které toky čekají na cykly procesoru. Jakmile je toku čekajícímu ve frontě procesoru dostupný nějaký procesor, tok lze přepnout na procesor a vykonat. Procesor může v jeden okamžik vykonávat jen jeden tok. Uvědomte si, že rychlejší procesory mohou zpracovávat delší fronty než pomalejší procesory.

Čas procesoru Jedná se o procentuální část času, kdy procesor vykonával jiný tok než tok procesu Idle (nečinný). Existuje jedna instance tohoto čítače pro každý procesor v systému, který je k dispozici operačnímu systému. Můžete jej použít k ověření, že jednotlivé procesory systému přispívají ke zpracování čekajících toků rovnoměrně.

Celkem přerušení/s Jedná se o rychlost, s jakou počítač přijímá a obsluhuje přerušení od hardwarových zařízení. Některými zařízeními, která mohou generovat přerušení, jsou systémový časovač, myš, datová komunikace, síťové karty a další periferní zařízení. Pomocí tohoto čítače můžete odhalit ovladače zařízení, které spotřebovávají nezvykle velké množství času procesoru.

Procentuální část celkového využití procesoru a délka fronty procesoru Toto jsou nejdůležitější čítače sloužící k identifikaci úzkých míst v systému způsobovaných nedostatkem výkonu procesoru. Čím je procesor vytíženější, tím vyšší je počet toků čekajících na vykonání ve frontě procesoru.

Vyhodnocení výkonu paměti

Kromě čítačů **Sledování systému** (System Monitor) zobrazuje ještě **Správce úloh** (Task Manager) hodnoty fyzické paměti, které mohou být velmi užitečné při určování výkonu paměti v terminálových službách. Hodnoty dostupné paměti, celkové paměti a mezipaměti systému najdete na kartě **Výkon** (Performance) nástroje **Správce úloh**.

Dvěma nejdůležitějšími čítači výkonu ve Správci úloh jsou dostupná paměť a vstup stránek/s. Chcete-li se vyhnout problémům s výkonem způsobeným pamětí, pozorně sledujte snižování hodnot v těchto čítačích. Snižování je dobrou indikací paměti potřebné pro jednoho uživatele. Obecně lze říci, že terminálový server je považován za plně vytížený z hlediska paměti, když je dostupná fyzická paměť menší než dvojnásobek průměrného požadavku paměti na uživatele. Zjistíte-li dramatický růst ve vstupu stránek/s, pravděpodobně došlo k překročení kapacity paměti a je zapotřebí do systému přidat paměť.

Hodnota dostupné paměti zobrazuje velikosti virtuální paměti, které jsou právě na seznámení vynulované, volné a připravené paměti. Vynulovaná a volná paměť je připravena k použití, přičemž vynulovaná paměť obsahuje nuly. Připravená paměť je paměť odstraněná z pracovní sady procesu, která je však stále k dispozici. Uvědomte si, že jde o okamžitý stav a nikoli o průměr v nějakém časovém intervalu.

Vstup stránek/s je počet stránek přečtených z disku v zájmu zajištění odkazů na stránky, které nebyly v okamžiku odkazu v paměti. Tento čítač zahrnuje stránkovací provoz způsobený systémovou mezipamětí při přístupu k datům souborů, která požadují aplikace. Jde o důležitý čítač, který musíte sledovat, máte-li starosti s velkými nároky na paměť a výsledným nadměrným stránkováním.

Vyhodnocení výkonu sítě

Výkon terminálových služeb může být považován za nepříjemný také díky zdržením v síťových komunikacích, přestože je k dispozici dostatek paměti i výkonu procesoru.

Úzká místa v síťových komunikacích se mohou vyskytovat ve čtyřech různých oblastech: síťové rozhraní klienta, fyzické síťové médium, síťové rozhraní klient/server serveru a síťové rozhraní serveru při komunikacích server/server-hostitel. Úzká místa v síťových komunikacích přímo ovlivňují práci uživatelů na klientských pracovních stanicích.

Nejužitečnějšími čítači Sledování systému (System Monitor) pro sledování využití sítě jsou čítače Segment sítě:

- % využití sítě je procentuální část šířky pásma sítě používané na sledovaném segmentu.
- Přijaté bajty celkem/s představuje celkový počet bajtů přijatých za sekundu na síťovém segmentu.
- Přijaté rámce celkem/s je celkový počet paketů přijatých za sekundu na síťovém segmentu.

Použití skupiny odborné pomoci a nástrojů správy

Terminálové služby umožňují vytvoření skupiny odborné pomoci uživatelům, která má k dispozici řadu nástrojů správy a funkce vzdáleného řízení, jež podporu uživatelů usnadňuje.

Vzdálené řízení

Funkce vzdáleného řízení umožňuje profesionálovi technické podpory dočasně převzít řízení připojení jiného uživatele a sledovat akce uživatele. Oddělení podpory může také interaktivně spolupracovat s uživatelem a vykonávat příkazy jeho jménem.

Chcete-li skupině technické pomoci umožnit práci se vzdáleným řízením, doporučujeme vám vytvořit v doméně skupinu odborné pomoci. Po vytvoření skupiny ji můžete pomocí modulu snap-in Konfigurace služby Terminal Services (Terminal Services Configuration) konzoly MMC přiřadit oprávnění používat funkci vzdáleného řízení.

Chcete-li využít vzdálené řízení prostřednictvím protokolu RDP, oba klienti musí být připojeni k terminálovému serveru systému Windows 2000.

Nástroje pro správu

Po instalaci terminálových služeb (služeb Terminal Services) systému Windows 2000 se ve složce Nástroje pro správu objeví další nástroje. Jsou jimi:

Vytváření klientů služby Terminal Services (Terminal Services Client Creator) Tento nástroj se používá k vytváření disket instalace klientského softwaru terminálových služeb na platformy Windows for Workgroups, Windows 95, Windows 98 a Windows NT.

Správce služby Terminal Services (Terminal Services Manager) Pomocí tohoto nástroje lze spravovat všechny servery systému Windows 2000 se spuštěnými terminálovými službami. Správci si mohou zobrazovat aktuální uživatele, servery a procesy. Navíc mohou správci odesílat zprávy určitým uživatelům, používat funkci vzdálené správy a ukončovat procesy.

Konfigurace služby Terminal Services (Terminal Services Configuration) Tento nástroj umožňuje správu konfigurace RDP. Úprava voleb v tomto nástroji je globální, pokud tedy nezadáte dědičnost informací ze stejných voleb umístěných v konfiguraci uživatele. Dostupnými volbami jsou: nastavení šifrování spojení, nastavení přihlašování, časy

vypršení, počáteční programy spouštěné při úspěšném přihlášení, možnosti vzdáleného řízení, připojování (mapování) tiskárny Windows, připojování portu LPT, připojování schránky a aplikování těchto voleb na určitou kartu LAN.

Správa licencí služby Terminal Services (Terminal Services Licensing) Pomocí tohoto nástroje lze ukládat a sledovat licence klientského přístupu k terminálovým službám systému Windows 2000. Je možné jej instalovat hned během instalace terminálových služeb nebo později. Když se klienti připojují k terminálovým službám, terminálové služby ověřují klientskou licenci. Nemá-li klient licenci nebo vyžaduje-li její náhradu, terminálové služby požadují licenci od licenčního serveru (License Server). Licenční server poskytne určitou licenci se svého seznamu dostupných licencí a terminálové služby ji předají klientovi. Nejsou-li k dispozici žádné licence, licenční server vystaví klientovi dočasnou licenci. Po svém vystavení se každá klientská licence přiřadí určitému počítači nebo terminálu.

Seznam úkolů plánování zavádění terminálových služeb

Tabulka 16.2 shrnuje úkoly, které musíte vykonat při plánování zavedení terminálových služeb.

Tabulka 16.2 Souhrn úkolů plánování terminálových služeb

Úkol	Umístění v kapitole
Vyberte režim vzdálené správy nebo aplikačního serveru.	Přehled terminálových služeb
Určete licenční požadavky.	Přehled terminálových služeb
Určete, jak se budou terminálové služby používat ve vašem podnikovém prostředí.	Vytváření plánu zavedení terminálových služeb
Zdokumentujte existující počítačové prostředí.	Vytváření plánu zavedení terminálových služeb
Popište, jak projekt zavedení splňuje určené požadavky.	Vytváření návrhu zavedení terminálových služeb
Vytvořte plán zavedení terminálových služeb včetně práce v síti, zabezpečení a struktury domén.	Vytváření návrhu zavedení terminálových služeb
Stanovte základní pravidla a standardy zavedení serverů včetně problémů procesorů, úložišť atd.	Konfigurování serverů na zavedení terminálových služeb
Připravte se na zavedení do klientského prostředí.	Příprava na zavedení klientů
Připravte se na testování a pilotní program vašeho plánu zavedení.	Plánování testování a pilotních programů
Připravte se na zajištění technické podpory.	Použití skupiny odborné pomoci a nástrojů správy

Pokročilá správa



Zejména pro manažery IT je užitečné porozumět funkcím pokročilé správy systému Microsoft Windows 2000, které zvyšují spolehlivost a dostupnost sítě. Část 5 poskytuje informace o strategiích zabezpečení při zpřístupnění Internetu, funkce škálovatelnosti a dostupnosti, možnosti správy úložišť a synchronizování služby Active Directory s adresářovou službou Microsoft Exchange Server.

V této části

Určení strategií zabezpečení sítě systému Windows 2000 509

Zajištění dostupnosti aplikací a služeb 529

Určení strategií správy úložišť systému Windows 2000 569

Synchronizování služby Active Directory s adresářovou službou programu Exchange Server 595

KAPITOLA 17

Určení strategií zabezpečení sítě systému Windows 2000

V dnešní době požaduje většina společností připojení své počítačové infrastruktury na Internet, protože tato síť zajišťuje cenné služby jejich zaměstnancům i zákazníkům. Služby zpřístupněné přes připojení k Internetu však mohou být zneužity, čemuž je zapotřebí zabránit zavedením strategií zabezpečení sítě. Systém Microsoft Windows 2000 obsahuje různé technologie, které můžete využít při plánování strategie zabezpečení své sítě. Tyto technologie vám mohou také pomoci v případě, kdy musíte řešit ve své organizaci interní problémy zabezpečení sítě nebo používáte-li jako externí síťová připojení linky k jiným sítím než je Internet. Další informace o interním zabezpečení najdete v kapitole „Plánování distribuovaného zabezpečení“ v této knize.

Tato kapitola popisuje strategické používání technologií zabezpečení k ochraně připojení sítě vaší společnosti k Internetu či jiným veřejným sítím. Kapitola neuvádí podrobnosti o instalaci a používání technologií zabezpečení sítě. Kapitola by si měli přečíst zejména architekti sítě účastníci se návrhu zabezpečení sítě a správci systému, jejichž starostí je správa zabezpečení sítě. Abyste mohli vykonávat úlohy uvedené v této kapitole, musíte být seznámeni se síťovými a internetovými technologiemi, jako jsou směrování, síťové protokoly a webové služby.

V této kapitole

Plánování zabezpečení sítě 510

Vývoj strategií zabezpečení síťových připojení 513

Zavádění technologií zabezpečení sítě 516

Seznam úkolů plánování určení strategií zabezpečení sítě 527

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Plán zabezpečení sítě
- Plán zavedení technologií zabezpečení sítě

Související informace v sadě Resource Kit

- Další informace o implementaci a používání souvisejících technologií zabezpečení sítě systému Windows 2000 najdete v knize *Microsoft Windows 2000 Server Internet-working*.
- Další informace o protokolu IPSec najdete v knize *Microsoft Windows 2000 Server Sítě TCP/IP*.

Plánování zabezpečení sítě

Připojení k Internetu umožní zaměstnancům vaší společnosti používat ke komunikaci s lidmi po celém světě zprávy elektronické pošty a získávat informace a soubory z obrovského množství zdrojů. Také to umožňuje vašim zákazníkům kdykoli získat informace a služby od vaší společnosti. Zaměstnanci vaší organizace navíc mohou využívat prostředky společnosti ze svých domovů, hotelů nebo jiných míst a partneři mohou používat určité speciální funkce, které jim umožní efektivněji spolupracovat s vaší společností.

Při plánování sítě musíte implementovat technologie zabezpečení, které budou odpovídat vaší organizaci. Budete-li se těmito otázkami zabývat již v počátečních fázích plánování zavedení systému Windows 2000, zaručíte tak, že nebude možné zabezpečení obejít a že budete schopni v případě potřeby zajistit nástroje zabezpečené práce v síti. Třebaže už pravděpodobně máte vytvořené zabezpečené síťové prostředí, je důležité podívat se na strategie zabezpečení z hlediska schopností systému Windows 2000. Zvažíte-li všechny důsledky nových technologií zabezpečení sítě v systému Windows 2000, může to vést ke změně plánu zabezpečení. Pro začátek vám doporučujeme splnit při vývoji plánu zabezpečení sítě tyto úkoly:

- Vyhodnoťte rizika zabezpečení sítě.
- Určete požadavky na velikost a umístění vašeho serveru.
- Připravte svůj personál.
- Vytvořte a publikujte zásady a postupy zabezpečení.
- Pomocí formální metodologie vytvořte plán zavedení technologií zabezpečení.
- Zjistěte skupiny uživatelů a jejich specifické potřeby a rizika zabezpečení.

Tyto položky jsou podrobně popsány v následujících oddílech.

Poznámka Další informace o plánování zavedení vaší sítě najdete v kapitole „Určení strategií konektivity sítě“ v této knize. Uvedená kapitola obsahuje strategie směřování, adresování, překladu názvů, síťových aplikací a podobných problémů práce v síti. Tato kapitola se zaměřuje na otázky zabezpečení sítě.

Vyhodnocení rizik zabezpečení sítě

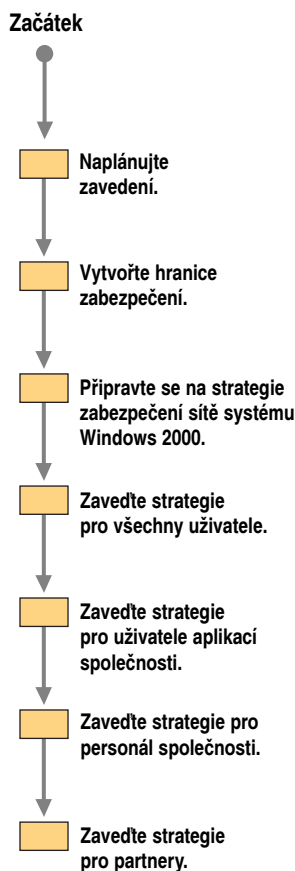
Bohužel je možnost sdílet a získávat informace doprovázena značnými riziky. Vaši konkurenti se mohou pokoušet o přístup k předběžným či nepublikovaným informacím o výrobku nebo se někdo může pokoušet měnit webové stránky se zlým úmyslem či přetěžovat vaše počítače do takové míry, že budou nepoužitelné. Také je tu možnost, že vaši zaměstnanci budou přistupovat k informacím, které by neměli vidět. V každém případě se chcete vyhnout uvedeným i dalším typům rizik zabezpečení a zaručit řádné

fungování vaší společnosti. Chcete-li zajistit, aby měli k prostředkům a datům přístup jen příslušné osoby, bude vhodné důkladně se zamyslet nad technologiemi zabezpečení sítě a dobře naplánovat svou strategii. Sem patří také vyvozování zodpovědnosti, kterého lze docílit sledováním používání síťových prostředků.

Obecný popis identifikování rizik zabezpečení a výběru příslušných strategií najdete v kapitole „Plánování distribuovaného zabezpečení“ v této knize.

Poznámka Některé organizace minimalizují bezpečnostní rizika sítě tím, že neumožňují připojení k Internetu a k jiným veřejným sítím. Tím se samozřejmě výrazně omezí okruh lidí, kteří mohou prostředky sítě zneužít. I v takové organizaci však stále existují bezpečnostní rizika a určitá bezpečnostní rizika mohou představovat i omezená síťová připojení. V těchto situacích je tedy také zapotřebí použít strategie a technologie zabezpečení sítě.

Obrázek 17.1 ukazuje hlavní kroky určování strategií zabezpečení sítě.



Obrázek 17.1 proces určení strategií zabezpečení sítě

Určení velikosti a umístění serveru

Při vytváření spojení mezi vaším intranetem a Internetem nebo jinou veřejnou sítí musíte pečlivě zvážit, kde spojení uskutečníte. Obvykle půjde o centrální část sítě vaší společnosti, aby se minimalizovala efektivní vzdálenost mezi vašimi servery a Internetem. Půjde také většinou o místo, kam mohou síťoví specialisté při údržbě snadno dojít.

V ideálním případě budete mít pro celou společnost jen jedno připojení na Internet. Tím se zjednoduší správa připojení a omezí se možná rizika zabezpečení vznikající díky nekonzistentnosti aplikovaných zásad a postupů.

Jakmile určíte místo připojení k Internetu, musíte se rozhodnout, jaký hardware serveru budete potřebovat k podpoře technologií zabezpečení vaší sítě. Charakteristiky těchto serverů budou záviset na technologiích, které plánujete zavést, a očekávaném zatížení, přinejmenším však musí být schopny provozovat systém Windows 2000 Server. Je sice možné provozovat na serverech se spuštěnými aplikacemi zabezpečení sítě také jiný software, tento postup vám však nedoporučujeme. Spouštění dalších aplikací omezuje schopnost serverů reagovat na potřeby zabezpečení sítě a může způsobit selhání serverů. Mají-li navíc takové aplikace bezpečnostní slabiny, mohou snižovat zabezpečení sítě.

Příprava personálu

Technologie zabezpečení musí být zaváděny a spravovány velmi schopnými a důvěryhodnými lidmi. Tito lidé musí integrovat celou síť a infrastrukturu zabezpečení sítě tak, aby byly její slabiny odstraněny nebo minimalizovány. Při změně prostředí a požadavků musí navíc zajistit kontinuitu integrity infrastruktury zabezpečení sítě.

Kritickým faktorem zajištění úspěchu personálu zabezpečení sítě je jejich dobré proškolení a průběžné seznamování se změnami technologií. Personál potřebuje určitý čas, aby se mohl seznámit se systémem Windows 2000 a zejména s jeho technologiemi zabezpečení sítě. Musí mít také možnost aplikovat své znalosti ze školení při experimentálních činnostech a praktických aplikacích.

Navíc se musí personál zabezpečení sítě důkladně seznámit s obecnými principy otáček zabezpečení sítě. Na toto téma existuje mnoho knih a na Internetu lze nalézt velké množství sídel, která se zabezpečením sítě zabývají.

Vývoj zásad a postupů zabezpečení

Zásady a postupy jsou důležité vždy, v případě zabezpečení jsou však kritické. Musíte vytvořit a publikovat své zásady a získat souhlas s tím, jak budete zpracovávat určité problémy zabezpečení. Zároveň musíte zajistit, aby tyto zásady byly všem naprosto jasné. Formální postupy zajistí, že správa a změny systému budou vždy uskutečněny promyšleným způsobem.

Jednou z otázek, nad kterou se musíte zamyslet, je, jak budete sledovat narušení nebo pokusy o narušení zabezpečení. Narušení a pokusy o prolomení zabezpečení lze minimalizovat, když o nich bude příslušný personál vědět co nejdříve. To je možné pouze při používání postupů sledování. Dobře definované zásady vám pomohou vytvořit postupy řešení takových bezpečnostních otázek.

Dalším důležitým problémem zabezpečení, kterému se musíte věnovat, je spolehlivost. Připravte si plán pro případ selhání nějaké komponenty infrastruktury zabezpečení. Předem si připravte příslušné akce pro všechna možná narušení zabezpečení a mějte k dispozici prostředky zajišťující co možná nejrychlejší odstranění problému.

Vytvoření plánu zavedení technologií zabezpečení

Pomocí formální projektové metodologie vytvořte jako součást celkového plánu zavedení systému Windows 2000 podrobný plán zavedení technologií zabezpečení sítě. To zajistí zavádění technologií systematickým a důkladným způsobem s minimální možností chyby. Mezi kritické kroky projektu patří předání zásad zabezpečení sítě všem dotčeným stranám a oznámení zásad a postupů uživatelům sítě.

Nejdůležitějším aspektem projektu zavádění je testování. Technologie zabezpečení sítě, které budete používat, musí být podrobeny významnému a realistickému testování v bezpečném prostředí. Tím se přesvědčíte o tom, že architektura funguje podle vašich představ, že jste dosáhli svých cílů zabezpečení a že je váš personál připraven na zavedení a podporu těchto technologií.

Zjištění kategorií uživatelů a jejich potřeb a rizik zabezpečení

Infrastruktura sítě má za úkol sloužit lidem ku prospěchu vaší organizace. Pro účely popisu strategií zabezpečení sítě v této kapitole jsou tyto lidé rozděleni do čtyř skupin uživatelů sítě:

Každý (všichni) Tato kategorie zahrnuje všechny osoby přistupující k vaší síti z libovolné organizace a z libovolného místa, což představuje personál, uživatele a partnery. Obvykle je nelze spolehlivě identifikovat, a proto musí být považovány za anonymní osoby.

Personál Tato skupina zahrnuje všechny osoby, které pracují pro vaši organizaci. Lze je jednoduše identifikovat pomocí standardizovaných interních postupů. Obvykle používají elektronickou poštu společnosti a váš intranet.

Uživatelé Tato skupina zahrnuje personál, který při své práci používá aplikace.

Partneři Tato skupina zahrnuje osoby z jiných organizací a míst, které mají k vaší organizaci nějaký zvláštní vztah. Jsou připraveni na vykonání standardizovaných postupů, takže je lze identifikovat. Mohou používat funkce podobné jako personál a uživatelé. Často se považují za součást extranetu.

Strategie zabezpečení sítě uvedené v této kapitole adresují potřeby a rizika jednotlivých kategorií uživatelů sítě a uvádějí podrobnosti o přístupech, kterými můžete uspokojit jejich potřeby a minimalizovat rizika. Navíc tu najdete celkovou strategii zabezpečení z obecného hlediska a celkovou strategii infrastruktury zabezpečení sítě.

Vývoj strategií zabezpečených síťových připojení

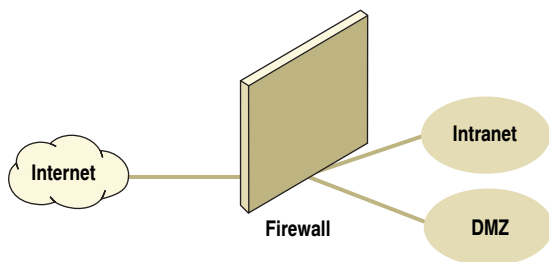
Zabezpečení sítě se stává nejdůležitějším, když připojujete své počítače k síti, které nemůžete plně důvěřovat. Řešení otázek zabezpečení sítě je v rámci organizace poměrně obvyklé; v takových případech však máte k dispozici nástroje zajišťující zodpovědnost a disciplínu, a navíc máte k dispozici oblast základních a distribuovaných technologií a technologií zabezpečení sítě, kterými lze tyto otázky řešit. Za hranicemi vaší organizace se však možnosti zodpovědnosti a disciplíny výrazně omezují, a proto se mnohem více musíte spoléhat na samotné strategie zabezpečení.

Vytváření hranic zabezpečení

Zabezpečení sítě mezi vaší organizací a vnějším světem je určeno jedním nebo více servery, na kterých implementujete technologie zabezpečení sítě. Tyto servery se logicky nacházejí na hranici mezi vaší organizací a vnějším světem. Aplikační servery zajišťující služby pro vnější svět se často nacházejí na stejném fyzickém místě.

Jedním z přístupů, jak maximalizovat zabezpečení těchto serverů, je logicky umístit je na jednoznačné místo v infrastruktuře vaší sítě. Oblast, ve které jsou umístěny, se často označuje za demilitarizovanou zónu (DMZ). Firewall (popisovaný v následujícím oddílu) má další síťový adaptér, který na základě sady adres přiřazených dané oblasti přeměrovává provoz na DMZ. Tento vztah zachycuje obrázek 17.2.

V rámci DMZ můžete zajistit, aby servery neměly přístup k prostředkům společnosti. Dojde-li k narušení zabezpečení na těchto serverech, narušitelé se pak nemohou přemístit na další počítače ve vašem intranetu.



Obrázek 17.2 Demilitarizovaná zóna

Zóna DMZ nesmí být, stejně jako interní komponenty sítě, fyzicky přístupná veřejnosti. Tím je zajištěno, aby nikdo (včetně vašich zaměstnanců) nemohl oslabit zabezpečení změnou uspořádání kabelů nebo použitím přihlášených účtů.

Není zapotřebí fyzicky oddělit DMZ od dalších počítačů a zařízení sítě. Vzhledem ke kritické roli DMZ při zabezpečení sítě je však vhodné na DMZ aplikovat speciální zásady a postupy. I ty nejmenší nesprávně zadané změny mohou dostačovat k vytvoření slabiny, které mohou narušitelé následně využít. Proto musí být zajištěno, aby DMZ mohl měnit pouze kvalifikovaný personál. To lze zajistit aplikováním dalšího fyzického zabezpečení DMZ.

Upozornění Klientské počítače a účty pečlivě zabezpečte a zajistěte tak, aby je mohli pro přístup k síti používat výhradně oprávnění uživatelé. Nemůžete-li fyzicky zabezpečit klientský počítač, pak zajistěte, aby na něm používané účty měly jen malá privilegia a používejte šifrování souborů, zabezpečené spořiče obrazovky a další strategie místního zabezpečení.

Zabezpečení proti všem

Abyste zabezpečili síť vaší organizace při přístupu z Internetu a na Intranet, musíte mezi tato dvě média vložit server. Tento server zajistí propojení personálu společnosti na Internet a zároveň bude minimalizovat rizika vyplývající z tohoto připojení. Současně

bude zabráňovat v přístupu na všechny počítače na vaší síti z Internetu ve všech případech s výjimkou počítačů, na které bude takový přístup specificky umožněn.

Na tomto serveru běží software firewallu nebo proxy-serveru. Má také dvě síťová rozhraní: jedno pro síť společnosti a jedno pro Internet. Software firewallu nebo proxy-serveru zkoumá všechny síťové pakety na obou rozhraních a určuje jejich cílové adresy. Jestliže pakety splňují zadaná kritéria softwaru, v případě potřeby jsou předány druhému rozhraní, které je distribuuje do další příslušné sítě.

V některých případech se obsah paketů předává dál, jako by přicházely z proxy-serveru, a výsledky se předávají požadujícímu počítači, když se vrátí na adresu proxy-serveru. To zajišťuje, aby lidé na Internetu nemohli získat adresy jiných počítačů ve společnosti, než je adresa proxy-serveru.

Použití programu Microsoft Proxy Server

Microsoft Proxy Server 2.0 zajišťuje funkce proxy-serveru i firewallu. Proxy Server 2.0 běží na systému Windows 2000 a v zájmu zajištění úplného zabezpečení sítě musí být oba systémy řádně nakonfigurovány. Máte-li verzi nástroje Proxy Server dřívější než 2.0 se servisním balíčkem 1, musíte jej během inovace serveru na systém Windows 2000 pro zajištění kompatibility inovovat.

V mnoha případech je objem provozu mezi sítí společnosti a Internetem větší, než může zvládnout jeden proxy-server. V těchto situacích můžete použít více proxy-serverů; provoz mezi nimi se pak automaticky koordinuje. Uživatelům na straně Internetu i intranetu se zdá, jako by existoval jen jeden proxy-server.

Chcete-li používat pokročilé funkce programu Microsoft Proxy Server, na počítačích musí být nainstalován klient Microsoft Proxy Server a musí být nakonfigurován tak, aby používal proxy-server. Počítače bez klienta (například ty na Internetu) budou od proxy-serveru získávat jen jeho základní funkce jako anonymní uživatelé.

Je důležité, abyste proxy-server, ještě před jeho připojením na Internet, otestovali. Vytvořte simulaci Internetu a vašeho intranetu v malém rozsahu a zařídte, aby klientské počítače přistupovaly v obou směrech k různým službám. Také se pokuste o neautorizovaná připojení a ověřte, že je vaše síť odmítne. Nezapomeňte vyzkoušet různé metody přístupu k síti a ověřit tak, že jsou všechny typy přístupu k síti zabezpečené. Vyzkoušejte různé techniky, které lze použít ke zjišťování bezpečnostních děr, a ujistěte se tak, že ve vašem prostředí se žádné takové díry nevyskytují. Konkrétní problémy, které můžete otestovat, najdete v knihách popisujících zabezpečení sítě. S takovým testováním vám také mohou pomoci výrobky jiných společností nebo konzultanti, kteří mají v této oblasti rozsáhlé zkušenosti.

Postupy používání programu Microsoft Proxy Server jsou součástí tohoto produktu. Další informace o nástroji Microsoft Proxy Server a podrobnosti o technologiích zabezpečení společnosti Microsoft najdete v odkazu Microsoft Security Advisor stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Sledování zabezpečení sítě

Technologie zabezpečení sítě, které budete implementovat, mohou splnit vaše cíle, pouze pokud je pečlivě naplánujete a nakonfigurujete. Když se na tuto práci důkladně připravíte, výsledkem bude její velmi úspěšný výsledek. Předvídat všechna možná rizika však může být velmi obtížné: stále se objevují nová rizika, systémy se hrouť a prostředí, ve kterém se vaše systémy nacházejí, se časem mění. Tato rizika může minima-

lizovat neustálá kontrola strategií zabezpečení vaší sítě. Musíte však také neustále sledovat skutečnou bezpečnostní aktivitu v síti, což vám pomůže odhalit její slabiny ještě před jejich zneužitím a odhalit pokusy o narušení zabezpečení ještě před jejich úspěšným provedením.

Abyste mohli sledovat bezpečnostní aktivity sítě, potřebujete nástroje, které dokáží zachycovat podrobné údaje o těchto činnostech a analyzovat tato data. Microsoft Proxy Server umožňuje protokolování událostí na dvou úrovních: normální a podrobné. Systém Windows 2000 také obsahuje protokolování událostí, které lze ještě vylepšit povolením auditování zabezpečení. Nástroj Internet Authentication Server, který je popsán dále v této kapitole, má také rozsáhlé možnosti zaznamenávání činností. Existují rovněž nástroje jiných výrobců, které vám pomohou se sledováním serverů a aplikací, a to včetně serverů a aplikací zabezpečení. V každém případě si důkladně prostudujte dokumentaci vámi používaných systémů a vyberte takové možnosti protokolování, které nejlépe odpovídají vašim požadavkům.

Připojení k externím sítím

Jakmile máte zavedený proxy-server společně s nástroji sledování a řádně připravený personál, můžete připojit svou síť k externí síti. O tom, že tato implementace řádně naplňuje vaše plány, se přesvědčte finální sadou testů. Musíte si být jisti, že jsou dostupné pouze ty služby, které jste povolili, a že riziko zneužití je prakticky nulové. Takové prostředí vyžaduje pečlivé sledování a správu, budete však zároveň připraveni na realizování dalších zabezpečených síťových služeb.

Poznámka Tato kapitola nepopisuje metody zajištění síťového připojení. Na toto téma existuje mnoho knih a připojení může zajistit váš poskytovatel síťových služeb, který vás také může odkázat na konzultanty, jež takové připojení vytvoří.

Zavádění technologií zabezpečení sítě

Jakmile máte připravenou celkovou strategii zabezpečení sítě, můžete určit použití pokročilých technologií zabezpečení sítě pro jednotlivé skupiny uživatelů definované v této kapitole: každý (všichni), personál, uživatelé a partneři. Pak lze zavést strategie zabezpečení sítě pro jednotlivé skupiny uživatelů sítě. Nejprve se zamyslete nad potřebami skupiny všech uživatelů a pak se podle požadavků obchodních či výrobních priorit zabýváte potřebami personálu společnosti, uživatelů aplikací společnosti a partnerů.

Před určením konkrétních zásad zabezpečení ve vaší organizaci si musíte být vědomi možností systému Windows 2000, které dokáží zabezpečení sítě vylepšit.

Příprava na technologie zabezpečení sítě systému Windows 2000

V některých případech závisejí technologie zabezpečení sítě systému Windows 2000 na jiných technologiích zabezpečení systému Windows 2000. Například protokol virtuální privátní sítě Layer Two Tunneling Protocol (L2TP) používá k zajištění zabezpečení směrem od vzdáleného klienta k serveru VPN protokol IPSec. Vyjednávání o zabezpečení protokolu IPSec vyžadují pro ověření připojení certifikátů. Proto je nutný certifikační server s příslušným nastavením. Certifikační server systému Windows 2000 je obvykle připojen k doméně. Doména určuje zásady skupiny (Group Policy) s nastavením infrastruktury veřejných klíčů (PKI), aby se mohli počítače automaticky zapisovat

v tomto certifikačním úřadu a získávat certifikáty počítačů potřebné pro protokol IPSec. L2TP vytváří potřebné zásady IPSec a zajišťuje tak zabezpečení provozu L2TP. Správci však mohou také vyžadovat zabezpečení jiného provozu mezi klienty a servery. To vyžaduje konfiguraci IPSec na každém klientovi a serveru. Protože protokol IPSec se konfiguruje pomocí zásad, po vytvoření v Active Directory můžete tytéž zásady aplikovat na všechny počítače na základě skupiny nebo domény. Zásady certifikátů a IPSec lze centralizovanou správou zavést na všechny počítače v doméně pomocí zásad skupiny v Active Directory.

Další informace o plánování zavedení certifikátů systému Windows 2000 najdete v kapitole „Plánování infrastruktury veřejných klíčů“ v této knize. Další informace o plánování služby Active Directory najdete v kapitole „Návrh struktury služby Active Directory“ v této knize.

Zavádění strategií pro všechny

Jakmile máte vytvořené připojení k Internetu, každá osoba, která jej nalezne, představuje potenciální nebezpečí ohrožení sítě. Proto je první komunitou uživatelů, o kterou se musíte postarat při zavádění celkové strategie zabezpečení sítě, skupina, kterou jsme dříve definovali jako každý neboli všichni. Částečně jste to již učinili tím, že jste zavedli proxy-server i zásady, postupy a technologie sledování zabezpečení.

Můžete se také zamyslet nad síťovými aplikacemi, které všem usnadní práci, a požadavky na zabezpečení, které tyto aplikace mají. Lze například nastavit službu Microsoft Internet Information Services (IIS) s interním webovým sídlem. IIS poskytuje mnoho voleb zabezpečení, které musíte opatrně zvážit a podle potřeby nakonfigurovat (IIS obsahuje rozsáhlou dokumentaci k tomuto tématu). Zvažte také použití serverů protokolu File Transfer Protocol (FTP) a dalších služeb, které mohou prospívat všem.

Zavádění strategií pro personál

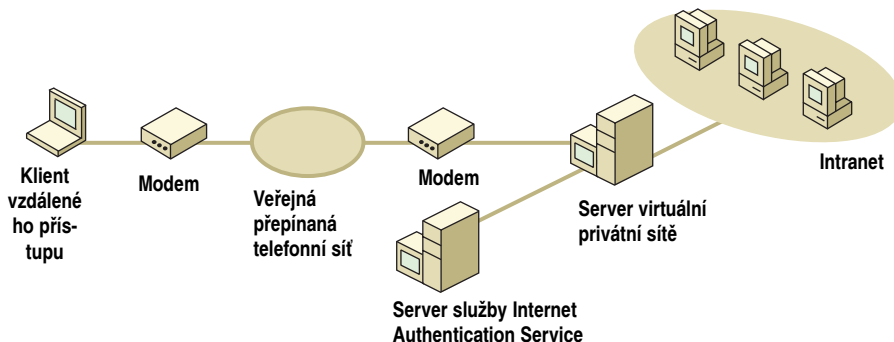
Lidé ve skupině personálu mohou například potřebovat, v zájmu přístupu k interním webovým sídlům, kopírování souborů, tisku dokumentů a dalším jednoduchým funkcím, přistupovat k síti společnosti z libovolného místa. Základním smyslem zabezpečení v těchto případech je před zaručením volného přístupu k síti ověřit, že je uživatel oprávněným zaměstnancem. Proto musí být počáteční připojení k síti zabezpečené, ale žádné další ověřování už není zapotřebí. Dalším problémem je, že musíte zabránit neoprávněným osobám v narušování a čtení provozu na síti.

Zaměstnanci mohou pro přístup na síť společnosti používat poskytovatele připojení k Internetu (ISP), takový přístup však nebude mít celý personál. Také třeba nebudete chtít zpřístupnit přes všechny intranetové služby nebo budete vyžadovat zaručenou kapacitu sítě vyhrazeného síťového připojení. Pomocí služby Směrování a vzdálený přístup (Routing and Remote Access) systému Windows 2000 lze velmi podrobně definovat zásady vzdáleného přístupu v tom, jak mohou uživatelé přistupovat k interní síti při připojování přes Internet.

Směrování a vzdálený přístup

Organizace obvykle na svých sídlech poskytují možnosti vzdáleného přístupu pro personál. Personál oddělení informačních technologií (IT) vytvoří pro tento účel vyhrazená telefonní čísla a k serveru, který je přímo připojen k intranetu, připojí modemy (nebo podobný hardware). Na serveru běží specializovaný software určený ke zpracování podrobností připojení a server zároveň ověřuje telefonicky připojeného uživatele jako oprávněného člena personálu.

Systém Windows 2000 obsahuje službu Směrování a vzdálený přístup (Routing and Remote Access), která vám umožňuje poskytovat uživatelům možnost telefonického připojení. Chcete-li centralizovat ověřování, autorizaci a služby účtů uživatelů v systému Windows 2000, můžete nastavením serveru Internet Authentication Service (IAS) používat vzdálený přístup nebo VPN. Obrázek 17.3 ilustruje jednu z možných konfigurací takových serverů.



Obrázek 17.3 Ukázka konfigurace služby Směrování a vzdálený přístup

Kniha *Microsoft Windows 2000 Server Internetworking* obsahuje informace o fungování služby Směrování a vzdálený přístup (Routing and Remote Access) a jí poskytovaných možnostech. Nápopověda systému Windows 2000 Server pak popisuje instalaci a použití služby Směrování a vzdálený přístup.

Při plánování zavedení služby Směrování a vzdálený přístup zvažte následující bezpečnostní problémy:

- Komu předáte telefonní čísla?
- Kdo bude mít oprávnění používat službu Směrování a vzdálený přístup?
- Jaké metody ověření se budou používat?
- Jak se bude používat šifrování dat (od klienta služby Směrování a vzdálený přístup k serveru této služby)?

Vyžadujete-li šifrování mezi koncovými body (od klienta vzdáleného přístupu celou trasou k aplikačnímu serveru na interní síti), použijte zabezpečený protokol Internet Protocol (IPSec), který je popsán dále v této kapitole.

- Jaké zásady vzdáleného přístupu se budou používat k řízení přístupu uživatelů?

Další informace o obecných otázkách zavedení služby Směrování a vzdálený přístup najdete v kapitole „Určení strategií konektivity sítě“ v této knize.

Zabezpečení služby Směrování a vzdálený přístup

Omezení distribuce telefonních čísel služby Směrování a vzdálený přístup (Routing and Remote Access) pomáhá minimalizovat počet lidí, kteří se budou pokoušet o telefonické připojení k vaší síti. Přesto však všechna telefonická připojení představují určité riziko, protože dané telefonní číslo může potenciálně získat kdokoli. Je například možné vytvořit automatický proces postupného vytáčení telefonních čísel, až dokud se ne-

najde modem, který odpoví. Proto musí být služba Směrování a vzdálený přístup zabezpečena tak, aby zajistila pouze oprávněný přístup. Minimem je, že uživatel musí službě Směrování a vzdálený přístup poskytnout platný počítačový účet a heslo. Tato úroveň zabezpečení je však otevřená všem obvyklým útokům na přihlášení, jako je například odhadování hesla.

Doporučujeme vám, abyste používali ještě další možnosti zabezpečení služby Směrování a vzdálený přístup. Můžete omezit použití služby Směrování a vzdálený přístup jen na osoby s potvrzenou potřebou používání telefonického připojování. Lze také nastavit službu Směrování a vzdálený přístup tak, aby po prvním vytvoření připojení spojení ukončila a potom zavolala zpět uživateli. Potom může uživatel přistupovat ke službě Směrování a vzdálený přístup výhradně z předdefinovaného telefonního čísla nebo může být jeho telefonní číslo zaznamenáno. V některých případech je také možné použít k záznamu telefonního čísla, které iniciovalo spojení, identifikátor volajícího.

Zvažte také, že technikami podobnými odposlouchávání někdo může zachytit uživatelské jméno a heslo v okamžiku, kdy se daný uživatel pokouší připojit ke službě Směrování a vzdálený přístup. Chcete-li tomu zabránit, nastavte službu Směrování a vzdálený přístup tak, aby používala nějakou zabezpečenou metodu ověřování uživatele, například protokoly Extensible Authentication Protocol (EAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) verze 1 a verze 2, Challenge Handshake Authentication Protocol (CHAP) nebo Shiva Handshake Authentication Protocol (SPAP).

Souvisejícím rizikem je uživatel, který si myslí, že se telefonicky připojuje k síti své společnosti, ale ve skutečnosti se právě připojuje k jinému místu, které nyní obdrží jeho identifikační informace. Chcete-li vyřešit tento problém, použijte vzájemné ověřování, jež zajišťuje nejen ověření uživatele, ale také ověření serveru služby Směrování a vzdálený přístup. To umožňují ověřovací protokoly EAP-Transport Layer Security (EAP-TLS) a MS-CHAP verze 2.

Podobné problémy platí i pro data přenášená přes připojení ke službě Směrování a vzdálený přístup. Ověřovací protokoly EAP-TLS a MS-CHAP verze 2 umožňují šifrování vysílaných dat pomocí metody Microsoft Point-to-Point Encryption (MPPE).

Zásady vzdáleného přístupu, ať už jsou implementovány jako místní zásady nebo jako součást zásad skupiny, si mohou vynucovat používání technik ověřování a šifrování, které chcete používat.

Další informace o práci v síti, ověřování služby Směrování a vzdálený přístup a technikách šifrování dat najdete v nápovědě systému Windows 2000 Server.

Virtuální privátní síť

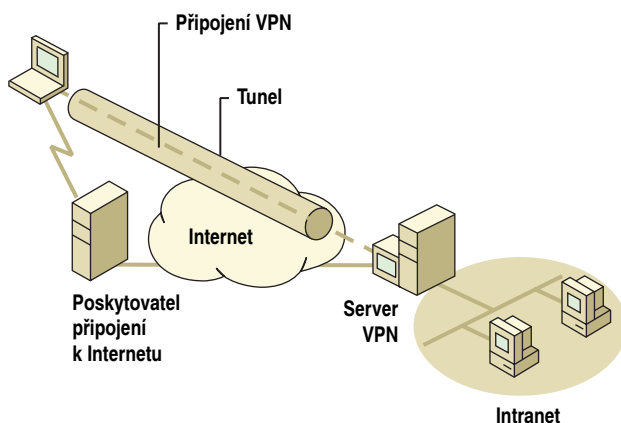
Virtuální privátní síť (VPN) zajišťují zabezpečené síťové služby přes veřejné síť podobně jako privátní síť, ale s nižšími náklady. Síť VPN dovolují personálu společnosti a dalším autorizovaným uživatelům připojovat se k síti společnosti ze vzdálených míst stejně bezpečně, jako ze síťového sídla společnosti. Proto lze přes VPN zabezpečeně nabízet všechny síťové služby společnosti. Pochopení, nastavení a podpora sítí VPN je složitější, než jak je tomu v případě nezabezpečených veřejných připojení, ale zajišťují plně zabezpečená připojení při použití levných internetových a podobných připojení.

Síť VPN lze používat ve spojení se službou Směrování a vzdálený přístup, není to však nutné. Síť VPN můžete mezi sídly vytvořit pomocí libovolného typu spojení a lze je také v zájmu zvýšení zabezpečení používat v rámci síťového sídla.

Virtuální privátní sítě obvykle fungují následujícím způsobem:

- Uživatel se telefonicky připojí k nějakému poskytovateli připojení k Internetu (ISP).
- Software klienta VPN přes Internet kontaktuje určený server VPN vlastněný vaší společností a iniciuje ověřování.
- Uživatel je ověřen a jsou zajištěny podrobnosti zabezpečení.
- Server VPN předá klientskému počítači novou adresu protokolu Transmission Control Protocol/Internet Protocol (TCP/IP) a klientský počítač je instruován tak, aby odesílal veškerý další síťový provoz s danou adresou přes server VPN.
- Všechny síťové pakety jsou pak během výměny plně zašifrovány takovým způsobem, že je dokáže dešifrovat jen klient VPN a server VPN.

Obrázek 17.4 ukazuje vztah mezi těmito počítači.



Obrázek 17.4 Ukázka konfigurace virtuální privátní sítě

Pomocí VPN lze také připojovat více počítačů na sídle k síti vaší společnosti nebo omezovat komunikaci s nějakou podsítí výhradně na oprávněný personál.

V systému Windows 2000 Server je software VPN součástí služby Směrování a vzdálený přístup (Routing and Remote Access), což je volitelná komponenta systému Windows 2000. Kniha *Microsoft Windows 2000 Server Internetworking* obsahuje obsáhlé informace o fungování sítí VPN systému Windows 2000 a jejich funkcích. Instalaci sítí VPN popisuje nápověda systému Windows 2000 Server.

Zavádění sítí VPN

Plánujete-li zavedení sítí VPN, musíte zvážit různé problémy, mezi něž patří:

- Jaký zabezpečený protokol se bude používat – protokol Point-to-Point Tunneling Protocol (PPTP) nebo protokol Layer Two Tunneling Protocol (L2TP).
- Zda se bude používat protokol IPSec (zvolíte-li protokol L2TP).
- Jaké certifikáty se budou používat při připojování pomocí L2TP/IPSec.
- Kam se server VPN umístí – před firewall, za něj, nebo vedle něj.

- Jak se bude používat nástroj Connection Manager (správce připojení) k předání přednastavených voleb uživatelům.
- Jak se budou sítě VPN používat jako součást vašich zásad vzdáleného přístupu.

PPTP versus L2TP

Protokol Point-to-Point Tunneling Protocol (PPTP) je síťový protokol TCP/IP, který zahrnuje protokoly IP, IPX a NetBIOS Enhanced User Interface (NetBEUI). Protokol PPTP umožňuje přenášet přes Internet (nebo podobné sítě) síťovou aktivitu, která neprobíhá v protokolu TCP/IP, neboli víceprotokolovou aktivitu. Sítě VPN založené na protokolu PPTP také zajišťují ověřování uživatelů, řízení přístupu a mají možnost pomocí telefonických profilů opatrně omezovat určité typy použití vzdáleného přístupu určitými uživateli. Protokol PPTP poskytuje vzdáleným klientům konfiguraci interní adresy, takže mohou být součástí interní sítě, jako by byli přímo připojeni. Protokol PPTP zajišťuje kompresi a volby standardního a silného šifrování RC4 (šifra symetrického toku) provozu přenášeného tunelem.

Protokol L2TP se protokolu PPTP velmi podobá, ale používá UDP a lze jej tedy používat také v sítích asynchronního režimu přenosu (ATM), Frame Relay a X.25. Je-li protokol L2TP aplikován na sítích IP, používá formát paketů UDP portu 1701 jak pro řídicí kanál tak i pro datový kanál. Protokol L2TP lze používat také ve spojení s protokolem IPsec a zajišťovat tak plně zabezpečené síťové připojení. Protokol IPsec nejprve pro provoz L2TP vyřídí bezpečnostní vyjednávání pomocí certifikátů ověření mezi klientem a serverem VPN. Protokol L2TP pak zajistí ověření pomocí uživatelského účtu a hesla nebo pomocí uživatelského certifikátu.

Zabezpečený protokol IP

Zabezpečený protokol IP (Internet Protocol Security – IPsec) je protokol sloužící k zabezpečení síťového provozu protokolu Internet Protocol (IP). Protokol IPsec zajišťuje úplné zabezpečení mezi dvěma počítači, takže žádná část připojení není nezabezpečená. Konfigurace protokolu IPsec se provádí pomocí zásad IPsec. Tyto zásady mohou obsahovat řadu různých pravidel zabezpečení, přičemž každé pravidlo pomocí filtrů, kterým jsou přiřazeny akce filtru a metody ověření, specifikuje určitý typ provozu. Zásady IPsec lze vytvářet a přiřazovat místně na počítači nebo ve službě Active Directory v rámci zásad skupiny (Group Policy).

Poznámka Protokol IPsec zajišťuje zabezpečení IP mezi koncovými body, nešifruje však všechny protokoly běžící přes IP. Protokol IPsec má zabudované výjimky pro určitý provoz, jako jsou vyjednávání Internet Key Exchange, ověřování Kerberos, vysílání IP a provoz vícesměrového vysílání IP. V případě potřeby lze další protokoly vymout tak, že se vytvoří pravidla IPsec s filtrem určujícím typ provozu a povolenou akci filtru.

Další informace o protokolu IPsec najdete v nápovědě systému Windows 2000 Server a v knize *Microsoft Windows 2000 Server Sítě TCP/IP*. Další informace o plánování zavedení vašeho certifikačního úřadu v infrastruktuře veřejných klíčů najdete v kapitole „Plánování infrastruktury veřejných klíčů“ v této knize.

Umístění serveru VPN

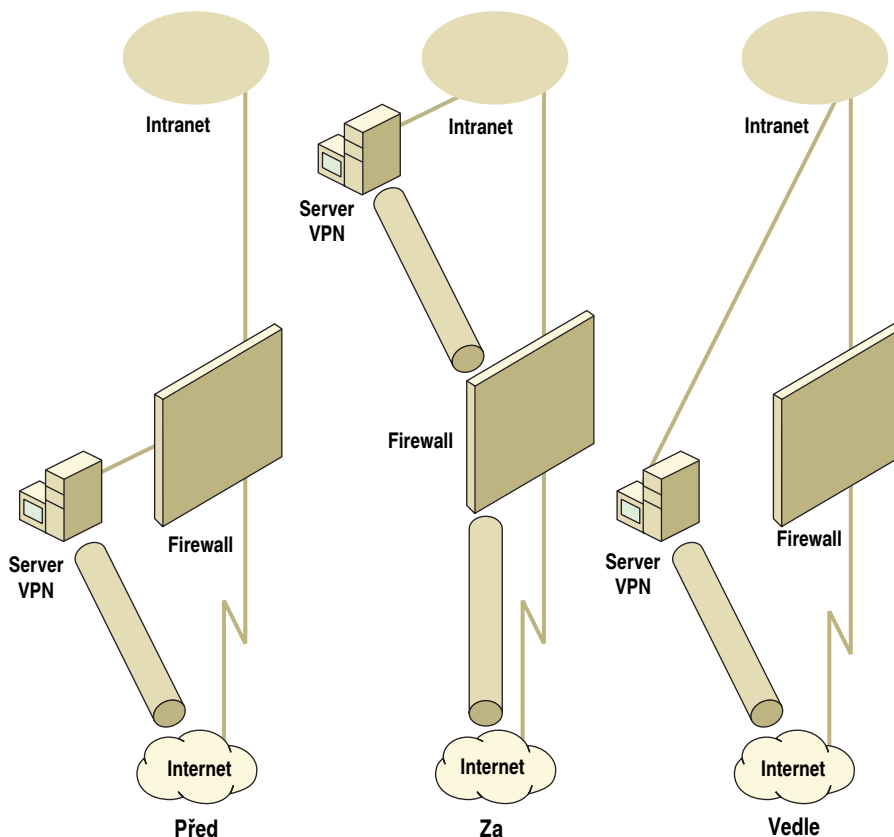
Sítě VPN lze používat ve spojení s firewalley. I když sítě VPN mohou vykonávat činnosti podobné činnostem firewallů, obě technologie nabízejí určité další specifické výho-

dy, a proto může být zapotřebí použít je obě současně. V takových situacích se zamyslete nad umístěním serveru VPN vzhledem k firewallu.

Fyzicky je možné instalovat obě technologie na stejný server. Tím se vytváří však jediný bod selhání v případě nedostupnosti serveru či narušení zabezpečení serveru. Menší počet serverů zase omezuje pravděpodobnost nedostupnosti serveru a také se snižují náklady na údržbu serverů. Mohou se také objevovat problémy s kapacitou. Svůj konkrétní návrh vytvořte na základě toho, jaký mají jednotlivé uvedené faktory vliv ve vaší situaci.

Důležitější sadou problémů je logický vztah serveru VPN k firewallu. Jak je patrné z obrázku 17.5, můžete mít server VPN logicky před firewallem, za ním, nebo vedle něj. Systém Windows 2000 dokáže poskytovat služby firewallu buď pomocí nástroje Proxy Server nebo pomocí směrování filtrem paketů. Další informace o těchto typech řešení najdete v kapitole „Směrování a vzdálený přístup“ v knize *Microsoft Windows 2000 Server Internetworking*.

Nachází-li se server VPN před firewallem, firewall poskytuje autorizovaným uživatelům VPN pouze svoje externí služby. Proto není zajištěn obecný přístup k Internetu nebo podobný přístup. Výjimkou je, když je na vzdáleném konci připojení VPN zajištěn přístup k Internetu



Obrázek 17.5 Ukázka logického umístění serveru VPN vzhledem k firewallu

Nachází-li se server VPN za firewallem, firewall poskytuje všechny své obvyklé služby, musí však být nakonfigurován tak, aby otevřel porty potřebné pro server VPN. Používáte-li síť VPN s protokoly L2TP a IPSec patří sem také porty potřebné pro protokol IPSec.

Když se server VPN nachází vedle firewallu, oba systémy poskytují své služby nezávisle. Taková konfigurace však vytváří dvě přístupové trasy do sítě společnosti, což zvyšuje potenciál narušení zabezpečení. Obvykle ani jedna služba nevytváří cestu kolem druhé služby, ale riziko je dvojnásobné už proto, že existují dvě cesty.

Výběr nejlepšího vztahu ve vašem případě závisí na tom, kterým problémům se zabezpečením nejlépe rozumíte. Budou-li servery vedle sebe, existují do vašeho intranetu dvě cesty a proto je bezpečnostní riziko dvojnásobné. Máte-li server VPN za firewallem, musíte otevřít více portů na firewallu. Je-li server VPN před firewallem, server VPN nemůže využít žádnou z výhod zabezpečení poskytovaných firewallem, veškerý jím zpracovávaný provoz má však z firewallu užitek.

Nástroj Connection Manager

Zajištění služeb VPN pro vaše uživatele vyžaduje určitou konfiguraci na všech klient-ských počítačích. Tato nastavení nemusí být právě jednoduchá, systém Windows 2000 však obsahuje nástroj Connection Manager (správce připojení), který instalační proces uživatelů zjednodušuje.

Connection Manager pracuje na počítačích se systémy Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows NT a Windows 2000. Servery se systémem Windows 2000 mají také sadu správy nazvanou *Connection Manager Administration Kit* (sada správy správce připojení), která vám umožňuje vytvořit pro uživatele upraveného správce připojení.

Další informace o připojeních, nástroji Connection Manager a sadě Connection Manager Administration Kit najdete v nápovědě systému Windows 2000 Server. Po vykonání instrukcí uvedených v nápovědě systému Windows 2000 Server a spuštění sady Connection Manager Administration Kit budete mít k dispozici program a dokumentaci, kterou můžete distribuovat uživatelům.

Zásady vzdáleného přístupu

Zásady vzdáleného přístupu vám umožňují určit, kteří lidé mohou používat službu Směrování a vzdálený přístup, a různé podmínky, jež se aplikují po jejich připojení. Zásady lze specifikovat na základě skupiny systému Windows 2000, do které uživatel patří, telefonního čísla, jaké používá, denní doby a dalších souvisejících informací. Zásady mohou určovat, že spojení má být přijato nebo odmítnuto, a na spojení lze také aplikovat profil. Takový profil specifikuje například, jak dlouho může připojení trvat, po jakou dobu může být nečinné, jaké typy komunikačních médií jsou povoleny, jaké adresy jsou povoleny, jaké metody ověřování jsou vyžadovány a zda je vyžadováno šifrování nebo VPN.

Zásady vzdáleného přístupu lze nastavit buď pro službu Směrování a vzdálený přístup (Routing and Remote Access) nebo pro službu Internet Authentication Service (IAS), což je popsáno dále v tomto oddílu. Další informace o zásadách vzdáleného přístupu včetně jejich vytvoření a možností jimi poskytovaných najdete v nápovědě systému Windows 2000 Server.

Opatrně zvažte aplikování různých zásad na různé skupiny či podmínky. Zásady se mohou překrývat a znemožnit tak připojení osobám, kterým jste to chtěli umožnit, nebo způsobit jiné problémy. Složitě kombinace zásad činí vznik takových problémů

pravděpodobnějším. Proto je nejlepší ve všech případech, kdy je to možné, minimalizovat počet zásad. Návodů systému Windows 2000 Server obsahuje doporučený postup řešení problémů se zásadami vzdáleného přístupu pro případ vzniku nějakých potíží.

Kapacita serveru VPN

Stejně jako u jiných serverů i servery VPN lze zahltit, mají-li zpracovávat nadměrnou aktivitu. Aby k tomu došlo, musíte používat opravdu mnoho spojení VPN; v případě velkých organizací to však může být reálný problém. V rámci svého pilotního programu můžete otestovat, jak asi velké zatížení budou vaši uživatelé pro dostupné servery VPN představovat. Můžete také vyzkoušet, jakou kapacitu dokáží vaše servery VPN zvládnout. Odhadněte počet uživatelů, kteří mohou server v jednom okamžiku používat, a pravděpodobně množství jimi odesílaných dat. Pak můžete odeslat stejné množství dat přes server VPN prostřednictvím malého počtu klientských počítačů přes místní síť (LAN) a vyzkoušet také velkoobjemové aktivity, jako je například kopírování velkého počtu souborů. Sledováním serveru VPN a jeho schopnosti reagovat pak určíte, zda vaše servery VPN budou na jim svěřenou roli dostačovat. Je-li to nezbytné, můžete zvětšit velikost svých serverů nebo přidat další servery VPN a jejich zatížení vyrovnávat pomocí služby Vyrovnávání zatížení sítě (Network Load Balancing) či technologií round robin systému DNS.

Služba Internet Authentication Service

Systém Windows 2000 Server obsahuje jako volitelnou součást službu Internet Authentication Service (IAS). Tato služba implementuje standardní bezpečný protokol síťového ověřování Remote Authentication Dial-In User Service (RADIUS), který umožňuje centralizaci autorizování účtů. Protokol RADIUS vám také dovoluje určit, jak dlouho může relace trvat a jakou adresu IP lze použít. Služba IAS může zároveň zaznamenávat podrobnosti o relaci, čímž je zajištěna zodpovědnost uživatelů, a poskytuje i možnosti protokolování.

Službu IAS lze také použít, chcete-li zajistit zprostředkování funkcí vzdáleného přístupu jinou společností, ale přitom mít stále možnost řídit ověřování lidí, kteří se snaží tyto funkce využít. V takovém případě může zprostředkující společnost přesměrovat požadavky na ověření ze svých serverů služby Směrování a vzdálený přístup na vaše servery IAS. Služba IAS ověřuje účty na základě nativních domén systému Windows 2000 a domén systému Windows NT 4.0.

Server IAS musíte umístit za firewall, přičemž na firewallu musí být otevřeny porty pro ověřování RADIUS a příslušné pakety protokolu User Datagram Protocol (UDP).

Další informace o instalování a použití služby IAS včetně provozních doporučení najdete v nápovědě systému Windows 2000 Server. Návodů systému Windows 2000 Server také obsahuje doporučené postupy dalších voleb zabezpečení a informace o škálování služby IAS v rozsáhlých prostředích a o efektivním používání přihlašování ke službě IAS.

Zavádění strategií pro uživatele

Někteří uživatelé budou vyžadovat přístup k zabezpečeným aplikacím společnosti i v době, kdy jsou mimo svou kancelář. Určité z takových aplikací jsou relativně jednoduché, například správa času, registrace podpůrných dávek společnosti a podobné programy. Jiné aplikace mohou být složité, například účetní systémy a obchodní apli-

kace. Musíte zajistit zabezpečení těchto aplikací tak, aby k jejich datům mohli přistupovat pouze oprávnění uživatelé a aby zároveň mohli zadávat jen autorizované změny. Tím je také zajištěna zodpovědnost uživatelů, protože používání aplikací jednotlivými uživateli lze sledovat.

Systém Windows 2000 obsahuje různé technologie zabezpečení, které poskytují vývojářům aplikací možnosti využívání síťového zabezpečení. Volba těchto technologií závisí na:

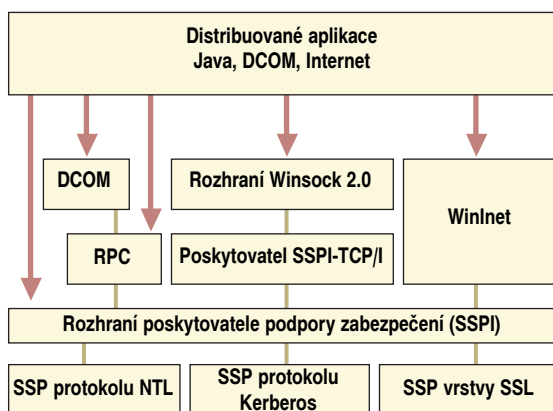
- bezpečnostních požadavcích aplikace,
- otázkách integrace,
- úrovni, do jaké vývojář dané technologii rozumí,
- dopadu na výkon sítě a aplikace,
- složitosti správy.

Mezi technologie zabezpečení sítě z hlediska aplikací patří:

- Rozhraní Security Support Provider Interface (rozhraní poskytovatele podpory zabezpečení – SSPI), což je rozhraní API zabezpečení obecného použití, které prostřednictvím standardního programovacího rozhraní zajišťuje přístup k mnoha bezpečnostním službám.
- Zabezpečení systému Windows protokolem NTLM, které je také známo jako zabezpečení na úrovni domény systému Windows NT.
- Ověřovací protokol Kerberos v5. Další informace najdete v kapitole „Plánování distribuovaného zabezpečení“ v této knize.
- Vrstva Secure Sockets Layer (SSL). Vrstva SSL byla vylepšena a standardizována organizací Internet Engineering Task Force (IETF) jako Transport Layer Security (TLS).
- Certifikáty, jak bylo popsáno dříve v této kapitole.

Tyto technologie zabezpečení sítě a síťové technologie, které k nim mohou přistupovat, jsou ve vzájemném vztahu naznačeném na obrázku 17.6. Označení SSP v obrázku znamená poskytovatel zabezpečení SSPI, což je rozhraní mezi funkcí zabezpečení a rozhraním SSPI. Remote Procedure Call (vzdálené volání procedur – RPC), Microsoft Distributed Component Object Model (distribuovaný komponentový objektový model – DCOM) a Windows Sockets (Winsock) jsou metody komunikace mezi procesy. WinInet (Windows Internet API – internetové rozhraní API systému Windows) je programovací rozhraní, které se používá k inicializaci a správě webových rozhraní.

Technologie zabezpečení sítě se nacházejí ve spodní polovině diagramu se začátkem na úrovni SSPI. Síťové technologie jsou v horní polovině diagramu a jsou umístěny pod obdélníkem aplikace, která je používá.



Obrázek 17.6 Vztah technologií zabezpečení ukázkové síťové aplikace

Společně se svými vývojáři aplikací společnosti a prodejci rozhodněte, které technologie zabezpečení sítě pro aplikace musíte zavést. Tyto technologie nevyžadují žádné další plánování infrastruktury; musíte však určit, jak mohou vývojáři využívat výhody mocnějšího zabezpečení sítě, které poskytuje systém Windows 2000. Při zavádění služby Směrování a vzdálený přístup a propojení VPN mohou například dosáhnout zabezpečeného ověřování uživatelů pomocí karet Smart Card.

Zavádění strategií pro partnery

Většina organizací pracuje ve složitém světě vztahů mezi zákazníky, prodejci, dceřinými společnostmi, dodavateli, konzultanty, regulátory a dalšími spolupracujícími lidmi. Mnoho z těchto partnerů, jak se často označují, může přímým přístupem k datům a aplikacím vaší společnosti získat velké výhody. Zajištění takového přístupu však může vytvářet značné riziko zpřístupnění neveřejných nebo citlivých informací nesprávným lidem. Je tu také riziko řízení infrastruktury počítačů těmito lidmi se zlým úmyslem. Právě pomocí efektivního zavedení strategií zabezpečení sítě je zapotřebí zajistit partnerům jen ten nejpotřebnější přístup.

Kolekce síťových a bezpečnostních technologií, které umožňují vašim partnerům přístup k síti vaší společnosti, se často nazývá *extranet*. Extranety nejednou využívají stejné technologie, které jsme již dříve popsali v rámci popisu zajištění přístupu personálu a uživatelů, jako jsou síť VPN a služba Směrování a vzdálený přístup. Zvláštní charakteristikou partnerů je však skutečnost, že mohou vždy komunikovat s vaší společností z určitého místa a přes předem definované spojení. Proto je možné nakonfigurovat proxy-server tak, aby umožnil extranetové připojení pouze z dané síťové adresy.

Při zvažování, kteří partneři budou používat váš extranet, nezapomeňte určit, s jakými obchodními jednotkami budou komunikovat. Partneři obvykle spadají do jasně definovaných kategorií, které komunikují převážně se samostatnými částmi vaší společnosti. Někteří partneři tak mohou spolupracovat s oddělením příjmu a odesílání, jiní s technickým oddělením a ostatní zase přímo s oddělením prodeje.

Zavádění strategií zabezpečení sítě pro partnery se od zavádění pro uživatele a personál liší zejména proto, že extranety se mohou pro vaše partnery stát absolutně nepo-

stradatelnými. Zaměstnanci společnosti mají obvykle možnost přijít do své kanceláře, když potřebují přistoupit k nějakým prostředkům společnosti. Partneri však mohou používat jenom extranet (nebo se uchýlit zpět k tradičním prostředkům). Zaměstnanci také většinou pracují jen s relativně malými objemy dat, zatímco partneři často vytvářejí značné objemy dat, které musí vaše počítače zpracovat a přenést vaší sítí.

Partnerské a obchodní jednotky jsou také velmi závislé na zajištění dočasnosti extranetové služby. Obchodní funkce jsou často závislé na vyměňovaných datech a zdržení mohou být velmi drahá. Extranet musí být spolehlivý a dojde-li k nějakým problémům, partnerské a obchodní jednotky musí mít možnost kontaktovat někoho, kdo dokáže tyto problémy rychle vyřešit.

Na obchodní či výrobní jednotky poskytující služby přes extranet se vztahují další problémy a omezení. Mohou mít také systémy a personál, jejichž historie je v porovnání s jinými částmi vaší společnosti zvláštní. Proto není neobvyklé, že některé obchodní či výrobní jednotky mají takové požadavky na extranet, které se od požadavků jiných obchodních jednotek výrazně odlišují.

Z těchto důvodů musí strategie zavádění zabezpečení sítě pro partnery klást důraz na spolehlivost, škálovatelnost, flexibilitu a schopnost podpory. Kritickým je zejména personál společně s pilotními programy, vývojem zásad a postupů a komunikací. Technologie zabezpečení sítě, které jsou součástí systému Windows 2000, poskytují základ zabezpečení extranetu, v zásadách a postupech však budou spočívat důležité rozdíly mezi strategií zabezpečení extranetu a strategiemi zabezpečení interní sítě.

Seznam úkolů plánování určení strategií zabezpečení sítě

Tabulka 17.1 uvádí souhrn úkolů, které musíte vykonat při plánování zabezpečení sítě.

Tabulka 17.1 Seznam úkolů plánování určení zabezpečení sítě

Úkol	Umístění v kapitole
Naplánujte zavedení.	Plánování zabezpečení sítě
Vytvořte hranice zabezpečení.	Vytváření hranic zabezpečení
Připravte se na technologie zabezpečení sítě systému Windows 2000.	Zavádění technologií zabezpečení sítě
Zavedte strategie pro všechny.	Příprava na technologie zabezpečení sítě systému Windows 2000
Zavedte strategie pro personál společnosti.	Příprava na technologie zabezpečení sítě systému Windows 2000
Zavedte strategie pro uživatele aplikací společnosti.	Zavádění strategií pro uživatele
Zavedte strategie pro partnery.	Zavádění strategií pro partnery

KAPITOLA 18

Zajištění dostupnosti aplikací a služeb

Nemůžete-li si dovolit ztráty produktivity způsobené přerušením důležité aplikace či služby nebo představují-li aplikace či služby pro vaši organizaci nějaké právní závazky, pak je pro vás tato kapitola naprosto zásadní.

Tato kapitola pomůže zejména správcům systému rozhodnout se, zda systém vyžaduje klastry, a pokud ano, jaká technologie klastrů nejlépe odpovídá aplikacím a službám běžícím ve vaší organizaci. Postupy v této kapitole vám pomohou vytvořit plán, který zajistí vysokou dostupnost důležitých a nepostradatelných aplikací a služeb pro uživatele za všech podmínek.

V této kapitole

Zajištění vysoké dostupnosti aplikací a služeb 530

Přehled clusteringu systému Windows 532

Určení strategií dostupnosti 532

Plánování služby Network Load Balancing 535

Plánování služby Cluster Service 545

Optimalizování klastrů 564

Plánování disků odolných proti chybám 564

Testování kapacity serveru 565

Plánování strategie zálohování a obnovení klastru 566

Seznam úkolů plánování klastrů systému Windows 2000 567

Další zdroje 568

Cíle kapitoly

Kapitola vám pomůže vyvinout následující dokument plánování:

- Plánovací list zavádění clusteringu

Související informace v sadě Resource Kit

- Další informace o clusteringu systému Microsoft Windows najdete v kapitole „Clustering systému Windows“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.
- Další informace o vytváření plánů testování najdete v kapitole „Vytvoření testovací laboratoře systému Windows 2000“ v této knize.

Zajištění vysoké dostupnosti aplikací a služeb

Selhání serveru, ať už jde o souborový, tiskový, webový nebo aplikační server, je prakticky ve všech organizacích velmi nákladné. Měření nákladů nedostupnosti serveru, aplikace nebo služby v organizaci však může být obtížné. Mezi potenciální ztráty patří:

- ztráta prodeje,
- ztráta dobrého jména u zákazníků,
- ztráta produktivity a důvěry zaměstnanců,
- zvýšení nákladů, způsobené časem potřebným na opravu,
- zmeškání smluvních závazků a možná právní odpovědnost,
- ztráta výrobků podléhajících zkáze,
- ztráta konkurenceschopnosti.

Ztráty způsobené vaší organizací díky přerušení funkce důležité aplikace nebo služby mohou být velmi vysoké. Jestliže nezajistíte vysokou dostupnost důležitých aplikací a služeb uživatelům, riskujete velmi mnoho.

Tato kapitola popisuje podrobnosti plánování zavedení podpory klastrů systému Windows. Clustering je funkce systému Windows 2000 Advanced Server, která přináší sítím a správcům systémů čtyři hlavní výhody:

- vysokou dostupnost aplikací a služeb,
- škálovatelnost určitých aplikací a služeb (při použití vyrovnavání zatížení),
- centralizovanou správu;
- postupnou inovaci (proces inovace jednotlivých uzlů klastru, zatímco ostatní uzly pokračují v zajišťování služby).

Přehled systému Windows 2000 Advanced Server

Do rodiny systémů Windows 2000 Server nyní patří systémy Windows 2000 Server a Windows 2000 Advanced Server. Windows 2000 Server poskytuje základní funkce odpovídající potřebám malých a středních organizací, které mají více pracovních skupin a poboček a které potřebují určité služby, jako je přístup k souborům, tisk, komunikace, infrastruktura a web. Systém Windows 2000 Advanced Server je vytvořen pro velmi důležité systémy (mission-critical), jako jsou velké datové sklady, online zpracování transakcí (OLTP), posílání zpráv, elektronická komerce či služby hostování webového obsahu středních a velkých organizací a pro potřeby poskytovatelů připojení k Internetu (ISP).

Systém Windows 2000 Advanced Server se vyvinul ze systému Microsoft Windows NT Server 4.0 Enterprise Edition. Zajišťuje obsáhlou clusteringovou infrastrukturu vysoké dostupnosti a škálovatelnosti aplikací a služeb, včetně podpory hlavní paměti do velikosti 8 gigabajtů (GB) na systémech Intel Page Address Extension (PAE). Advanced Server je navržen pro náročné podnikové aplikace a podporuje nové systémy s až 8cestným symetrickým multiprocessingem (SMP). SMP umožňuje libovolnému z více procesorů počítače provádět libovolný úkol operačního systému nebo aplikace současně s ostatními procesory v systému. Windows Advanced Server je vhodný pro náročné databázové činnosti a poskytuje serverový clustering a vyrovnavání zatížení. Dosahuje tak vynikající dostupnosti systému a aplikací.

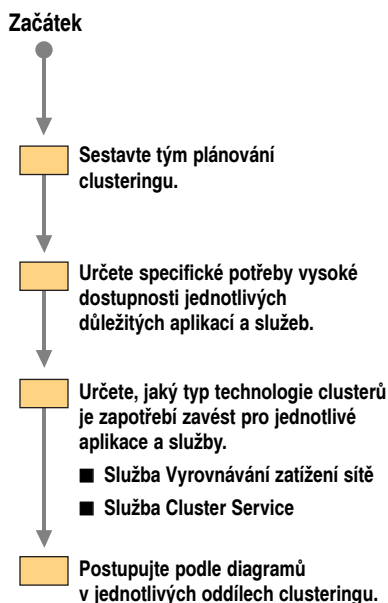
Systém Windows 2000 Advanced Server zahrnuje všechny funkce systému Windows 2000 Server a přidává k nim vysokou dostupnost a škálovatelnost potřebnou v podnikových řešeních a řešeních větších oddělení. Mezi klíčové funkce systému Advanced Server patří:

- vyrovnávání zatížení sítě (Network Load Balancing) pro protokol TCP/IP;
- vylepšené dvouuzlové serverové klastry vycházející ze služby Microsoft Windows Cluster Server (MSCS) uvedené již dříve v systému Windows NT Server 4.0 Enterprise Edition;
- až 8 GB hlavní paměti na systémech Intel PAE;
- až 8cestný SMP.

Poznámka Nejste-li si jisti, zda máte počítačový systém Intel PAE, kontaktujte svého prodejce hardwaru.

Proces zajištění vysoké dostupnosti aplikací a služeb

Při plánování zavedení clusteringu systému Windows je důležité zvážit řešení, která vám pomohou vyhnout se selháním serveru, aplikace nebo služby ve vaší organizaci. Během plánování zajištění vysoké dostupnosti aplikací a služeb postupujte podle procesu znázorněného ve vývojovém diagramu na obrázku 18.1.



Obrázek 18.1 Plánování dostupnosti aplikací a služeb

Než se pustíte do plánování, musíte dokonale porozumět klíčovým komponentám clusteringu systému Windows, které zajistí vysokou dostupnost důležitých aplikací a služeb koncovým uživatelům ve vaší organizaci.

Přehled clusteringu systému Windows

Klaster je skupina nezávislých počítačů, které spolupracují při spouštění společné sady aplikací či služeb a které představují pro klienta a aplikaci jediný systém. Počítače v klasteru jsou fyzicky propojeny kabely a programově propojeny softwarem klasteru. Tato spojení umožňují počítačům využívat funkce řešení problémů, jako je vyvznávání zatížení a překlopení, které nejsou při práci s jediným počítačem k dispozici.

Vyrovznávání zatížení (load balancing) rozděljuje zatížení serveru na všechny nakonfigurované servery a zabráňuje tak přetížení jednoho ze serverů. To vám následně umožňuje podle potřeb postupně zvyšovat dostupnou kapacitu. *Překlopení* (failover) zajišťuje neustálou podporu uživatelů, protože automaticky přesunuje prostředky ze selhávajícího nebo nepřipojeného serveru klasteru na fungující server. Uživatelé klasteru tak mají stálý přístup k potřebným prostředkům. Clustering systému Windows v současné době zajišťuje dvě následující technologie:

Služba Vyrovznávání zatížení sítě (Network Load Balancing) Vyrovznávání zatížení sítě zaručuje škálovatelnost a vysokou dostupnost aplikací a služeb vycházejících z protokolu TCP/IP tím, že kombinuje až 32 serverů se spuštěným systémem Windows 2000 Advanced Server do jediného klasteru vyrovznávajícího zatížení. Nejčastějším použitím služby Vyrovznávání zatížení sítě je rozdělování příchozích požadavků na webové služby do klasteru internetových serverových aplikací (jako jsou například aplikace služby Internet Information Services).

Služba Cluster Service Při použití systému Advanced Server vám klastrová služba dovoluje zkombinovat dva servery tak, aby společně fungovaly jako serverový klaster a zajišťovaly trvalou dostupnost důležitých aplikací a prostředků uživatelům. Serverové klastery umožňují uživatelům a správcům přistupovat k určitým prostředkům na serverech neboli *uzlech* (node) jako na jediný systém a nikoli jako na samostatné počítače.

Při plánování a zavádění vysoké dostupnosti aplikací a služeb je důležité definovat doporučené postupy v organizaci. Společnost Microsoft vytvořila řadu průvodců doporučenými postupy při zajišťování vysoké dostupnosti. Další informace o těchto průvodcích najdete v odkazu Microsoft TechNet High Availability stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Určení strategií dostupnosti

Jakmile porozumíte schopnostem clusteringu systému Windows, můžete začít s fází plánování zavedení klasterů, které zajistí vysokou dostupnost důležitých aplikací a služeb uživatelům ve vaší společnosti.

Sestavení týmu plánování clusteringu

Při určování požadavků na clustering je týmová práce velmi důležitá. Plánování strategie clusteringu musí být projektem, kterého se budou společně účastnit správci systému počítačové sítě a správci následujících aplikací a služeb:

- programu Microsoft SQL Server nebo jiné databáze,
- programu Microsoft Exchange Server nebo jiného nástroje skupinové spolupráce,
- služby Microsoft Internet Information Services (IIS) nebo jiné webové služby,
- terminálových služeb systému Windows 2000,
- služby Windows Internet Name Service (WINS),

- protokolu Dynamic Host Configuration Protocol (DHCP),
- interně vyvinutých obchodních aplikací,
- aplikací jiných výrobců,
- sdílení souborů a tisku.

Ve většině organizací musí být právě uvedené aplikace a služby uživatelům vysoce dostupné.

Jádro týmu plánování clusteringu musí určit specifické potřeby vysoké dostupnosti jednotlivých uvedených důležitých aplikací a služeb. Tento tým bude mít dostatek informací o použití těchto aplikací a služeb a použití sítě, aby se dokázal vyhnout potenciálním nákladným omylům.

Jakmile máte určenu strategii clusteringu, naplánujte si jednání s jádrem týmu plánování clusteringu, abyste mohli rozhodnout o personálních požadavcích konfigurace klastru ve vaší organizaci. Prostředky a aplikace běžící na klastru mohou být spravovány jiným způsobem než stejné prostředky na samostatném serveru. Musíte určit rozsah těchto rozdílů a potřebným způsobem proškolit personál. Také se ujistěte, že je váš personál seznámen s požadavky vysoké dostupnosti a že rozumí tomu, jak jejich akce mohou omezit či snížit dostupnost systému. Například správce, který přidá do skupiny obsahující stovky prostředků další prostředek, může při nesprávné konfiguraci nového prostředku způsobit selhání celé skupiny (společně se všemi prostředky, které obsahuje).

Zjištění potřeb vysoké dostupnosti aplikací a služeb

Chcete-li zjistit konkrétní potřeby vysoké dostupnosti důležitých aplikací a služeb ve vaší společnosti, určete položky následujícího výčtu:

- Základní charakteristiky aplikace nebo služby, jako jsou:
 - používaný software,
 - speciální hardwarové požadavky (další informace najdete v oddílu „Určení hardwarové kompatibility pokročilých funkcí“ dále v této kapitole),
 - množství dat,
 - počet uživatelů,
 - dobu provozu.
- Očekávané změny v požadavcích na velikost a výkon, jako jsou:
 - sezónní nebo jiné plánované špičky zatížení,
 - očekávaný růst počtu uživatelů,
 - očekávaný růst objemu dat.
- Hardwarové požadavky při počátečním zavedení, během doby špičkových zatížení a v rámci plánovacího horizontu projektu. Odhad uskutěčňte na základě charakteristik aplikací a služeb a předpokládaných změn.
- Plány zálohování a obnovení po poškození aplikací, služeb a operačního systému.
- Maximální toleranci výpadků (tedy maximální dobu, po kterou může systém nebo uživatelé tolerovat nedostupnost nějaké aplikace nebo služby). To je velmi důležité, protože eliminování všech možných výpadků může být drahé. V případě mnoha aplikací a služeb mohou být občasné krátké výpadky přijatelnější než značné investice do vysoké dostupnosti.

- Vliv doby výpadku. Kvalitativně odhadněte, jaký bude mít doba výpadku aplikace nebo služby vliv na vaši organizaci. Příklady zahrnují ztrátu prodeje, ztrátu produktivity a snížení spokojenosti zákazníků.
- Měřitelné náklady na dobu výpadku. Kvantitativně odhadněte náklady na výpadek jednotlivých aplikací nebo služeb překračující určenou maximální dobu výpadku, kterou může vaše společnost tolerovat.
- Určete všechny potenciální jediné body selhání (single point of failure) v plánované konfiguraci.
- Určete požadavky na personál.
- Aktuální dostupnost. Nemáte-li k dispozici údaje o dostupnosti, ihned začněte se sběrem potřebných dat. V systému Windows NT 4.0 SP4 lze jednoduše vypočítat dobu dostupnosti pomocí nástroje Uptime.exe sady *Microsoft Windows NT 4.0 Server Resource Kit*. Nástroj Uptime.exe používá k výpočtu potřebných čísel položky uložené v protokolu událostí. Aby to bylo možné, musíte povolit protokolování událostí. Nástroj Uptime.exe také nabízí sada *Microsoft Windows 2000 Server Resource Kit*.

Jediný bod selhání je libovolná komponenta ve vašem prostředí, která v případě svého selhání zablokuje data nebo aplikace.

Tabulka 18.1 uvádí obvyklé body selhání v serverovém prostředí a popisuje, zda je možné chránit takový bod selhání řešením clusteringu společnosti Microsoft nebo řešením jiné nezávislé společnosti.

Tabulka 18.1 Obvyklé body selhání

Bod selhání	Řešení clusteringu	Jiná řešení
Síťový rozbočovač (hub)	Nelze	Redundantní síť
Síťový směrovač (router)	Nelze	OSPF
Výpadek napájení	Nelze	Zdroj nepřerušitelného napájení (UPS) <ul style="list-style-type: none"> ■ Generátor ■ Připojení k více napájecím sítím
Připojení serveru	Překlopení	Nelze
Disk	Překlopení	Hardwarové nebo softwarové pole RAID, které zajistí zachování specifických dat na určitém počítači a zajistí nepřerušenu obsluhu
Další hardware serveru, jako je procesor nebo paměť	Překlopení	Náhradní komponenty, jako jsou základní desky a řadiče rozhraní SCSI (všechny náhradní komponenty včetně síťových komponent a komponent SCSI musí přesně odpovídat původním součástem).
Software serveru, jako je operační systém nebo specifické aplikace	Překlopení	Nelze
Propojení rozsáhlé sítě (WAN), jako jsou směrovače a vyhrazené linky	Nelze	Redundantní linky zajišťující další možnost přístupu ke vzdáleným připojením
Telefonická připojení	Nelze	Více modemů a služba Směrování a vzdálený přístup (RRAS)

Určení hardwarové kompatibility pokročilých funkcí

Přesvědčete se, že počítačové systémy a adaptéry, které máte v současné době nainstalované nebo plánujete jejich koupi, jsou uvedeny v seznamu Hardware Compatibility List (HCL) společnosti Microsoft. Uvedení příslušného hardwaru v tomto seznamu a tedy jeho kompatibilitu zjistíte v odkazu Microsoft Windows Hardware Compatibility List stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Plánujete-li zavádět počítačové systémy s pokročilými schopnostmi, jako je například clustering nebo podpora velkého množství paměti, musíte splnit ještě další podmínky.

Máte-li například počítače se systémem Advanced Server obsahující více než 4 GB paměti RAM, musíte upravit přepínač PAE souboru Boot.ini a povolit používání paměti v režimu PAE. Tuto změnu lze zadat, jakmile se ujistíte o podpoře všech komponent. Nejsou-li některé komponenty podporovány, musíte jejich podporu nejprve zajistit, protože jenom tak se vyhnete možným pozdějším problémům.

Pokud je již systém zapojen do výrobního prostředí a vy do něj chcete přidat nové adaptéry nebo ovladače, rozhodně vám doporučujeme před jakýmkoli změnami systém kompletně zálohovat.

Poznámka Změny v registru a určité úpravy souboru Boot.ini, které způsobily nesprávnou nebo nestabilní funkci systému počítače, můžete obejít tak, že restartujete počítač a použijete klávesu F8, jež umožňuje přeskočit mnoho přepínačů a ovladačů. To vám umožňuje upravit soubor Boot.ini nebo jiné oblasti podle potřeby o obnovit tak správnou funkci počítače.

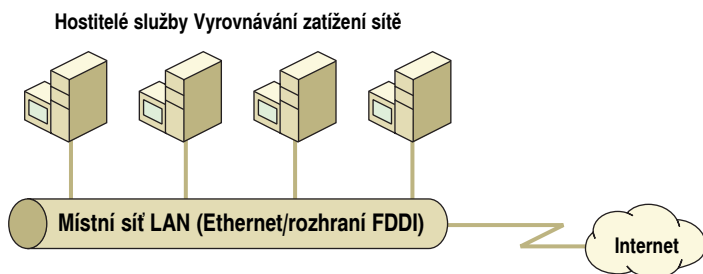
Určení požadavků clusteringu

Jakmile máte určené konkrétní potřeby vysoké dostupnosti důležitých aplikací a služeb, identifikovali jste potenciální jediné body selhání a zaručili jste kompatibilitu svého hardwaru se systémem Windows 2000, musíte určit, která klastrová technologie bude nejlépe odpovídat potřebám vaší organizace. Před naplánováním klastru se seznámte s požadavky na určení příslušného typu klastru.

Plánování vyrovnávání zatížení sítě

Služba Vyrovnávání zatížení sítě (Network Load Balancing) vytváří klastr skupiny počítačů, na kterých jsou spuštěny serverové programy, používající síťový protokol TCP/IP. Služba Vyrovnávání zatížení sítě zlepšuje dostupnost a škálovatelnost webových serverů, serverů FTP, serverů multimediálních datových proudů, serverů virtuálních privátních sítí (VPN) a dalších důležitých programů. Vyrovnávání zatížení sítě poskytuje tato vylepšení prostřednictvím klastru dvou nebo více spolupracujících hostitelských počítačů (serverů, které jsou členy klastru).

Jediný počítač se systémem Windows 2000 Advanced Server dokáže zajistit jen omezenou úroveň spolehlivosti serveru a škálovatelného výkonu. Po zkombinování prostředků dvou nebo více počítačů se systémem Windows 2000 Advanced Server do jediného klastru však dokáže služba Vyrovnávání zatížení sítě zajistit dostupnost, kterou webové servery a další důležité programy ke své nejlepší výkonnosti potřebují. Obrázek 18.2 ukazuje klastr služby Vyrovnávání zatížení sítě obsahující čtyři hostitele.



Obrázek 18.2 Čtyři hostitelé v klastru služby Vyrovnávání zatížení sítě

Na každém hostiteli běží samostatné kopie požadovaných serverových programů, jako je webový server, FTP, Telnet a zpracování zpráv. V případě určitých programů, například u webového serveru, běží kopie programu na všech hostitelích v klastru a služba Vyrovnávání zatížení sítě (Network Load Balancing) rozděljuje zatížení mezi servery. U jiných služeb, například u zpracování zpráv, zpracovává zatížení jen jedna kopie dané služby v klastru. Místo vyrovnávání zatížení takových služeb umožňuje služba Vyrovnávání zatížení sítě síťovému provozu tok k jednomu z hostitelů a pouze v případě selhání serveru provoz přesune na jiného hostitele. Služba Vyrovnávání zatížení sítě umožňuje, aby byly všechny počítače v klastru adresovány stejnou sadou adres internetového protokolu (IP) klastru, a přitom zároveň udržuje i jejich existující vyhrazené adresy IP. Služba Vyrovnávání zatížení sítě rozděljuje mezi hostitele příchozí požadavky klientů ve formě provozu TCP/IP včetně připojení TCP a dat protokolu UDP.

Aby bylo možné škálovat výkon serverů, služba Vyrovnávání zatížení sítě rozděljuje příchozí připojení TCP/IP mezi všechny hostitele v klastru. Podle potřeby lze nakonfigurovat velikost zatížení jednotlivých hostitelů. Je také možné do klastru dynamicky přidávat hostitele – pak je možné zpracovávat zvýšené zatížení. Služba Vyrovnávání zatížení sítě může navíc přeměrovat veškerý provoz protokolů TCP/UDP (který není nakonfigurován na vyrovnávání zatížení) na jediného určeného hostitele označovaného za „výchozího hostitele“. To je velmi výhodné, protože máte možnost provozovat všechny služby, které nejsou explicitně nastaveny na vyrovnávání zatížení, na jediném hostiteli. Služba Vyrovnávání zatížení sítě spravuje provoz TCP/IP tak, aby udržovala vysokou dostupnost serverových programů.

Dojde-li na nějakém hostiteli k selhání nebo odpojení, služba Vyrovnávání zatížení sítě automaticky překonfiguruje klaster a začne směřovat požadavky klientů na zbývající počítače. V případě programů s vyrovnáváním zatížení se zátěž automaticky přerozdělí mezi počítače, které ještě fungují. Provoz programů spuštěných na jediném serveru se přeměruje na zadaného hostitele. Připojení k serveru, který selhal nebo přešel do režimu offline, jsou ztracena. Po dokončení potřebné údržby se odpojený počítač může znovu transparentně připojit ke klastru a převzít svůj díl zátěže.

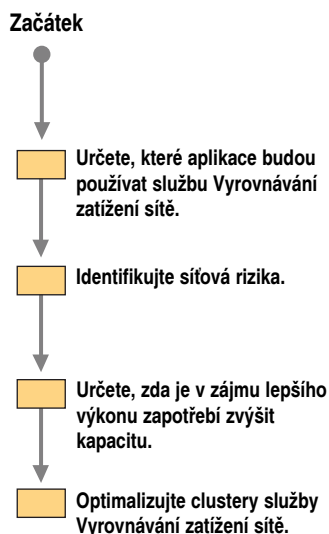
Služba Vyrovnávání zatížení sítě nedetekuje selhání aplikací. Je spíše navržena tak, aby mohla být řízena programy sledování aplikací, které kontrolují a zajišťují správnou funkci svých přiřazených aplikací. Zjistí-li například nástroj sledování nějaké aplikace skutečnost, že daná služba selhala, může instruovat službu Vyrovnávání zatížení sítě v tom smyslu, aby až do doby vyřešení problému odstranila dotčeného hostitele z klas-

tru. Navíc služba Vyrovnávání zatížení sítě detekuje řádné i neplánované vypnutí hostitele a selhání síťového adaptéru.

Jestliže hostujete nějakou službu TCP/IP (například webový server), jejíž výkon musí být natolik škálovatelný, aby dokázala plnit vzrůstající požadavky klientů, a která musí být stále dostupná, je jasné, že vaše organizace vyžaduje zavedení služby Vyrovnávání zatížení sítě. Například internetová elektronická komerce zaznamenáva prudký nárůst požadavků a výpadky na takových sídlech jsou pro zákazníky nepřijatelné. Tradiční prostředky škálování těchto služeb, jako je například použití techniky round robin služby DNS, nemohou samy o sobě zajistit tak vysokou dostupnost, jakou poskytuje služba Vyrovnávání zatížení sítě. Technika round robin systému DNS je řešení umožňující jen omezenou formu vyrovnávání zatížení TCP/IP na webových serverech.

Proces plánování klastrů služby Vyrovnávání zatížení sítě

Tento oddíl uvádí základní instrukce, kterých byste se měli držet při plánování zavádění klastrů služby Vyrovnávání zatížení sítě ve vaší organizaci. Při plánování klastrů služby Vyrovnávání zatížení sítě postupujte podle vývojového diagramu procesu plánování na obrázku 18.3.



Obrázek 18.3 Proces plánování klastrů vyrovnávání zatížení sítě

Určení aplikací, které budou používat vyrovnávání zatížení sítě

Se službou Vyrovnávání zatížení sítě dokáže spolupracovat mnoho aplikací. Tento oddíl nabízí základní postupy jak určit, které aplikace se k tomuto účelu hodí.

V zásadě lze říci, že služba Vyrovnávání zatížení sítě dokáže škálovat všechny aplikace a služby, které používají jako svůj síťový protokol TCP/IP a jsou přiřazeny určitému portu TCP nebo UDP.

Služba Vyrovnávání zatížení sítě (Network Load Balancing – NLB) používá „pravidla portů“ (port rules) popisující, jaký provoz se má vyrovnávat a jaký provoz se má игно-

rovat. Ve výchozím stavu nakonfiguruje služba Vyrovnávání zatížení sítě všechny porty na vyrovnávání zatížení. Máte však možnost změnit konfiguraci jednotlivých portů určující, jak se zatížení přichozího provozu vyrovnává. Chcete-li změnit výchozí chování, vytvořte pravidla portů zahrnující určité rozsahy portů.

Některými příklady služeb a jim přiřazených portů jsou:

- HTTP přes TCP/IP: Webové servery, například Microsoft Internet Information Server (IIS): Port 80.
- HTTPS přes TCP/IP: Protokol HTTP přes vrstvu Secure Sockets Layer (SSL) šifrování webového provozu: Port 443.
- FTP přes TCP/IP: Protokol FTP: Port 21, port 20 a porty 1024–65535.
- TFTP přes TCP/IP: Servery protokolu Trivial File Transfer Protocol (TFTP), které jsou využívány aplikacemi, jako je například Bootstrap Protocol (BOOTP): port 69.
- SMTP přes TCP/IP: Protokol Simple Mail Transport Protocol (SMTP), který používá ji poštovní aplikace jako například Microsoft Exchange: Port 25.
- Microsoft Terminal Services: Port 3389.

Aby bylo možné úspěšně vyrovnávat zatížení nějaké aplikace či služby, musí být daná aplikace či služba vytvořena tak, aby umožňovala současný běh více instancí (více kopií programu), jedné na každém hostiteli v klastru. Aplikace například nesmí aktualizovat nějaký soubor, který bude následně synchronizován s aktualizacemi skutečnými jinými instancemi aplikace, pokud tedy explicitně neposkytuje pro takové chování prostředky. Chcete-li se tomuto problému vyhnout, vytvořte pomocný databázový server, který bude synchronizované aktualizace zpracovávat jako sdílené informace.

Služba Vyrovnávání zatížení sítě se často používá ve spojení s těmito prvky:

■ **Servery VPN**

Server VPN umožňuje vytvoření privátní sítě, které zahrnuje spojení přes sdílené či veřejné sítě, jako je například Internet.

■ ***Servery multimediálních datových proudů***

Software (například Microsoft Media Technologies) zajišťující podporu multimédií a umožňující odesílání obsahu pomocí formátu Advanced Streaming Format přes intranet nebo Internet.

Služba Vyrovnávání zatížení sítě je dobrou volbou pro servery VPN a servery multimediálních datových proudů v případě, kdy zjistíte, že vaše organizace může mít užitek z vyrovnávání provozu PPTP či multimediálních datových proudů.

Poznámka Dříve než použijete službu Vyrovnávání zatížení nějaké aplikace v klastru služby Vyrovnávání zatížení sítě, seznamte se s licencí aplikace nebo kontaktujte jejího prodejce. Každý prodejce určuje své vlastní zásady licencování aplikací běžících na klastrech.

Budete-li používat k vyrovnávání zatížení mezi klienty PPTP službu Vyrovnávání zatížení sítě se servery VPN, je zapotřebí správně nakonfigurovat vlastnosti protokolu TCP/IP a zajistit kompatibilitu s klienty provozujícími dřívější verze systému Windows (například Windows 98 a Windows NT 4.0). Toho dosáhnete tím, že síťovému adaptéru používanému službou Vyrovnávání zatížení sítě přiřadíte jedinou virtuální adresu IP a na této podsíti nepřidáte adaptéru vyhrazenou adresu IP. Toto omezení neplatí pro klienty systému Windows 2000.

Další informace o konfigurování služby Vyrovnávání zatížení sítě pro VPN a další aplikace najdete v kapitole „Clustering systému Windows“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.

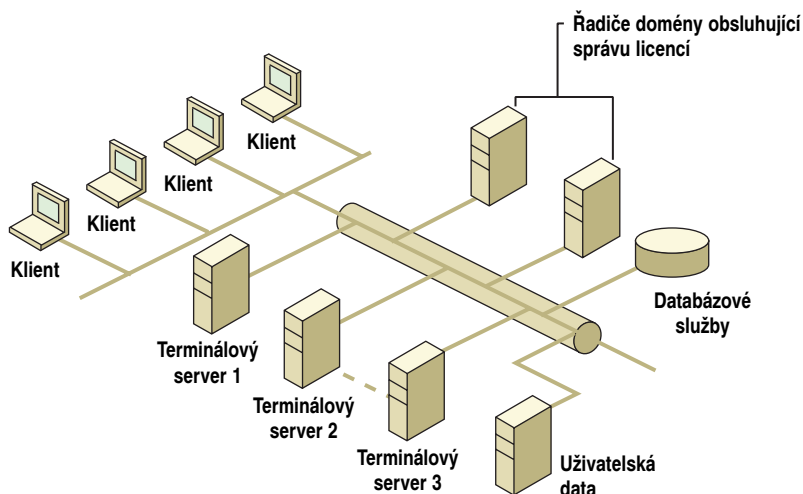
Zavádění klastrů terminálových serverů pomocí vyrovnávání zatížení sítě

Služba Terminal Services systému Windows 2000, je-li nakonfigurovaná na režim aplikačního serveru, umožňuje centralizované zavádění aplikací a jejich vykonávání vzdálenými uživateli. Pomocí služby Vyrovnávání zatížení sítě můžete rozdělit velké množství klientů do skupiny terminálových serverů. To je nejvhodnější v situacích, kdy je aplikace terminálového serveru převážně nestavová, například při poskytování aplikace zadávání dat pro oddělení prodeje nebo sklad.

Potřebují-li se cestující uživatelé opakovaně připojovat k existujícím relacím terminálových serverů, nelze používat službu Vyrovnávání zatížení sítě. Jelikož služba Vyrovnávání zatížení sítě trasuje uživatele na hostitele klastru na základě adresy IP, uživatel, který se připojuje z různých míst nebo používá protokol DHCP a mezi relacemi se odpojuje, nemůže být vždy nasměrován zpět na daný počítač, a proto ani nemůže dosáhnout odpojené relace. V takových situacích může služba Vyrovnávání zatížení sítě zajistit opakované připojení zastavených relací nebo trvalé trasování, jen když má uživatel pevnou adresu IP. Není-li udržování odpojených relací nutné, můžete službu Vyrovnávání zatížení sítě používat efektivně prakticky pro všechny druhy aplikací terminálového serveru.

Používáte-li službu Vyrovnávání zatížení sítě, doporučujeme vám, abyste všechny terminálové servery nakonfigurovali na ukončení odpojených relací po nějaké rozumné době, například po 30 minutách. Tato konfigurace vám umožní obnovovat zastavené relace, ale nepřipustí příliš dlouhé trvání odpojených relací. Trvalé relace mohou být problémem v situacích, kdy je uživatel přesměrován na jiné počítače, protože tyto počítače nebudou schopny opakovaného připojení. Uvedená konfigurace může spotřebovávat značné množství prostředků, protože každý uživatel bude mít na různých počítačích otevřené různé relace, a v nejhorším případě mohou být uživatelé dokonce zablokováni, jelikož jejich prostředky se už používají někde jinde.

Při zavádění klastru terminálových služeb pomocí služby Vyrovnávání zatížení sítě musí být každý server schopen obsloužit všechny uživatele. Toho dosáhnete ukládáním informací o jednotlivých uživateli, systémových informací a společných dat na nějakém přístupném místě, například na pomocném souborovém serveru. Implementaci služby Vyrovnávání zatížení sítě a služby Terminal Services ukazuje obrázek 18.4.



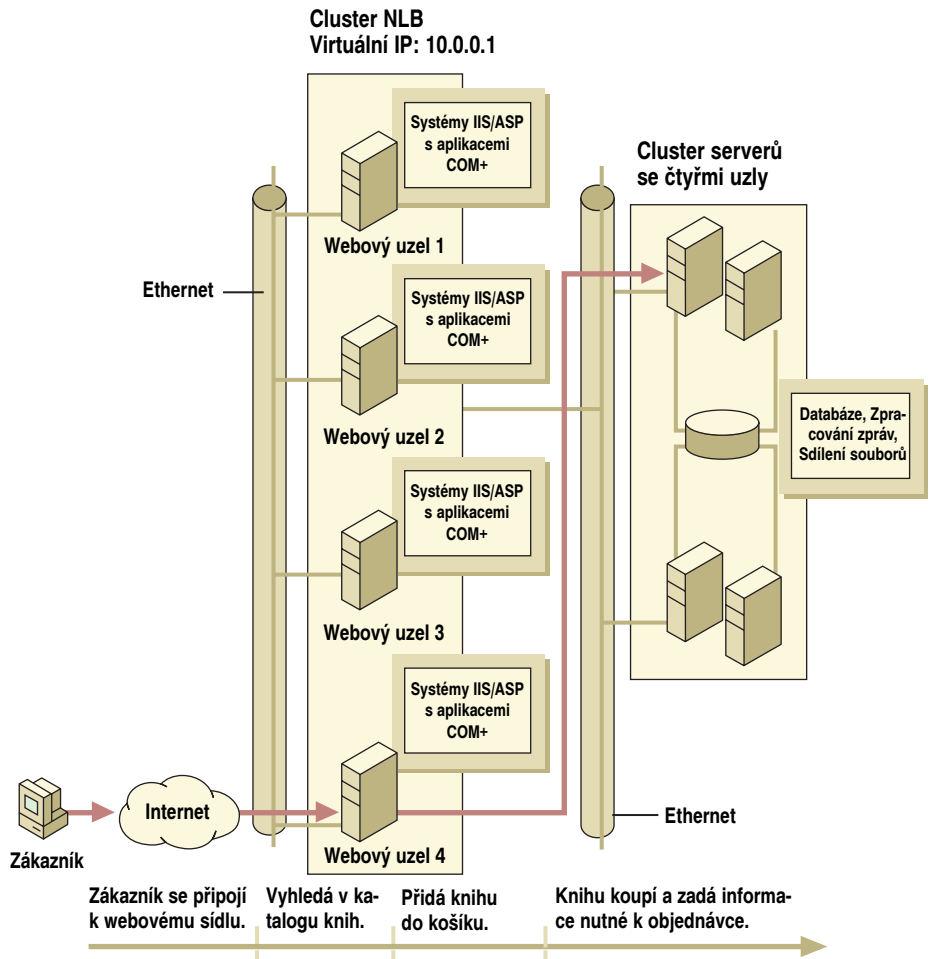
Obrázek 18.4 Služba Vyrovnávání zatížení sítě zajišťuje vyrovnávání zatížení mezi terminálovými servery

Všimněte si zakreslení samostatných serverů pro obchodní databázové aplikace a ukládání dat o jednotlivých uživateli. Každý takový server musí být implementován pomocí clusteringu a dalších vhodných technologií jako vysoce dostupný server. Taková implementace navíc zlepšuje škálovatelnost rozdělením zatížení, takže požadovanou úroveň výkonu dokáže zajistit více terminálových serverů.

Další informace o terminálových službách najdete v kapitole „Zavádění terminálových služeb“ v této knize.

Konfigurování klastrů vyrovnávání zatížení sítě pro servery se spuštěnými aplikacemi IIS/ASP a COM+

Klíčovou komponentou webových sídel elektronického obchodování jsou servery se spuštěnými aplikacemi COM+. V příkladu uvedeném na obrázku 18.5 zpracovává server se spuštěným systémem COM+ požadavky na objekty nákupního košíku online prodejny knih.



Obrázek 18.5 **Zavádění aplikací COM+ na stejných fyzických serverech jako IIS**

Aby byly tyto objekty dostupné v okamžiku, kdy je potřebujete, a aby byl maximalizován výkon sídla jako celku, doporučujeme vám zavést COM+ na stejných fyzických serverech jako službu IIS. Aplikační servery pak budou moci využívat výhody škálovatelnosti a dostupnosti zajišťované existujícím klastrem služby Vyrovnávání zatížení sítě a není zapotřebí zavádět další samostatnou vrstvu vyhrazených serverů s běžícím systémem COM+.

Budete-li používat jediný fyzický klastr serverů služby Vyrovnávání zatížení sítě, který je nakonfigurován na služby IIS/ASP i COM+, a nebudete-li tedy vytvářet oddělenou fyzickou vrstvu aplikačních serverů, omezíte tím náklady na hardware a správu, protože budete potřebovat méně serverů.

Určení síťových rizik

Při určování síťových rizik musíte identifikovat možná selhání, která mohou způsobit přerušení přístupu k síťovým prostředkům. Mezi jediné body selhání patří hardware, software nebo externí závislé prvky, jako je například energie dodávaná rozvodnou společností či vyhrazené linky rozsáhlé sítě (WAN).

Obecně lze říci, že maximální dostupnosti dosáhnete, když:

- minimalizujete počet jediných bodů selhání (single point of failure) ve svém prostředí;
- zajistíte mechanismy udržení funkčnosti služby i v případě výskytu selhání.

Při používání služby Vyrovnávání zatížení sítě také zajišťujete maximální dostupnost, když:

- vyrovnáváte zatížení jen těch aplikací, které se pro službu Vyrovnávání zatížení sítě hodí;
- se ujistíte, že aplikační servery jsou řádně nakonfigurovány pro aplikace, které na nich běží (další informace o správné konfiguraci najdete v oddílu „Určení požadavků na kapacitu serverů“ dále v této kapitole).

Hlavním smyslem služby Vyrovnávání zatížení sítě je zajistit zvýšenou dostupnost. Klastř dvou nebo více počítačů zaručuje, že když jeden z počítačů selže, může ve zpracovávání požadavků klientů pokračovat jiný počítač. Služba Vyrovnávání zatížení sítě však nemůže chránit všechny aspekty vašeho pracovního prostředí za všech okolností. Není tak například alternativou k zálohování dat. Služba Vyrovnávání zatížení sítě jen chrání přístup k datům a nikoli data samotná. Také nechrání před přerušením napájení, které způsobí výpadek celého klastru.

Systém Windows 2000 Advanced Server má zabudované funkce, jež během selhání ochraňují určité procesy počítačů a sítě. Tyto funkce zahrnují redundantní pole nezávislých disků RAID 1 (zrcadlení disků) a RAID 5 (prokládání disků s paritou – stripe set with parity). Při plánování prostředí vyrovnávání zatížení sítě se snažte vyhledat oblasti, kde vám tyto prvky mohou pomoci způsoby, které služba Vyrovnávání zatížení sítě neumožňuje.

Plánování vyrovnávání zatížení sítě

Tento oddíl vám pomůže určit počet serverů služby Vyrovnávání zatížení sítě, které budete ve své organizaci potřebovat, a pomůže vám je také nakonfigurovat.

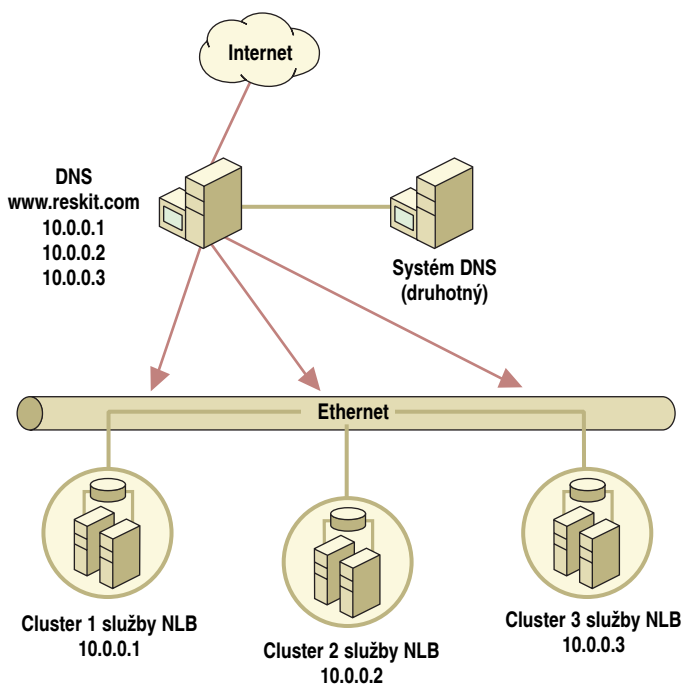
Velikost klastru, která je definovaná jako počet hostitelů, jež jsou součástí klastru (v clusteringu systému Windows jich může být až 32), vychází z počtu počítačů potřebných ke zvládnutí očekávaného zatížení vytvářeného klienty pro určitou aplikaci.

Určíte-li například, že ke zvládnutí očekávaných požadavků klientů webových služeb budete potřebovat šest počítačů se spuštěnou službou IIS, pak bude služba Vyrovnávání zatížení sítě pracovat na všech šesti počítačích a váš klastř se bude skládat ze šesti hostitelů.

Obecně platí, že je zapotřebí přidávat servery, dokud klastř nedokáže bez problémů zpracovat zatížení vytvářené klienty, aniž by docházelo k jeho přetížení. Maximální potřebná velikost klastru je určena síťovou kapacitou na dané podsíti. Přesný počet závisí na podstatě aplikace.

Poznámka Vždy musíte zajistit dostatek nadbytečné serverové kapacity, aby v případě selhání jednoho serveru zbývající servery zvládly zvýšené zatížení.

Jakmile se podsít klastru blíží k saturaci sítě, přidejte na jinou podsít další klastr. K nasměrování klientů na takové klastry použijte techniku round robin systému DNS. Podobným způsobem můžete pokračovat v přidávání klastrů podle potřeb růstu sítě. Protože technika round robin systému DNS obsahuje pouze adresy IP klastrů, klienti jsou vždy nasměrováni na klastry a nikoli na jednotlivé konkrétní servery, a proto se nikdy nemohou setkat s výpadkem způsobeným selháním serveru. V určitých nasazeních vyžadujících velké šířky pásma můžete pomocí techniky round robin systému DNS rozdělovat příchozí provoz mezi více identickými klastry služby Vyrovnávání zatížení sítě. Na obrázku 18.6 zjistí požadavek IP systém DNS (www.reskit.com), který přeloží virtuální adresu IP klastru 1 služby Vyrovnávání zatížení sítě (10.0.0.1) a požadavek předá tomuto klastru služby Vyrovnávání zatížení sítě (Network Load Balancing – NLB). Následující požadavky jsou pak odeslány klastru 2 (10.0.0.2) a klastru 3 (10.0.0.3) a pak se všechno opakuje stále dokola.



Obrázek 18.6 Technika round robin systému DNS mezi identickými klastry vyrovnávání zatížení sítě

Poznámka Používáte-li síťové přepínače (switch) a zároveň chcete zavést dva nebo více klastrů, zvažte umístění klastrů na samostatné přepínače, aby byl příchozí provoz klastrů zpracováván odděleně. *Přepínač* se používá k připojení hostitelů klastru ke směrovači nebo jinému zdroji příchozích síťových připojení.

Je důležité uvědomit si, že přepínač lze použít k oddělování příchozího provozu v případech, kdy máte více než jeden klastr.

Určení požadavků na kapacitu serverů

Jakmile jste určili velikost klastru, můžete nakonfigurovat jednotlivé hostitele v klastru. Obecně lze říci, že toto určení bude vycházet z typů aplikací, které chcete vyrovnávat, a požadavků klientů, které na těchto aplikacích očekáváte. Určité serverové aplikace, například souborové a tiskové servery, jsou velmi náročné na práci s diskem a vyžadují velmi velké diskové kapacity a rychlý vstup a výstup (I/O). Nejprve si přečtete dokumentaci všech aplikací, které chcete spouštět, a pak určete, jak je zapotřebí nakonfigurovat servery v klastru.

Je-li někde možné nahradit dva či tři velmi výkonné servery větším počtem méně výkonných počítačů, obvykle je vhodnější použít větší počet serverů. Použijete-li více serverů, umožníte tak rovnoměrnější rozdělení zatížení klientů, takže když dojde k selhání jednoho serveru, nárůst potřebného výkonu na ostatních serverech je menší.

Optimalizování klastrů služby Vyrovnávání zatížení sítě

Existují určité hardwarové a konfigurační možnosti, kterými lze zlepšit výkonnost klastru služby Vyrovnávání zatížení sítě. Tyto volby jsou popsány v následujících oddílech.

Jsou-li hostitelé v klastru přímo připojeni na přepínač, aby mohly být přijímány požadavky klientů, příchozí provoz od klientů se automaticky odesílá na všechny porty přepínače. Ve většině aplikací je příchozí provoz od klientů jen malou částí celkového provozu v klastru. Jsou-li však k jednomu přepínači připojeny ještě další klustry nebo počítače, tento provoz klastru spotřebovává část šířky pásma jejich portu.

Chcete-li se vyhnout tomuto problému, můžete připojit všechny hostitele v klastru na rozbočovač nebo opakovač, který připojíte na jeden z portů nadřazeného přepínače.. Potom veškerý příchozí provoz od klientů teče z rozbočovače nebo směrovače na jediný port přepínače a následně se předává současně všem hostitelům v klastru. Jestliže na přepínač dorazí provoz od klientů z více portů přepínače, můžete každému hostiteli přidat druhý vyhrazený síťový adaptér, který bude připojen přímo k jednomu z portů nadřazeného přepínače. Použití dvou síťových adaptérů v každém hostiteli na podsíti klastru pomáhá směřovat síťový provoz přes hostitele v klastru. Příchozí provoz od klientů prochází přepínacím rozbočovačem ke všem hostitelům, zatímco odchozí provoz teče přímo na porty přepínače.

Požadavky na službu Vyrovnávání zatížení sítě

Aplikace může pracovat na klastru služby Vyrovnávání zatížení sítě za následujících podmínek:

- Připojení s klienty musí být nakonfigurováno na použití protokolu IP.
- Aplikace, jejíž zatížení se bude vyrovnávat, musí používat porty TCP nebo UDP.
- Musí být možné provozovat současně na samostatných serverech více identických instancí dané aplikace. Pokud více takových instancí sdílí nějaká data, musí existovat nějaký způsob synchronizace aktualizací.

Služba Vyrovnávání zatížení sítě (Network Load Balancing) je vytvořena tak, aby v systému Windows 2000 Advanced Server fungovala jako standardní síťový ovladač zařízení. Protože služba Vyrovnávání zatížení sítě poskytuje podporu clusteringu pouze serverovým programům používajícím TCP/IP, musí být nainstalován protokol TCP/IP.

Jenom tak lze využívat výhody služby Vyrovnávání zatížení sítě. Současná verze služby Vyrovnávání zatížení sítě funguje na rozhraní Fiber Distributed Data Interface (FDDI) nebo místních sítí v klastru vycházejících z Ethernetu. Byla úspěšně testována na ethernetových sítích s kapacitou 10 megabitů za sekundu (Mb/s), 100 Mb/s i na gigabitových sítích s velkým množstvím různých síťových adaptérů.

Služba Vyrovnávání zatížení sítě zabírá méně než 1 megabajt (MB) diskového prostoru a v závislosti na zatížení sítě používá při práci s výchozími parametry mezi 250 kilobajty (KB) a 4 MB paměti RAM. Výchozí parametry můžete upravit a povolit použití až 15 MB paměti. Typická spotřeba paměti se pohybuje mezi 500 KB a 1 MB.

Chcete-li zajistit optimální výkon klastru, naplánujte instalaci druhého síťového adaptéru na všechny hostitele služby Vyrovnávání zatížení sítě, který se bude starat o síťový provoz adresovaný danému serveru jako individuálnímu počítači na síti. V této konfiguraci první síťový adaptér, na kterém je povolena služba Vyrovnávání zatížení sítě, zpracovává síťový provoz mezi klienty a klastrem, adresovaný serveru jako součásti klastru. Druhý síťový adaptér sice není nutný, zlepšuje však celkový výkon sítě například při přístupu k podpůrné databázi. Když je služba Vyrovnávání zatížení sítě povolena v tomto výchozím režimu jednosměrového vysílání, druhý adaptér je zapotřebí ke komunikaci mezi servery v klastru, například při replikování souborů mezi servery.

Další informace o systémových požadavcích a parametrech klastru a hostitele najdete v kapitole „Clustering systému Windows“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.

Použití směrovače

Služba Vyrovnávání zatížení sítě může pracovat ve dvou režimech: jednosměrového (unicast) vysílání a vícesměrového (multicast) vysílání. Standardně je nastaveno jednosměrové vysílání, které zaručuje správnou funkci na všech směrovačích. Můžete však také vybrat režim vícesměrového vysílání, protože pak není pro komunikace v rámci klastru zapotřebí druhý síťový adaptér. Jestliže klienti služby Vyrovnávání zatížení sítě přistupují ke klastru (nakonfigurovanému na vícesměrové vysílání) přes směrovač, musíte zajistit, aby směrovač přijímal odpověď protokolu Address Resolution Protocol (ARP) na (jednosměrové) adresy IP klastru adresou řízení přístupu k médium vícesměrového vysílání v přenášení dat struktury ARP. ARP je protokol TCP/IP, který k překladu logicky přiřazených adres IP používá omezené vysílání do místní sítě (limited broadcast).

To umožňuje směrovači mapovat primární adresu IP klastru a další adresy obsluhované více adaptéry k odpovídající adrese řízení přístupu k médium. Nesplňuje-li váš směrovač tento požadavek, můžete ve směrovači vytvořit statickou položku ARP nebo můžete službu Vyrovnávání zatížení sítě provozovat v jejím výchozím režimu jednosměrového vysílání.

Některé směrovače vyžadují zadání statických položek ARP, protože nepodporují překlad adres IP jednosměrového vysílání na adresy řízení přístupu k médium (MAC address – media access control address) vícesměrového vysílání.

Plánování služby Cluster Service

Služba Cluster Service systému Windows 2000 Advanced Server poskytuje základy pro serverové klustry. Když jeden ze serverů v klastru selže nebo přejde do režimu offline, operace chybujícího serveru převezme jiný server v klastru. Klienti používající prostřed-

ky serveru někdy mohou zaznamenat krátké přerušení své práce během doby, kdy se podpora prostředků přesouvá z jednoho serveru na druhý.

Na *serverových klastrech* spravuje veškeré činnosti související s klastrem služba Cluster Service. Na každém uzlu v klastru běží jedna instance služby Cluster Service. Služba Cluster Service zpracovává především následující operace:

- Spravuje objekty klastru, disky klastru a konfiguraci.
- Koordinuje se s dalšími instancemi služby Cluster Service v klastru.
- Zajišťuje operace překlopení (failover).
- Zpracovává upozornění na události.
- Umožňuje komunikaci mezi dalšími softwarovými komponentami.

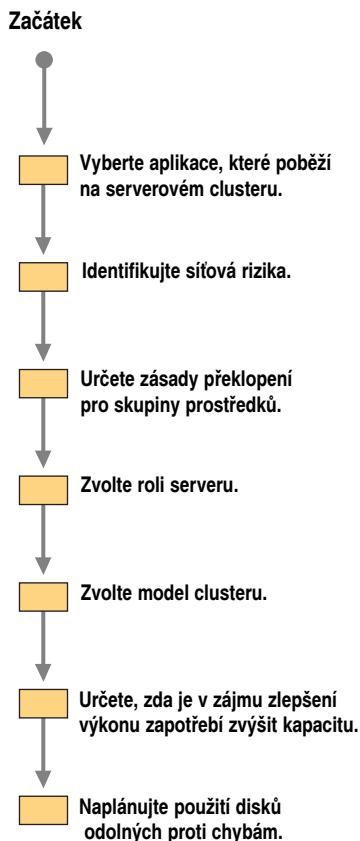
Vaše organizace bude potřebovat serverové klastry, pokud:

- vaši uživatelé závisejí na pravidelném přístupu k důležitým obchodním datům a aplikacím, jinak by nemohli vykonávat svou práci;
- nemůžete tolerovat doby výpadků služby (neplánované i plánované) delší než 30 minut;
- náklady na záložní server jsou nižší než ztráty způsobené nedostupností důležitých obchodních dat a aplikací během selhání.

Poznámka Termín „záložní server“ obvykle znamená, že jeden server nic nedělá až do okamžiku, než je zapotřebí jeho služeb. To však není základním smyslem serverového klastru, i když je možné jej tímto způsobem nakonfigurovat.

Proces plánování serverových klastrů

Tento oddíl popisuje základní prvky, které musíte zvážit při plánování serverových klastrů ve vaší organizaci. Použijte proces plánování zachycený na obrázku 18.7.



Obrázek 18.7 Proces plánování serverových klastrů

Volba aplikací běžících na serverovém klastru

Na libovolný server, který je v klastru, lze zavést libovolnou aplikaci. Ne všechny aplikace však podporují překlopení a z těch, které překlopení podporují, nemusí být některé nastaveny jako prostředky klastru. Tento oddíl shrnuje základní principy potřebné pro učinění takových rozhodnutí.

Následující kritéria vám pomohou určit, zda se určitá aplikace dokáže adaptovat na mechanismy překlopení clusteringu serverů:

- Klientské a serverové aplikace musí používat protokol TCP/IP (nebo model DCOM, pojmenované kanály či vzdálené volání procedur přes TCP/IP), aby mohly jejich síťové komunikace běžet na serverovém klastru. Aplikace, která využívá pouze protokoly NetBIOS Enhanced User Interface (NetBEUI) nebo Internetwork Packet Exchange (IPX), nemůže překlopení v klastru používat.
- Místo, kde si aplikace ukládá data, musí být konfigurovatelné.

Aplikace spuštěná na serverovém klastru musí být schopna ukládat si svá data na konfigurovatelné místo, tedy na disky připojené ke sdíleným diskovým sběrnicím. Některé z aplikací, které neukládají svá data na konfigurovatelné místo, lze přesto

nastavit na podporu překlopení. V takových případech je však přístup k datům aplikace při překlopení ztracen, protože data jsou dostupná pouze na disku uzlu, který selhal. V této situaci může pomoci replikování takových dat mezi uzly v klastru.

- Při selhání lze aplikaci restartovat.
- Aplikaci je možné nainstalovat na všechny uzly v klastru.
- Klientské aplikace, které se připojují k serverové aplikaci, se musí po dočasných selháních sítě pokoušet o opakované připojení a obnovení spojení.

Během překlopení se dočasně přeruší spojení klientské aplikace se serverem.. Na konfiguruje-li klientskou aplikaci tak, aby se dokázala zotavit z dočasných problémů s připojením k síti, může pokračovat ve své funkci i po překlopení serveru.

Aplikace podporující překlopení lze rozdělit do dvou skupin: ty, které používají rozhraní Cluster API, a ty, které je nepoužívají.

Aplikace podporující rozhraní Cluster API se definují jako „navržené pro klastr“ (cluster-aware). Takové aplikace se mohou zaregistrovat ve službě Cluster Service a získávat stavové a upozorňující informace a ke správě klastrů mohou používat rozhraní Cluster API.

Aplikace nepodporující rozhraní Cluster API se definují jako „nenavržené pro klastr“ (cluster-unaware). Pokud aplikace neznalé klastrů splňují kritéria TCP/IP a vzdáleného úložiště, můžete je v klastru používat a dokonce je lze často nakonfigurovat na podporu překlopení.

V obou případech platí, že aplikace, které si významné stavové informace udržují v paměti, nejsou vhodnými aplikacemi pro clustering, protože informace neuložené na disku se během překlopení ztratí. Výsledek se pak podobá restartu serveru nebo situaci, kdy na serveru dojde k výpadku napájení.

Identifikace síťových rizik

Při konfiguraci klastru identifikujte možné výpadky, které mohou přerušit přístup k prostředkům. Jedinými body selhání může být hardware, software nebo externí závislé prvky, jako je například elektrická energie dodávaná rozvodnou společností nebo vyhrazené linky WAN.

Obecně lze říci, že maximální dostupnost zajistíte, když:

- minimalizujete počet jediných bodů selhání ve svém prostředí;
- zajistíte mechanismy zabezpečení služby i pro případ selhání.

V systému Windows 2000 Advanced Server můžete k zajištění zvýšené dostupnosti využít serverové klastry a nové procedury správy. Serverové klastry však nefungují jako ochrana všech komponent vašeho pracovního prostředí za všech okolností. Klastry tak například nejsou alternativou k zálohování dat; zajišťují jen dostupnost dat a nikoli data samotná.

Systémy Windows 2000 Server mají zabudované funkce, které během selhání ochraňují určité procesy počítačů a sítě. Tyto funkce zahrnují zrcadlení disků (RAID 1) a prokládání disků s paritou (RAID 5). Při plánování klastru se snažte vyhledat oblasti, kde vám tyto prvky mohou pomoci způsoby, které klastry samotné neumožňují.

Poznámka K ochraně disků spravovaných službou Cluster Service nelze použít softwarové pole RAID, které nabízí Správce logického svazku (Logical Volume Manager) systému Windows 2000. K ochraně takových disků musíte použít hardwarové pole RAID.

Chcete-li ještě více zvýšit dostupnost síťových prostředků a zabránit ztrátě dat, zvažte také následující body:

- V každé lokalitě mějte k dispozici náhradní disky a zařízení. Připravené náhradní díly musí vždy přesně odpovídat originálním součástem; sem patří i síťové komponenty a prvky SCSI. Náklady na dva náhradní řadiče SCSI mohou být jen zlomkem ceny zaplacené za to, že stovky klientů nemohou pracovat s vašimi daty.
- Jednotlivým počítačům a síti samotné (včetně rozbočovačů, mostů a směrovačů) zajistěte ochranu zdrojem nepřerušitelného napájení (UPS). V zařízeních UPS slouží k zajištění chodu počítače po určitou dobu po výpadku napájení baterie. Počítače se systémem Windows 2000 Server podporují UPS. Řešení UPS musí zajistit dostatečně dlouhé napájení operačního systému, aby byl schopen při výpadku napájení normálně skončit.

Určení zásad překlopení a zpětného překlopení pro skupiny prostředků

Skupina prostředků je asociace závislých či souvisejících prostředků. Závislé prostředky potřebují ke svému úspěšnému fungování jiné prostředky. Jednotlivé prostředky se nemohou překlápět nezávisle. Prostředky se překlápějí společně se všemi ostatními prostředky v jedné skupině prostředků.

Zásady překlopení je zapotřebí přiřadit všem skupinám prostředků v klastru. *Zásady překlopení* přesně určují, jak se skupina chová během překlopení. Pro každou nastavenou skupinu prostředků tak můžete vybrat ty nejvhodnější zásady.

Mezi zásady překlopení pro skupiny patří tři nastavení:

Načasování překlopení (failover timing)

Skupinu lze nastavit na okamžité překlopení v okamžiku, kdy dojde k selhání prostředku ovlivňujícího skupinu, nebo můžete instruovat službu Cluster Service, aby se selhávající prostředek pokusila několikrát restartovat a teprve potom iniciovala překlopení. Je-li možné vyhnout se selhání prostředku tím, že se restartují všechny prostředky ve skupině, pak nastavte službu Cluster Service na restartování skupiny.

Preferovaný uzel (preferred node)

Skupinu lze nastavit tak, aby vždy pracovala na určitém uzlu, je-li tento uzel dostupný. To je užitečné, když je jeden z uzlů lépe vybaven pro hostování skupiny. Toto nastavení má však vliv pouze dojde-li k překlopení v důsledku selhání uzlu. V jiných případech musíte ručně nastavit uzel, který hostí skupinu prostředků.

Načasování překlopení zpět (failback timing)

Překlopení zpět je proces přesunu prostředků, jednotlivě nebo ve skupině, zpět na jejich preferovaný uzel poté, co došlo k selhání uzlu a jeho následnému opětovnému přechodu do režimu online.

Skupinu lze nastavit tak, aby se překlápěla zpět na svůj preferovaný uzel ihned, jakmile služba Cluster Service zjistí obnovení funkce chybějícího uzlu, nebo můžete instruovat službu Cluster Service tak, aby čekala na zadanou denní hodinu (např. po skončení pracovní doby).

Další informace o plánování skupin prostředků najdete v oddílu „Plánování skupin prostředků“ dále v této kapitole.

Volba role serveru

Uzly v serverovém klastru mohou být členskými servery nebo řadiči domény. V obou případech však musí oba uzly patřit do stejné domény.

Chcete-li nakonfigurovat uzly klastru jako řadiče domény, musíte nejprve zajistit hardware potřebný pro jejich podporu. Další informace najdete v oddílu „Určení požadavků na kapacitu pro službu Cluster Service“ dále v této kapitole.

Chcete-li nakonfigurovat všechny uzly klastru jako členské servery, pak dostupnost klastru závisí na dostupnosti řadiče domény. Klaster je dostupný, pouze pokud je dostupný také řadič domény. Abyste zajistili požadovanou úroveň dostupnosti, musíte naplánovat použití dostatečného počtu řadičů domény. Další informace o zvýšení dostupnosti najdete v oddílu „Identifikace síťových rizik“ dříve v této kapitole.

Musíte také počítat s dodatečnými nároky vyplývajícími ze služeb řadiče domény. Ve velkých sítích se systémem Windows 2000 Advanced Server mohou řadiče domény při vykonávání replikace adresářů a ověřování klientů spotřebovávat značné prostředky. Z tohoto důvodu se u mnoha aplikací, například SQL Serveru a u služby Message Queuing, doporučuje, abyste je neinstalovali na řadič domény, chcete-li dosáhnout nejlepšího výkonu. Máte-li však malou síť, ve které se informace o účtech mění jen málokdy a ve které se uživatelé často nepřihlašují a neodhlašují, můžete řadiče domény použít jako uzly klastru.

Volba modelu serverového klastru

Serverové klustry lze z hlediska složitosti rozdělit na tři konfigurační modely. Tento oddíl popisuje jednotlivé modely a uvádí příklady typů aplikací, které jsou pro dané modely vhodné. Tyto modely sahají od klastru s jediným uzlem až po klaster, kde všechny servery aktivně poskytují služby. Vyberte si model klastru, který nejlépe odpovídá potřebám vaší společnosti.

Model 1: Konfigurace serverového klastru s jediným uzlem

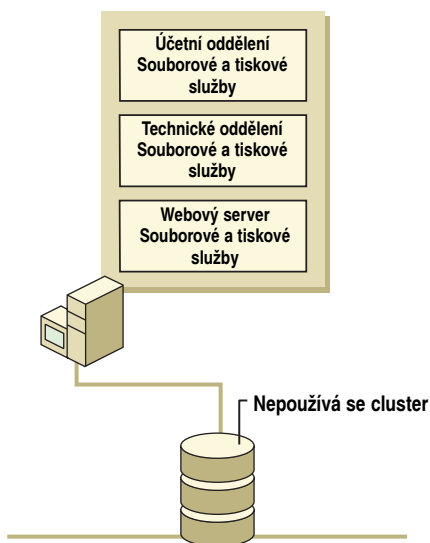
Model 1 ukazuje, jak je možné používat koncept virtuálního serveru s aplikacemi na serverovém klastru s jediným uzlem.

Tento model klastru nepoužívá překlopení. Představuje pouze způsob organizování prostředků na serveru v zájmu jednoduchosti správy a pohodlí vašich klientů. Hlavní výhodou tohoto modelu je, že jak správci tak i klienti okamžitě vidí na síti popisně pojmenované virtuální servery a nemusí ke sdíleným místům, která chtějí využít, procházet seznamem skutečných serverů.

Mezi další výhody tohoto modelu patří:

- Po obnovení počítače následně po selhání prostředku služba Cluster Service automaticky restartuje různé aplikační a závislé prostředky. To je výhodné pro aplikace, které mají užitek z funkce automatického restartování, ale samy nemají mechanismy jejího vykonání.
- Později můžete tento jediný uzel spojit do klastru s dalším uzlem a skupiny prostředků již budete mít připraveny. Jakmile nakonfigurujete zásady překlopení pro skupiny, virtuální servery mohou začít pracovat.

Obrázek 18.8 ukazuje příklad klastru s jediným uzlem, který nepoužívá funkci překlopení.



Obrázek 18.8 Konfigurace serverového klastru s jediným uzlem

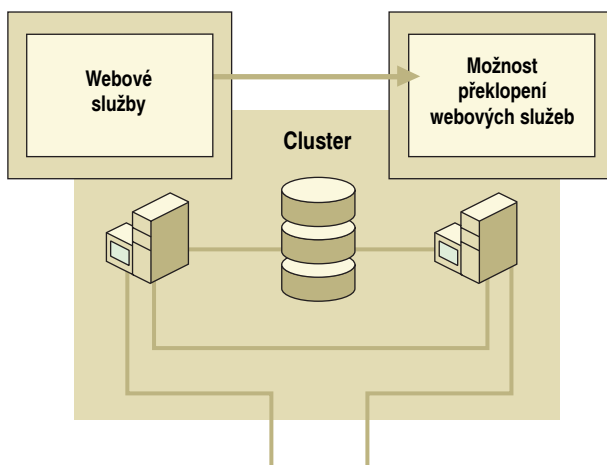
Tento model lze využít například pro umístění všech souborových a tiskových prostředků vaší organizace na jediný počítač, přičemž vytvoříte pro jednotlivá oddělení samostatné skupiny. Když se klienti z některého oddělení potřebují připojit k příslušnému místu sdílení souborů nebo tiskáren, najdou takové místo stejně jednoduše jako vlastní virtuální server oddělení.

Poznámka Některé aplikace, například SQL Server verze 6.5 a 7.0, nelze instalovat na klastr s jediným uzlem.

Model 2: Vyhrazený sekundární uzel

Model 2 zajišťuje maximální dostupnost a výkon pro vaše prostředky, vyžaduje však investice do hardwaru, který se většinu času vůbec nevyužívá.

Jeden z uzlů, označovaný za „primární uzel“, podporuje všechny klienty a doprovodný uzel je přitom nečinný. Doprovodný uzel je vyhrazený server, který je připraven k okamžitému použití v případě selhání na primárním uzlu. Dojde-li k selhání primárního uzlu, vyhrazený sekundární uzel okamžitě převeze všechny operace a pokračuje v obsluze klientů, která se rychlostí a výkonem podobá nebo je rovna schopnostem primárního uzlu. Tento postup se často označuje za konfiguraci aktivní/pasivní. Přesný výkon závisí na kapacitě sekundárního uzlu. Obrázek 18.9 představuje příklad použití vyhrazeného sekundárního uzlu.



Obrázek 18.9 Konfigurace aktivní/pasivní

Model 2 se nejlépe hodí pro nejdůležitější aplikace a prostředky ve vaší organizaci. Používá-li například vaše společnost k prodeji síť World Wide Web, můžete pomocí tohoto modelu zajistit druhotné uzly všech serverů vyhrazených pro podporu webového přístupu, například serverů se spuštěnými službami Internet Information Services (IIS). Náklady na zdvojnásobení hardwaru v této oblasti jsou ospravedlněny schopností ochránit přístup klientů k vaší organizaci. Selže-li jeden z webových serverů, další je plně nakonfigurován a připraven na převzetí jeho operací.

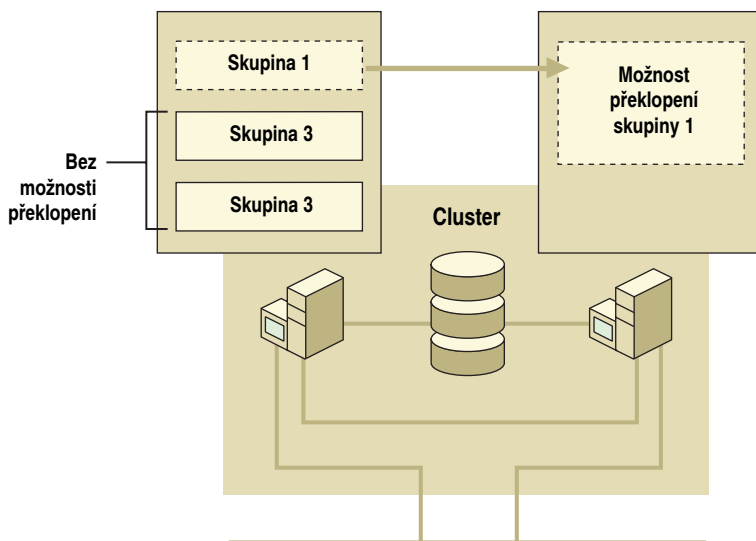
Umožňuje-li váš rozpočet zavedení sekundárního serveru se stejnou kapacitou, jako má primární uzel, pak nemusíte pro žádnou ze skupin nastavovat preferovaný server. Má-li jeden ze serverů větší kapacitu, udržíte výkon na co nejvyšší možné úrovni tak, že nastavíte zásady překlacení skupin preferující větší server.

Má-li sekundární uzel stejnou kapacitu jako primární uzel, nastavte pro všechny skupiny zásady zabráňující zpětnému překlacení. Jestliže má sekundární server menší kapacitu než primární uzel, nastavte zásady na okamžité překlacení zpět nebo překlacení zpět v zadanou hodinu mimo pracovní dobu.

Příklad zavedení: Konfigurace rozdělení aktivní/pasivní

Konfigurace rozdělení aktivní/pasivní představuje jeden z příkladů vyhrazeného sekundárního uzlu. Konfigurace rozdělení aktivní/pasivní demonstruje, že uzly v serverovém klastru nejsou omezeny jen na zajištění aplikací používajících clustering. Uzly poskytující prostředky v klastrech mohou také zajišťovat aplikace, které nejsou navrženy pro klastr a které selžou, když server přestane fungovat.

Jedním z kroků při plánování skupin prostředků je identifikovat aplikace, které nenakonfigurujete na podporu překlápění. Takové aplikace se mohou nacházet na serverech tvořících klastry, svá data si však musí ukládat na místní disky a nikoli na disky na sdílené sběrnici. Je-li důležitá vysoká dostupnost takových aplikací, musíte nalézt jiné metody jejího zajištění. Obrázek 18.10 ukazuje příklad konfigurace rozdělení aktivní/pasivní.



Obrázek 18.10 Konfigurace rozdělení aktivní/pasivní

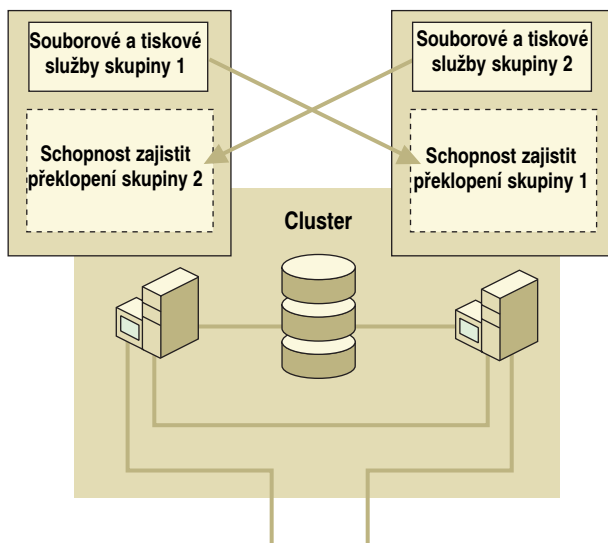
Aplikace v ostatních skupinách také obsluhují klienty na jednom ze serverů, protože však nejsou navrženy pro klastr, nevytvoříte pro ně zásady překlopení. Můžete tak například vytvořit uzel se spuštěným poštovním serverem, který není naprogramován na podporu překlopení, nebo s účetní aplikací, kterou používáte tak málo, že její dostupnost není důležitá.

Dojde-li k selhání uzlu, aplikace, kterým jste nepřiradili zásady překlopení, nebudou dostupné, pokud nemají zabudované své vlastní mechanismy překlopení. Zůstanou nedostupné až do okamžiku, než dojde k obnově uzlu, na němž běží; musíte je buď restartovat ručně nebo nastavit systém Windows 2000 Advanced Server na jejich automatické spuštění při startu systému. Aplikace nakonfigurované zásadami překlopení se překlopí v závislosti na nastavených zásadách překlopení.

Model 3: Konfigurace vysoké dostupnosti

Model 3 zaručuje spolehlivost a přijatelný výkon, i když je online jen jeden uzel, a vysokou dostupnost a výkon, když jsou online oba uzly. Tato konfigurace představuje maximální využití hardwarových prostředků.

V tomto příkladu zavedení každý uzel zpřístupňuje síti ve formě virtuálních serverů svou sadu prostředků, které mohou klienti detekovat a používat. V serverovém klastru je *virtuální server* sada prostředků včetně prostředku síťového názvu a prostředku adresy IP, které jsou obsaženy ve skupině prostředků. Kapacita jednotlivých uzlů je volena tak, aby prostředky na každém uzlu fungovaly s optimálním výkonem, ale zároveň aby každý uzel mohl v případě překlopení dočasně převzít zátěž vytvářenou prostředky spuštěnými na druhém uzlu. V závislosti na specifikacích kapacity prostředků a serverů mohou zůstat dostupnými během překlopení a po něm všechny klientské služby, může však dojít ke snížení výkonu. Obrázek 18.11 ukazuje příklad konfigurace aktivní/aktivní.



Obrázek 18.11 Konfigurace aktivní/aktivní

Tuto konfiguraci lze například použít v případě klastru vyhrazeného pro služby sdílení souborů a řazení tiskových úloh. Několik míst sdílení souborů a tiskáren je vytvořeno jako samostatné skupiny, každá na jednom uzlu. Dojde-li k selhání jednoho uzlu, ostatní uzly dočasně zajistí služby sdílení souborů a řazení tiskových úloh pro všechny uzly. Zásady překlopení skupiny, která je dočasně přemístěna, jsou nastaveny na preferování jejího původního uzlu. Jakmile dojde k obnovení porouchaného uzlu, přemístěná skupina vrátí řízení svému preferovanému uzlu a operace se dále vykonávají s normálním výkonem. Služby jsou po celou dobu s výjimkou krátkých přerušení dostupné klientům.

Následující příklady zavedení představují několik typů konfigurací s vysokou dostupností.

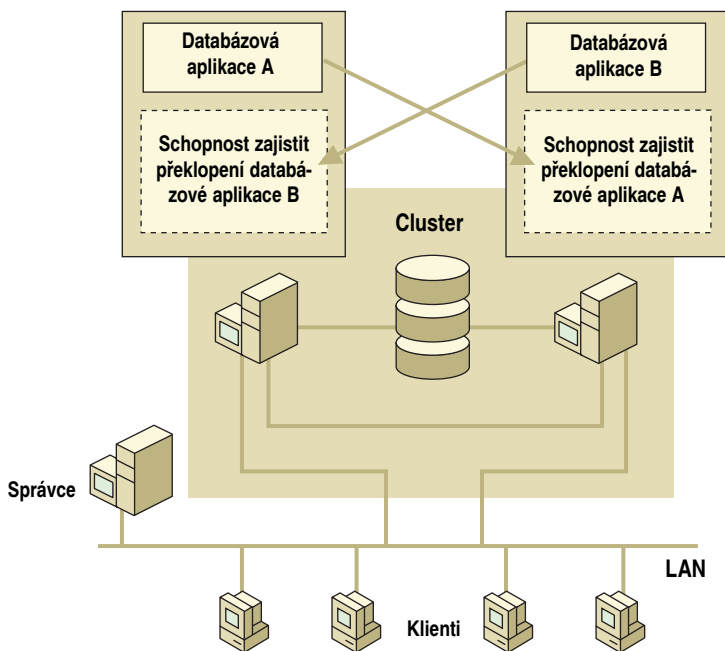
Příklad zavedení 1: Clustering aplikace jednoho typu

Tento příklad demonstruje, jak můžete vyřešit dva problémy často se vyskytující ve větších počítačových prostředích. První problém nastává, když na jediném serveru běží více velkých aplikací, což způsobuje snížení výkonu serveru. Tento problém vyřešíte tak, že k prvnímu serveru přidáte do klastru další server nebo více serverů a aplikace se tak rozdělí mezi servery.

Druhý problém se týká souvisejících aplikací spuštěných na samostatných serverech. Nejsou-li servery propojeny, vzniká problém dostupnosti. Když servery umístíte do klastru, zaručíte tak klientům vyšší dostupnost obou aplikací.

Představme si, že se intranet vaší společnosti spoléhá na server, na kterém běží dvě rozsáhlé databázové aplikace. Obě tyto databáze jsou velmi důležité pro stovky uživatelů, kteří se po celý den k serveru opakovaně připojují. Problémem je, že v okamžicích špičkového zatížení server nestačí zpracovávat požadavky a jeho výkon často klesá.

Problém zmírníte tak, že k přetíženému serveru připojíte druhý server, vytvoříte klastr a zatížení serverů budete vyrovnávat. Nyní máte více serverů a na každém běží jedna z databázových aplikací. Dojde-li k selhání jednoho serveru, může sice dojít ke snížení výkonu, ale jenom dočasně. Jakmile je porouchaný server obnoven, aplikace, která na něm běžela, se přeploží zpět a začne opět fungovat. Toto řešení znázorňuje obrázek 18.12.

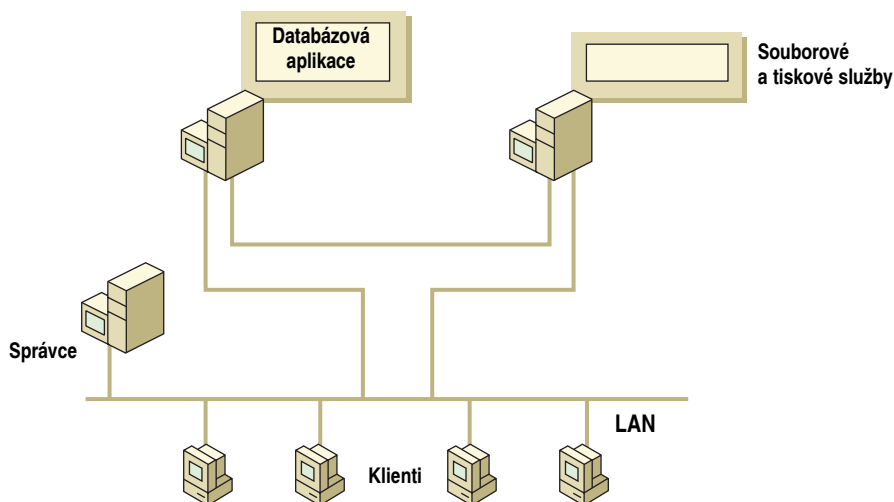


Obrázek 18.12 Připojením dalšího serveru k přetíženému serveru vytvoříte klastr

Příklad zavedení 2: Clustering více aplikací

Představme si, že se váš maloobchodní prodej spoléhá na dva samostatné servery. Jeden zajišťuje služby poštovního serveru a druhý poskytuje databázovou aplikaci informací o inventáři a objednávkách.

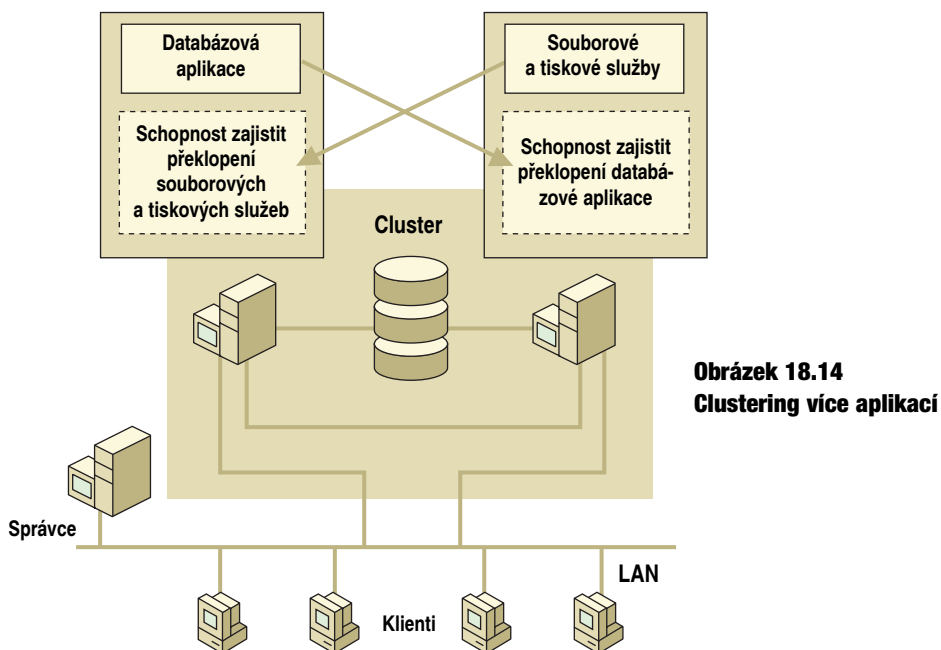
Obě tyto služby jsou pro vaši činnost zásadní. Zaměstnanci se spoléhají na služby poštovního serveru při své každodenní práci. Bez přístupu k databázové aplikaci si nemohou zákazníci objednávat zboží a zaměstnanci nemohou přistupovat k informacím o inventáři a dodávkách. Obrázek 18.13 ukazuje konfiguraci v typické rizikové situaci, kdy se důležité aplikace a služby spoléhají na samostatné servery.



Obrázek 18.13 Samostatné servery důležitých aplikací a služeb

Abyste zajistili dostupnost všech služeb, spojte počítače do klastru.

Vytvoříte klastr obsahující dvě skupiny, jednu pro každý uzel. První skupina bude obsahovat všechny prostředky potřebné k fungování aplikací podpory zpráv a druhá skupina bude obsahovat všechny prostředky potřebné pro databázovou aplikaci včetně samotné databáze. Obrázek 18.14 ukazuje řešení zajišťující dostupnost aplikací v takovém případě.



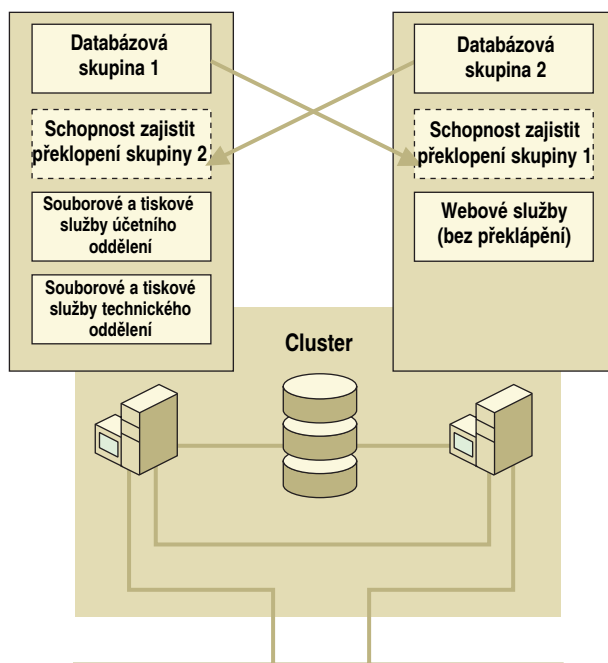
Obrázek 18.14 Clustering více aplikací

V zásadách překlopení skupin určíte, že obě skupiny mohou pracovat na obou uzlech, a tak zajistíte jejich dostupnost v případě selhání jednoho uzlu.

V systému Windows 2000 Advanced Server detekuje služba Cluster Service ztrátu připojení mezi servery a klientskými systémy. Dokáže-li software služby Cluster Service izolovat daný problém na určitý server, pak služba Cluster Service detekuje selhání sítě a překlápí závislé skupiny na jiný server (prostřednictvím fungujících sítí).

Příklad zavedení 3: Složitá hybridní konfigurace

Složitá hybridní konfigurace je spojením ostatních modelů. Hybridní konfigurace vám umožňuje využít výhody předchozích modelů a zkombinovat je do jednoho klastru. Máte-li k dispozici dostatečné kapacity, může na všech uzlech současně existovat mnoho scénářů typů překlopení. Ke všem činnostem překlopení dochází normálním způsobem podle nastavených zásad. Obrázek 18.15 zachycuje příklad více sdílených databázových míst umožňující poněkud snížený výkon v situaci, kdy se tato sdílená místa nacházejí na jediném uzlu.



Obrázek 18.15 Složitá hybridní konfigurace

V zájmu zjednodušení správy jsou místa sdílení tiskových a souborových služeb v klastru (který nemusí podporovat překlopení) logicky seskupena po odděleních a nakonfigurována jako virtuální servery. Aplikace, která nepodporuje překlopení, existuje na jednom z klastrů a funguje běžným způsobem (bez ochrany překlopením).

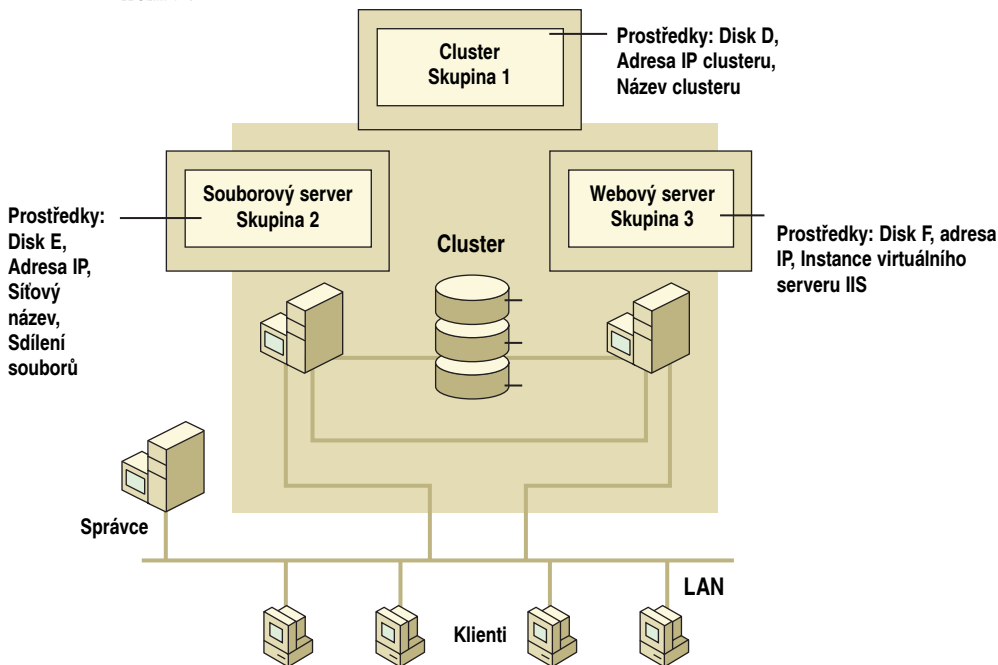
Plánování služby Cluster Service

Jakmile máte vyhodnoceny své potřeby clusteringu, můžete určit, kolik serverů potřebujete a jaké musí být jejich specifikace, jako je množství paměti a diskového prostoru.

Plánování skupin prostředků

Protože se všechny prostředky ve skupině přesunují mezi uzly jako jednotka, závislé prostředky nikdy nepřekračují hranice jedné skupiny (prostředky nemohou být závislé na prostředcích v jiných skupinách).

Obrázek 18.16 znázorňuje, jak jsou závislé prostředky sloučeny tak, aby tvořily skupinu. Uzel vlevo obsahuje skupinu Souborový server, která je tvořena čtyřmi prostředky, na nichž tato služba závisí: síťovým názvem, adresou IP, místem sdílení souborů a diskem E.



Obrázek 18.16 Skupina závislých prostředků

Typické klastry zahrnují jednu skupinu pro každou nezávislou aplikaci nebo službu, která je na klastru spuštěna. Typické skupiny klastrů obsahují následující typy prostředků:

- adresu IP;
- síťový název;
- fyzický disk;
- obecnou či vlastní aplikaci nebo službu.

Chcete-li zorganizovat své aplikace a další prostředky do skupin, postupujte podle následujících šesti kroků:

1. Vytvořte seznam všech svých serverových aplikací.

Většina skupin obsahuje jednu nebo více aplikací. Vytvořte seznam všech aplikací ve svém prostředí, bez ohledu na to, zda plánujete jejich používání ve spojení se

službou Cluster Service. Přidáním celkového počtu skupin (virtuálních serverů), které plánujete společně provozovat ve svém prostředí, k celkovému množství softwaru, který plánujete provozovat nezávisle na skupinách, určete celkové požadavky na kapacitu.

2. Určete, které z vašich aplikací mohou používat překlopení.

Stejně tak vytvořte seznam aplikací, které se budou nacházet na uzlech klastru, ale které nebudou používat funkci překlopení, protože je to v jejich případě nevhodné, zbytečné nebo dané aplikace není možné na překlápění nakonfigurovat. I když pro tyto aplikace nebudete definovat zásady překlopení ani je nebudete seskupovat, budou spotřebovávat část kapacity serveru.

Před zavedením aplikace do klastru si přečtěte příslušnou licenci nebo kontaktujte prodejce aplikace. Každý prodejce aplikací definuje své vlastní licenční zásady pro provozování aplikací v klastrech.

3. Vytvořte seznam všech prostředků, které nejsou aplikacemi.

Určete, který hardware, připojení a software operačního systému může serverový klastr ve vašem síťovém prostředí chránit.

Služba Cluster Service může například překlápět řazení tiskových úloh a chránit tak přístup klientů k tiskovým službám. Dalším příkladem je prostředek souborového serveru, který lze nastavit na překlápění a zachovávat tak přístup klientů k souborům. To má v obou případech vliv na kapacitu, jako je například paměť RAM potřebná k obsluze klientů v případě překlopení.

4. Vytvořte seznam všech závislostí jednotlivých prostředků.

Služba Cluster Service udržuje hierarchii závislostí prostředků a zaručuje tak, že všechny prostředky, na nichž určitá aplikace závisí, budou uvedeny do režimu online ještě *před* danou aplikací. Zároveň je zaručeno, že aplikace a všechny prostředky, na kterých závisí, v případě selhání jednoho z prostředků budou buď restartovány nebo překlopeny na jiný uzel.

Vytvořte seznam závislostí, který vám pomůže určit, jak vaše prostředky a skupiny prostředků závisí jedna na druhé a jaké je optimální rozdělení prostředků mezi všemi skupinami. Zahrňte všechny podpůrné prostředky podporující hlavní prostředky. Dojde-li například k překlopení aplikace webového serveru, pak aby webový server dále fungoval, musí se zároveň překlápnout webové adresy a disky obsahující soubory dané aplikace na sdílených sběrnících. Všechny tyto prostředky musí být ve stejné skupině. Tím je zajištěno, že služba Cluster Service bude udržovat vzájemně nezávislé prostředky vždy pohromadě.

Poznámka Při seskupování prostředků mějte na paměti, že prostředek a na něm závislé prvky musí být společně v jedné skupině, protože jeden prostředek nemůže zasahovat do více skupin.

Pamatujte, že skupina prostředků je základní jednotkou překlopení. Jednotlivé prostředky nelze překlápět nezávisle. Prostředky se překlápějí společně se všemi ostatními prostředky v jedné skupině prostředků.

Protože většina aplikací si ukládá svá data na disk, doporučujeme vám vytvořit pro každý disk skupinu prostředků. Umístěte aplikaci společně se všemi dalšími prostředky, na nichž závisí, do skupiny obsahující disk, na který si ukládá svá data. Jinou aplikaci umístěte společně s jejím diskem do jiné skupiny. Tato konfigurace

umožní aplikacím nezávislé překlápění neboli přesunování bez vlivu na jiné aplikace.

5. Učiňte předběžná rozhodnutí o skupinách prostředků.

Dalším důvodem přiřazení aplikací do jedné skupiny je pohodlná správa. Je tak možné vložit několik aplikací do jediné skupiny, protože zobrazení těchto určitých aplikací jako jediné entity usnadňuje správu sítě.

Obvyklým použitím této techniky je zkombinování prostředků sdílení souborů a prostředků řazení tiskových úloh do jediné skupiny. Zkombinujete-li tyto prostředky, všechny závislé prvky daných aplikací se musí také nacházet ve stejné skupině. Takovou skupinu můžete pro část společnosti, které slouží, nějak jednoznačně pojmenovat, například ÚčtárnaSoubory&Tisk. Kdykoli potřebujete pracovat s činnostmi sdílení souborů a tiskáren daného oddělení, najdete si příslušnou skupinu v nástroji Správce klastru (Cluster Administrator).

Další obvyklou praxí je vložit do jediné skupiny všechny aplikace které závisejí na určitém prostředku. Předpokládejme, že aplikace webového serveru zajišťuje přístup k webovým stránkám a že výstupem těchto webových stránek jsou sady výsledků, ke kterým klienti přistupují pomocí dotazování databázové aplikace SQL serveru. (Dotazování se uskutečňuje prostřednictvím formulářů hypertextového jazyka se značkami HTML). Když webový server a databázi SQL vložíte do jedné skupiny, data obou hlavních aplikací se mohou nacházet na určitém diskovém svazku. Protože obě aplikace existují ve stejné skupině, můžete také vytvořit adresu IP a síťový název specificky pro tuto skupinu prostředků.

6. Učiňte konečné přiřazení skupin.

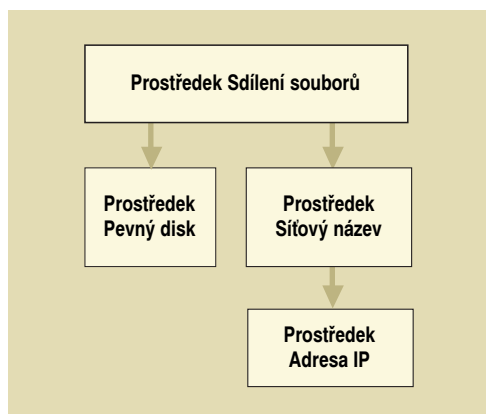
Po seskupení prostředků dohromady dejte každé skupině jiný název a vytvořte strom závislostí. Strom závislostí vizuálně zachycuje vztahy závislosti mezi prostředky.

Chcete-li vytvořit strom závislostí, vypište si všechny prostředky v určité skupině. Pak zakreslete šipky z jednotlivých prostředků na všechny prostředky, na nichž daný prostředek bezprostředně závisí.

Přímá závislost mezi prostředkem A a prostředkem B znamená, že mezi oběma prostředky se nenacházejí žádné zprostředkující prostředky. Nepřímá závislost se objevuje, když mezi prostředky existuje tranzitivní (přenosný) vztah. Jestliže prostředek A závisí na prostředku B a prostředek B závisí na prostředku C, existuje mezi prostředkem A a prostředkem C nepřímá závislost. Prostředek A však není přímo závislý na prostředku C.

Ve skupině Webový server na obrázku 18.16 závisejí prostředky Síťový název a Instance virtuálního serveru IIS na prostředku Adresa IP. Mezi prostředkem Síťový název a prostředkem Instance virtuálního serveru IIS však neexistuje žádná závislost.

Obrázek 18.17 ilustruje jednoduchý strom závislostí ukazující některé prostředky v konečném rozdělení do skupin.



Obrázek 18.17 Jednoduchý strom závislostí

Na obrázku 18.17 závisí prostředek Sdílení souborů na prostředku Síťový název, který dále závisí na prostředku Adresa IP. Prostředek Sdílení souborů však není přímo závislý na prostředku Adresa IP.

Poznámka Fyzické disky nezávisejí na žádném dalším prostředku a mohou se překlápat nezávisle.

Určení požadavků na kapacitu pro službu Cluster Service

Požadavky na kapacitu hardwaru pro jednotlivé servery v klastru dokážete specifikovat po splnění následujících bodů:

- Vyberte model klastru.
- Určete, jak seskupíte své prostředky.
- Určete zásady překlopení jednotlivých prostředků.

V následujících odstavcích najdete návrhy kritérií, jež vám pomohou určit hardwarové požadavky počítačů, které budete používat jako uzly klastru.

Požadavky na místo na pevném disku Každý uzel v klastru musí mít dostatek prostoru na pevném disku, aby zde bylo možné uložit trvalé kopie všech aplikací a dalších prostředků potřebných k provozování všech skupin. Tuto hodnotu vypočtete pro všechny uzly tak, jako by všechny prostředky v klastru běžely pouze na daném uzlu, i když ve skutečnosti poběží většina nebo všechny takové skupiny také na jiném uzlu. Tento nadbytečný diskový prostor naplánujte proto, aby mohl každý uzel během selhání s dostatečným výkonem provozovat všechny prostředky.

Poznámka

Služba Cluster Service nepodporuje dynamické disky a nové funkce zajišťované nástrojem Správce logického svazku (Logical Volume Manager). Zejména platí, že nelze rozšiřovat oddíly systému souborů NTFS na disku spravovaném službou Cluster Service. Proto musíte naplánovat kapacitu disku a zajistit dostatek prostoru pro další růst.

Požadavky na procesor Překlopení může znamenat značný nárůst potřeby kapacity zpracování procesoru uzlu v okamžiku, kdy převezme řízení prostředků z jiného uzlu, který selhal. Bez řádného naplánování může být procesor fungujícího uzlu během překlopení zahlcen nároky překračujícími jeho praktickou kapacitu, což bude mít za následek prodloužení doby odezvy na požadavky uživatelů. Kapacitu procesoru na každém uzlu naplánujte tak, aby dokázala zvládnout nové prostředky bez neúnosného zvýšení doby odezvy pro klienty.

Požadavky na paměť RAM Při plánování kapacity musíte zajistit, aby měl každý uzel v klastru dostatek paměti RAM ke spuštění všech aplikací, které mohou pracovat na všech ostatních uzlech. Také nezapomeňte stránkovací soubor systému Windows 2000 Advanced Server nastavit tak, aby odpovídal množství paměti RAM definovanému v jednotlivých uzlech.

Omezení serverových klastrů

Důležitými omezeními klastrů systému Windows 2000 Server jsou:

- Vyměnitelná úložiště
 - Na sdílenou sběrnici SCSI používanou klastrem neinstalujte zařízení vyměnitelných úložišť.
 - Nekonfigurujte zařízení vyměnitelných úložišť, jako jsou například páskové jednotky, jako prostředky klastru.
- Konfigurace disku
 - Na úložištích klastru musíte k naformátování disků použít systém souborů NTFS a disky musíte nakonfigurovat jako základní disky (basic disc). Systém NTFS nepodporuje použití dynamických disků (dynamic disc) jako úložišť klastru.
 - Na úložišti klastru nelze používat šifrovaný systém souborů (EFS), vzdálená úložiště (remote storage), připojené svazky (mounted volumes) a body změny zpracování (repase points).
- Na interním řadiči RAID nelze povolit zápis přes mezipaměť, protože data v mezipaměti se při překlopení ztratí. Příkladem interního řadiče je karta PCI uvnitř uzlu. V závislosti na konkrétním řadiči RAID může být možné povolit zápis přes mezipaměť na externím řadiči RAID. Externí řadič RAID se obvykle nachází v diskové skříni a data v mezipaměti se při překlopení zachovávají.
- Softwarové pole RAID je možné používat pouze na místních discích (tedy jednotkách nespravovaných službou Cluster Service). K ochraně dat na disku klastru lze používat pouze hardwarové pole RAID.
- Konfigurace sítě
 - Služba Cluster Service podporuje pouze protokol TCP/IP.
 - Všechna síťová rozhraní používaná na všech uzlech v serverovém klastru musí být na stejné síti. Všechny uzly klastru musí mít alespoň jednu společnou podsít.
- Služby Terminal Services

Terminálové služby lze používat pro vzdálenou správu uzly serverového klastru. Terminálové služby nelze na uzlu serverového klastru používat v režimu aplikačního serveru.

Důležité V současné není podporováno současné používání služeb Vyrovnávání zatížení sítě a Cluster Service na jednom serveru.

Nástroje automatizace zavedení služby Cluster Service

Existují určité nástroje automatizace zavedení služby Cluster Service ve vašem podniku. Tyto nástroje se nacházejí na kompaktním disku (CD) produktu Windows 2000 a uvádí je tabulka 18.2.

Tabulka 18.2 Nástroje automatizace zavedení služby Cluster Service

Nástroj	Popis
Sysprep	Nástroj umožňující duplikování disků. Operační systém Windows 2000 Advanced Server a aplikace můžete nainstalovat na jeden počítač a pak tuto instalaci duplikovat na libovolný počet systémů.
Cluscfg.exe	Tento nástroj je součástí základu operačního systému. Jakmile nainstalujete na systém službu Cluster Service, musíte jej spustit a službu nakonfigurovat.
Správce instalace (Setup Manager)	Nástroj s rozhraním průvodce, který vám pomůže s vytvořením bezobslužných skriptů a místa síťového sdílení distribuce potřebného k obvyklým bezobslužným zaváděním a zaváděním pomocí nástroje Sysprep.

Následující příklady ukazují použití těchto nástrojů.

Máte-li na systémech, kam chcete zavést službu Cluster Service, naprosto různé hardwarové konfigurace, můžete k vytvoření těchto systémů použít bezobslužnou instalaci. Ta spočívá ve vytvoření souboru Unattend.txt a místa sdílení distribuce v síti (volitelně), které se použijí k automatizaci vykonání instalačního programu včetně nakonfigurování služby Cluster Service systému Windows 2000.

Máte-li podobné hardwarové konfigurace, můžete vytvořit pomocí nástroje Sysprep obraz systému a urychlit tak proces instalace a zavedení. Abyste mohli k zavedení služby Cluster Service systému Windows 2000 použít nástroj Sysprep, musíte nejprve nainstalovat službu Cluster Service (pomocí Průvodce součástmi systému Windows). Po zavedení obrazu na systém spustíte soubor Cluscfg.exe. Spuštění souboru Cluscfg.exe lze automatizovat tak, že jej umístíte do oddílu [GuiRunOnce] souboru odpovědí nástroje Sysprep. Pak se soubor Cluscfg.exe spustí na všech systémech po skončení činnosti nástroje Sysprep. Nástroj Cluscfg.exe lze zautomatizovat prostřednictvím souboru odpovědí.

Další informace o těchto nástrojích najdete v kapitole „Clustering systému Windows“ v knize *Microsoft Windows Server 2000 Distribuované systémy*.

Optimalizování klastrů

Systém Windows 2000 Advanced Server používá adaptovatelnou architekturu a z hlediska výkonu se do značné míry sám vyladuje. Navíc je systém Advanced Server schopen alokovat prostředky dynamicky podle měnících se požadavků.

Cílem vyladění serveru a aplikací, jejichž zatížení se vyrovnává, je určit, na který hardwarový prostředek budou kladeny největší požadavky, a následně upravit konfiguraci tak, aby dokázala zpracovat všechny požadavky při maximální propustnosti.

Je-li například hlavní rolí klastru zajišťovat vysokou dostupnost souborových a tiskových služeb, bude díky velkému počtu souborů, k nimž se bude přistupovat, zatížen převážně disk. Souborové a tiskové služby také představují velkou zátěž síťových adaptérů, protože se přenáší velké množství dat. Je důležité zajistit, aby vaše síťové adaptéry a podsítě klastru dokázali zatížení zpracovat. V tomto případě nejsou obvykle kladeny velké nároky na paměť RAM, i když její použití může být také významné v situacích, kdy je mezipaměti systému souborů vyhrazen velký prostor v paměti RAM. V tomto prostředí je také obvyklé malé využití výkonu procesoru. V takových situacích tedy není zapotřebí optimalizovat paměť a procesor do stejné míry, jako jiné komponenty. Paměť lze často použít ke snížení zatížení disku, zejména u operací čtení z disku.

Naproti tomu prostředí serverové aplikace (například Microsoft Exchange) klade na procesor a paměť RAM mnohem větší požadavky než typický server prostředí souborů a tisku, protože na serveru dochází k mnohem rozsáhlejšímu zpracování dat. V takových případech je nejlepší použít vysoce výkonné víceprocesorové servery. Zatížení disku a sítě jsou spíše nižší, jelikož množství přenášených dat je menší. Služba Microsoft Cluster service vyžaduje při komunikacích mezi hostiteli i pro funkci samotného klastru jen malé systémové prostředky.

Plánování disků odolných proti chybám

Selhání disku může mít za následek neobnovitelnou ztrátu důležitých dat a způsobí zastavení funkce služby vyrovnávání zatížení i serveru včetně všech jeho aplikací. Proto zvažte použití speciálních metod ochrany disků před selháním.

Mnoho skupin prostředků obsahuje diskové prostředky na sdílených sběrnicích. V některých případech se jedná o obvyčné fyzické disky, jindy jde však o složitý diskový podsystém obsahující více disků. Téměř všechny prostředky závisí na discích na sdílených sběrnicích. Neobnovitelné selhání diskového prostředku má za následek neodvratné selhání skupiny, která daný prostředek obsahuje. Proto byste měli používat určité metody ochrany disků a diskových podsystémů před chybami.

Jedním z obvyklých řešení je používat hardwarové pole RAID. Podpora pole RAID zajišťuje vysokou dostupnost dat obsažených na sadách disků v klastru. Některá z těchto hardwarových řešení jsou považována za odolná vůči chybám, což znamená, že ani při selhání disku z diskové sady neztratíte žádná data.

Hardwarové pole RAID

Seznam HCL systému Microsoft Windows 2000 obsahuje mnoho různých hardwarových konfigurací RAID pro klastry. Řada řešení hardwarových polí RAID zajišťuje v jediné skříni redundanci napájení, sběrnici a kabelů. Firmware pole RAID dokáže sledovat stav jednotlivých komponent v hardwaru. Význam těchto schopností spočívá v tom, že za-

jišťují dostupnost dat pomocí více redundancí a řeší tak problémy některých bodů selhání. Hardwarová řešení RAID mohou také využívat vlastní procesor a mezipaměť.

Systém Windows 2000 Advanced Server může tyto disky používat jako standardní diskové prostředky.

I když jsou hardwarová pole RAID dražší než softwarová řešení (která jsou součástí systému Windows 2000 Advanced Server), obecně se hardwarová pole považují za lepší řešení.

Obnovení po chybě

Počítače se spuštěnými službami vyrovnávání zatížení systému Windows 2000 Advanced Server podléhají stejným rizikům selhání jako jiné počítače. Počítače mohou selhat z mnoha různých důvodů a je-li to možné, je vždy vhodné se před těmito potenciálními body selhání nějakými prostředky bránit. Mezi takové prostředky patří softwarová a hardwarová pole RAID, zdroje nepřerušitelného napájení a protokolování a obnovení transakcí, což je funkce systému souborů NTFS. Abyste mohli tuto službu využívat, musíte nainstalovat službu vyrovnávání zatížení na oddíl naformátovaný systémem NTFS.

Pomocí protokolování a obnovení transakcí systém NTFS zaručuje, že nedojde k porušení struktury svazku, takže i po selhání systému budou všechny soubory přístupné. NTFS také používá techniku obnovení nazývanou „přemapování klastru“ (klastr se v této souvislosti míní skupina sektorů na disku – pozn. překl.). Když systém Windows 2000 Advanced Server vrátí systému NTFS chybu vadného sektoru, NTFS dynamicky nahradí diskový klastr, který obsahuje vadný sektor, a pro data vyhradí nový diskový klastr. Dojde-li k chybě během čtení, systém NTFS vrátí volajícímu programu chybu při čtení a data jsou ztracena (nejsou-li chráněna polem RAID odolným proti chybám). Dojde-li k chybě během zápisu, systém NTFS zapíše data na nový diskový klastr a k žádné ztrátě dat nedojde. Systém NTFS vloží adresu diskového klastru, který obsahuje špatný oddíl, do souboru špatných sektorů, takže se špatný oddíl již nebude opakovaně používat.

I při používání protokolování a obnovení transakcí a přemapování diskového klastru můžete ztratit uživatelská data. To může být způsobeno poruchou hardwaru, pokud nepoužíváte diskové řešení odolné proti chybám.

Testování kapacity serveru

Je velmi důležité otestovat kapacitu serveru a vyhnout se selhání serveru při zavádění vysoké dostupnosti aplikací a služeb ve vaší organizaci.

Následující seznam uvádí některé z hardwarových komponent, které byste měli otestovat:

- Jednotlivé komponenty počítačů, jako jsou pevné disky, a řadiče, procesory a paměť RAM.
- Externí komponenty, jako jsou směrovače, mosty, přepínače, kabely a konektory.

Další seznam uvádí některé ze zátěžových testů, které byste měli vykonat:

- Vysoké síťové zatížení.
- Vysoké zatížení vstupů a výstupů na jednom disku.
- Náročné používání souborových, tiskových a aplikačních serverů.
- Vysoký počet současných přihlašování.

Otestovat a vyladit výkon svých aplikací můžete pomocí sady Windows DNA Performance Kit. Tato sada vám dovoluje vyladit aplikace v systémech Windows NT 4.0 Microsoft Transaction Server (MTS), COM+, IIS a SQL Server a zvýšit výkon vyrovnávání zatížení komponent.

Sada obsahuje informace o výkonu COM+ a IIS i nástroje simulující vliv mnoha uživatelů přistupujících k vaší aplikaci IIS nebo COM+. Simulování mnoha uživatelů je důležitým krokem ve vyhodnocení hardwarových požadavků vaší aplikace.

Poznámka Sada Windows DNA Performance Kit je určena pro použití v systémech Windows 2000 Server a v systému Windows NT Server 4.0 se sadou Windows NT Option Pack.

Další informace o sadě Windows DNA Performance Kit a o tom, jak si tuto sadu stáhnout, najdete v odkazu Windows DNA Performance Kit stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Další informace o vytváření plánů testování najdete v kapitole „Vytváření testovací laboratoře systému Windows 2000“ v této knize.

Plánování strategie zálohování a obnovení klastru

Úplná záloha klastru zahrnuje:

- Dokumentaci konfigurace klastru včetně vazby klíčů registru k jednotlivým prostředkům, neboť každý klíč registru prostředku je identifikován výhradně globálně jednoznačným identifikátorem (GUID) prostředku.
- Katalog záloh.
- Zálohování a uložení médií na bezpečné místo.
- Vytvoření záchranné opravné diskety (emergency repair disc) pro každý uzel. Takovou disketu lze v případě potřeby použít k obnovení systému Windows 2000 Advanced Server na uzlu.

Záchranná opravná disketa je disketa, kterou vytváří nástroj Zálohování (Backup) a která obsahuje informace o aktuálním nastavení vašeho systému Windows. Tuto disketu lze použít k opravě počítače v případě, kdy systém nespustí nebo jsou-li poškozené či vymazané systémové soubory.

Další informace o vytváření záchranné opravné diskety najdete v nápovědě systému Windows 2000 Advanced Server.

Výše uvedená doporučení předpokládají, že jste:

- Vyvinuli a zdokumentovali postupy obnovení.
- Nahradili všechny fyzicky zničené klastry funkčně identickým hardwarem (s certifikátem HCL), přičemž všechny disky klastru mají stejnou nebo větší kapacitu.

Dobrý plán zálohování bude řešit následující problémy:

- Synchronizace zálohování
- Vytváření ukládacího prostoru pro zálohovací média.
- Ukládání zálohovacích médií
- Správa katalogu záloh

Další informace o rutinách zálohování a obnovení a nástrojích clusteringu najdete v kapitole „Clustering systému Windows“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.

Seznam úkolů plánování klastrů systému Windows 2000

Seznam úkolů plánování klastrů systému Windows 2000 v tabulce 18.3 představuje referenční seznam informací o důležitých úkolech uvedených v této kapitole, který vám může pomoci s vytvořením strategie dostupnosti aplikací a služeb vaší společnosti.

Tabulka 18.3 Seznam úkolů plánování klastrů systému Windows 2000

Úkol	Umístění v kapitole
Sestavte tým plánování clusteringu.	Určení strategií dostupnosti
Identifikujte specifické potřeby vysoké dostupnosti aplikací a služeb.	Určení strategií dostupnosti
Určete své požadavky na clustering.	Určení strategií dostupnosti
Rozhodněte, které aplikace budou používat službu Vyrovnávání zatížení sítě.	Plánování vyrovnávání zatížení sítě
Pomocí služby Vyrovnávání zatížení sítě zaveďte klastry terminálových serverů.	Plánování vyrovnávání zatížení sítě
Nakonfigurujte službu Vyrovnávání zatížení sítě pro servery se spuštěnými aplikacemi IIS/ASP a COM+.	Plánování vyrovnávání zatížení sítě
Identifikujte síťová rizika.	Plánování vyrovnávání zatížení sítě
Naplánujte kapacitu pro službu Vyrovnávání zatížení sítě.	Plánování vyrovnávání zatížení sítě
Určete požadavky na kapacitu serveru.	Plánování vyrovnávání zatížení sítě
Optimalizujte klastry služby Vyrovnávání zatížení sítě.	Plánování vyrovnávání zatížení sítě
Vyberte aplikace, které budou pracovat na serverovém klastru.	Plánování služby Cluster Service
Identifikujte síťová rizika.	Plánování služby Cluster Service
Určete zásady překlopení a překlopení zpět pro skupiny prostředků.	Plánování služby Cluster Service
Vyberte roli serveru.	Plánování služby Cluster Service
Vyberte model klastru.	Plánování služby Cluster Service
Vykonejte plánování kapacity služby Cluster Service.	Plánování služby Cluster Service
Vyberte nástroje, která vám pomohou automatizovat zavádění služby Cluster Service.	Plánování služby Cluster Service
Optimalizujte klastry.	Optimalizování klastrů
Naplánujte použití disků odolných proti chybám.	Plánování disků odolných proti chybám
Otestujte kapacitu serveru.	Testování kapacity serveru
Naplánujte strategii zálohování a obnovení.	Plánování strategie zálohování a obnovení klastru

Další zdroje

- Další informace o clusteringu v systému Windows najdete v nápovědě systému Windows 2000 Advanced Server.
- Další informace o rozhraní Clustering API systému Windows najdete v odkazu Microsoft Platform SDK stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.
- Další informace o sadě WinDNA Performance Kit najdete v odkazu WinDNA Performance Kit stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.
- Další informace o různých hardwarových konfiguracích polí RAID najdete v odkazech:
 - Microsoft Windows Hardware Compatibility List stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>;
 - Microsoft TechNet stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

KAPITOLA 19

Určení strategií správy úložišť systému Windows 2000

S novými funkcemi správy úložišť systému Microsoft Windows 2000 Server by se měli seznámit správci sítě, kteří mají na starosti každodenní síťové operace a kteří jsou seznámeni s požadavky na správu dat a systémy úložišť.

Při plánování zavedení systému Windows 2000 vám doporučujeme zahrnutí těchto nových funkcí do strategie správy úložišť. Funkce správy úložišť vám pomohou usnadnit nástroje **Správa disků** (Disk Management), **Vyměnitelné úložiště** (Removable Storage), **Vzdálené úložiště** (Remote Storage), clustering systému Windows, distribuovaný systém souborů, Služba Indexing Service a další prvky.

Tato kapitola také popisuje úvahy o výběru systému ukládání dat, strategiích zálohování a odolnosti proti chybám a způsoby, jakými lze zlepšit možnosti zotavení po havárii.

V této kapitole

Zlepšení funkcí správy úložišť 570

Správa diskových prostředků 574

Optimalizace správy dat 580

Vylepšení ochrany dat 588

Zlepšení schopností zotavení po havárii 591

Seznam úkolů plánování správy úložišť 594

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Zásady konfigurace úložišť
- Plán zotavení po havárii
- Plán správy úložišť

Související informace v sadě Resource Kit

- Další informace o použití služeb Vyměnitelné úložiště a Vzdálené úložiště najdete v kapitole „Ukládání a správa dat“ v knize *Microsoft Windows 2000 Server Správa systému*.

- Další informace o plánování zálohování, strategiích a postupech najdete v kapitolech „Zálohování“ a „Plánování spolehlivé konfigurace“ v knize *Microsoft Windows 2000 Server Správa systému*.
- Další informace o zotavení po havárii najdete v kapitole „Opravy, zotavování a obnovování“ knihy *Microsoft Windows 2000 Server Správa systému*.

Zlepšení funkcí správy úložišť

Zlepšení systémů úložišť a jejich správy není důležitým prvkem výhradně zavádění systému Microsoft Windows 2000 Server, ale také zásadní součástí každé infrastruktury podnikové sítě. Protože v podnikovém prostředí je zapotřebí chránit obrovská množství dat, musíte se seznamovat s nejnovějšími technologiemi, abyste dokázali vybrat hardware a software nejlépe vyhovující vašim potřebám.

Systém Microsoft Windows 2000 nabízí několik nástrojů správy diskových prostředků, zvýšení výkonu a ochrany dat. Mezi tyto prvky patří:

Správa disku (Disk Management) pro nastavení a organizování systémů diskových úložišť.

Vyměnitelné úložiště (Removable Storage) pro správu nové třídy zařízení ukládání dat.

Vzdálené úložiště (Remote Storage) pro přesun nepoužívaných souborů na vzdálené úložiště.

Efektivnější správy dat vám pomohou dosáhnout následující prvky systému Windows 2000:

Clustering systému Windows pro snadnější správu a vyšší dostupnost dat a aplikací.

Vylepšení systému souborů pro zlepšení výkonu, dostupnosti, zabezpečení a možnosti správy sdílených informací a prostředků včetně systému souborů NTFS a správy kvót.

Distribuovaný systém souborů (DFS) pro spojování míst sdílení do jediného oboru názvů, což zjednodušuje vyhledávání a správu dat.

Služba Indexing Service pro rychlé vyhledávání souborů podle jejich obsahu a vlastností.

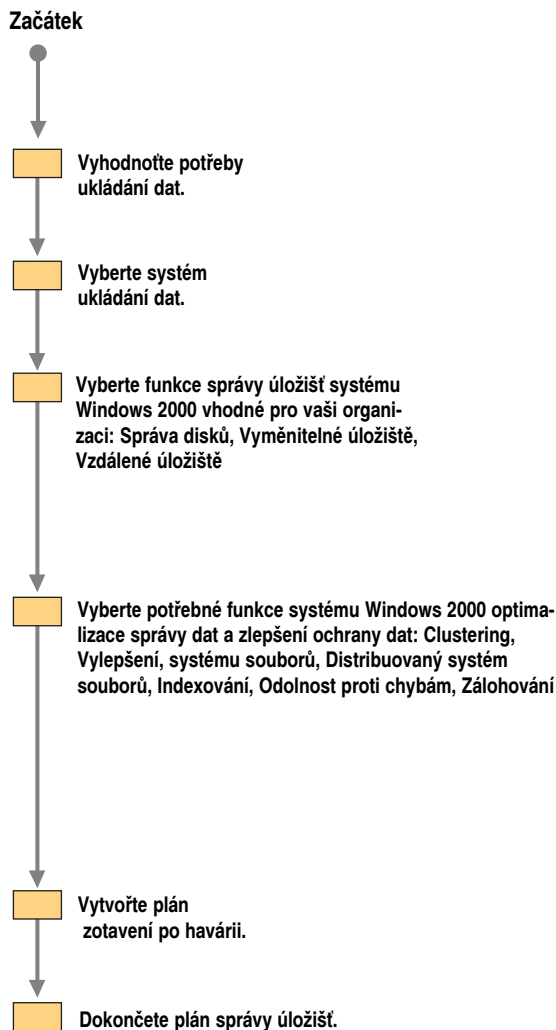
Kromě těchto prvků nabízí systém Windows 2000 funkce odolnosti proti chybám a nástroj Zálohování, které pomáhají zlepšit ochranu dat.

Následující oddíly pojednávají o uvedených prvcích podrobněji. Nejenže se musíte seznámit s funkcemi správy úložišť systému Windows 2000, ale mezi dokumenty plánování zavedení musíte zařadit také plán správy úložišť.

Vytvoření plánu správy úložišť

Během vytváření plánu správy úložišť se budete muset věnovat mnoha otázkám. Větší organizace by měly zvážit vytvoření týmu správy úložišť, který bude mít za úkol určit potřeby ukládání dat a vytvořit související plány. V případě některých organizací může být výhodnější řešit problémy uvedené v této kapitole prostřednictvím různých týmů, jako je například tým zálohování a zotavení, tým správy dat a tým řešící problémy úložišť. Každý tým začne vyhodnocením požadavků na ukládání dat vaší organizace a vytvořením strategie správy úložišť.

S vytvořením plánu správy úložišť vám může pomoci diagram uvedený na obrázku 19.1.



Obrázek 19.1 Proces vývoje strategie správy úložišť

Vyhodnocení potřeb ukládání dat

Jak se zvyšuje počet a zvětšuje velikost podnikových sítí, řešení síťového ukládání dat jsou stále dostupnější. Každá organizace má různé priority pro výběr médií a metod ukládání dat. Některé jsou omezeny náklady, jiné dávají před ostatními pohledy přednost výkonu.

Při vyhodnocování potřeb ukládání dat musíte porovnat možnost ztráty dat, produktivity a obchodu s náklady na systém ukládání dat, který zajistí vysokou spolehlivost a dostupnost dat. Před vývojem strategie správy úložišť se zamyslete nad následujícími body:

- Technologie, které jsou pro vaši organizaci z hlediska nákladů nejvýhodnější.
- Odpovídající kapacita úložišť, která může snadno růst se sítí.
- Potřeba rychlého, 24hodinového přístupu k důležitým datům.
- Zabezpečené prostředí ukládání dat.

Při hledání cenově nejvýhodnějšího řešení musíte vyvážit náklady na nákup a správu hardwaru a softwaru a následky havarijní ztráty dat. Mezi tyto náklady patří:

- Počáteční investice do hardwaru, jako jsou páskové a diskové jednotky, zajištění napájení a řadiče.
- Potřebná média, jako jsou magnetické pásky a kompaktní disky.
- Software, jako jsou nástroje správy úložišť a nástroje zálohování.
- Náklady na neustálou údržbu hardwaru a softwaru.
- Požadavky na personál.
- Školení v používání nových technologií.
- Zařízení ukládání dat, která se nacházejí mimo síťové sídlo.

Tyto náklady porovnejte s těmito položkami:

- Náklady na náhradu souborových, poštovních nebo tiskových serverů.
- Náklady na náhradu serverů spouštějících aplikace, jako je například Microsoft SQL Server nebo Microsoft Systems Management Server (SMS).
- Náklady na náhradu serverů bran se spuštěnou službou Směrování a vzdálený přístup (Routing and Remote Access), Microsoft SNA Server, Microsoft Proxy Server nebo Novell NetWare.
- Náklady na náhradu pracovních stanic osob v různých odděleních.
- Náklady na náhradu komponent jednotlivých počítačů, jako je pevný disk nebo síťová karta.

Dalším důležitým faktorem, který musíte vzít v úvahu při výběru systému ukládání dat, je rychlost zotavení dat. Ztratíte-li data na serveru, jak rychle se vám je podaří znovu zavést? Po jakou dobu může být server (nebo celá síť) mimo provoz, než to začne mít vážné dopady na vaše obchodní zájmy?

Technologie ukládání dat se velmi rychle mění, proto je před rozhodnutím o koupi zapotřebí seznámit se s relativními výhodami jednotlivých typů zařízení. Systém ukládání dat, který budete používat, musí mít více než dostatečnou kapacitu pro zálohování všech vašich nejdůležitějších dat. Měl by také během operací zálohování a obnovování zaručovat detekci chyb a potřebné korekce.

Výběr systému ukládání dat

Systém ukládání dat, který bude nejlépe odpovídat vašim požadavkům, určíte zodpovězením následujících otázek:

Jaké množství dat musíte v současné době ukládat?

Musíte-li ukládat velmi velké množství dat, asi pro vás bude nejlepší volbou systém ukládání na pásky. Náklady na média na megabajt jsou v případě pásky významně menší než u všech ostatních typů médií ukládání dat.

Jaké jsou vaše projektované potřeby ukládání dat?

Potřeby na ukládání dat se v mnoha organizacích každý rok zdvojnásobují. Zamyslete se nad koupí většího systému pro ukládání dat, než v současné době potřebujete k uspokojení požadavků, nebo koupí škálovatelného systému, který lze rozšiřovat podle potřeb. Chcete-li vyhodnotit, nakolik může tento faktor ovlivnit vaši situaci, porovnejte nároky na ukládání dat před několika lety se současnými úrovněmi a zjištěný nárůst použijte pro odhad svých budoucích potřeb.

Kolik uživatelů nebo aplikací současně přistupuje k systému ukládání dat?

Většina prodejců nabízí systémy s více jednotkami, které umožňují přístup k několika jednotkám najednou. Pak může k systému přistupovat více uživatelů nebo aplikací najednou, aniž by to mělo dopad na výkon.

Jak důležitý je čas přístupu k datům?

Je-li vaše knihovna určena převážně pro přístup k datům používaným v reálném čase, pak je právě toto vaším nejdůležitějším problémem. Řešení vycházející z použití disků CD-ROM je nejlepší v případech, kdy je doba přístupu vaším hlavním problémem, protože schopnost náhodného přístupu k datům na discích CD-ROM omezuje čas hledání na minimum. Doba přístupu k datům má dvě části: dobu hledání a rychlost přenosu. Nevýhody tohoto řešení spočívají v rychlosti a nákladech: rychlost přenosu dat může být nižší než u páskových systémů, pokud tedy nejsou použity nejnovější vysokorychlostní jednotky, a také náklady na megabajt jsou vyšší než u páskových médií.

Jak důležitá je rychlost přenosu dat?

Používáte-li systém ukládání dat převážně pro archivování a zálohování dat, pak bude vaším nejdůležitějším problémem rychlost přenosu dat. Je-li to váš případ, pak řešení vycházející z pásky může být nejlepší, protože rychlost přenosu dat na páskových jednotkách je téměř desetinásobkem rychlosti jednotek disků CD-ROM. Páskové systémy také představují menší náklady na megabajt. Nevýhodou pásky je doba přístupu k souborům, která se pohybuje až v minutách, jelikož přístup k souborům je lineární.

Jaký je váš rozpočet?

Znovu platí, že než určíte, kolik peněz si můžete dovolit utratit, zvažte také potenciální náklady při ztrátě nebo poškození dat a dobu výpadku, způsobeného problémy s nespolehlivým hardwarem. Jsou-li ukládaná data pro vaši organizaci velmi důležitá, tato rizika nemusí mít cenu úspor dosažených koupí laciného řešení.

Také se zamyslete nad celkovými náklady. Koupě určitého hardwaru může být relativně laciná, ale cena za megabajt pak docela vysoká. To platí především u systémů s disky CD-ROM. Je také obvyklé, že časem se spotřebuje více peněz za média než za prvotní hardware.

Při výběru systému ukládání dat vám pomůže, když si vytvoříte dva nebo více modelů představujících různá hardwarová a softwarová řešení pro různé stupně kapacity úložiště a ochrany dat. Nezapomeňte projektovat také plánovaný růst.

Tabulka 19.1 ukazuje *relativní* schopnosti možných hardwarových a softwarových řešení ukládání dat: hodnota 5 znamená nejlepší dostupné řešení a hodnota 1 představuje nejméně vhodné řešení. Tabulka vám pomůže určit typy úložišť pro vaši organizaci.

Tabulka 19.1 Vybraná hardwarová a softwarová řešení úložišť

Řešení	Dostup- nost	Doba reakce	Kapacita	Podpora více uživatelů
CD-ROM/DVD-ROM	4	3	2–3	2
Knihovna CD-ROM	4	2	5	5
Pole jednotek CD-ROM	5	4	4	4
DFS	5	3–4	5	5
Disky	3	4	3	3
Zrcadlení disků se dvěma řadiči (Duplex)	5	4	2–3	2
Sada prokládaných disků	1	5	4	4
Sada prokládaných disků s paritou	4	3	3–4	4
Pásky	3	2	4	1
Knihovna pásků	3	1	5	4

Po sestavení týmu správy úložišť, identifikaci požadavků na ukládání dat a určení rozpočtu musíte vyhodnotit možnosti ukládání dat systému Windows 2000.

Správa diskových prostředků

Systém Windows 2000 nabízí několik funkcí ukládání dat, které vám pomohou s ukládáním a správou dat. Patří sem Správa disků (Disk Management), Vyměnitelné úložiště (Removable Storage) a Vzdálené úložiště (Remote Storage). Následující pododdíly představují úvod do těchto funkcí.

Správa disků

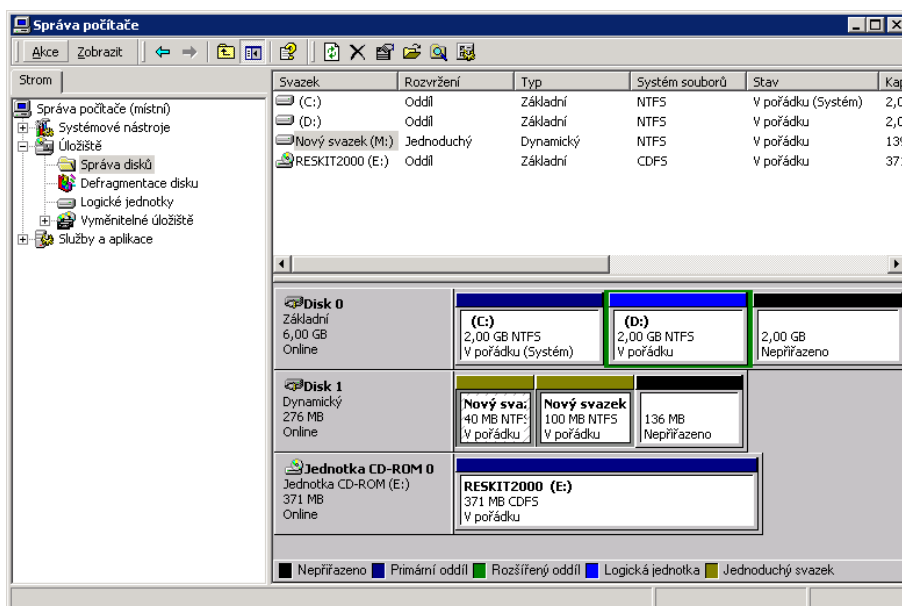
Modul snap-in Správa disků (Disk Management) konzole Microsoft Management Console (MMC) je nástrojem správy systémů ukládání dat. S vytvářením oddílů nebo svazků a inicializací nebo inovováním disků vám pomáhají průvodci. Mezi nové klíčové funkce správy disků systému Windows 2000 Server patří:

Online správa disků Většinu úloh správy lze vykonat bez vypnutí systému či přerušení práce uživatelů. Bez restartování systému tak lze například vytvářet různá rozvržení oddílů a vybírat strategie ochrany, jako je zrcadlení a prokládání. Také je možné bez restartování přidávat disky. Většina změn konfigurace začne platit okamžitě.

Vzdálená správa disků Jako správce můžete spravovat libovolný vzdálený (nebo místní) počítač se spuštěným systémem Windows 2000.

Obrázek 19.2 zachycuje jednu z kombinací možností nabídky Zobrazit (View), které lze používat v modulu Správa disků (Disk Management).

(soubor 19-02.bmp v adresáři \obrá)



Obrázek 19.2 Modul Správa disků (Disk Management) konzoly MMC

Základní a dynamická úložiště

V systému Windows 2000 existují dva typy diskových úložišť: základní a dynamické. *Základní úložiště* podporuje disky s oddíly. Základní disk může obsahovat primární oddíly, rozšířené oddíly a logické jednotky. Základní disky mohou také obsahovat rozložené svazky (sady svazků), zrcadlené svazky (sady zrcadlení), prokládané svazky (sady stripe set) a redundantní pole nezávislých disků nebo svazky RAID-5. V systému Microsoft Windows NT verze 4.0 a dřívějších se pole RAID-5 označovaly za sady stripe set (prokládání) s paritou. Chcete-li, aby mohly počítače přistupovat k takovým svazkům, a je-li na daných počítačích spuštěn systém Windows NT 4.0 či dřívější, Microsoft Windows 98 či dřívější nebo Microsoft MS-DOS, musíte vytvořit základní svazky.

Dynamická úložiště podporují disky orientované na svazky, což je nová funkce systému Windows 2000. Překonávají omezení organizování disků orientovaných na oddíly a umožňují vytváření vícediskových systémů odolných proti chybám. Pomocí dynamického úložiště lze zadávat správu disku a svazku bez potřeby restartování operačního systému. Na dynamickém disku je úložiště rozděleno do svazků a nikoli do oddílů. Svazek se skládá z části nebo částí jednoho nebo více fyzických disků v libovolném z následujících rozvržení: jednoduchý, rozložený, zrcadlený a prokládaný svazek a svazek RAID-5. Dynamické disky nemohou obsahovat oddíly nebo logické jednotky a nelze k nim přistupovat systémy MS-DOS nebo Microsoft Windows 98 a dřívějšími verzemi. Použijete-li více disků, můžete pomocí dynamického úložiště vytvořit systém odolný proti chybám.

Když připojíte k počítači nový disk, musíte jej nejprve inicializovat a pak teprve můžete vytvářet svazky nebo oddíly. Během inicializace disku vyberte dynamické úložiště, chcete-li vytvořit na disku jednoduché svazky nebo plánujete-li sdílet disk s jinými di-

sky a vytvářet tak rozložený, prokládaný nebo zrcadlený svazek nebo svazek RAID-5. Základní úložiště vyberte, chcete-li na disku vytvářet oddíly a logické jednotky.

Tabulka 19.2 ukazuje úlohy, které lze vykonat na základních a dynamických discích pomocí Správy disků.

Tabulka 19.2 Úlohy pro základní a dynamické disky

Úloha	Základní disk	Dynamický disk
Vytváření a odstraňování primárních a rozšířených oddílů.	X	
Vytváření a odstraňování logických jednotek v rozšířených oddílech.	X	
Formátování a vytváření jmenovek oddílů a jeho označení za aktivní.	X	
Odstraňování sady svazků.	X	
Odstraňování zrcadla ze sady zrcadlení.	X	
Opravování sady zrcadlení.	X	
Opravování sady prokládání (stripe set) s paritou.	X	
Inovování základního disku na dynamický disk.	X	
Vytváření a odstraňování jednoduchých, rozložených, prokládaných a zrcadlených svazků a svazků RAID-5.		X
Rozšiřování svazku přes jeden nebo více disků.		X
Přidávání zrcadlení nebo odstraňování zrcadlení ze zrcadleného svazku.		X
Opravování zrcadleného svazku.		X
Opravování svazku RAID-5.		X
Prověřování informací o discích, jako je kapacita, dostupný volný prostor a aktuální stav.		X
Zobrazování informací o svazku a oddílu, jako je velikost.	X	X
Vytváření a změna přiřazení písmen svazkům pevných disků nebo oddílům a zařízením CD-ROM.	X	X
Vytváření bodů připojení svazku.	X	X
Nastavování a kontrola sdílení disku a uspořádání přístupu ke svazku nebo oddílu.	X	X

Správa svazku

Systém Windows 2000 představuje významné vylepšení architektury správy svazků. Správa svazků zahrnuje procesy vytváření, odstraňování, změny a údržby svazků úložišť v systému. Nová architektura zlepšuje možnosti správy a obnovování svazků v podnikovém prostředí.

Do této architektury byl začleněn nástroj Správce logických disků (Logical Disk Manager – LDM), aby rozšířil funkci odolnosti proti chybám, vylepšil obnovení systému, obsáhl informace o svazku v zájmu jednoduchého přesouvání disků a zajistil zlepšení funkce správy. Tato služba je zodpovědná za vytváření a odstraňování svazků, funkce odolnosti proti chybám (RAID) a sledování svazků. Ke správě místních a vzdálených svazků se používá modul snap-in Správa disků (Disk Management).

Správa svazku zahrnuje následující funkce:

- Lze vytvářet libovolný počet svazků ve volném prostoru fyzického pevného disku nebo vytvářet svazky zasahující přes dva nebo více disků.
- Každý svazek na disku může mít jiný systém souborů, jako je například systém s alokační tabulkou souborů (FAT) nebo systém souborů NTFS.
- Většina změn na disku se projeví okamžitě. Aby došlo k zavedení změn, nemusíte opouštět Správce disků, změny ukládat nebo počítač restartovat.

Body připojení svazku

Jako součást Správce disků (Disk Management) můžete vytvářet body připojení svazku. Body připojení svazku vám umožňují rychle převádět data online a offline. Jedná se o objekty systému souborů v interním oboru názvů systému Windows 2000, které představují svazky úložišť. Když umístíte bod připojení svazku do prázdného adresáře NTFS, můžete do oboru názvů „naroubovat“ nové svazky, aniž by byla nutná další písmena jednotek. Příkladem možného použití bodů připojení svazků je, když máte počítač s jedinou jednotkou a svazkem naformátovaným jako C, k němuž připojujete další disk jako C:\Hry.

Mezi možná použití bodů připojení svazků patří:

Zajištění dalšího prostoru pro programy Můžete disk připojovat třeba jako C:\Program Files. Když pak potřebujete další diskový prostor, přidáte do systému disk a pomocí rozložení je spojíte s diskem na C:\Program Files.

Vytvoření různých tříd úložišť Vytvořte třeba sadu prokládání s vysokým výkonem, kterou připojte jako C:\Návrhy, a vytvořte jinou zrcadlenou sadu s vysokou robustností, kterou připojte jako C:\Projekty. Uživatelé normálně uvidí adresáře, adresář Návrhy však bude velmi rychlý a adresář Projekty bude chráněn sadou zrcadlení.

Vytvoření více bodů připojení pro svazek Svazek může být například připojen jako C:\Hry a C:\Projekty. Dávejte si však pozor na to, že v oboru názvů nic nebrání cyklům. Připojte-li svazek jako D a zároveň jako D:\Dokumenty, pak vytvořte v oboru názvů cyklus, protože jednotka D je připojena sama pod sebou. Aplikace vykonávající výčty se na takovém svazku dostanou do nekonečné smyčky.

Body připojení svazků jsou odolné proti změnám systému, ke kterým dochází při přidání hardwarových zařízení do počítače nebo jejich odstranění. Nyní už nejste u svazků, které můžete vytvářet, omezení na počet písmen jednotek.

Defragmentace disku

Dalším prvkem Správce disků je Defragmentace disku (Disk Defragmenter). Tento nástroj lze použít k lokalizování souborů a složek, které jsou fragmentované, a ke změně organizace klastrů na logickém diskovém svazku. Nástroj Defragmentace disku uspořádává klastry tak, aby byly soubory, adresáře a volný prostor fyzicky spojitější. Výsledkem je výkonnější přístup systému k souborům a složkám a rychlejší ukládání nových položek. Dosáhnete-li vysoké fragmentace, nástroj Defragmentace disku může celkový výkon vašeho systému z hlediska vstupů a výstupů disku výrazně zvýšit.

Funkce Defragmentace disku rozhoduje o tom, kde by se měly soubory na disku nacházet, vlastní klastry však přesunuje systém NTFS a FAT.

Tento nástroj lze používat na diskových svazcích naformátovaných systémy FAT16, FAT32 a NTFS.

Úvahy o použití dynamického úložiště

Při vytváření svazků zvažte také následující body:

- Dynamické úložiště používá k uspořádání disku schéma orientované na svazky. Systém Windows NT Server není kompatibilní s dynamickými disky.
- Při inovaci na systém Windows 2000 Server lze ke konfiguraci diskového prostoru použít instalační program systému.

Poznámka Nové svazky a oddíly lze vytvářet na nepřirazených částech disku bez ztráty dat na existujících svazcích. Plánujete-li však změnu topologie svazku, musíte si všechna data zálohovat, protože změny existujících svazků mažou všechna existující data.

- Interní pevný disk nového počítače lze konfigurovat během počáteční instalace, když nainstalujete software operačního systému Windows 2000 Server. Změny disku po instalaci se zadávají prostřednictvím Správy disků.

Další informace o správě disků najdete v kapitolách „Koncepce disků a odstraňování problémů“ a „Ukládání a správa dat“ knihy *Microsoft Windows 2000 Server Správa systému*.

Vyměnitelné úložiště

Služba Vyměnitelné úložiště (Removable Storage) je nová technologie, která umožňuje více aplikacím sdílet místní knihovny a páskové a diskové jednotky a zajišťuje tak lepší funkci správy úložiště. Pomocí služby Vyměnitelné úložiště můžete používat samostatné zařízení ukládání dat, spravovat online knihovny médií a automatické měniče a sledovat vyměnitelné pásky a disky. Samostatná zařízení zahrnují CD-ROM, DVD-ROM, pásky (4 mm, DLT, 8 mm a další) a vysokokapacitní diskové jednotky.

Služba Vyměnitelné úložiště také řídí vyměnitelná média v systému s jediným serverem. Navíc vykonává funkce ve spojení se službami Zálohování a Vzdálené úložiště. Klíčovým aspektem služby Vyměnitelné úložiště je schopnost aplikací vytvářet fondy médií, které daná aplikace vlastní a používá.

Zařízení ukládání dat jsou často připojena k systémům pomocí adaptérů rozhraní SCSI nebo rozhraní IDE, která se používají také ve většině pevných disků. Stále častěji se používají nové technologie zajišťující jednodušší užití a vyšší výkon, jako jsou Fiber Channel, IEEE 1394 a Intelligent I/O (I2O). Samostatná zařízení se obvykle používají v systémech s jediným uživatelem.

Knihovny obsahují více jednotek CD-ROM, DVD-ROM, magnetooptických (MO) disků nebo pásků. Jejich součástí jsou automatické ovládací prvky, které zajišťují rozsáhlou automatizaci správy jednotlivých médií nebo úložiště. Kapacity sahají od malých, třídiskových automatických měničů CD-ROM až po páskové a diskové knihovny používané ve spojení se sofistikovanými aplikacemi ve velkých korporacích. Knihovny se nejčastěji používají ve spojení se servery, ale stále častěji se připojují také k jednorázovému systémům.

Mezi úlohy, které lze vykonat pomocí služby Vyměnitelné úložiště, patří:

- Sledování médií, které jsou online a offline
- Připojování a odpojování médií
- Vkládání médií do knihovny a jejich vyjímání

- Zobrazování stavu médií a knihoven
- Vytváření fondů médií a nastavování jejich vlastností
- Zadávání parametrů zabezpečení médií a fondů médií
- Vykánávání inventářů knihoven

Poznámka Aby bylo možné využívat tyto funkce, musí být váš zálohovací software kompatibilní se službou Vyměnitelné úložiště.

Vzdálené úložiště

Vzdálené úložiště (Remote Storage) je systém hierarchické správy úložišť systému Windows 2000 Server. V rámci služby Vzdálené úložiště (Remote Storage) používáte k přesunování nepoužívaných souborů do knihovny pásků modul snap-in Správa vzdáleného úložiště (Remote Storage Manager) konzoly MMC. Pravidelnou migrací souborů lze zvýšit množství volného prostoru na disku. Z hlediska uživatele zůstávají migrované soubory aktivní, ale přístup k nim trvá déle.

Hierarchie úložiště má dvě úrovně. Vyšší úroveň se označuje za místní úložiště a je tvořena místními svazky NTFS počítače se spuštěnou službou Vzdálené úložiště na serveru systému Windows 2000. Místní diskové svazky, které řídí služba Vzdálené úložiště, se nazývají *spravované svazky*.

Nižší úroveň hierarchie úložiště, která se označuje za vzdálené úložiště, ukládá data zkopírovaná z místního úložiště do online knihovny nebo jiného zařízení ukládání dat.

Jakmile množství volného prostoru na místním svazku klesne pod potřebnou úroveň, služba Vzdálené úložiště odstraní data místních souborů, která byla již dříve zkopírována na vzdálené úložiště, a poskytne tak další volný diskový prostor. Po přesunu dat zůstane na místě zástupný symbol souboru, který umožní přístup k danému souboru. Služba Vzdálené úložiště spravuje přesun dat podle principů zadaných správcem pro jednotlivé svazky místních úložišť. Můžete určit časový plán přesunu souborů z určitých svazků a nastavit kritéria a pravidla pro soubory, které se mají přesunout. Přesněji řečeno, můžete:

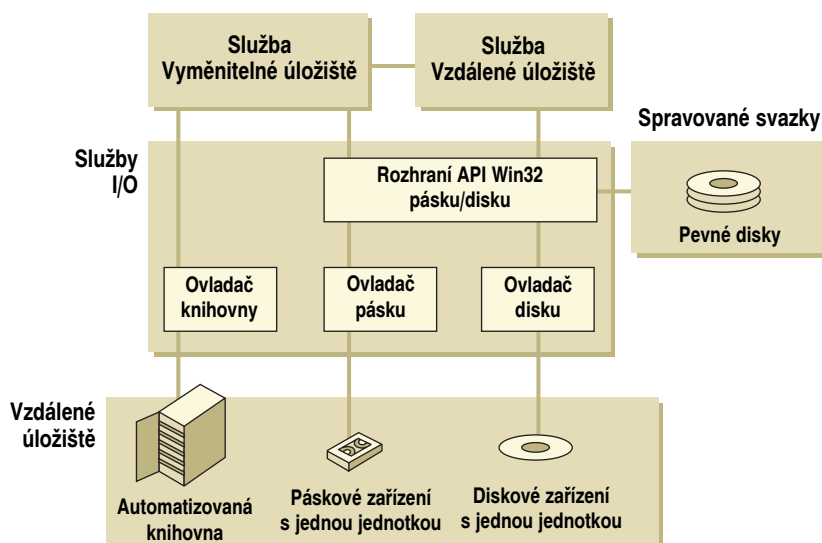
- přiřazovat a konfigurovat zařízení a média vzdálených úložišť;
- nastavovat možnosti funkcí služby Vzdálené úložiště platné v celém systému;
- konfigurovat nastavení správy svazků pro svazky spravované službou Vzdálené úložiště;
- zobrazovat si informace o činnostech služby Vzdálené úložiště;
- obnovovat data po haváriích médií;
- vytvářet a předávat úlohy.

Protože vyměnitelné pásky v knihovně jsou z hlediska ceny za megabajt dat lacinější než pevné disky, je to ekonomický způsob zajištění jak maximálního prostoru pro data tak i optimálního výkonu místních disků.

Poznámka Váš antivirový a zálohovací software musí být kompatibilní se službou Vzdálené úložiště. Správci musí před aktivováním služby Vzdálené úložiště zajistit vykonání celosvazkových souborových operací, aby nebylo nutné všechna data vracet zpět na disk. Zálohování čte data přímo z pásky.

Vztah mezi službou Vzdálené úložiště a službou Vyměnitelné úložiště

Služba Vzdálené úložiště používá ke kopírování dat na online knihovny obsahující vyměnitelná média službu Vyměnitelné úložiště. Přehled vztahu těchto systémů ukládání dat a různých zařízení ukládání dat zobrazuje obrázek 19.3.



Obrázek 19.3 Vztah mezi službami Vzdálené úložiště a Vyměnitelné úložiště a zařízeními ukládání dat

Úvahy o použití služby Vzdálené úložiště

Použití služby Vzdálené úložiště nabízí následující výhody:

- Virtuální rozšiřování místního prostoru pro ukládání prostřednictvím levnějšího vzdáleného úložiště.
- Transparentní automatický přístup k datům ve vzdáleném úložišti.
- Automatizace časově náročné práce související s denními ručními operacemi správy dat.
- Centralizované sdílení vzdáleného úložiště pro více svazků.

Služba Vzdálené úložiště není náhradou zálohování, protože vždy existuje jen jedna instance dat. Je důležité svazek pravidelně zálohovat. Nástroj Zálohování je integrován se službou Vzdálené úložiště, takže nemusíte přesunovat vše zpět na disk; zálohování čte data přímo z pásky.

Optimalizace správy dat

Mezi funkce systému Windows 2000, které vám mohou pomoci s efektivnější správou dat v podnikovém prostředí, patří:

- clustering systému Windows;
- systém souborů NTFS;

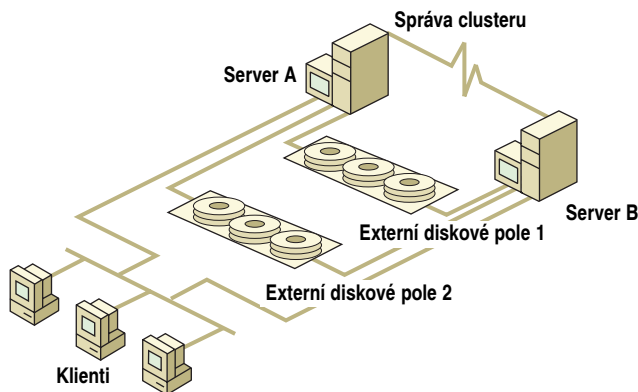
- správa kvót;
- distribuovaný systém souborů (DFS);
- služba Indexing Service.

Clustering systému Windows

Potřebujete-li dosáhnout větší dostupnosti a zjednodušené správy, zvažte ve své strategii ukládání dat na podnikové síti použití clusteringu. Clustering omezuje doby výpadků, protože poskytuje architekturu zajišťující fungování systému i v případě selhání jednoho serveru.

Pomocí clusteringu systému Windows můžete spojit dva nebo více serverů, které tak vytvoří klastr serverů spolupracujících jako jediný systém. Každý server se označuje za uzel a každý uzel může fungovat nezávisle na jiných uzlech v klastru. Podpora klastrů zabudovaná do systému Windows 2000 vychází z otevřených specifikací, standardního hardwaru a požadavků na jednoduchost použití.

Každý uzel má svou vlastní paměť, systémový disk, operační systém a podmnožinu prostředků klastru. Jestliže dojde k selhání jednoho uzlu, pak prostřednictvím procesu označovaného za překlopení druhý uzel převezme vlastnictví prostředků porouchaného uzlu. Server klastru zaregistruje síťovou adresu prostředku na novém uzlu a provoz klientů bude přeměrován na dostupný systém, jenž daný prostředek nyní vlastní. Když se porouchaný prostředek později opět vrátí do režimu online, můžete příslušným nastavením zajistit další přerozdělení prostředků serveru klastru a požadavků klientů. Standardní nastavení klastru systému Windows 2000 ukazuje obrázek 19.4.



Obrázek 19.4 Typické uspořádání klastru se dvěma uzly

Služba Cluster Service má následující výhody:

Společná správa Pomocí modulu snap-in Správce klastru (Cluster Administrator) konzoly MMC lze spravovat klastr jako jediný systém. Také klienti pracují s klastrem, jako by šlo o jediný server.

Vyrovňování zatížení V rámci klastru lze ručně vyrovňovat zatížení nebo odpojovat servery při plánované údržbě, aniž by došlo k převedení dat a aplikací do režimu offline.

Vysoká dostupnost Clustering zajišťuje vysokou dostupnost tím, že automaticky zotavuje důležitá data a aplikace z mnoha obvyklých typů selhání. Dojde-li k selhání uzlu v klastru, clustering systému Windows selhání detekuje a vykoná zotavení procesů, které byly v době selhání aktivní. Selhání uzlu v klastru nemá vliv na druhý uzel.

Není-li clustering ještě součástí vaší sítě a vy jej chcete začít používat, musíte v rámci fáze plánování zavedení systému Windows 2000 Server vyřešit několik problémů souvisejících s vytvořením prostředí s klastry. Další informace o plánování prostředí s klastry najdete v kapitole „Clustering systému Windows“ v knize *Microsoft Windows 2000 Server Distribuované systémy* a také v nápovědě systému Windows 2000 Advanced Server.

Poznámka V řešeních s klastry používejte výhradně certifikované konfigurace, které jsou dokumentovány v seznamu kompatibilního hardwaru (HCL), k němuž můžete přistoupit také online. Další informace o tomto seznamu najdete v odkazu Microsoft Windows Hardware Compatibility List stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Úvahy o použití klastrů ve strategii ukládání dat

Zamyslete se nad následujícími výhodami zahrnutí prostředí s klastry do plánování úložišť:

- Clustering zajišťuje vysokou dostupnost, aniž by bylo nutné data replikovat, a proto zaručuje konzistentnost dat bez velkého dopadu na požadavky na úložiště a objemy síťového provozu.
- Clustering zajišťuje možnost jednoduchého zotavení ze softwarových selhání.
- Servery sdílejí diskové pole s více porty. Hardwarové řadiče RAID zaručují nejlepší výkon externích diskových polí.
- Clustering zajišťuje vysokou dostupnost dat, nechrání však integritu dat.

Vylepšení systému souborů

Systém Windows 2000 podporuje systém souborů NTFS a dva systémy souborů s alokačními tabulkami (FAT): FAT16 a FAT32.

Systém FAT je určen pro menší disky s jednoduchou strukturou složek. FAT16 je součástí systému Windows 2000 proto, aby byla možná inovace dřívějších verzí produktů kompatibilních se systémem Windows, a navíc je kompatibilní s většinou operačních systémů nepocházejících od společnosti Microsoft. FAT32 podporuje svazky větší, než dokáže zpracovávat systém FAT16, a poprvé se objevil v Microsoft Windows 95. Systém Windows 2000 podporuje systémy souborů FAT32.

NTFS

Verze NTFS používaná v systému Windows 2000 zajišťuje výkon, spolehlivost a další funkce, které nejsou v systémech souborů FAT k dispozici. Datové struktury NTFS vám umožňují využívat nové funkce systému Windows 2000, jako je adresářová služba Microsoft Active Directory, změna a správa konfigurace, body změny zpracování (spojování adresářů a body připojení svazků), podporu řídice používaných souborů, identifikátory objektů, rozšířené atributy vlastností, deník změn a mnoho nových vylepšení ukládání dat.

V systému Windows 2000 byly datové struktury NTFS inovovány tak, aby umožnily zavedení mnoha nových prvků. U existujících svazků NTFS dochází k inovaci na novou verzi NTFS během instalace systému Windows 2000. Do tohoto formátu lze také kdykoli převést svazky FAT16 a FAT32.

Jestliže naformátujete oddíly systému Windows NT pomocí NTFS a nikoli FAT, budete moci používat prvky zotavení a komprese, které jsou dostupné pouze v systému NTFS. Zároveň tím dosáhnete vyšší rychlosti přístupu a další možnosti zabezpečení souborů a složek.

Důležité Verzi systému NTFS používanou ve Windows 2000 dřívější verze nativně nerozpoznají. V systémech duálního spouštění, kde potřebuje instalace systému Windows NT 4.0 číst ze svazku NTFS, který byl vytvořen systémem Windows 2000 nebo jím byl inovován, vyžaduje instalace systému Windows NT 4.0 dodatečnou podporu (Service Pack 4 nebo novější).

Správa kvót

Diskové kvóty jsou novou funkcí verze systému NTFS používané ve Windows 2000. Diskové kvóty zajišťují přesnější řízení síťových úložišť. Diskové kvóty lze používat ke sledování a omezování diskového prostoru jednotlivých uživatelů na svazcích.

Když se poprvé uživatelé pokusí uložit data na nějaký svazek, automaticky se přidají do tabulky kvót a přiřadí se jim výchozí hodnota kvóty. To znamená, že správce nemusí zadávat nastavení kvóty pro každého uživatele.

Uživatelům se započítávají soubory, které vlastní. Složka každého uživatele na \\Marketing\Veřejný může být například omezena na 5 megabajtů (MB) diskového prostoru. Jestliže uživatelé zkopírují do své složky 5 MB souborů, nemohou do této ani do žádné jiné složky na \\Marketing\Veřejný kopírovat další soubory ani je zde vytvářet. Mohou však soubory přesunovat a odstraňovat. Uživatelům se nezapočítává žádný dodatečný diskový prostor, jestliže upraví existující soubor, který vlastní někdo jiný. Pamatujte však, že některé aplikace, například Microsoft Office, mění vlastníka dokumentu na uživatele, který jej naposledy upravoval. Nastavení kvót jsou mezi svazky nezávislé. To znamená, že kvóta na jednotce C nemá vliv na kvótu na jednotce D.

Funkci kvót modulu snap-in Správce disku (Disk Management) konzoly MMC lze používat k:

- povolení nebo zákazu kvót na diskovém svazku;
- zabránění uživatelům v používání více prostoru, než určuje maximum jejich kvóty;
- zobrazování informací o kvótách jednotlivých uživatelů svazku;
- nastavení výchozího prahu varování kvóty a maxima kvóty pro nové uživatele svazku;
- blokování vyhrazování dalšího diskového prostoru a protokolování události překročení zadaného diskového prostoru uživatelem; uživatelé mohou číst, odstraňovat a upravovat soubory za předpokladu, že se nepokusí vyhradit si více diskového prostoru.

Můžete nastavovat jak hranice kvóty tak i její maximum. Po povolení používání kvót lze nastavit dvě hodnoty:

Maximální kvóta Určuje maximální množství diskového prostoru, které může uživatel využít.

Hranice varování kvóty Určuje hodnotu, při které je správce upozorněn na to, že se blíží dosažení maximální hodnoty kvóty. Jedná se o formu zprávy události.

Jako správce můžete určit, aby se automaticky protokolovaly události překročení hranice varování a maxima kvóty uživateli. Maximum diskové kvóty uživatele tak můžete nastavit například na 50 MB a hranici varování kvóty na hodnotu 45 MB. Uloží-li si uživatel na svazek více než 45 MB souborů, systém kvót zaprotokoluje systémovou událost.

Máte také možnost odepřít diskový prostor uživatelům, kteří se pokusí překročit maximum své kvóty. Vyberete-li tuto možnost, uživatelé nemohou na svazek zapisovat další data, dokud neodstraní nebo nepřesunou některé z existujících souborů ze svazku. Pokusí-li se uživatel vyhradit si více prostoru než určuje maximum kvóty, systém NTFS zobrazí chybovou zprávu „nedostatek místa na disku“.

Systém Windows 2000 obsahuje podporu diskových kvót pro tyto prvky:

- Zásady pro rozsáhlou vzdálenou správu diskových kvót.
- Vylepšená podpora vyhledávání všech souborů vlastněných určitým uživatelem.

Poznámka Systém Windows 2000 Server podporuje diskové kvóty pouze na svazcích naformátovaných jako NTFS.

Při vytváření své strategie správy úložišť si uvědomte následující výhody používání diskových kvót:

- Sledování používání diskového prostoru na jednotlivých svazcích jednotlivými uživateli umožňuje lepší plánování diskových prostředků.
- Omezení diskového prostoru vám umožňuje spravovat prostředky ukládání dat efektivněji, protože budete uživatele nutit pravidelně odstraňovat nepotřebné soubory.
- Použití diskových kvót může představovat efektivní způsob snížení nákladů na zálohovací média a snížení časů obnovení.

Distribuovaný systém souborů

Distribuovaný systém souborů (DFS) společnosti Microsoft je software programu Windows 2000 Server, který usnadňuje vyhledávání a správu dat na podnikové síti. DFS zajišťuje připojování (mapování) a jednotnou pojmenovávací konvenci pro kolekce serverů, míst sdílení a souborů. DFS navíc přidává možnost uspořádání souborových serverů a jejich míst sdílení do logické hierarchie, což výrazně zjednodušuje správu a používání informačních prostředků.

Prostřednictvím DFS můžete vytvořit jediný strom adresářů, který bude zahrnovat více serverů a míst sdílení souborů ve skupině, v oddělení nebo v celém podniku. Kořenový adresář systému DFS a svazky DFS může hostit libovolný server se systémem Windows 2000. Kořenový adresář systému DFS je místní místo sdílení, které slouží jako počáteční bod a hostitel pro ostatní místa sdílení. Síť může hostit mnoho jednotlivých svazků DFS, přičemž každý svazek bude mít jiný název. Topologie DFS je jediným oborem názvů systému Domain Name System (DNS). K distribuci sdílených prostředků vaší organizace můžete použít jedinou topologii nebo více topologií DFS.

Funkce DFS jsou integrovány do adresářové služby Active Directory; topologie DFS se publikuje do Active Directory. Protože změny doménové topologie DFS se automaticky synchronizují se službou Active Directory, lze vždy, když kořenový adresář DFS

z nějakého důvodu přejde do režimu offline, obnovit topologii DFS. Systémy DFS používané na samostatných počítačích si ukládají topologii do registru.

Systém DFS má následující funkce:

- Nabízí zjednodušené zobrazení sdílených síťových prostředků, které může správce upravit.
- Umožňuje klientům systémů Microsoft Windows 95 a Windows 98 přistupovat ke sdíleným položkám pomocí protokolu SMB.
- Podporuje připojování replik sdílených síťových položek v zájmu vyrovnavání zatížení a lepší dostupnosti dat.

Služba Active Directory použití sítě dále optimalizuje tím, že přesměrovává klienty, kteří tuto službu podporují, na bod sdílení DFS v síťovém sídle klienta.

- Integruje službu Replikace souborů (File Replication – FRS) a umožňuje tak volitelnou replikaci čtení/zápisu dat mezi více místy sdílení.
- Umožňuje uživatelům přihlásit se pouze jednou a pak přistupovat k více prostředkům.

Ke svazku DFS lze přistoupit pomocí názvu jednotné pojmenovávací konvence (UNC). Je sice možné používat názvy UNC, většinou však bude pro uživatele jednodušší použít písmeno jednotky. Všimněte si například fyzických umístění ve vztahu k logickým cestám, jak je uvedeno v tabulce 19.3.

Tabulka 19.3 přístup ke svazku DFS

Logická cesta DFS	Fyzické umístění	Popis	Cesta k připojené jednotce
\\MS Server\Root	\\MS Server\Root	Kořen sdílení	X
\\MS Server\Root\Uživatelé	\\MS Uživatelé1\Zaměstnanci	Spojení do adresářů zaměstnanců	X:\Uživatelé
\\MS Server\Root\Soukromé\JanaD	\\Právní\Data\JanaD	Spojení na počítač Jany D.	X:\Soukromé\JanaD
\\MS Server\Root\Soukromé\ZuzanaV	\\Lidské zdroje\ZuzanaV	Spojení na počítač Zuzany V.	X:\Soukromé\ZuzanaV

Protože DFS připojuje fyzické úložiště do logického obrazu, fyzické umístění dat se pro uživatele a data stane transparentním. Systém DFS eliminuje nutnost, aby uživatelé přesně věděli, kde je informace fyzicky uložena. Protože uživatelé nemusí znát název serveru nebo místa sdílení, můžete fyzicky přesunout informace uživatelů na jiný server, aniž by se museli uživatelé znovu seznámit s tím, kde najdou svá data. To zlepšuje možnosti správy souborů.

Úvahy o použití systému DFS ve strategii ukládání dat

Jako součást plánování úložišť zvažte následující výhody použití míst sdílení DFS:

- Active Directory replikuje topologie DFS všech doménových topologií DFS na každý server kořenového adresáře DFS. Tím se distribuuje zatížení na účastnických serverech a implementuje se odolnost proti chybám kořenového adresáře DFS.
- Doménové kořenové adresáře DFS a alternativní místa mohou hostit více serverů. Dojde-li k selhání kořenu, DFS chybu detekuje a kořenový adresář převezme jiný server. Tento proces překlopení zvyšuje dostupnost dat.
- Pod stejným logickým názvem DFS může být připojeno více kopií míst sdílení na samostatných serverech. Tím jsou zajištěna alternativní místa přístupu k datům a následně vyrovňování zatížení a lepší dostupnost dat.
- Existence více kopií na místech sdílení také umožňuje správcům vykonávat preventivní údržbu na serverech. Server, který hostí jednu repliku, lze převést do režimu offline, aniž by to mělo vliv na uživatele, protože systém DFS automaticky přesměruje požadavky na repliku, která je online.
- Systém DFS zaručuje prostřednictvím distribuce kopií vašeho souboru v sídle, že uživatelé budou používat nejbližší repliku. Tím se omezuje zatížení rozlehlé sítě (WAN).
- Transparentnost umístění řeší problém inovace na nové servery, protože umožňuje publikování dalších úložišť v podadresářích.

Je-li ve vaší organizaci splněna některá z následujících podmínek, zvažte implementování systému DFS:

- Uživatelé, kteří přistupují ke sdíleným prostředkům, se nacházejí na různých místech celého síťového sídla nebo v různých sídlech.
- Většina uživatelů potřebuje přístup k více sdíleným prostředkům.
- Uživatelé vyžadují nepřerušitelný přístup ke sdíleným prostředkům.
- Vyrovňování zatížení ve vaší síti lze zlepšit distribucí sdílených prostředků.
- Vaše organizace má data uložená na více místech sdílení v síti.

Další informace o návrhu stromu DFS najdete v nápovědě systému Windows 2000 Server.

Služba Indexing Service

Služba Microsoft Indexing Service usnadňuje uživatelům vyhledávání dat na klientských počítačích a serverech. Služba Indexing Service prochází soubory na serverových a klientských počítačích systému Windows 2000 a vytváří indexy obsahu a vlastností, které výrazně zlepšují kapacitu a výkon vyhledávání. Je-li tato služba spuštěná, uživatelé mohou vyhledat slova a fráze v tisících souborů v několika sekundách.

Služba Indexing Service má následující funkce:

- Hledání podle obsahu (vyhledá například všechny soubory obsahující „předpoklady příjmů“).
- Hledání podle vlastností dokumentu (vyhledá například všechny soubory, kde vlastnost AUTOR obsahuje „Sára“).
- Hledání s logickými operátory (například AND, OR a NOT).

- Používá hledání s volným textem, které umožňuje uživatelům zadat libovolnou kombinaci slov, přičemž není nutné učit se konkrétní syntaxi hledání.
- Může indexovat svazky na místním počítači i na sdílených místech na síti včetně serverů systému NetWare a UNIX.
- Poskytuje zabezpečené výsledky hledání.
Vrací pouze dokumenty, které mohou uživatelé číst. Používá standardní seznamy řízení přístupu (ACL) systému Windows 2000.
- V zájmu lepšího výkonu a spolehlivosti je integrována se systémem NTFS.
- V zájmu zajištění možnosti hledání na internetových a intranetových webových sídlech je integrována se službou Internet Information Services (IIS).
- Pomocí OLE-DB nebo skriptů Microsoft ActiveX Data Objects (ADO) si můžete vytvořit své vlastní formuláře vyhledávání a uživatelská rozhraní.
- Indexuje různé formáty souborů včetně Microsoft Office 97, Microsoft Office 2000, textových souborů a stránek HTML.
- Je integrována s uživatelským rozhraním systému Windows 2000 a Průzkumníkem Windows.
- Prostřednictvím modulu snap-in konzoly Microsoft Management Console umožňuje jednoduchou správu.

Když na systému běží služba Indexing Service, sleduje na serveru změny souborů. Dojde-li k úpravě souboru, soubor se otevře a jeho obsah indexuje. Otevření souboru má na starosti proces s nízkou prioritou pracující na pozadí, takže dopady na celkový výkon serveru jsou minimální. Při použití NTFS navíc služba Indexing Service používá mnoho pokročilých funkcí tohoto systému, čímž se celkové dodatečné zatížení systému minimalizuje.

Poznámka Po prvním spuštění si musí služba vytvořit indexy úplně od začátku. To znamená projít všemi soubory na svazku. Počáteční vytváření indexů představuje až do dokončení indexů rozsáhlé přístupy k disku. Jakmile jsou indexy vytvořeny, jsou nutné jen postupné aktualizace během úprav souborů, takže následné aktualizace jsou prakticky nepostřehnutelné. Ve všech případech je aktualizace indexu úloha s nízkou prioritou, která se zastaví v případě, kdy musí prostředky serveru vykonávat jiné operace.

Chcete-li vyhledávat dokumenty, stačí jen zadat příkaz hledání souborů a složek Průzkumníka Windows nebo nabídky Start. Objeví se formulář vyhledávání, který umožňuje uživatelům zadat hledaná slova. Je-li služba Indexing Service spuštěná na souborovém serveru, uživatelé mohou výkonně prohledávat také místa sdílení na síti, protože vyhledávání se uskuteční na serveru a přes síť se odesílají jen výsledky hledání.

Integrace se součástmi systému Windows 2000

Služba Indexing Service je v zájmu spolehlivosti a výkonu integrována s mnoha dalšími součástmi systému Windows 2000. Služba také používá funkce NTFS, jako je hromadné zpracování ACL, zajišťující mnohem rychlejší kontroly zabezpečení před vrácením výsledků hledání. Také používá řídce používané soubory NTFS k optimalizaci indexů bez další spotřeby diskového prostoru. Služba používá ke sledování změn souborů na svazku protokol změn NTFS. Tímto způsobem služba opakovaně nevyhledává změněné soubory na celém svazku, jako to dělá mnoho jiných vyhledávacích nástrojů. Je-li změněn určitý soubor, pouze tento soubor se prohledá a indexuje.

Služba Indexing Service také chápe, že soubory mohou být migrovány službou Vzdálené úložiště (Remote Storage). Proto násilně nevyvolává soubory, aby je mohla indexovat, a také neopakuje procházení souborem po jeho migraci na sekundární úložiště. To znamená, že i po migraci souborů na pásky je mohou uživatelé stále prohledávat. Používáte-li k údržbě archivovaných dokumentů službu Vzdálené úložiště, je tato situace ideální.

Službu Indexing Service lze přepnout do režimu, kdy může jen číst, což umožňuje správci zálohovat indexy. V režimu pouze pro čtení pokračuje služba ve vykonávání dotazů, indexy však neaktualizuje. Je tak zaručena konzistentnost a stabilita indexů, takže je lze řádně zálohovat. Po zálohování můžete obnovit normální provoz služby – všechny úpravy souborů zadané během zálohování se obvyklými postupy zpracují.

Fultextový indexovací nástroj používaný v systému Windows 2000 je také kompatibilní s funkcemi fultextového indexování programu Microsoft SQL Server verze 7.0. Použijete-li procesor distribuovaných dotazů v programu SQL Server, můžete dotazy zadávat prostřednictvím strukturovaného jazyka dotazů (SQL) a vykonávat je současně v systému souborů i v databázi.

Úvahy o použití služby Indexing Service ve strategii ukládání dat

Zvažte následující výhody začlenění služby Indexing Service do plánování úložišť:

- Uživatelé mohou na souborových a webových serverech snadno a rychle vyhledat dokumenty, které potřebují.
- Většina uživatelů se nemusí učit žádnou syntaxi, pokročilým uživatelům je však k dispozici výkonný jazyk vyhledávání.
- Jediný souborový server a služba indexování může uspokojit dotazy na více míst sdílení na síti včetně souborů na souborových serverech, které nepracují pod operačním systémem společnosti Microsoft.
- Zlepší se výkon a omezí se zatížení systému, což je zapříčiněno úzkou integrací s infrastrukturou systému Windows 2000.
- Zabezpečený vyhledávací nástroj zaručuje, že uživatelé nemohou najít také dokumenty, které si nemohou zobrazit nebo přečíst.
- Uživatelské rozhraní lze jednoduše upravit pomocí programovacích rozhraní OLE a ADO.

Nad implementací služby Indexing Service se vážně zamyslete, je-li ve vaší organizaci splněna alespoň jedna z následujících podmínek:

- Uživatelé nedokáží na serverech dokumenty najít nebo zapomínají jejich umístění.
- Souborové servery obsahují stovky nebo tisíce dokumentů, takže vyhledávání dokumentů procházením je zdlouhavé nebo zcela nemožné.
- Musíte zajistit možnosti vyhledávání pro webové sídlo.

Vylepšení ochrany dat

V podnikových sítích se k ochraně dat používá kombinace různých strategií. Ochranu svých dat můžete zlepšit použitím nástroje Zálohování (Backup) a funkcemi odolnosti proti chybám systému Windows 2000.

Odolnost proti chybám

Odolnost proti chybám je schopnost systému pokračovat ve fungování i po selhání části systému. Odolnost proti chybám bojuje proti problémům, jako jsou selhání disků, výpadky napájení nebo poškození operačního systému, které mohou mít vliv na spouštěcí soubory, samotný operační systém nebo systémové soubory. Systém Windows 2000 Server obsahuje funkce odolnosti proti chybám.

Třebaže jsou data v systému odolném proti chybám vždy dostupná a aktuální, musíte uskutečňovat zálohování na pásky a chránit tak informace o diskovém podsystemu před chybami uživatelů a přírodními katastrofami. Odolnosti proti chybám disku není alternativou k strategii zálohování na úložiště, které se nachází mimo síťové sídlo.

Diskové systémy odolné proti chybám jsou standardizovány a kategorizovány v šesti úrovních, známých jako pole RAID úrovně 0 až 5. Každá úroveň nabízí specifickou kombinaci výkonu, spolehlivosti a nákladů.

Správa disků

Správa disků (Disk Management) systému Windows 2000 zahrnuje pole RAID úrovně 1 a 5:

Úroveň 1: Zrcadlené svazky (sady zrcadlení v systému Windows NT 4.0)

Zrcadlené svazky zajišťují vytvoření identické kopie vybraného svazku. Všechna data zapsaná na primární svazek se zapíše také na sekundární svazek neboli zrcadlení. Dojde-li k selhání jednoho disku, systém použije data z druhého disku. Protože je každý soubor uložen na dvou místech, potřebujete k implementaci této technologie dvojnásobek obvyklého prostoru k ukládání dat.

Úroveň 5: Svazky RAID-5 (prokládání s paritou)

Svazky RAID-5 sdílejí data na všech discích v poli. Systém vytváří malé množství dat označované za informace o paritě, které se používá v případě selhání disku k rekonstrukci ztracených informací. Pole RAID-5 je unikátní, protože informace o paritě zapisuje na všechny disky. Pro případ selhání disku je redundance dat dosaženo uspořádáním datového bloku a jeho informací o paritě různých disků v poli. Tato úroveň vyžaduje minimálně tři disky. S dalšími disky přidávanými do sady RAID-5 se množství nadbytečného prostoru snižuje z maximální hodnoty 50 procent (tři disky jsou potřebné pro uložení dat, která jsou obvykle na dvou discích). Výhody použití mnoha disků v sadě RAID-5 se snižují, jakmile je v poli sedm nebo více disků.

Výběr strategie pole RAID

Mezi strategie RAID patří hardwarová a softwarová řešení. Volba mezi svazky RAID-1 a RAID-5 závisí na vašem počítačovém prostředí. Při volbě strategie RAID vezměte v potaz také tyto body:

- V porovnání se svazky RAID-5 představuje implementace zrcadleného svazku menší počáteční náklady, vyžaduje méně systémové paměti, poskytuje lepší celkový výkon a během selhání se neprojeví žádné snížení výkonu. Cena za megabajt je však vyšší než u svazků RAID-5.
- Softwarová implementace svazku RAID-5 nabízí lepší výkon při čtení a nižší cenu za megabajt, vyžaduje však více systémové paměti a chybí-li v poli nějaký disk, ztrácí výhodu vyššího výkonu.

- Hardwarové a softwarové svazky RAID-5 představují dobré řešení redundance dat v počítačovém prostředí, v němž většina činností spočívá ve čtení dat. Svazek RAID-5 je například vhodné aplikovat na serveru, který se používá k udržování všech kopií programů vašeho sídla. Umožňuje vám chránit programy při ztrátě jednoho disku v prokládaném svazku. Navíc se díky současným čtením z různých disků, které tvoří svazek RAID-5, zlepšuje výkon při čtení.
- V prostředí, kde dochází k častým aktualizacím informací, bude asi lepší použít zrcadlené svazky. Svazek RAID-5 však můžete použít, vyžadujete-li redundanci nebo jsou-li dodatečné náklady na zrcadlení příliš vysoké.

Zálohování

Program **Zálohování** (Backup) vám pomáhá s ochranou dat před náhodnou ztrátou způsobenou selháním hardwaru nebo softwaru. Pomocí Zálohování můžete vytvořit duplikovanou kopii dat na pevném disku a data archivovat na jiném zařízení ukládání dat, například pevném disku nebo pásku. Data lze zálohovat na velké množství vyměnitelných médií ukládání dat s vysokou kapacitou. Pro účely archivování je také program Zálohování integrován se službou Vzdálené úložiště.

Pomocí průvodců programu Zálohování můžete vykonat tyto akce:

- Vytvořit archivovanou kopii vybraných souborů a složek na pevném disku.
- Naplánovat pravidelná zálohování, čímž zajistíte vždy aktuální stav archivovaných dat.
- Obnovovat archivované soubory a složky na pevný disk, k němuž máte přístup.
- Zálohovat adresářovou službu Active Directory. Kopii Active Directory můžete uložit na média, která se pak budou nacházet mimo vaše síťové sídlo.
- Zálohovat data služby Vzdálené úložiště, nastavení registru a mnoho dalších dat připojovacích bodů.

Strategie ochrany dat na podnikových sítích

Během vytváření zásad ochrany dat zvažte následující strategie zálohování a odolnosti proti chybám:

- Pro případ selhání disku zálohujte celý svazek. Je vhodnější obnovit pak v jediné operaci celý svazek.
- Vždy zálohujte databázi adresářových služeb na řadiči domény, abyste zabránili ztrátě uživatelských účtů a informací o zabezpečení.
- U svých nejdůležitějších počítačů můžete implementovat softwarové zrcadlení dvou oddělených hardwarově řízených polí RAID. V této konfiguraci budou operace pokračovat i v případě selhání nějakého disku nebo celého pole.
- Pro případ selhání počítače se spuštěným systémem Windows 2000 Server byste měli mít připravený náhradní počítač s již instalovaným systémem Windows 2000 Server, na který bude možné přesunout datové disky.

Úvahy o návrhu systému ukládání dat odolného proti chybám

Mezi problémy, nad kterými byste se měli zamyslet při plánování strategie ukládání dat, patří také ty následující:

- Obecně platí, že konfigurace odolné proti chybám je zapotřebí používat jen u informací, které musíte mít vždy k dispozici v případě selhání hardwaru nebo neobnovitelných chyb disku, když primární zdroj dat z nějakého důvodu přejde do režimu offline.
- Máte-li aplikace na jediném počítači se systémem Windows 2000 Server, musíte je spouštět na svazku odolném proti chybám, pouze pokud nemůžete tolerovat jejich nedostupnost po dobu, jakou vám bude trvat obnovení aplikací ze zálohy.
- Svazek aplikací je zapotřebí zálohovat, kdykoli nainstalujete novou aplikaci nebo změníte výchozí nastavení nějaké aplikace.
- Je-li vaším problémem prostor, můžete naformátovat aplikační svazek systémem souborů NTFS a používat kompresi NTFS složek a souborů na svazku.

Zlepšení schopností zotavení po havárii

Protože havárie počítače nebo síťového sídla může překonat i ty nejlepší strategie ochrany dat, musíte vytvořit plán zotavení systému po havárii. Havárie představuje vše od neschopnosti spustit počítač až po zničení sítě při přírodní katastrofě.

Chcete-li být dobře připraveni na selhání systému, musíte mít:

- dobře zdokumentované plány a postupy zotavení ze selhání;
- diskety, které vám umožní restartovat počítač máte-li potíže s použitím systémového, aktivního nebo spouštěcího svazku;
- zdokumentované softwarové a hardwarové konfigurační informace svých počítačů.

Chcete-li snížit čas zotavení systému, doporučujeme vám:

- umístit systémové a spouštěcí a datové svazky systému Windows 2000 Server na samostatné disky;
- uložit data konfigurace disku, kdykoli změníte konfiguraci pomocí Správy disků;
- mít k dispozici vytištěný záznam diskových svazků a jejich velikostí.

Zbývající část tohoto oddílu popisuje funkce ochrany systému Windows 2000, kterými můžete svou společnost připravit na potenciální havárii sítě.

Vytváření zásad zálohování a ukládání dat mimo síťové sídlo

Váš plán zotavení po havárii musí zahrnovat zásady a postupy zálohování a obnovení jednotlivých počítačů a celých systémů. Vaší cílem musí být vytvoření jasných instrukcí obnovení dat.

Zásady zálohování

Při vytváření zásad zálohování zvažte následující strategie:

Zálohujte všechny počítače nebo jen vybrané počítače. Plánujete zálohovat celou síť, nebo budete zálohovat pouze servery s důležitými uživatelskými soubory?

Vytvořte síťové zálohování nebo místní zálohování. Budete mít několik zálohovacích serverů s páskovými zařízeními, které budou číst data přes síť ze všech vybraných serverů, nebo budou všichni uživatelé odpovědní za zálohování svých dat?

Použijte centralizované zásady zálohování nebo distribuované zásady zálohování. Bude jediná skupina IT zálohovat všechny servery organizace, nebo bude každá skupina pro-

vědět své vlastní zálohování? Nastane-li druhá situace, vytvoříte pravidla toho, kdy a jak se má zálohovat?

Váš plán zálohování musí obsahovat implementaci následujících činností:

- Zabezpečení zařízení úložiště i zálohovacích médií.
- Vytvoření kopií všech potřebných ovladačů zařízení, aby bylo možné v případě havárie používat zařízení ukládání dat. K operaci obnovení jsou zapotřebí určité ovladače zařízení.
- Vytvoření a zaručení připravenosti tištěných kopií protokolů zálohování. Ty jsou důležité pro obnovení dat.
- Příprava tří kopií médií. Alespoň jednu kopii uložte mimo síťové sídlo v řádně kontrolovaném prostředí.
- Pravidelné vykonávání zkušebních obnovení. Tím prověříte, že sadu zálohování lze číst a že obsahuje všechny soubory, které chcete zálohovat. Další informace o použití specifických metod a postupů zálohování najdete v kapitole „Zálohování“ v knize *Microsoft Windows 2000 Server Správa systému*.

Úvahy o ukládání mimo síťové sídlo

Při plánování ukládání dat mimo síťové sídlo zvažte ukládání následujících dat a informací:

- Plná záloha celého systému vykonávaná pravidelně každý týden.
- Originály všech instalovaných programů a potřebných ovladačů zařízení.
- Dokumenty potřebné k uplatnění náhrady škody, jako jsou záznamy inventáře hardwaru a softwaru a kopie objednávek nebo účtenek hardwaru a softwaru počítačů.
- Kopie informací potřebných k opakované instalaci a konfiguraci síťového hardwaru.

Vytváření plánu zotavení po havárii

Abyste mohli určit opatření pro částečnou nebo úplnou ztrátu dat, musíte zjistit celkové náklady opakovaného vybudování nebo náhrady dat, která vaše organizace používá. Zodpovězte si tyto otázky:

- Jaké jsou náklady na rekonstrukci finančních, personálních a jiných obchodních dat vaší společnosti?
- Čeho se týká pojištění vaší společnosti z hlediska náhrady ztracených dat?
- Jak dlouho bude trvat rekonstrukce obchodních dat? Jak se to projeví ve ztracených zakázkách?
- Jaké jsou náklady na hodinu výpadku serveru?

Během vývoje zevrubného plánu zotavení po havárii se musíte zabývat několika oblastmi. Váš plán ochrany dat musí zodpovědět tyto otázky:

- Jaká data musíte zálohovat a jak často je zapotřebí zálohování vykonat?
- Jak budete chránit informace o konfiguraci důležitých počítačů a jiného hardwaru, které se během normálního zálohování neukládají?
- Jaká data musí být uložena na síťovém sídle a jak je budete fyzicky skladovat?
- Jaká data musí být uložena mimo síťové sídlo a jak je budete fyzicky skladovat?

- Jaká školení jsou zapotřebí, aby operátoři a správci serverů dokázali rychle a efektivně reagovat v případě havárie?

Otestujte svůj plán zotavení a obnovení důležitých dat vaší organizace a kopie plánu zotavení po havárii mějte k dispozici jak na sídle tak i mimo něj.

Testování strategií obnovení systému

Testování je důležitou součástí přípravy na zotavení po havárii. Dovednosti a zkušenosti správců a operátorů jsou důležitými faktory při zajištění co nejrychlejšího návratu porouchaného počítače nebo sítě zpět do režimu online s minimálními náklady a přerušáním výrobních činností. Potřebujete personál IT, který je proškolen v řešení problémů a vykonávání postupů obnovení systému.

Před zavedením nového serveru do výrobního prostředí nezapomeňte postupy obnovení otestovat. Testování musí zahrnovat:

- zajištění správné funkce spouštěcích disků systému Windows 2000;
- testování zdrojů nepřerušitelného napájení (UPS) na počítačích se spuštěným systémem Windows 2000 Server a na rozbočovačích, směrovačích a dalších součástech;
- testování plánu obnovení po havárii;
- vykonání celkového nebo částečného obnovení z médií denní, týdenní nebo měsíční zálohy.

Praktikování postupů obnovení

Během testování se můžete pokusit předpovědět situace selhání a v praxi vyzkoušet postupy obnovení. Nezapomeňte na zátěžové testy a testy všech funkcí.

Mezi selhání, která musíte otestovat, patří:

- individuální součásti počítačů, jako jsou pevné disky a řadiče, procesory a paměť RAM;
- externí součásti, jako jsou směrovače, mosty, přepínače, kabely a konektory.

Prováděné zátěžové testy by měly zahrnovat:

- vysoké zatížení sítě;
- vysoké zatížení vstupů a výstupů jednoho disku;
- náročné používání souborových, tiskových a aplikačních serverů;
- vysoké zatížení způsobené uživateli, kteří se přihlašují v jeden okamžik.

Dokumentování postupu obnovení

Musíte také vyvinout postupy obsahující jednotlivé kroky převedení počítače nebo sítě po havárii zpět do režimu online. Vytvořte operační příručku obsahující následující procedury:

- Vykonávání zálohování
- Implementování zásad ukládání dat mimo síťové sídlo
- Zotavení serverů a sítě

Při zadání změn konfigurace počítačů nebo sítě musíte také potřebným způsobem opravit dokumentaci. Aktualizace dokumentace je důležitá zejména při instalaci nových verzí operačního systému nebo změně nástrojů a utilit, které používáte ke správě systému.

Seznam úkolů plánování správy úložišť

Tabulka 19.4 shrnuje úkoly, které můžete využít při určování svých potřeb ukládání dat a jejich řešení.

Tabulka 19.4 Souhrn úkolů plánování úložišť

Úkol	Umístění v kapitole
Vyhodnoťte své potřeby ukládání dat.	Zlepšení funkcí správy úložišť
Výberte systém ukládání dat.	Zlepšení funkcí správy úložišť
Naplánujte správu úložiště včetně vyměnitelného a vzdáleného úložiště.	Správa diskových prostředků
Vytvořte strategie optimalizace správy úložišť.	Optimalizace správy dat
Vytvořte strategie ochrany dat.	Vylepšení ochrany dat
Vytvořte strategie zálohování a zotavení po havárii.	Zlepšení schopností zotavení po havárii

KAPITOLA 20

Synchronizování služby Active Directory s adresářovou službou programu Exchange Server

Toto je velmi důležitá kapitola plánování pro personál správy adresářových služeb ve vaší organizaci, plánujete-li implementovat adresářovou službu Active Directory systému Microsoft Windows 2000 Server a nyní používáte adresářovou službu programu Microsoft Exchange Server verze 5.5. Koncepty a postupy synchronizace adresářů popsané v této kapitole vám pomohou určit z hlediska ceny nejvýhodnější a nejvýkonnější metodu správy služby Active Directory systému Windows 2000 Server a adresářové služby programu Exchange Server 5.5. Příklady vám také pomohou zjistit, které možnosti konfigurace synchronizace a správy budou pro vaši organizaci nejvhodnější.

Než začnete číst tuto kapitulu, přečtěte si kapitoly „Návrh struktury služby Active Directory“ a „Určení strategií migrace domén“ v této knize. Tyto kapitoly vám pomohou porozumět novým konceptům a klíčovým součástem služby Active Directory a problémům souvisejícím s migrací domén.

V této kapitole

Přehled synchronizace adresářů 596

Vytvoření plánu dohody o spojení služby ADC 601

Ochrana před náhodnou ztrátou dat 623

Seznam úkolů plánování synchronizace adresářů 625

Další zdroje 625

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujícího dokumentu plánování:

- Plán dohody o spojení služby Active Directory Connector (ADC)

Související informace v sadě Resource Kit

- Další informace o službě Active Directory, plánování oborů názvů a správě domény najdete v kapitole „Návrh struktury služby Active Directory“ v této knize.
- Další informace o migraci na systém Windows 2000 Server najdete v kapitole „Určení strategií migrace domén“ v této knize.

- Další informace o standardech zabezpečení systému Windows 2000 Server najdete v kapitole „Plánování distribuovaného zabezpečení“ v této knize.
- Další informace o vytváření plánů testování najdete v kapitole „Vytvoření testovací laboratoře systému Windows 2000“ v této knize.

Přehled synchronizace adresářů

Synchronizace adresářů je proces zajištění synchronizace dvou samostatných adresářových služeb. Změny objektů v jednom adresáři se pak automaticky promítnou do druhého adresáře.

Synchronizace adresářů mezi službou Active Directory systému Windows 2000 Server a adresářovou službou programu Exchange Server 5.5 vám umožní v počáteční fázi zaplnit novou službu Active Directory atributy uživatelů a objekty Exchange Serveru 5.5. Protože navíc Exchange Server 5.5 podporuje adresářové služby elektronické pošty jiných výrobců, můžete do programu Exchange Server zkopírovat atributy uživatelů a objekty adresářů jiných výrobců a dále je pak přenést z Exchange Serveru do služby Active Directory.

Po počátečním zaplnění Active Directory mohou oba adresáře produktivně existovat současně. Pomocí předem nakonfigurovaných automatizovaných operací synchronizace můžete udržovat konzistentnost informací ve službě Active Directory a adresáři programu Exchange Server 5.5.

Proces synchronizace adresářů

Než začnete plánovat strategii synchronizace adresářů, podívejte se na proces plánování uvedený ve vývojovém diagramu na obrázku 20.1.

Ještě před započatím fáze plánování synchronizace adresářů je důležité, abyste dokonale rozuměli klíčovým součástem, které budete při vykonávání operace synchronizace adresářů používat.

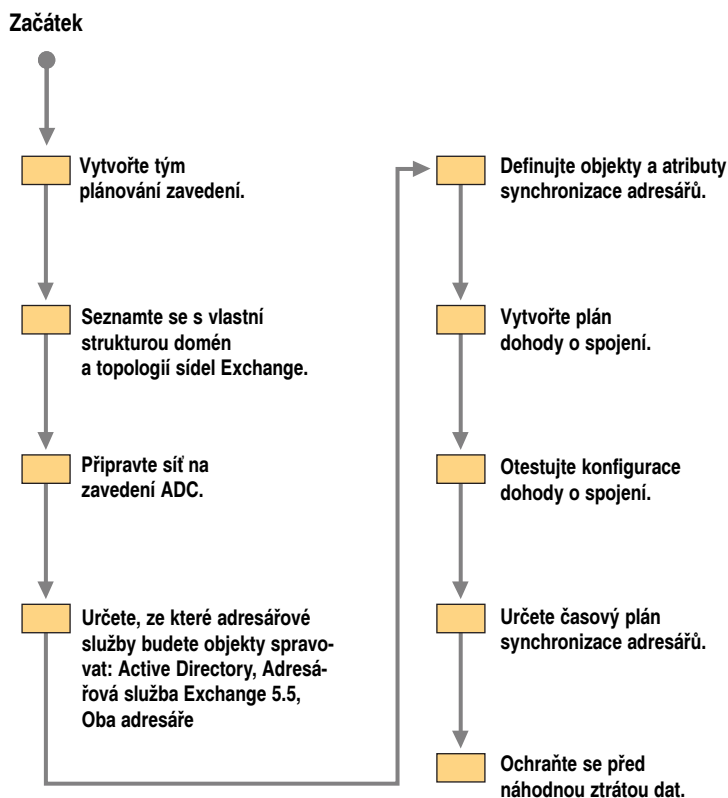
Softwarové součásti systému Windows 2000 Server

Služba Active Directory Connector (ADC) a Microsoft Management Console (MMC) jsou softwarové součásti systému Windows 2000 Server, které vám umožňují synchronizovat a spravovat komunikace mezi službou Active Directory a adresářovou službou programu Exchange Server 5.5. Pomocí protokolu Lightweight Directory Access Protocol (LDAP) zajišťuje ADC možnost automatického udržování konzistentnosti adresářových informací mezi Active Directory a adresářovou službou Exchange Serveru. Ke konfiguraci ADC pro vykonávání určitých funkcí se používá konzola MMC, moduly snap-in a rozšíření konzoly MMC související se službou ADC. Bez ADC budete muset ručně zadat nová data a změny do obou adresářových služeb.

Klíčovými prvky a funkcemi ADC jsou:

- Obousměrná synchronizace

Tento prvek umožňuje automatické předání změn zadaných v adresáři programu Exchange Server službě Active Directory a naopak. To vám dovoluje spravovat změny v obou adresářích.



Obrázek 20.1 Proces synchronizace služby Active Directory a adresářové služby programu Exchange Server 5.5

■ Synchronizace vybraných atributů

K synchronizaci můžete určit konkrétní atributy Active Directory a Exchange Serveru a můžete účelově zrušit synchronizaci jiných atributů.

■ Synchronizace změn

Při synchronizaci s Exchange Serverem aktualizuje systém Windows 2000 Server pouze změny na úrovni objektů. Upravíte-li například 20 objektů uživatelů ze 100 000 uživatelů, systém bude aktualizovat pouze oněch 20 objektů uživatelů. Tím se omezuje čas duplikování a přenášení i provoz v síti.

■ Změny na úrovni atributů

Při synchronizaci dvou objektů porovná ADC hodnoty atributů a určí, které atributy je zapotřebí synchronizovat. Dojde-li například ke změně telefonního čísla poštovní schránky Exchange Serveru, ADC porovná atributy poštovní schránky s odpovídajícím objektem uživatele ve službě Active Directory a synchronizuje pouze změněné atributy. V našem případě dojde pouze k synchronizaci telefonního čísla.

■ Konzistentní nástroje správy

Pomocí modulu snap-in Uživatelé a Počítače služby Active Directory (Active Directory Users and Computers) konzoly MMC můžete spravovat uživatele, kontakty a skupiny.

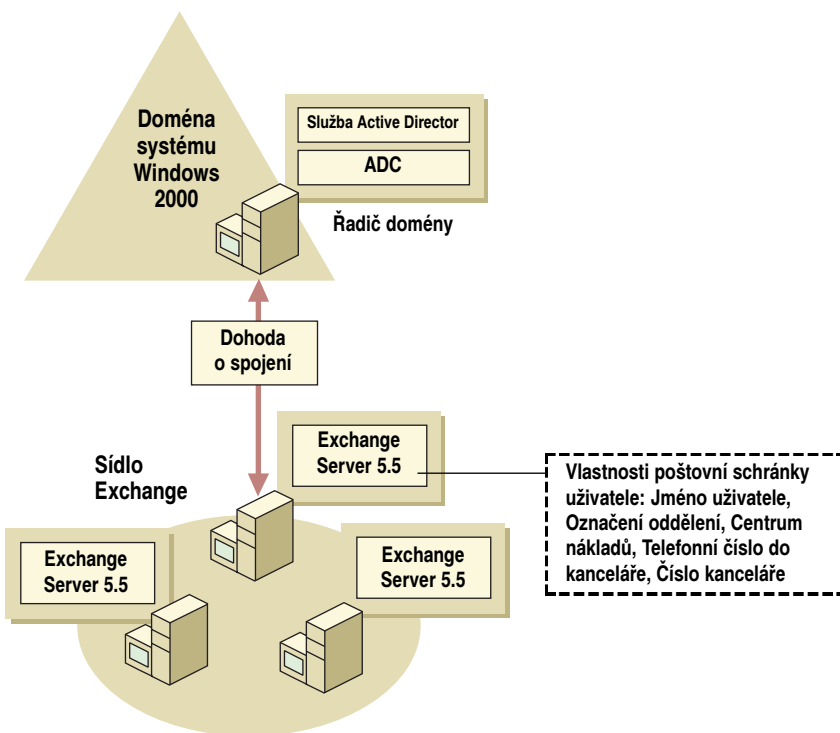
Další informace o nástroji Microsoft Management Console a modulech snap-in a rozšířeních konzoly MMC najdete v nápovědě systému Windows 2000 Server.

Hlavní výhody použití ADC

Použití ADC zajišťuje tyto výhody:

Správa z jediného zdroje

Po inovaci domény systému Windows NT Server 4.0 na službu Active Directory systému Windows 2000 Server můžete jednoduše a automaticky nakonfigurovat službu ADC tak, aby zaplnila nový adresář Active Directory adresářovými informacemi Exchange Serveru 5.5, jako jsou vlastnosti poštovní schránky uživatele uvedené na obrázku 20.2.



Obrázek 20.2 Správa z jediného zdroje

Možnosti akutní správy a delegování

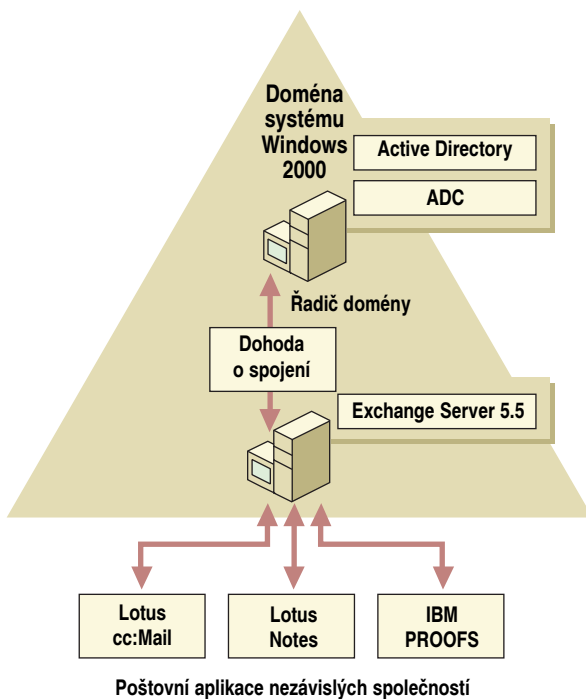
ADC lze používat k synchronizaci a správě adresáře Exchange Serveru přes službu Active Directory, což vám umožňuje výhodně používat možnosti přesnějšího delegování správy nabízené systémem Windows 2000 Server. V systému Windows 2000 Server to-

tiž můžete nastavovat oprávnění na úrovni atributů a nikoli na úrovni objektů. To umožňuje správcům delegovat různým uživatelům úlohy související s určitými atributy. Uživatelé mohou mít například oprávnění aktualizovat údaje střediska nákladů svého oddělení a také si zobrazovat a aktualizovat některá telefonní čísla. Pomocí Exchange Serveru 5.5 si mohou zobrazovat vlastnosti, ale nemohou je přímo aktualizovat. V systému Windows 2000 Server může správce systému tyto úkoly delegovat tak, aby daní uživatelé mohli upravovat pole střediska nákladů a telefonního čísla domů. Určité úkoly můžete delegovat oprávněným uživatelům, ale zároveň jim zabránit v přístupu k dalším oblastem dat, jako je členství ve skupinách a oprávnění zabezpečení. Výsledky těchto autorizovaných změn správy můžete pak do adresáře Exchange Serveru uložit pomocí ADC.

Další informace o různých úrovních možností delegování a správy ve službě Active Directory najdete v kapitole „Návrh struktury služby Active Directory“ v této knize.

Možnost spolupráce s adresářovými službami elektronické pošty jiných společností

Pomocí Exchange Serveru můžete zaplnit službu Active Directory informacemi o uživateli a skupinách z adresářů elektronické pošty jiných společností. Exchange Server podporuje obousměrnou synchronizaci adresářů služeb elektronické pošty nezávislých společností, pokud tyto služby obsahují agenty synchronizování adresářů. Obrázek 20.3 zachycuje možnost spolupráce mezi Exchange Serverem a adresářovými službami elektronické pošty pocházejícími od jiné společnosti.



Obrázek 20.3 Obousměrná synchronizace adresářů s adresářovými službami elektronické pošty nezávislých společností

Snadné vyhledávání uživatelů sítě

Nástroj Active Directory Client umožňuje koncovým uživatelům, kteří mají systémy Windows 2000 Server nebo Windows 9x s nainstalovaným nástrojem Active Directory Client, jednoduše vyhledávat jiné uživatele pomocí příkazu hledání osob. Když zkombinujete schopnosti služby ADC s nástrojem Active Directory Client, dosáhnete rychlého zavedení Active Directory ve formě adresáře uživatelů. To se bude podobat způsobu používání telefonního seznamu.

Další informace o nástroji Active Directory Client najdete v kapitole „Příprava infrastruktury sítě na systém Windows 2000“ v této knize.

Vytváření vztahů pomocí dohod o spojení

Instalace ADC na server přidá do systému Windows 2000 a služby Active Directory další službu. Chcete-li vytvořit vztah mezi existujícím sídlem Exchange Serveru a Active Directory, musíte nakonfigurovat dohodu o spojení (connection agreement). Dohoda o spojení obsahuje informace, jako jsou názvy serverů kontaktovaných při synchronizaci, třídy objektů, které se mají synchronizovat, cílové kontejnery a časový plán synchronizace. Je možné definovat více dohod o spojení na jediné službě ADC; každé spojení může směřovat od Active Directory k jinému nebo k témuž sídlu Exchange Serveru.

Dohoda o spojení specificky definuje tyto údaje:

- Adresář nebo adresáře, které se mají synchronizovat
- Objekty synchronizace systému Windows 2000 Server
- Objekty synchronizace Exchange Serveru 5.5
- Směr, v jakém k synchronizaci dochází
- Časový plán synchronizace
- Metodu odstraňování objektů
- Podrobnosti související s některými pokročilejšími volbami, jako:
 - Atributy připojování (mapování)
 - Vytváření nových objektů
 - Ověřování všech adresářů
 - Určení, které organizační jednotky (OU) nebo kontejnery chcete synchronizovat

Služba ADC vykonává výhradně synchronizaci adresářů mezi programem Exchange Server 5.5 s balíčkem Service Pack 1 (SP1) nebo novějším a systémem Windows 2000 Server. Máte-li však dřívější verze Exchange Serveru s SP1 v sídle Exchange Serveru 5.5, takový Exchange Server se automaticky synchronizuje s dřívější verzí Exchange Serveru. V takovém případě jsou všechny adresářové informace stejné v celém sídle Exchange Serveru a v organizaci.

Na jednom počítači se spuštěným systémem Windows 2000 Server může být sice aktivní jen jedna instance služby ADC, lze však vytvořit více dohod o spojení. Každou dohodu o spojení lze nakonfigurovat na vykonávání jedinečných úloh synchronizace. Například jedna dohoda o spojení může neustále aktualizovat Active Directory systému Windows 2000 Server, zatímco druhá dohoda o spojení může denně v zadaný čas předávat kontakty systému Windows 2000 Server do adresáře Exchange Serveru.

Vytvoření plánu dohody o spojení služby ADC

Jakmile porozumíte schopnostem služby ADC a důležitosti dohod o spojení, budete moci začít fázi plánování synchronizace adresářů. Tento oddíl vás provede sběrem informací potřebných k vytvoření plánu dohody o spojení služby ADC.

Sestavení týmu plánování zavedení

Díky vysoké úrovni provázanosti různých prvků je pro zajištění hladké a výkonné synchronizace mezi službou Active Directory systému Windows 2000 Server a adresářovou službou programu Exchange Server týmová práce velmi důležitá.

Plánování strategie synchronizace adresářů musí být projekt, na kterém budou spolupracovat klíčové osoby procesu rozhodování a techničtí vedoucí následujících skupin:

- Management IT
- Správa Exchange Serveru
- Správa Active Directory
- Skupina správců schéma (Schema Administrators)
- Síťové služby

Společně bude mít tento tým dostatek znalostí o topologii sídel Exchange Serveru, návrhu služby Active Directory a topologii sítě, aby se dokázal vyhnout možným nákladným omylům.

Jakmile sestavíte tým plánování zavedení, můžete začít fázi plánování synchronizace adresářů.

Tým plánování zavedení synchronizace adresářů by se měl zabývat těmito otázkami:

- Přiřazení konkrétní zodpovědnosti a cílů jednotlivým správcům systému v týmu zavedení synchronizace adresářů.
- Určení, zda budou správci systému pro provozování služby ADC příslušného modulu snap-in konzoly MMC potřebovat školení. Je-li zapotřebí školení, rozhodněte o jeho uskutečnění.
- Získání oprávnění k instalaci.

Protože právo zápisu do schématu je omezeno na členy skupiny Schema Administrators, budete muset z této skupiny získat oprávnění k instalaci služby ADC. Správci schématu však mohou spouštět instalaci ADC výhradně za účelem rozšíření schématu. Správa ADC nesouvisí se schématem, pokud však z nějakého důvodu bude některá následující verze služby ADC zahrnovat změnu schématu, bude zapotřebí pomoc skupiny správců schématu. Informace o instalování služby ADC najdete v oddílu „Strategie implementace služby ADC“ dále v této kapitole.

Další informace o schématu Active Directory najdete v kapitole „Návrh struktury služby Active Directory“ v této knize a také v knize *Microsoft Windows 2000 Server Distribuované systémy*.

- Určete, jaké výrobní či obchodní procesy lze pomocí této operace synchronizace automatizovat nebo optimalizovat.
- Získejte souhlas managementu s implementováním svého plánu synchronizace adresářů.

Získání informací o struktuře domény a topologii sídla Exchange Serveru

Než začnete shromažďovat informace pro plán dohody o spojení služby ADC, musíte pochopit strukturu sídel Exchange 5.5, domén systému Windows NT Server a služby Active Directory systému Windows 2000 Server ve vaší organizaci. Jakmile získáte diagramy topologie sídla Exchange Serveru a struktury domén, doporučujeme vám použít tento postup:

Zinventarizujte sídla Exchange Serveru. Musíte vědět, kolik sídel Exchange Serveru máte, jak jsou spravována a zda jsou kandidáty pro synchronizaci. V případě sídel Exchange Serveru, která se budou synchronizovat, budete potřebovat podrobné informace o jejich kontejnerech příjemců a objektech, jež se budou synchronizovat.

Instalujte službu ADC na systém Windows 2000 Server. Službu ADC budete muset instalovat na server globálního katalogu, členský server, nebo řadič domény se systémem Windows 2000 Server každé domény Active Directory, která se účastní synchronizace adresářů.

Určete umístění poštovních schránek všech uživatelů v doméně. Mnoho organizací má topologii domén s více hlavními počítači, kde uživatelské účty existují ve více než v jedné doméně. Je důležité určit, kde jsou v jednotlivých doménách umístěny poštovní schránky uživatelů. Nejjednodušší je situace, kdy jsou všechny poštovní schránky v hlavní doméně na jediném sídle Exchange Serveru.

Zjistěte, aby měl každý adresář objekty potřebné pro účely synchronizace. Sídla Exchange Serveru mohou obsahovat poštovní schránky, které jsou přiřazeny účtům systému Windows 2000 Server z více domén. Můžete vytvořit více dohod o spojení z jediného sídla Exchange Serveru na více domén Active Directory a služba ADC přiřadí poštovní schránky Exchange Serveru k odpovídajícímu objektu uživatele. V případě vlastních příjemců (Custom Recipients), distribučních seznamů (Distribution Lists) a poštovních schránek (Mailboxes) Exchange Serveru, které nemají odpovídající objekt uživatele ve službě Active Directory, vytvoří ADC v jedné z domén Active Directory nové objekty. Budete muset určit, ve které doméně služby Active Directory má služba ADC vytvářet nové objekty.

Příprava sítě na zavedení služby ADC

Na jednom počítači se spuštěným systémem Windows 2000 Server může být aktivní jen jedna instance služby ADC. ADC však může podporovat více dohod o spojení. Chcete-li se připravit na zavedení ADC, zamyslete se nad požadavky a doporučeními popsanými v následujícím oddílu.

Zvážení specifických síťových požadavků

Při získávání informací pro plán dohody o spojení služby ADC musíte vykonat dva zvláštní úkoly v síti. Jedná se o tyto úkoly:

Vyberte servery, které budou předmostím.

Servery předmostí přijímají a posílají dále provoz elektronické pošty na obou koncích dohody o spojení, což se podobá úloze brány. Servery, které budou fungovat jako předmostí ADC, by měly splňovat tyto podmínky:

- Musí mít odpovídající prostředky (procesor a paměť) pro podporu provozu synchronizace a zpracování příchozích relací LDAP.

- Musí být správně připojeny k síti. Jestliže například sídlo Exchange Serveru zahrnuje více fyzických míst v síti s osou a rameny (hub-and-spoke), jeho server předmostí by měl být umístěn v ose.
- Není-li ADC server předmostí serverem globálního katalogu, musí být alespoň na stejném segmentu místní sítě (LAN), jako je server globálního katalogu. Důvodem je skutečnost, že ADC se při vykonávání hledání odpovídajících cílů pokouší kontaktovat globální katalog. Když služba ADC vyzvedne nový objekt z Exchange Serveru, nechce náhodně vytvořit odpovídající objekt Active Directory v jedné doméně. Prohledáním globálního katalogu služba ADC minimalizuje šanci, že vytvoří duplikovaný objekt.
- Jestliže prostředí Exchange Serveru zahrnuje servery konektoru, které nehostí poštovní schránky, zvažte nakonfigurování těchto serverů jako předmostí ADC.

Určete použití prostředků.

Prostředky sítě spotřebovává jak synchronizace adresářových objektů mezi adresáři, tak i replikace, k níž dochází v prostředí replikací adresářů Active Directory a Exchange Serveru.

Jakmile se stane služba Active Directory po inovaci ze systému Windows NT Server 4.0 na Windows 2000 Server a po synchronizaci s Exchange Serverem relativně statickou, mezi adresářovými službami Active Directory a Exchange Serveru 5.5 budou procházet jen malá množství dat. Změny v adresáři Exchange Serveru 5.5, které se synchronizují s adresářem Active Directory, způsobují o něco více provozu než změny v Active Directory, které se synchronizují na Exchange Serveru.

Požadavky na počítače

Během přípravy na použití služby ADC zajistíte splnění těchto technických požadavků na počítače:

- Musíte mít alespoň jeden server se systémem Windows 2000 Server.
- Musíte mít alespoň jeden program Exchange Server 5.5 s balíčkem SP1 (minimálně) nainstalovaným na každém serveru Exchange definovaném v dohodě o spojení.

V závislosti na časovém plánu synchronizace může server ADC a další adresářové servery, se kterými spolupracuje, čelit značnému zatížení. Je důležité, aby tyto počítače byly řádně vybaveny (procesorem a pamětí) a správně připojeny k síti – v ideálním případě by se měly nacházet na stejné místní síti. Je-li plán nastaven v uživatelském rozhraní na **Vždy** (Always), ADC se pokusí synchronizovat změny mezi Active Directory a adresářem Exchange Serveru. (To se liší od funkce časových plánů replikování adresářů v prostředí Exchange Serveru 5.x.) K této synchronizaci dochází v cyklech maximální doby spojitě replikace a pětiminutového zpoždění synchronizace.

Očekávané použití prostředků na serverech s procesorem třídy Pentium (200 MHz) se 128 MB pamětí a s nakonfigurovanou jednou dohodou o spojení je uvedeno v tabulce 20.1.

Tabulka 20.1 Využití procesoru třídy Pentium na serveru

Použití procesoru (přibližně každých 5 minut)	Využití
Server se spuštěnou službou ADC	8–24 %
Řadič domény	6–66 %
Připojení předmostí Exchange 5.5	0–91 %

Chcete-li porovnat rozdíly mezi typy a rychlostmi procesorů, podívejte se na využití prostředků v serverech se dvěma procesory třídy Pentium II (450 MHz) s 256 MB pamětí, které je uvedené v tabulce 20.2.

Tabulka 20.2 Využití procesorů serveru se dvěma procesory třídy Pentium II

Použití procesoru (přibližně každých 5 minut)	Využití
Server se spuštěnou službou ADC	1–12 %
Řadič domény	0–30 %
Připojení předmostí Exchange 5.5	20–36 %

Při zavádění Exchange Serveru 5.5 a Active Directory v podnikovém rozsahu musíte pečlivě naplánovat dodatečnou spotřebu prostředků, kterou bude vytvářet služba ADC a její dohody o spojení. To je důležité zejména pro ty, kteří potřebují přesně nastavit kapacitu serverů a sítě. Ještě důležitější je to v situacích, kdy jsou server ADC, řadič domény a server Exchange Server 5.5 spojeny relativně pomalými linkami.

Doporučení zavádění

Chcete-li dosáhnout úspěšného zavedení, věnujte pozornost také následujícím doporučením:

Active Directory zaplňte účty uživatelů pomocí inovování primárního řadiče domény (PDC) na systém Microsoft Windows 2000 Server.

K opětnému zaplnění již existujících účtů Active Directory adresářovými daty z adresáře Exchange Serveru použijte ADC. To umožní objektům synchronizovaným z Exchange Serveru připojit se (mapovat) k objektům zabezpečení v Active Directory.

K replikaci adresářů Exchange Serveru mezi sídly Exchange Serveru použijte servery předmostí replikace adresářů.

Je-li to možné, použijte je jako servery předmostí ADC pro dohody o spojení.

Je-li to možné, umístěte server hostící službu ADC na stejnou podsít', jako je předmostí adresáře Exchange Serveru a Active Directory.

Používáte-li ADC v prostředí rozlehlé sítě (WAN), umístěte tuto službu na nějaké strategické místo, například do osy topologie osy s rameny.

Synchronizujte celé sídlo Exchange Serveru a nikoli jen jednotlivé kontejnery příjemců.

Je možné vybrat celé sídlo Exchange Serveru jako zdroj a cíl na Exchange Serveru a také vybrat doménu Active Directory jako zdroj a cíl na sídle Active Directory. Tím se vlastně synchronizuje hierarchie kontejnerů příjemců v Exchange Serveru s hierarchií OU v systému Windows 2000 Server. Později můžete zvolit změnu hierarchie OU nebo umístění jednotlivých příjemců vytvořených v Active Directory pomocí ADC. Když

přesunete příjemce nebo OU na nové místo, pak ADC při následující synchronizaci najde nové umístění a synchronizuje je s existujícími příjemci – je-li to v oblasti hledání definovaných kontejnerů importu a exportu.

Nejlepšího výkonu dosáhnete, když nainstalujete službu ADC na nějaký členský server v doméně systému Windows 2000 Server.

Jestliže nakonfiguruje službu ADC s více dohodami o spojení, pak může v závislosti na časovém plánu synchronizace spotřebovávat značné množství času procesoru. Zamýšlíte-li instalovat ADC na řadič domény nebo globální katalog, musíte zajistit, aby hardware serveru zvládl přidáné zatížení.

Bud' vytvořte dohody o spojení ADC mezi globálním katalogem a Exchange Serverem nebo zaveďte ADC síťově blízko ke globálnímu katalogu.

V prostředí s více doménami prohledává ADC globální katalog a to i v případě, kdy neexistuje žádná dohoda o spojení, která by vyžadovala synchronizaci s globálním katalogem. Smyslem prohledávání globálního katalogu je zajistit, aby služba ADC nevytvářela v doménové struktuře duplikované objekty.

Strategie implementace služby ADC

Chcete-li úspěšně nainstalovat ADC a nakonfigurovat dohodu o spojení (connection agreement), musíte být schopni přihlásit se k systému Windows 2000 Server prostřednictvím účtu se zvláštními oprávněními. Oprávněními potřebnými k vykonávání různých úkolů jsou:

Počáteční instalace služby ADC

Když poprvé instalujete ADC v doménové struktuře Windows 2000, instalační program ADC rozšíří schéma Active Directory rozšířeními schéma Exchange. Aby to bylo možné, účet, z něhož instalační program spouštíte, musí patřit členovi skupiny Schema Administrators nebo musí mít oprávnění k rozšíření schématu.

Navíc vytváří instalační program ADC v konfiguračním kontejneru Active Directory další objekty. Proto je nezbytné, aby účet, ze kterého instalační program spouštíte, patřil členovi skupiny Domain Administrators nebo měl oprávnění k vytváření objektů v kontejnerech Services (služby) a Sites (sídla).

Instalační program ADC také vytváří v místní doméně dvě skupiny se zabezpečením – jednou je „Exchange Services“ a druhou „Exchange Administrators“. To vyžaduje, aby účet, z něhož instalační program spouštíte, patřil členovi skupiny Domain Administrators nebo měl oprávnění vytvářet objekty v kontejneru Users (uživatelé).

Následující instalace služby ADC

Následující instalace služby ADC ve stejné doménové struktuře nevyžadují oprávnění člena Schema Administrator. Vyžadují však buď oprávnění člena skupiny Domain Administrators nebo jiná konkrétní oprávnění, která vám umožní vytvářet nové objekty pod kontejnery Sites a Services v kontextu pojmenování konfigurace. Dodatečné instalace ve stejné doméně nevyžadují vytvoření skupiny Exchange Services ani skupiny Exchange Administrators. První instalace ADC do každé jiné domény systému Windows 2000 Server však vyžaduje vytvoření těchto skupin a tedy také potřebná oprávnění k provedení tohoto úkonu.

Konfigurace služby ADC

Zásady ADC lze nakonfigurovat po zobrazení stránek vlastností uzlu nejvyšší úrovně v modulu snap-in ADC Management konzoly MMC. Úpravou zásad můžete řídit sady

atributů synchronizovaných z obou adresářů a také sadu pravidel používaných službou ADC k vyhledávání stejných objektů v obou adresářích.

Schéma ADC a mapování objektů

Každá dohoda o spojení používá mapu tabulkového schéma pro většinu atributů objektů synchronizovaných mezi oběma adresáři. Výchozí mapa je umístěna v objektu zásad ADC v Active Directory. Je sice možné povolit a zakázat podmnožinu atributů, které se v jednotlivých směrech synchronizují, v modulu snap-in ADC Management konzoly MMC však není možné upravit mapování (připojování) schématu.

Tabulky 20.3, 20.4, 20.5 a 20.6 uvádějí mnoho mapování definovaných ve výchozí mapě schématu.

Tabulka 20.3 definuje mapování atributů všech objektů ve Windows 2000 a v Exchange. Pokud hodnota atributu, který se má mapovat, ve zdrojovém adresáři neexistuje, dané mapování se ignoruje.

Tabulka 20.3 Mapování atributů všech objektů

Atribut Windows 2000 (název LDAP) Všechny třídy objektů	Atribut Exchange (Název LDAP) Všechny třídy objektů
description	Admin-description
autoReply	AutoReply
businessRoles	Business-Roles
co	co
company	company
delivContLength	deliv-Cont-Length
department	department
displayName	cn
displayNamePrintable	name
distinguishedName	distinguishedName
dnQualifier	dnQualifier
employeeID	employeeNumber
extensionAttribute1	Extension-Attribute-1
extensionAttribute2	Extension-Attribute-2
extensionAttribute3	Extension-Attribute-3
extensionAttribute4	Extension-Attribute-4
extensionAttribute5	Extension-Attribute-5
extensionAttribute6	Extension-Attribute-6
extensionAttribute7	Extension-Attribute-7
extensionAttribute8	Extension-Attribute-8
extensionAttribute9	Extension-Attribute-9
extensionAttribute10	Extension-Attribute-10
extensionAttribute11	Extension-Attribute-11
extensionAttribute12	Extension-Attribute-12
extensionAttribute13	Extension-Attribute-13
extensionAttribute14	Extension-Attribute-14

extensionAttribute15	Extension-Attribute-15
facsimileTelephoneNumber	facsimileTelephoneNumber
generationQualifier	generationQualifier
homephone	homephone
homePostalAddress	homePostalAddress
houseIdentifier	houseIdentifier
info	info
initials	initials
l	l
Language	Language
mail	mail
mailnickname	uid
mobile	mobile
otherTelephone	Telephone-Office2
otherHomePhone	Telephone-Home2
telephoneAssistant	telephone-Assistant
pager	pager
personalPager	personalPager
personalTitle	personalTitle
physicalDeliveryOfficeName	physicalDeliveryOfficeName
postalCode	postalCode
secretary	secretary
sn	sn
st	st
street	street
streetAddress	postalAddress
telephoneNumber	telephoneNumber
telexNumber	telexNumber
teletexTerminalIdentifier	teletexTerminalIdentifier
textEncodedORAddress	textEncodedORAddress
title	title
userCertificate	userCertificate
userCert	user-Cert
userSMIMECertificate	userSMIMECertificate
url	url
x121Address	x121Address
autoReplyMessage	conferenceInformation
importedFrom	Imported-From

Tabulka 20.4 definuje mapování atributů všech objektů User (uživatel) a objektů Mailbox (poštovní schránka) v systému Windows 2000 a v programu Exchange.

Tabulka 20.4 Mapování objektů podle tříd

Atribut Windows 2000 (Název LDAP) Objekt User	Atribut Exchange (Název LDAP) Objekt Mailbox
givenName	givenName
manager	manager
altRecipient	Alt-Recipient
publicDelegates	public-Delegates
mdbUseDefaults	mdb-use-defaults
mdbOverQuotaLimit	MDB-Over-Quota-Limit
mdbStorageQuota	MDB-Storage-Quota
submissionContLength	submission-cont-length
mDBOverHardQuotaLimit	DXA-task
protocolSettings	protocol-Settings
mapiRecipient	mapi-recipient
msExchHomeServerName	home-MDB
msExchHomeServerName	home-MTA
deliverAndRedirect	deliver-and-redirect
garbageCollPeriod	garbage-coll-period
securityProtocol	security-Protocol
deletedItemFlags	DXA-Flags
objectSID	Assoc-NT-Account
authOrig	Auth-Orig
unauthOrig	Unauth-Orig
dLMemSubmitPerms	DL-Mem-Submit-Perms
dLMemRejectPerms	DL-Mem-Reject-Perms
folderPathname	Folder-Pathname

Tabulka 20.5 definuje mapování atributů objektů Contact (kontakt) a objektů Custom (vlastní) v systému Windows 2000 a v programu Exchange.

Tabulka 20.5 Mapování objektů podle tříd

Atribut Windows 2000 (Název LDAP) Objekt Contact	Atribut Exchange (Název LDAP) Objekt Custom
givenName	givenName
Manager	Manager
targetAddress	target-Address
protocolSettings	protocol-Settings
mapiRecipient	mapi-Recipient
AuthOrig	Auth-Orig
UnauthOrig	Unauth-Orig
dlMemSubmitPerms	dl-Mem-Submit-Perms
dlMemRejectPerms	dl-Mem-Reject-Perms

Tabulka 20.6 definuje mapování atributů objektů Group (skupina) a objektů Distribution List (distribuční seznam) v systému Windows 2000 a v programu Exchange.

Tabulka 20.6 Mapování objektů podle tříd

Atribut Windows 2000 (Název LDAP) Objekt Group	Atribut Exchange (Název LDAP) Objekt Distribution List
member	member
msExchExpansionServerName	home-MTA
managedby	owner
oOFReplyToOriginator	OOF-Reply-To-Originator
reportToOriginator	Report-To-Originator
reportToOwner	Report-To-Owner
hideDLMembership	Hide-DL-Membership
authOrig	Auth-Orig
unauthOrig	Unauth-Orig
dLMemSubmitPerms	DL-Mem-Submit-Perms
dLMemRejectPerms	DL-Mem-Reject-Perms

Určení počtu dohod o spojení potřebných ve vaší organizaci musí vycházet z vašeho konkrétního síťového prostředí včetně cílů a požadavků zavedení a vašich očekávání výsledků implementace. Musíte se také seznámit s atributy objektů Exchange Serveru a Active Directory, které není možné synchronizovat. Tyto atributy jsou uvedeny v tabulce 20.7.

Tabulka 20.7 Atributy objektů, které nelze synchronizovat

Active Directory systému Windows 2000 Server	Adresářová služba programu Exchange Server 5.5
Všechny informace o účtech, jako jsou Account Logging (protokolování účtů), Account Password (hesla účtů) atd.	Pokročilá nastavení zabezpečení
Informace o profilu	Seznamy řízení přístupu (ACL)
Oprávnění telefonického připojení služby Směrování a vzdálený přístup (Routing and Remote Access)	Domovské úložiště informací
Seznamy řízení přístupu (ACL)	

Správa objektů

Musíte určit, ze které adresářové služby budete objekty spravovat. Jak již bylo v této kapitole zmíněno, můžete pomocí ADC spravovat objekty z Active Directory, Exchange Serveru nebo z obou adresářových služeb.

Je důležité uvědomit si, že služba ADC zpracovává synchronizaci odstraněných objektů mezi těmito dvěma adresáři jinak, než jiné upravené objekty. ADC standardně nesynchronizuje odstranění objektů ze zdrojového adresáře do cílového adresáře. ADC místo toho zapíše na disk soubor importu, který obsahuje položky, jež se mají odstra-

nít. Správce si může v tomto souboru importu odstraněné objekty prohlédnout a podle potřeby může zadat import tohoto souboru, čímž odstraní sadu cílových objektů. Chcete-li používat přímou synchronizaci odstraňování objektů mezi adresáři, můžete potřebnou volbu zadat na kartě **Odstranění** (Deletion) stránek vlastností dohody o spojení. Můžete také ovládat, jak služba ADC zpracovává jednotlivé směry obousměrné dohody o spojení.

Správa objektů z Active Directory

Vyberete-li si správu objektů ze služby Active Directory, budete muset zavést všechny dohody o spojení tak, aby mohly zapisovat do adresáře Exchange Serveru. Pro každé sídlo Exchange Serveru, jehož příjemce budete spravovat z Active Directory, musíte vytvořit dohodu o spojení ze serveru v daném sídle na příslušnou doménu systému Windows 2000 Server. Příkladem vhodného nasazení tohoto modelu správy může být organizace, která spravuje informace o zaměstnancích v Active Directory nebo jiném adresářovém systému, jenž se s Active Directory synchronizuje. Pomocí ADC můžete aktualizovat adresář Exchange Serveru změnami v informacích o zaměstnancích.

Správa objektů z adresářové služby programu Exchange Server 5.5

Budete-li nadále spravovat objekty pomocí nástroje Exchange Administrator, měli byste své dohody o spojení nakonfigurovat jako „jednosměrné“, aby bylo možné zaplňovat a aktualizovat adresář Active Directory. Je možné vytvořit jedinou jednosměrnou dohodu o spojení pouze na jedno sídlo Exchange Serveru a prostřednictvím této jediné dohody o spojení synchronizovat celý adresář Exchange Serveru s adresářem Active Directory. Tím se odstraňuje potřeba vytvářet a spravovat více dohod o spojení mezi jednotlivými sídly Exchange. Je-li dohoda o spojení nakonfigurována na předávání informací z Exchange do Active Directory, můžete jako zdrojový kontejner vybrat libovolné sídlo Exchange Serveru.

Vyberete-li jako zdrojové kontejnery všechna sídla, budete moci synchronizovat celou sadu příjemců v adresáři Exchange Serveru. Tento model správy je vhodný při počátečním zavádění ADC. Model předává již vytvořená adresářová data Exchange Serveru do Active Directory, aniž by to mělo vliv na schopnost systému Exchange Server pokračovat v normálním provozu. Jakmile potřebným způsobem zaplníte Active Directory a porozumíte funkci ADC ve výrobním prostředí, můžete změnit své dohody o spojení na obousměrné nebo přenášet informace z Active Directory do Exchange.

Poznámka Jestliže jste za zdroje jednosměrné dohody o spojení určili více sídel Exchange Serveru a později se rozhodnete pro vytvoření obousměrné dohody o spojení, musíte z dané dohody o spojení odstranit kontejnery ze všech sídel, která nejsou místní. Abyste mohli upravovat objekty v nějakém sídle Exchange Serveru, musíte vytvořit samostatnou dohodu o spojení k libovolnému Exchange Serveru 5.5 v daném sídle.

Správa objektů z adresářové služby Active Directory i Exchange Serveru 5.5

Budete-li spravovat data z adresáře Active Directory i z adresáře Exchange Serveru 5.5, pak musíte vytvořit obousměrnou dohodu o spojení mezi sadou sídel a domén, které budete synchronizovat. Informace popisující, kam je zapotřebí dohody o spojení umístit, najdete v oddílu „Nastavení dohod o spojení“ dále v této kapitole. Vyberete-li si

správu objektů z obou adresářů, může být výsledkem složitější topologie dohod o spojení.

Tento model správy použijte, existují-li nějaká data, která spravujete z Exchange Serveru, a jiná data, která spravujete z Active Directory. Dojde-li ke změně stejného objektu v obou adresářích, bude platit nejnovější úprava. Synchronizace takového objektu však může trvat dva synchronizační cykly. To závisí na tom, zda byl objekt upraven před prvním synchronizačním cyklem nebo během prvního synchronizačního cyklu služby ADC.

Definování objektů synchronizace adresářů

Při definování objektů synchronizace adresářů mezi adresářem Exchange Serveru 5.5 a Active Directory musí být vašimi hlavními cíli:

- Poskytnutí důležitých či užitečných objektů z jednoho prostředí do druhého.
- Umožnění uživatelům, správcům a vývojářům snadný přístup k objektům.

Toho dosáhnete uspořádáním objektů systému Windows 2000 Server, jako jsou Users, Contacts a Groups, do kontejnerů příjemců, které zrcadlí kontejnery příjemců Exchange Serveru. Dále je uveden příklad, jak toho lze dosáhnout:

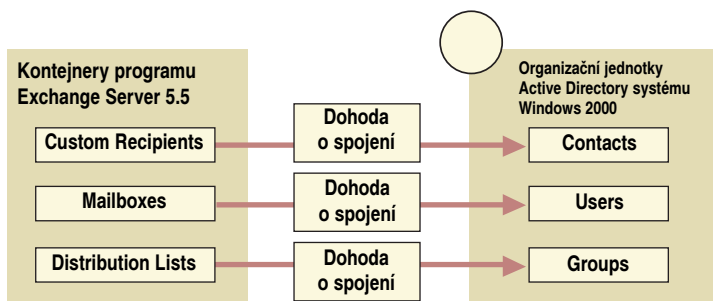
- V adresářové službě Exchange Serveru 5.5 vytvořte tři kontejnery příjemců:
 - Custom Recipients (vlastní příjemci)
 - Mailboxes (poštovní schránky)
 - Distribution Lists (distribuční seznamy)
- V systému Windows 2000 Server nakonfigurujte následující čtyři organizační jednotky (OU):
 - Contacts (kontakty)
 - Users (Uživatelé)
 - Groups (skupiny)
 - Computers (počítače)

Poznámka Nevytvářejte kontejner příjemců odpovídající organizační jednotce počítačů systému Windows 2000 Server, protože Exchange Server nesynchronizuje počítače.

Všechny interní uživatele ve vaší společnosti umístěte do kontejneru Users, všechny položky Custom Recipients vložte do kontejnerů Contacts a všechny položky Distribution Lists umístěte do kontejneru Groups. Nyní synchronizujte adresáře.

Existují dvě různé metody nastavení synchronizace mezi kontejnery Exchange Serveru a organizačními jednotkami Active Directory. Tady jsou:

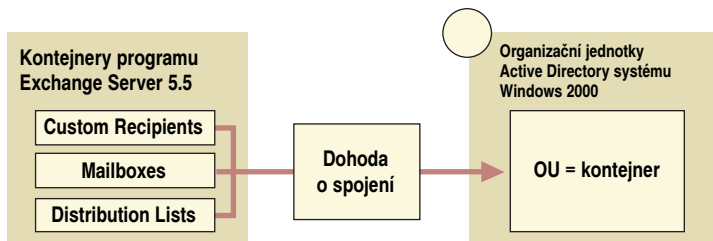
- První metoda vám dovoluje vytvořit tři samostatné dohody o spojení, které budou mapovat (připojovat) jednotlivé kontejnery Exchange Serveru k odpovídajícím jednotkám OU Active Directory. Například kontejner Custom Recipients v Exchange Serveru se připojí ke kontejneru Contacts v Active Directory atd.. Příklad této metody je uveden na obrázku 20.4.



Obrázek 20.4 Připojení kontejnerů Exchange Serveru k organizačním jednotkám systému Windows 2000 Server pomocí více dohod o spojení

- Alternativou k první metodě je vytvoření jediné dohody o spojení mezi nadřazeným kontejnerem všech podkontejnerů v Exchange Serveru a nadřazeným kontejnerem všech podkontejnerů v Active Directory. Při první synchronizaci adresářů ADC automaticky vytváří kontejnery pod nadřazeným kontejnerem systému Windows 2000 Server, kam se zrcadlí kontejnery v Exchange Serveru. V našem případě se objekty obsažené v kontejnerech Mailboxes, Custom Recipients a Distribution Lists replikují do příslušných kontejnerů, přičemž se zachovává hierarchie adresáře. Replikují se pouze kontejnery obsahující alespoň jeden objekt s podporou elektronické pošty.

Obrázek 20.5 ukazuje příklad vytvoření jediné dohody o spojení k připojení dat z určených kontejnerů Exchange Serveru do organizačních jednotek Active Directory.



Obrázek 20.5 Jediná dohoda o spojení připojuje kontejnery z Exchange Serveru do Active Directory systému Windows 2000 Server

Druhé metodě se dává přednost před první metodou, protože vytváříte méně dohod o spojení a systém vykonává většinu činností za vás.

Nastavení dohod o spojení

Když začnete nastavovat dohody o spojení, musíte vyhodnotit domény systému Windows 2000 Server a sídla Exchange Serveru a určit minimální počet dohod o spojení, které potřebujete pro zajištění optimálních operací. Doporučujeme vám nevytvářet dohodu o spojení mezi každým sídlem Exchange Serveru a doménou systému Windows 2000 Server ve vašem podniku.

V zájmu dosažení nejlepšího výkonu se při určování počtu dohod o spojení ve vaší organizaci zamyslete nad následujícími položkami:

- Rychlost, počet procesorů a množství paměti RAM pro každý server Exchange, Windows 2000 a ADC.
- Šířka pásma sítě.
- Celkový počet poštovních schránek (Mailboxes) Exchange Serveru a uživatelů (Users) Active Directory.
- Celkový počet vlastních příjemců (Custom Recipients) Exchange Serveru a kontaktů (Contacts) Active Directory.
- Celkový počet distribučních seznamů (Distribution Lists) Exchange Serveru a skupin (Groups) Active Directory.

Při implementaci použijte k vytvoření a konfiguraci dohod o spojení ve vaší organizaci ADC a modul snap-in Active Directory Connector Management.

Návrh dohod o spojení

Existuje několik kombinací, pro které lze nastavit dohody o spojení, aby docházelo k synchronizaci adresářové služby Exchange Serveru s Active Directory. Při plánování a vytváření dohod o spojení vycházejte z následujících základních kroků:

- Určete, která ze čtyř dále popsaných modelových organizací nejlépe odpovídá prostředí systému Windows 2000 Server a sídlu Exchange Serveru ve vaší organizaci.
- Vytvořte první návrh dohody o spojení, kterým začnete svůj plán dohody o spojení ADC.
- Připravte se na obhájení oprávněnosti svého návrhu a od managementu získejte souhlas se započítáním implementace.

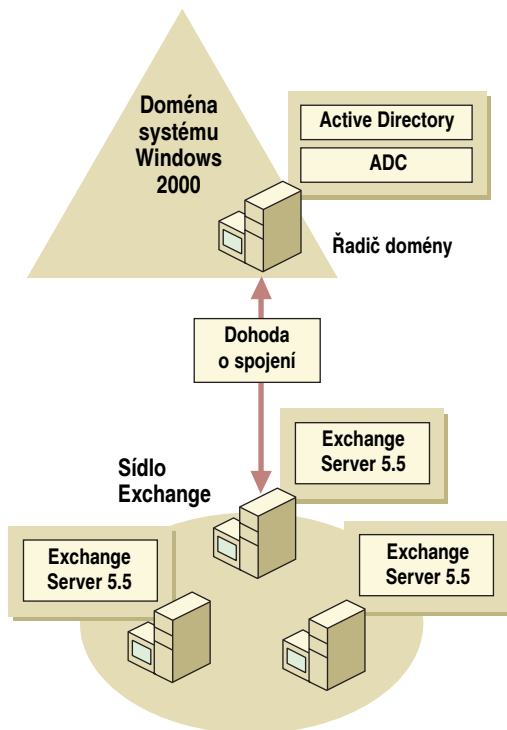
Během zavádění budete vytvářet dohody o spojení pomocí ADC a modulu snap-in Active Directory Connector Management.

Poznámka Ve všech dále uvedených modelech spojení ADC se předpokládá, že domény a sídla Exchange se nacházejí v jediné doménové struktuře. Jsou-li vaše domény a sídla Exchange roztroušeny v různých doménových strukturách, musíte pro každou doménovou strukturu vytvořit samostatnou topologii ADC.

Model spojení ADC číslo 1: Jedna doména systému Windows 2000 Server s jediným sídlem programu Exchange Server

Nejjednodušší architekturou domén v topologii systému Windows 2000 Server je jediná doména systému Windows 2000 Server s jediným sídlem Exchange. Tento model spojení obvykle přebírají menší organizace s jediným, centralizovaným sídlem a s průměrným počtem asi 5000 uživatelů.

Obrázek 20.6 představuje příklad toho, jak je možné vytvořit obousměrnou dohodu o spojení mezi jednou doménou systému Windows 2000 Server a jedním sídlem Exchange Serveru.



Obrázek 20.6 Jedna doména systému Windows 2000 Server s jedním sídlem Exchange Serveru

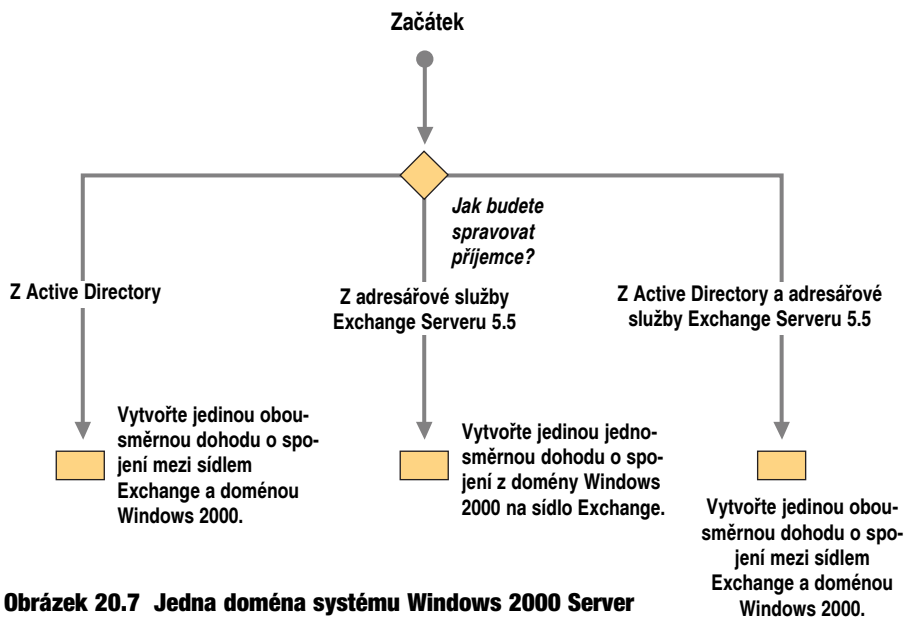
Své dohody o spojení můžete vytvořit tak, abyste mohli spravovat příjemce výhradně z Active Directory systému Windows 2000 Server, z Exchange Serveru 5.5 nebo z obou adresářů.

Odpovídá-li prostředí vaší organizace model spojení ADC číslo 1, použijte k vytvoření plánu dohody o spojení služby ADC ve vaší organizaci vývojový diagram uvedený na obrázku 20.7.

Model spojení ADC číslo 2: Jedna doména systému Windows 2000 Server s více sídly Exchange Server

Tento model spojení shledají optimálním pro své výrobní a obchodní potřeby menší a středně velké organizace s až 20 000 uživateli nebo organizace s více místními a vzdálenými sídly.

Obrázek 20.8 ukazuje příklad toho, jak lze vytvořit obousměrné dohody o spojení mezi jednou doménou systému Windows 2000 Server a více vybranými sídly Exchange Serveru.



Obrázek 20.7 Jedna doména systému Windows 2000 Server s jedním sídlem Exchange Serveru

Odpovídá-li nejlépe prostředí vaší organizace model spojení ADC číslo 2, použijte k vytvoření plánu dohody o spojení služby ADC ve vaší organizaci vývojový diagram uvedený na obrázku 20.9.

Poznámka Pokud se jedná o modely spojení ADC s více doménami nebo sídly, není nutné vytvářet dohodu o spojení mezi každou doménou systému Windows 2000 Server a každým sídlem Exchange Serveru. Dohodu o spojení mezi sídlem programu Exchange Server a doménou systému Windows 2000 Server je zapotřebí vytvořit jen v případě, kdy se v dané doméně nacházejí poštovní schránky Exchange s primárním účtem systému Windows NT Server.

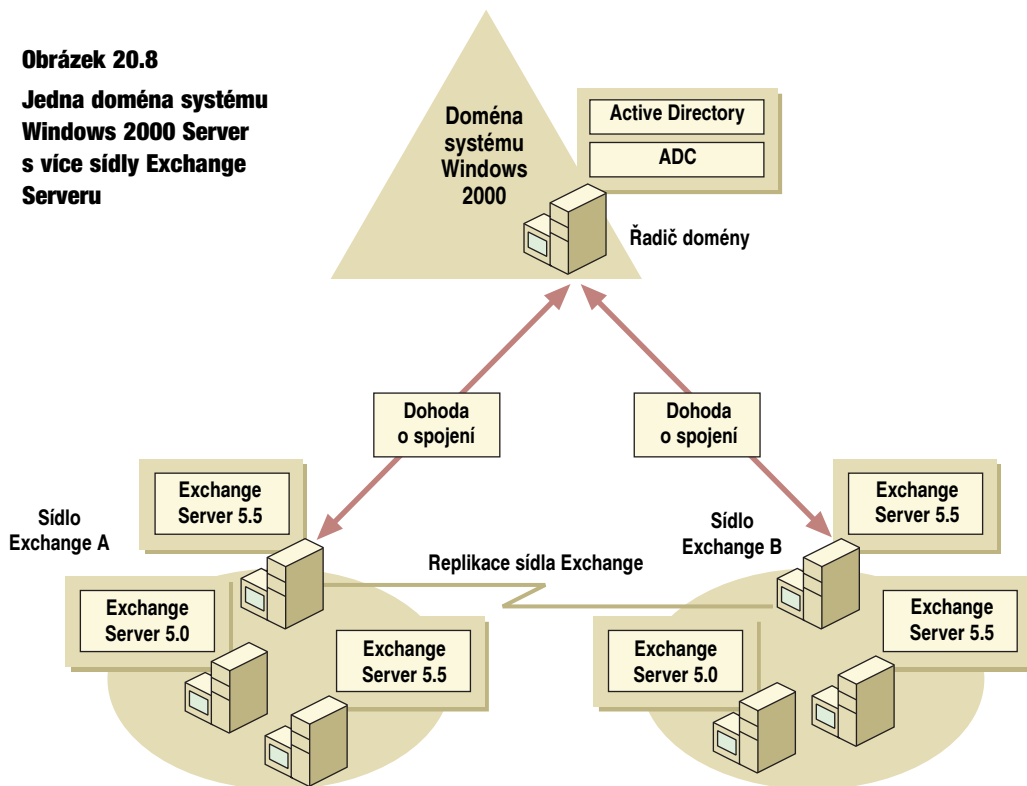
Model spojení ADC číslo 3: Více domén systému Windows 2000 Server s jediným sídlem programu Exchange Server

Tento model spojení lze aplikovat v plánu ADC pro střední až větší organizace nebo pro jedno oddělení velké, decentralizované organizace.

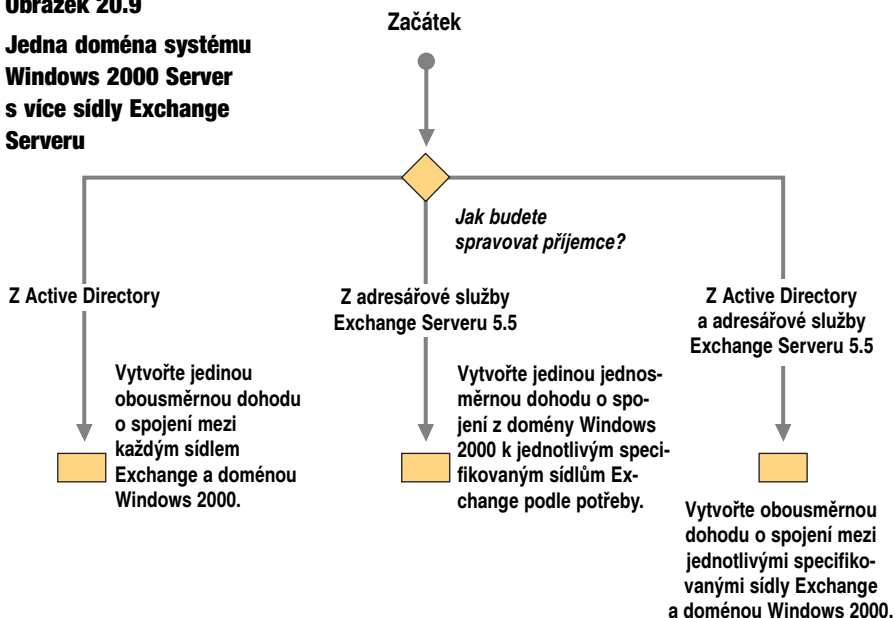
Obrázek 20.10 představuje příklad toho, jak lze vytvořit obousměrné dohody o spojení mezi více doménami systému Windows 2000 Server a jediným sídlem Exchange Serveru.

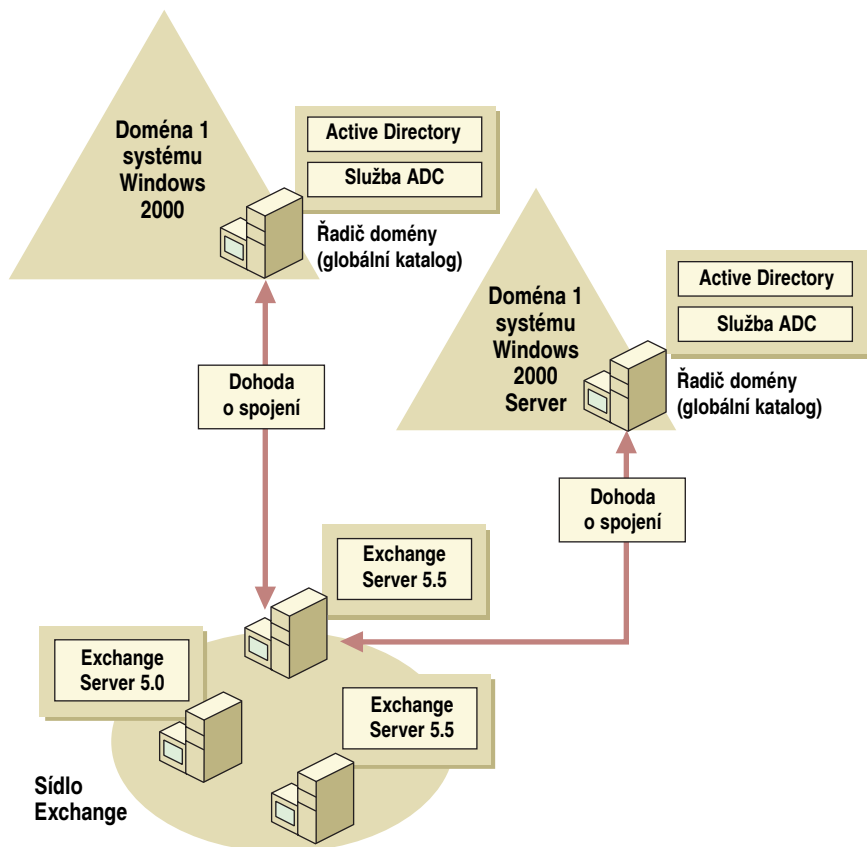
Obrázek 20.8

**Jedna doména systému
Windows 2000 Server
s více sídly Exchange
Serveru**

**Obrázek 20.9**

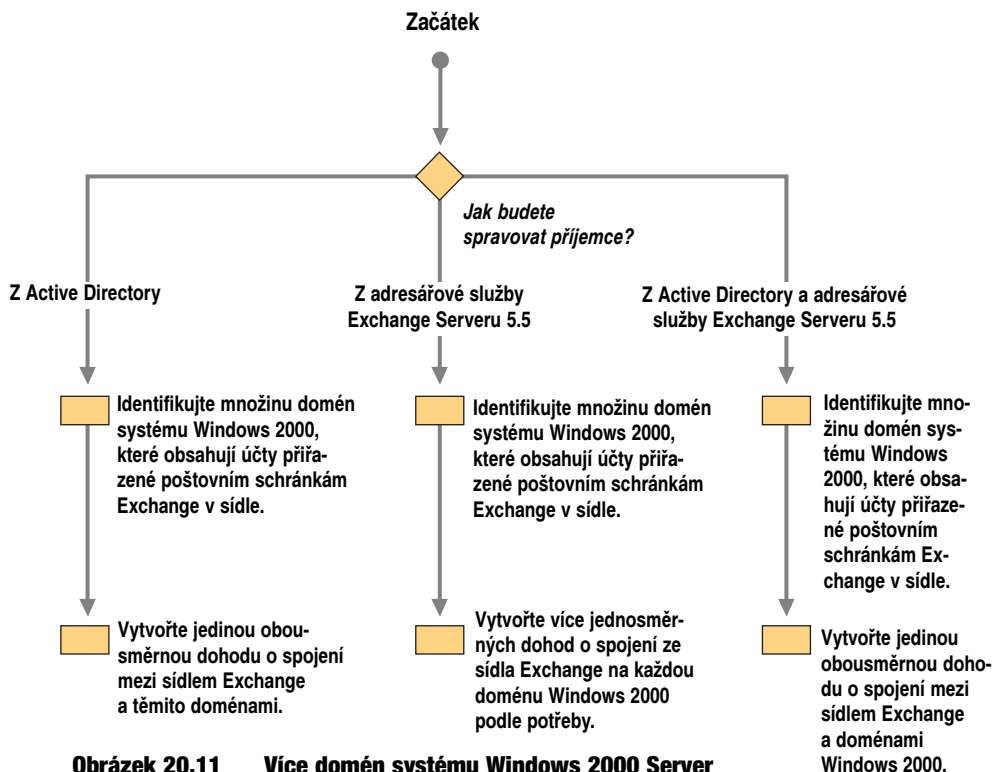
**Jedna doména systému
Windows 2000 Server
s více sídly Exchange
Serveru**





Obrázek 20.10 Více domén systému Windows 2000 Server s jedním sídlem Exchange Serveru

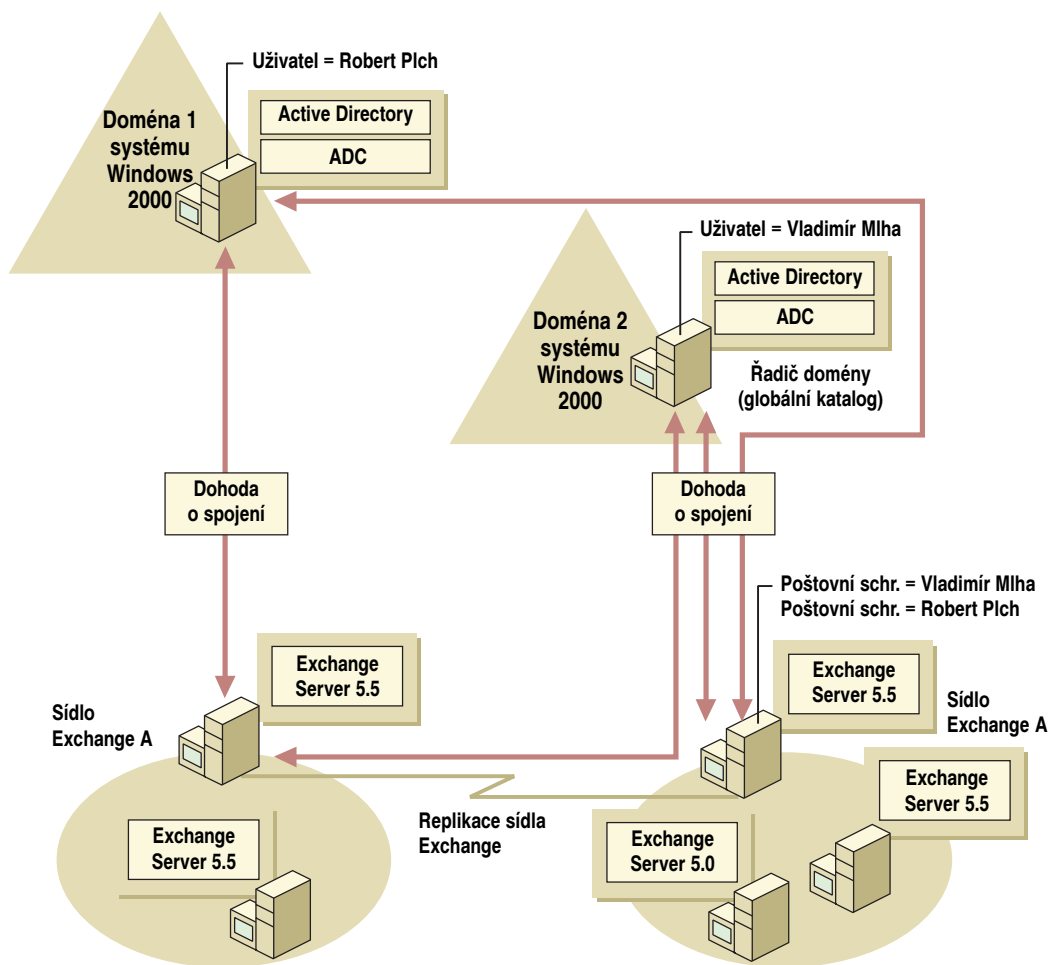
Odpovídá-li nejlépe prostředí vaší organizace model spojení ADC číslo 3, použijte k vytvoření plánu dohody o spojení služby ADD ve vaší organizaci vývojový diagram uvedený na obrázku 20.11. Tento diagram vám pomůže určit, jak budete spravovat příjemce v prostředí s více doménami systému Windows 2000 Server a jedním sídlem Exchange Serveru.



Model spojení ADC číslo 4: Více domén systému Windows 2000 Server s více sídly programu Exchange Server

Máte-li prostředí s více doménami a více sídly Exchange Serveru, váš návrh dohody o spojení může být poměrně složitý. Musíte si dokonale ujasnit smysl každé dohody o spojení, které plánujete vytvořit.

Obrázek 20.12 představuje příklad toho, jak lze vytvořit obousměrné dohody o spojení mezi více doménami systému Windows 2000 Server a více sídly Exchange Serveru.

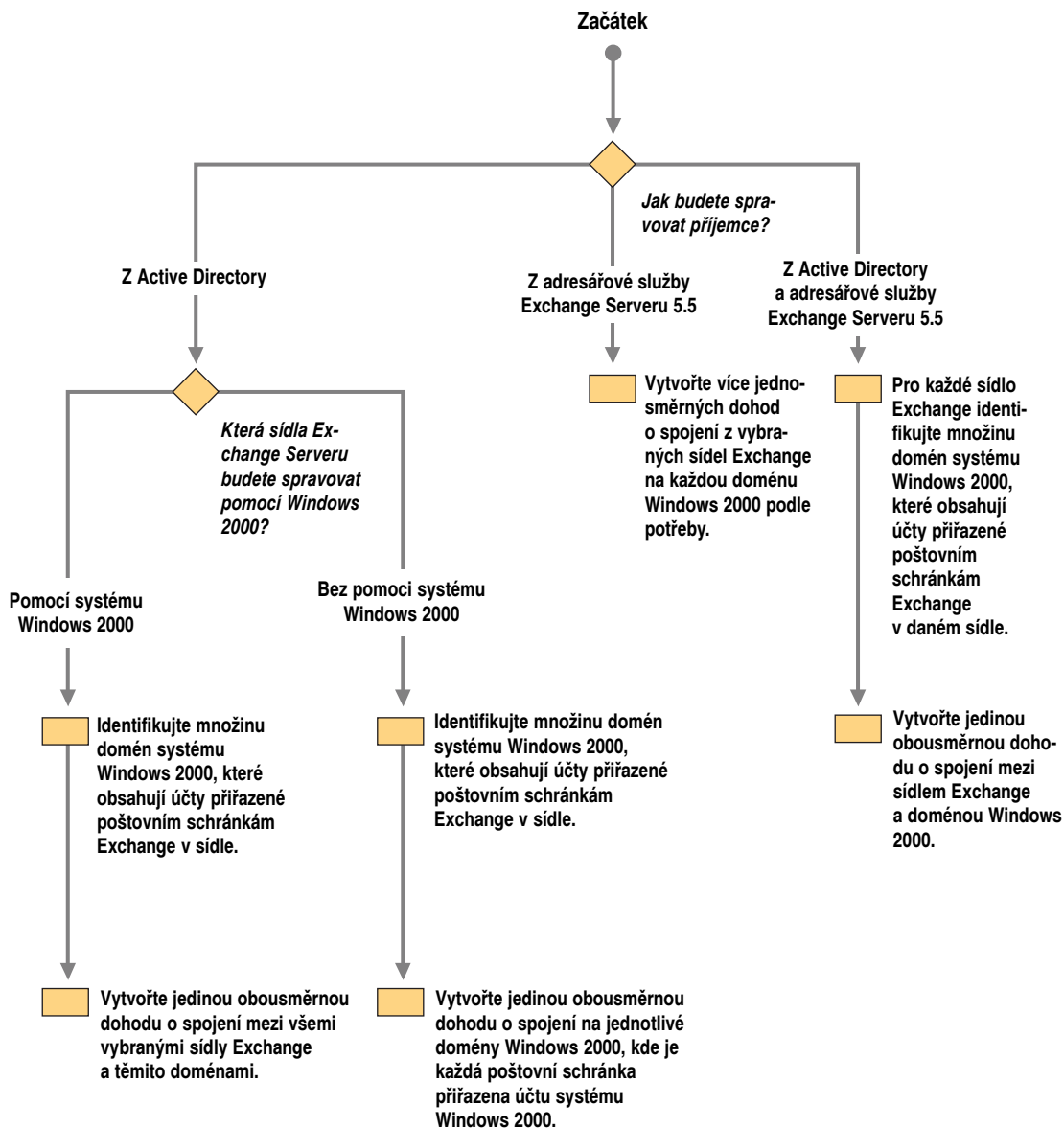


Obrázek 20.12 Více domén systému Windows 2000 Server s více sídly programu Exchange Server

Máte-li sadu domén systému Windows 2000 Server a sídel programu Exchange Server propojených pomocí služby ADC, může ADC obsahovat více dohod o spojení, přes které bude možné synchronizovat určitý konkrétní objekt. K rozhodování mezi dohodami o spojení ADC používá pravidel shodnosti založených na primárním účtu systému Windows NT Server poštovní schránky v Exchange Serveru a odpovídajícím účtu v Active Directory. Jestliže je služba ADC schopna přiřadit poštovní schránku k nějakému účtu systému Windows 2000 Server v některé z domén, se kterými se spojuje, bude synchronizovat tyto dva objekty.

Například na obrázku 20.12 se poštovní schránky Roberta Plcha a Vladimíra Mlhy v sídle Exchange Serveru B synchronizují s objekty uživatelů, které se nacházejí ve dvou samostatných doménách systému Windows 2000 Server.

Odpovídá-li nejlépe prostředí vaší organizace model spojení ADC číslo 4, použijte k vytvoření plánu dohody o spojení služby ADC ve vaší organizaci vývojový diagram uvedený na obrázku 20.13.



Obrázek 20.13 Více domén systému Windows 2000 Server s více sídly programu Exchange Server

Dokumentování plánu dohody o spojení ADC

V tomto okamžiku celého procesu byste se měli setkat s jádrem poradního týmu synchronizování adresářů a týmem zavedení a vytvořit profil, který bude zahrnovat tyto položky:

- Požadavky správců a koncových uživatelů.
- Vyhodnocení rizik.
- Hlášení o aktuálním stavu prostředí domén systému Windows NT Server nebo systému Windows 2000 Server a sídel programu Exchange Server.
- Úvahy o ideálním prostředí sídel systému Windows 2000 Server a programu Exchange Server.
- Uspořádání praktického prostředí systému Windows 2000 Server a sídel Exchange Serveru.

Abyste to mohli udělat, musíte získat všechny informace potřebné k vytvoření svého vlastního plánu dohod o spojení ADC. Plán musí dokumentovat dokončení následujících úkolů:

- Výběr jednoho z modelů spojení uvedených v předchozím oddílu.
- Určení požadavků síťové infrastruktury ADC a znalosti toho, jak se připravit na zavedení ADC.
- Určení adresářové služby, kterou budete používat ke správě objektů.
- Definování důležitých či užitečných objektů, které se budou synchronizovat mezi adresáři.

K vytvoření první verze plánu dohody o spojení ADC použijte své diagramy topologie domén systému Windows 2000 Server a sídel Exchange Serveru.

Testování konfigurace dohod o spojení

Program Active Directory Connector má v testovacím a výrobním prostředí zvláštní role. ADC použijte v testovacím prostředí k:

- vyhodnocení ADC;
- určení charakteristik výkonu ADC;
- vyhodnocení umístění dohod o spojení;
- vyhodnocení návrhu Active Directory s adresářovými informacemi z provozního adresáře Exchange Serveru.

Doporučujeme vám vytvořit si plán testování. Při plánování testování konfigurací dohod o spojení berte v úvahu tyto prvky:

- Vytvořte testovací laboratoř, která bude zrcadlit strukturu vašeho sídla Exchange Serveru a domén systému Windows NT Server nebo Windows 2000 Server.
- Budete-li vykonávat inovace hlavních domén účtů systému Windows NT 4.0 Server přímo na místě, musíte vytvořit řadiče domény systému Windows 2000 Server v testovací laboratoři tak, že převedete záložní řadiče domény (BDC) se systémem Windows NT 4.0 Server ve výrobním prostředí do režimu offline, přesunete je do testovací laboratoře a pak je budete inovovat na řadiče domény se systémem Windows 2000 Server. Jen tak zajistíte efektivní testování ADC.

- Vytvořte prostředí testovací laboratoře tak, abyste dokonale pochopili, jak bude ADC zaplňovat vaše provozní řadiče domény daty z Exchange Serveru. Určete, kdy v takovém případě bude ADC hledat shodu s existujícími objekty systému Windows 2000 Server a nebude tak vytvářet nové objekty systému Windows 2000 Server. Pravidla shody upravte podle potřeby tak, abyste zajistili řádné zaplnění adresáře Active Directory.
- V prostředí s více doménami a více sídly otestujte a vyhodnoťte plán dohody o spojení ADC, který jste vytvořili, a využití možností předmostí ADC k zajištění řádného zaplnění adresáře Active Directory.
- Budete-li zavádět paralelní doménu systému Windows 2000 Server, která se bude používat ve spojení s Exchange Serverem, otestujte ADC při vytváření nových uživatelů v rámci plánování celkové kapacity paralelní domény systému Windows 2000 Server.

Další informace o vytváření plánů testování najdete v kapitole „Vytvoření testovací laboratoře systému Windows 2000“ v této knize.

Určení časového plánu synchronizace adresářů

Jednotlivým dohodám o spojení lze zadat synchronizaci v určitou denní nebo noční dobu. Každá dohoda o spojení má svůj vlastní přiřazený časový plán. Jako správce určíte nejvhodnější dobu jednotlivých synchronizačních operací. Síť s velkým počtem uživatelů může vyžadovat častější synchronizaci než menší síť. V některých sítích je také zapotřebí synchronizovat určité objekty častěji než jiné objekty.

Následující výčet tvoří určité úvahy o vytváření časového plánu synchronizace.

- Určete, zda budete synchronizovat více než 100 000 uživatelů a poštovních schránek. Je-li tomu tak, můžete zlepšit výkon vytvořením více dohod o spojení sloužících k synchronizaci různých objektů v různých časech.
- Zadáváte-li změny v adresářích denně a jestliže vám stačí, když se tyto změny projeví v druhém adresáři až další den, měli byste zadat synchronizaci na noc.
- Seznamte se s interními časovými plány replikace jak Active Directory tak i adresáře Exchange Serveru. Chcete-li zajistit časově vhodné a výkonné využití prostředků, naplánujte synchronizaci ADC tak, aby byly synchronizace a interní replikace adresářů rovnoměrně rozloženy.
- Dochází-li k manipulaci s adresáři obvykle v určitém čase v týdnu, nastavte synchronizaci tak, aby k procesu synchronizace došlo krátce po zadání změn a pouze po zadání změn.

Hodina	Ne	Po	Út	St	Čt	Pá	So
0-1							
1-2							
2-3							
3-4							
4-5							
5-6							
6-7							
7-8							
8-9							
9-10							
10-11							
11-12							
12-13							
13-14							
14-15							
15-16							
16-17							
17-18							
18-19							
19-20							
20-21							
21-22							
22-23							
23-24							

	Hlavní pracovní hodiny
	Hodiny po pracovní době
	Denní synchronizace adresářů

Obrázek 20.14 Časový plán výroby a synchronizace adresářů

Při vytváření plánu dohody o spojení služby ADC vytvořte také časový plán synchronizace adresářů podobný tomu na obrázku 20.14. Šablonu listu plánování dohody o spojení služby ADC, kterou můžete využít při vytváření svého časového plánu synchronizace, najdete v příloze A.

Ochrana před náhodnou ztrátou dat

Ještě než vytvoříte první dohodu o spojení (connection agreement), musíte vyvinout plán zrušení operace synchronizace adresářů a zálohování a obnovení dat. Plán zálohování obnovení pro synchronizaci adresářů, který se stane součástí hlavního plánu zálohování a obnovení, vytvořte ve spolupráci se správcí sítě.

Tento oddíl popisuje, jak je možné zrušit operaci synchronizace, ať už data pocházejí z adresářové služby Exchange Serveru 5.5 nebo z Active Directory. Navíc zde najdete některé návrhy týkající se zálohování adresářů a popis nástrojů, které vám s takovým zálohováním pomohou.

Může nastat situace, kdy budete potřebovat zastavit operaci synchronizace adresářů v okamžiku, kdy již probíhá, a zrušit všechny změny uskutečněné službou ADC. Ve všech případech musíte před spuštěním procesu obnovení odstranit dohodu o spojení nebo ji zakázat. Metoda obnovení Active Directory do původního stavu se liší podle toho, jak je dohoda o spojení ADC nakonfigurována na synchronizaci dat.

Vždy byste měli pomoci příslušných zálohovacích nástrojů systému Windows 2000 Server zálohovat každý řadič domény, ke kterému se ADC připojuje (nebo na který se zapisuje). Samozřejmě musíte zálohovat také adresář nebo adresáře Exchange Serveru 5.5, ke kterým je služba ADC připojena. Nástroje zálohování, které používáte, musí podporovat autoritativní obnovení, aby dokumentované metody obnovení fungovaly. Autoritativní obnovení uvede doménu nebo kontejner zpět do stavu, v jakém byla nebo byl v okamžiku zálohování, a přepíše všechny změny zadané od posledního zálohování.

Další informace o autoritativním obnovení najdete v kapitole „Zálohování a obnovení služby Active Directory“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.

Dvěma situacemi, které mohou vyžadovat přerušení právě vykonávané synchronizace, jsou:

Příklad 1: Zaplnění Active Directory novými objekty

Dohoda o spojení je nakonfigurována na zavádění nových objektů (Contacts a Distribution Groups) v Active Directory. V tomto konkrétním případě vytvoříte vyhrazenou organizační jednotku, kam umístíte pouze objekty vytvořené ADC. Metoda obnovení bude spočívat v odstranění organizačních jednotek zadaných v dohodě o spojení. Tím se odstraní všechny objekty vytvořené dohodou o spojení v OU. Jestliže jsou v dané organizační jednotce umístěny nějaké jiné objekty Active Directory (například Users nebo Printers), při odstranění OU se také odstraní. Chcete-li zabránit ztrátě dat, objekty Users a Printers musíte před odstraněním OU někde přesunout.

Příklad 2: Zaplnění atributů (polí) existujících objektů

Služba ADC je nakonfigurována na zaplnění polí existujících objektů informacemi uloženými v adresáři Exchange Serveru. Objekty lze rozšířit do různých kontejnerů na řadiči domény. Zrušení změn vykonaných službou ADC vyžaduje v této situaci autoritativní obnovení. Tím se zruší změny zadané ADC, ale může to také způsobit ztrátu dat. Zároveň se ztratí všechny změny zadané od posledního zálohování ve vybrané doméně nebo kontejneru.

Autoritativní obnovení lze spustit také jen na určitých kontejnerech. Nejprve určíte, které kontejnery byly ovlivněny, a pak zadáte jejich autoritativní obnovení.

Další informace o zotavení po havárii najdete v kapitole „Určení strategií správy úložiště systému Windows 2000“ v této knize a v kapitolách „Zálohování“ a „Oprava, zotavení a obnovení“ v knize *Microsoft Windows 2000 Server Správa systému*.

Seznam úkolů plánování synchronizace adresářů

Seznam úkolů plánování synchronizace adresářů uvedený v tabulce 20.8 je přehledným výčtem odkazů na témata této kapitoly, který vám pomůže vyhledat důležité úkoly vytváření plánu dohody o spojení pro vaši organizaci.

Tabulka 20.8 Seznam úkolů plánování synchronizace adresářů

Úkol	Umístění v kapitole
Vytvořte plán dohody o spojení služby ADC.	Vytvoření plánu dohody o spojení služby ADC
Sestavte tými plánování a zavedení.	Vytvoření plánu dohody o spojení služby ADC
Prozkoumejte strukturu domén a topologii sídla Exchange Serveru.	Vytvoření plánu dohody o spojení služby ADC
Připravte síť na zavedení služby ADC.	Vytvoření plánu dohody o spojení služby ADC
Zamyslete se nad specifickými síťovými požadavky.	Vytvoření plánu dohody o spojení služby ADC
Určete, ze které adresářové služby budete objekty spravovat.	Vytvoření plánu dohody o spojení služby ADC
Spravujte objekty ze služby Active Directory.	Vytvoření plánu dohody o spojení služby ADC
Spravujte objekty z adresářové služby Exchange Serveru 5.5.	Vytvoření plánu dohody o spojení služby ADC
Definujte objekty pro synchronizování adresářů.	Vytvoření plánu dohody o spojení služby ADC
Připojte kontejnery Exchange Serveru k organizačním jednotkám systému Windows 2000 Server.	Vytvoření plánu dohody o spojení služby ADC
Nastavte dohody o spojení.	Vytvoření plánu dohody o spojení služby ADC
Navrhňte dohody o spojení.	Vytvoření plánu dohody o spojení služby ADC
Zdokumentujte plán dohody o spojení služby ADC.	Vytvoření plánu dohody o spojení služby ADC
Otestujte konfigurace dohod o spojení.	Vytvoření plánu dohody o spojení služby ADC
Určete časový plán synchronizace adresářů.	Vytvoření plánu dohody o spojení služby ADC
Zrušte práve vykonávanou synchronizaci.	Ochrana před náhodnou ztrátou dat

Další zdroje

- Další informace o programu Exchange Server 5.5 najdete v knize *Microsoft Exchange Server 5.5 Resource Guide*, která je součástí sady *Microsoft BackOffice Resource Kit, Second Edition*.
- Další informace o všech tématech této kapitoly najdete v odkazu Microsoft TechNet stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Zavádění klientů – systém Windows 2000 Professional



Při zavádění systému Windows 2000 je velmi důležité, kdy a jak nainstalujete klientské počítače. Část 6 vám nabízí informace plánování o automatizování instalace klientů a zavádění technologií správy změn a konfigurace.

V této části

Testování kompatibility aplikací se systémem Windows 2000 629

Definování strategie konektivity klientů 651

Definování standardů správy a konfigurace klientů 671

Aplikování správy změn a konfigurací 707

Automatizování instalace a inovace klientů 745

KAPITOLA 21

Testování kompatibility aplikací se systémem Windows 2000

Během plánování zavedení nového operačního systému vás už samotný rozsah tohoto počínu může svádět k tomu, zapomenout na aplikace, které na něm budou pracovat. Velmi důležitými kroky v projektu zavedení je však určení aplikací, které mohou během zavádění způsobovat problémy, a vyřešení všech souvisejících problémů ještě před začátkem zavádění.

Aby bylo zajištěno vyřešení možných problémů ještě před zaváděním, váš manažer testování aplikací musí začít s vývojem plánu testování aplikací pro systém Windows velmi brzy. Tato kapitola vás provede procesem testování kompatibility aplikací se systémem Microsoft Windows 2000.

V této kapitole

Přehled testování aplikací 630

Správa testování aplikací 631

Identifikování obchodních aplikací a určení jejich priorit 632

Příprava plánu testování aplikací 635

Testování aplikací 639

Sledování výsledků testování 645

Řešení nekompatibility aplikací 647

Seznam úkolů plánování testování aplikací 648

Další zdroje 649

Cíle kapitoly

Tato kapitola vám pomůže vyvinout následující dokumenty plánování:

- Seznam obchodních aplikací seřazených podle priorit
- Plán testování kompatibility aplikací
- Systém sledování a protokolování testování

Související informace v sadě Resource Kit

- Další informace o vytváření plánů testování najdete v kapitole „Vytvoření testovací laboratoře systému Windows 2000“ v této knize.
- Další informace o definování aplikačních standardů najdete v kapitole „Definování standardů správy a konfigurace klientů“ v této knize.

Přehled testování aplikací

Vzhledem k významným novým technologiím v systému Windows 2000 musíte jako součást svého projektu zavedení Windows 2000 otestovat kompatibilitu aplikací s operačním systémem. I když v současné době používáte systém Windows NT, nemůžete předpokládat, že všechny vaše aplikace budou stejným způsobem fungovat i ve Windows 2000. Vylepšení, jako například zlepšené zabezpečení znamenají, že musíte opakovaně otestovat všechny aplikace, které byly vyvinuty pro předchozí verzi Windows. Takové aplikace nemusí plně využívat nové funkce dostupné v systému Windows 2000, měly by však na tomto systému fungovat stejně dobře jako na vaší aktuální platformě.

Definice obchodní aplikace

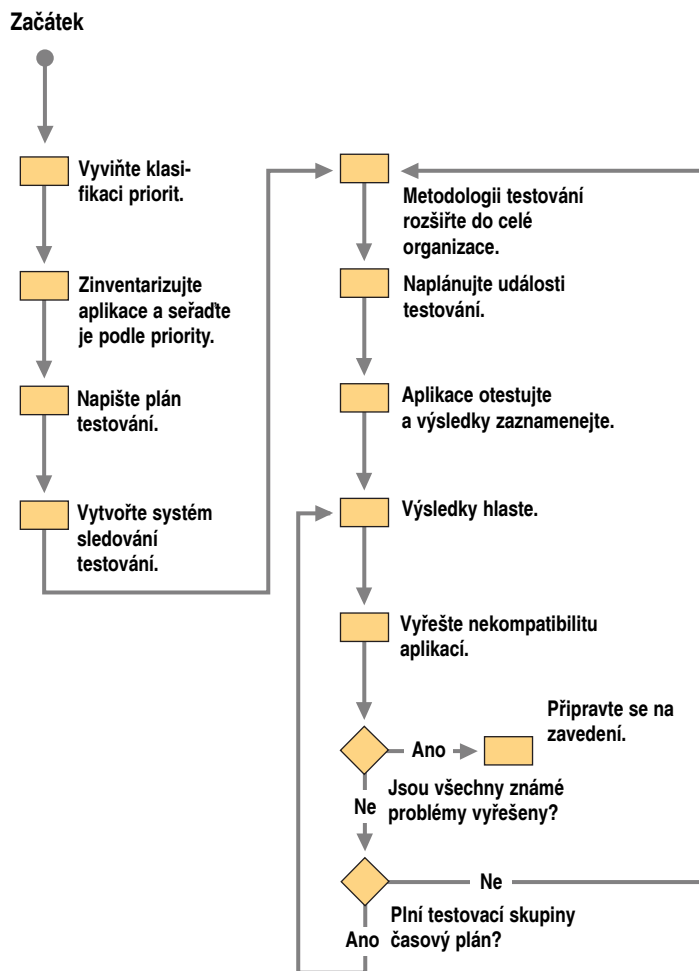
V této kapitole označuje termín „obchodní aplikace“ libovolnou aplikaci, která je pro vaši výrobu nebo obchod důležitá. Obchodní aplikace mohou představovat rozsáhlé obchodní systémy i specializované nástroje. Zvažte všechny aplikace, které pracují na klientských počítačích i serverech včetně normálně zakoupených komerčních produktů, upravených systémů od nezávislých společností a interně vyvinutých systémů.

Poznámka Třebaže se tato kapitola často odkazuje na klientské aplikace, metody a problémy zde popisované platí jak pro klientské tak i pro serverové aplikace.

Pokud se vaše organizace podobá jiným obvyklým organizacím, asi používá víc aplikací, než budete moci otestovat. V takovém případě musíte aplikace uspořádat podle priorit a pak otestovat ty, které jsou pro vaše základní výrobní či obchodní operace nepostradatelné. Další informace o vytvoření priorit aplikací najdete v oddílu „Identifikování obchodních aplikací a určení jejich priorit“ dále v této kapitole.

Proces testování aplikací

Obrázek 21.1 ilustruje kroky procesu testování aplikací. Nejprve musíte identifikovat aplikace systému Windows a seřadit je podle důležitosti pro váš provoz. Během této inventarizace můžete začít plánovat, jak budete testování koordinovat. Pak během testování musíte managementu pravidelně hlásit aktuální stav a řešit problémy s kompatibilitou, které odhalíte. Tato kapitola podrobně popisuje uvedené kroky.



Obrázek 21.1 Kroky testování aplikací

Správa testování aplikací

Vzhledem k rozsáhlosti testování aplikací vám doporučujeme vybrat manažera, který bude vyvíjet a plánovat metodologii testování a sledovat postup testování. Jestliže je vaše organizace nadnárodní nebo vysoce decentralizovaná, jmenujte manažery testování ve více místech, zejména pokud se v různých místech používají jiné sady aplikací. Použijete-li tento přístup, manažeri testování se mohou soustředit na potřeby specifické pro dané místo, jako jsou například jiní síťoví klienti nebo požadavky na výkon.

Základní prvky testování aplikací vytvořte již v ranných fázích projektu zavádění systému Windows 2000, abyste měli čas vyřešit problémy, které se mohou objevit. Projekt testování koordinuje manažer testování, který je zodpovědný za úkoly, jako je:

- vývoj systému seřazení aplikací podle priorit;
- koordinace procesů inventarizace a řazení podle priorit;
- vývoj metodologie testování;
- určení prostředků potřebných pro testování včetně hardwaru, softwaru a personálu;
- vytvoření časového plánu testování;
- zápis plánu testování;
- návrh nebo zakoupení systému sledování testování a hlášení;
- zdůrazňování důležitosti a strategií testování aplikací v zájmu dobré spolupráce s aplikačními experty;
- sledování postupu testování a jeho hlášení managementu, interním skupinám vývoje aplikací a externím prodejcům;
- bližší kontrola skupin, které neplní své závazky testování.

Identifikování obchodních aplikací a určení jejich priorit

Prvním úkolem přípravy na testování je získání informací o aplikacích, které jsou instalované na počítačích (na klientech i serverech). Získané informace, jako je četost použití dané aplikace a kolik uživatelů ji asi využívá, vám pomohou určit důležitost aplikace pro vaši výrobu nebo obchod.

Již při jejich identifikování řadte aplikace podle priority. Zvážit musíte každou aplikaci, i když se třeba zdá nepodstatná. Každá aplikace, která nefunguje správně, může mít velmi výrazný vliv, pokud ji někteří lidé nutně potřebují ke své práci.

Určení aplikací

Nemáte-li ještě inventář aplikací instalovaných na klientských a serverových počítačích, musíte jej vytvořit. Nezapomeňte do něj zahrnout provozní a administrativní nástroje včetně antivirových, kompresních a zálohovacích programů a programů vzdáleného řízení.

Získávání informací o aplikacích

Je-li vaše organizace velká nebo decentralizovaná, vytvoření úplného seznamu aplikací může být časově náročné. Používáte-li ke správě síťových počítačů server Microsoft Systems Management Server nebo jiný nástroj inventarizace softwaru, můžete ke sběru potřebných informací použít proces inventáře softwaru. Pak můžete spustit dotaz zajišťující kategorizaci informací a vytvoření potřebných sestav. Další informace o použití serveru Systems Management Server ke správě softwaru najdete v kapitole „Analýza infrastruktury sítě pomocí serveru Systems Management Server“ v této knize.

Nemáte-li možnost automatizovaně vyhledat aplikace instalované na počítačích, musíte vyvinout proces získání potřebných informací. Můžete například vytvořit dotazník nebo webový formulář, který vyplní manažeři jednotlivých obchodních či výrobních jednotek. Spolehnete-li se na takový ruční proces, měli byste o pomoc se získáním rychlých odpovědí požádat vyšší management.

Během vytváření seznamu aplikací určete, jaké aplikace jednotlivé obchodní či výrobní jednotky potřebují. Následující seznam obsahuje příklady některých informací o jednotlivých aplikacích, které můžete potřebovat:

- Název a verze aplikace
- Název výrobce
- Aktuální stav (například v provozu, ve vývoji nebo nepoužívá se)
- Počet uživatelů a jejich obchodní či výrobní jednotky
- Priorita neboli důležitost pro vaši organizaci
- Aktuální platformy, kde se aplikace používá

Také určete, zda se jedná o klientskou nebo serverovou aplikaci, a jaké komponenty jsou na klientovi nebo serveru umístěny.

- Adresy webových sídel (URL) v případě webových aplikací
- Požadavky na instalaci (například nastavení zabezpečení a instalační adresáře)
- Vývojový nástroj nebo technologie (pokud byla aplikace vyvinuta interně)
- Kontaktní jména a telefonní čísla (interní a prodejců)

Naleznete-li více kontaktů na jednoho prodejce, pokuste se je sjednotit.

Informace o aplikacích vložte na jediné místo, kam k nim můžete snadno přistupovat a aktualizovat je dalšími informacemi a kde je také možné vytvářet priority aplikací. Jakmile začnete aplikace testovat, můžete toto místo používat také k zadávání výsledků testování a hlášení stavu. Další informace o sledování a hlášení výsledků testů najdete v oddílu „Sledování výsledků testování“ dále v této kapitole.

Zjednodušení aplikačního prostředí

Proces inventarizace je vhodný také k získání dalších informací, které vám mohou pomoci při zajištění jednodušší a cenově výhodnější správy prostředí aplikací. Čím více toto prostředí zjednodušíte, tím snazší bude otestovat kompatibilitu aplikací, tím snazší bude přejít na systém Windows 2000 a tím lépe se bude výsledné prostředí spravovat.

Informace popsané v tomto oddílu mohou usnadnit testování a snížit budoucí náklady na podporu.

Informace o řešení problémů

Následující podrobné informace o aplikacích mohou pomoci pracovníkům testování odhalit problémy již během testování systému Windows 2000 a omezit tak budoucí nároky kladené na pracovníky technické podpory:

- Soubory instalované aplikací na pevný disk
- Datum vytvoření jednotlivých souborů
- Velikost jednotlivých souborů v bajtech
- Umístění instalovaných souborů
- Nastavení registru

Tyto informace byste měli získat spíš během instalace aplikací v testovací laboratoři a nikoli při inventarizaci aplikací. Když instalujete aplikace v řízeném prostředí, jako je laboratoř, mnohem pravděpodobněji získáte úplné seznamy bez nadbytečných informací o uživatelských souborech, které se nashromáždí během používání aplikace.

Nadbytečné aplikace

Používá-li vaše organizace mnoho podobných aplikací, bude proces inventarizace vhodnou dobou k vyhodnocení jejich nadbytečnosti a standardizaci těch nejpoužívanějších aplikací. Můžete například zjistit, že vaše organizace používá různé aplikace nebo verze nástrojů práce s textem. Standardizace jediné aplikace a verze může dramaticky zjednodušit testování systému Windows 2000 a omezit náklady na podporu klientů. Aplikační standardy mohou sice vyhodnocovat a vytvářet různé týmy, tým testování s nimi však musí úzce spolupracovat, aby se mohl zaměřit na testování příslušných aplikací. Další informace o standardizaci klientských konfigurací najdete v kapitole „Definování standardů správy a konfigurace klientů“ v této knize.

Neautorizované aplikace

Při vytváření seznamu aplikací můžete najít neautorizované aplikace, které si uživatelé stáhli z Internetu nebo přinesli z domova. Takové aplikace během procesu inventarizace odstraňte a také proveďte, že máte licence pro veškerý používaný software.

Aplikace licencované na síťovém sídle

Proces inventarizace je také vhodným okamžikem k identifikování aplikací licencovaných na sídle, jako jsou kompresní a antivirové programy, a vytvoření strategie jejich správy. Plánujete-li implementovat nástroj IntelliMirror, pak jeho prostřednictvím takové aplikace inzerujte. Použijete-li k inzerování aplikací IntelliMirror, můžete snadno nastavit redundantní servery a maximalizovat tak přístup uživatelů k těmto aplikacím. Další informace o použití nástroje IntelliMirror k podpoře klientů najdete v kapitole „Aplicování správy změn a konfigurací“ v této knize.

Neplánujete-li implementaci nástroje IntelliMirror, měli byste pro aplikace licencované na sídle vytvořit sdílené jednotky. Takovému serveru přiřadte název, který si lze snadno zapamatovat, například \\licencované_produkty.

Určení priority aplikací

Dokonce ještě než začnete vytvářet seznam aplikací, můžete už vymýšlet způsob jejich klasifikace a seřazení podle priority. Máte-li takové schéma k dispozici již v okamžiku inventarizace, můžete aplikace klasifikovat ihned po jejich nalezení. Schéma seřazení podle priorit potřebujete ze dvou důvodů:

- Nemáte třeba čas na řádné otestování všech aplikací do data zavedení systému.
- Potřebujete vědět, které aplikace jsou kritické a nejdůležitější, tedy které musí řádně fungovat, aby mohlo zavádění pokračovat.

Konečným cílem seřazení podle priority je identifikovat základní skupinu aplikací, které musí řádně fungovat, ještě před začátkem zavádění systému Windows 2000. Při vývoji schématu seřazení podle priority zvažte tyto otázky:

- Důležitost aplikace pro organizaci
- Počet uživatelů, na které má aplikace vliv
- Dostupnost novějších verzí
- Potřeby lokalizace

Ve vaší organizaci již může existovat schéma klasifikace, které lze použít nebo upravit. Třeba jste již vytvořili priority aplikací v rámci svého plánu zotavení po havárii. Jestliže již znáte aplikace, které musí být po havárii jako první online, tyto aplikace budou mít pravděpodobně nejvyšší prioritu i v testování kompatibility.

Složitost schéma řazení aplikací podle priorit závisí na takových faktorech, jako je počet aplikací a různorodost obchodních nebo výrobních funkcí, které podporují.

Jedna společnost pracující v oblasti nejnovějších technologií vyvinula čtyři úrovně priority. Své priority definovala takto:

Velmi důležité Tyto aplikace musí být po havárii online jako první. Jsou zapotřebí k zajištění příjmů společnosti nebo ke splnění právních závazků. Organizace nechce připustit žádné nebo jen velmi malé riziko selhání těchto aplikací a cena za selhání bude velmi vysoká.

Důležité Tyto aplikace musí být po havárii online jako druhé. Jsou zapotřebí pro fungování infrastruktury výroby či obchodu. Příkladem důležitých aplikací jsou aplikace lidských prostředků. Organizace připouští jen malé riziko selhání a cena za selhání bude střední.

Potřebné Tyto aplikace jsou zapotřebí pro fungování výroby nebo obchodu, mohou však být offline i po delší dobu. Organizace připouští střední riziko selhání a cena za selhání je nízká.

Ostatní Tyto aplikace nepatří do žádné z předchozích kategorií a výroba či obchod může probíhat i bez nich.

Jiná organizace pracující v oblasti nejnovějších technologií měla jen dvě kategorie aplikací: důležité a nedůležité. Tato organizace chtěla zajistit úplné testování všech důležitých aplikací a vyřešení všech problémů ještě před zaváděním nového systému, pokud bude mít pro testování k dispozici dostatek času.

Příprava plánu testování aplikací

Jedním z hlavních úkolů přípravy na testování je vytvoření plánu testování. V plánu testování určujete rozsah a cíle testování a použitou metodologii. Do plánu zahrňte také následující informace:

- **Rozsah**
Úrovně priorit, kterými se budete během testování zabývat.
- **Metodologie**
Kdo testování provádí a jaká je úloha účastníků.
- **Požadavky**
Jaký hardware, software, personál, školení a nástroje potřebujete k testování.
- **Kritéria úspěchu a neúspěchu**
Faktory určující úspěšné a neúspěšné testování aplikace.
- **Časový plán**
V jakém časovém horizontu plánujete dokončit testování.

V závislosti na počtu aplikací a přístupu k testování může testování aplikací vyžadovat rozsáhlou spolupráci s různými obchodními jednotkami ve vaší organizaci. Velmi brzy identifikujte nejdůležitější uživatele aplikací a požádejte je o revizi a schválení plánu testování nebo od nich získejte souhlas s možností využívat jejich prostředky v určitém dohodnutém rozsahu.

Další informace o vytváření plánu testování najdete v kapitole „Vytvoření testovací laboratoře systému Windows 2000“ v této knize.

Určení rozsahu testování

Jestliže vaše organizace používá mnoho aplikací, nemusíte mít dostatek času k otestování všech aplikací v úrovni, jaké byste rádi dosáhli. Nejprve otestujte aplikace s nejvyšší prioritou nebo nejčastěji používané či nejrozšířenější aplikace, testování však neomezujte jen na tyto aplikace.

Otestujte serverové i klientské aplikace. Klientské aplikace se obvykle testují nejobtížněji a jejich testování trvá nejdéle, což je dáno už pouhým jejich počtem.

I když byly komerční aplikace, které používáte, již otestovány nějakou externí organizací, měli byste je ještě otestovat ve svém prostředí. Testy určující kompatibilitu s různými technologiemi systému Windows 2000 nemusí zaručovat, že dané aplikace budou fungovat i ve vašem prostředí způsobem, jakým je používáte. Další informace o externě testovaných komerčních aplikacích najdete v oddílu „Testování aplikací“ dále v této kapitole.

Definování metodologie testování

Hlavní částí vašeho plánu testování bude popis strategie testování. Při plánování metodologie zvažte tyto otázky:

- Kde se bude testovat?
- Kdo bude testovat?
- Jak budete komunikovat a spolupracovat s účastníky?
- Jaký bude časový plán testování?
- Jak budete řešit problémy s aplikacemi?

Jednou z možností testování aplikací je převedení této odpovědnosti na externí nezávislou společnost. Při volbě této metody si zodpovězte následující otázky:

- Máte pro testování k dispozici personál?
- Má váš personál odpovídající úroveň znalostí?
- Jaké jsou interní náklady v porovnání s náklady na využití externích služeb?
- Jaký je váš časový rámec? Lze testování urychlit pomocí využití externích služeb?
- Jaké jsou požadavky na zabezpečení? Budete muset externí organizaci poskytnout důvěrná data?

Při interním testování vyberte zkušené testovací pracovníky. Má-li vaše organizace skupinu pracovníků testování aplikací, využijte jejich služby. Nemáte-li takovou skupinu nebo není-li možné tyto pracovníky na tento úkol nasadit, prozkoumejte možnosti využití různých prostředků k získání co nejlepších výsledků v rozumném čase. Můžete například s pomocí několika zkušených testovacích pracovníků vyvinout sady testovacích případů a pak proškolit jiné osoby v jejich používání. Zkušení testovací pracovníci mohou také vykonat základní sady testů a pak lze vyzvat výrobní či obchodní jednotky, aby do laboratoře poslali své experty, kteří pak vykonají funkce běžně používané při práci.

Vymyslete proces časového plánování testovacích dnů a komunikace s testovacími pracovníky. Můžete třeba vytvořit na intranetu webové sídlo, kde se každý může seznámit s daty testování, hlášeními o stavu, kontaktními jmény a dalšími souvisejícími dokumenty.

Vytvořte proceduru správy výsledků testování. Popište role a odpovědnosti včetně následujících položek:

- Kdo vyplňuje hlášení o problémech v systému sledování událostí?
- Jak se určuje prioritizace problémů a jejich přiřazení a vyřešení?
- Kdo sleduje řešení problémů a opakované testování aplikací?
- Jak testovací pracovníci zadávají výsledky testů do systému sledování a hlášení testování?

Studijní případ 1: Festivaly testování

Velká organizace pracující s nejnovější technologií požádala své vývojáře, aby otestovali kompatibilitu aplikací se systémem Windows 2000. Manažer testování pracoval s jinými manažery a tak dosáhl spolupráce s jejich týmy. Protože manažer testování podával hlášení řediteli oddělení IT a získal jeho plnou podporu pro tento program, bylo pro něj snazší dosáhnout aktivního zapojení dalších účastníků. Naplánoval testovací sezení v laboratoři a oznámení o sezení odeslal vývojářům. Laboratoř byla vybavena již nastavenými počítači, takže testovací pracovníci mohli ihned nainstalovat své aplikace. Testovací pracovníci mohli nainstalovat své aplikace z disků CD nebo ze sítě. Aby byla celá událost zábavnější, manažer zajistil jídlo a nápoje, čímž si sezení vysloužila označení „festivaly testování“.

Studijní případ 2: Předběžný program

Významná výrobní společnost vyvinula předběžný program testování systému Windows 2000 Professional. Tento program použila k testování klientských aplikací. Organizace nejprve prověřila, že je sada protokolů používaných na klientských počítačích se systémem Windows 2000 kompatibilní s jejich provozním prostředím systému Windows NT 4.0. Pak zavedla systém Windows 2000 Professional v omezených lokacích na provozní síti a vytvořila tak místo pro testování aplikací.

Tým projektu vytvořil webové sídlo s informacemi o tomto programu. Uživatelé, kteří se chtěli zúčastnit předběžného programu, vyplnili na webovém sídle formulář žádosti. Aby se omezil počet účastníků a zajistilo se dokonalé otestování, vedoucí projektu a manažer zaměstnanců prověřili a schválili žádosti. Program, který se omezil na 50–100 účastníků, zaručil účast velkého počtu pracovníků pro testování aplikací. Testovací pracovníci posílali své problémy na webové sídlo.

Určení požadavků na prostředky

Při plánování testování kompatibility aplikací mějte na paměti budoucí stav vašeho počítačového prostředí. Plánujete brzkou inovaci některého softwaru na verze, které plně využívají nové funkce systému Windows 2000? Plánujete implementovat nové standardní konfigurace počítačů nebo používat terminálové služby? Tyto otázky určují potřebné prostředky a aplikace, které se budou testovat jako celek.

Plánujete-li během postupného zavádění používat nové aplikace společně se systémem Windows 2000, otestujte tyto aplikace s aktuálními aplikacemi.

Testování umožníte tak, že vytvoříte laboratoř, kde budou moci testovací pracovníci vykonávat své testy. V takové laboratoři můžete mít vždy k dispozici potřebné nástroje a vybavení. Některé organizace vytvářejí laboratoř testování aplikací nezávisle na testovací laboratoři systému Windows 2000. Nemáte-li dostatečné prostředky pro samostatnou laboratoř, můžete sdílet laboratoř s jiným projektem nebo programem školení. Bu-

dele-li sdílet laboratoř, snažte se vybrat takovou, která má odpovídající časové plánování a splňuje požadavky na vybavení.

V laboratoři nastavte testovací počítače na duální nebo trojitě spouštění, aby mohli testovací pracovníci rychle použít režim, ve kterém potřebují nainstalovat své aplikace. Budete-li třeba postupovat podle strategie uvedené v oddílu „Testování aplikací“ dále v této kapitole, můžete k testování aplikací v rámci inovace potřebovat systémy Windows NT 4.0 i Windows 2000. Aby mohli testovací pracovníci snadno uvést počítače do původního stavu, vytvořte diskové obrazy jednotek se základními operačními systémy.

Také se zamyslete nad tím, zda je zapotřebí připojit laboratoř k síti společnosti. Abyste mohli instalovat určité aplikace ze sítě, můžete například potřebovat přístup k místům sdílení sítě, a vyvíjíte-li webový systém sledování, budete potřebovat přístup k intranetu společnosti. Potřebujete-li takový přístup, nejprve ověřte, že je sada protokolů používaná na klientských počítačích kompatibilní s vaším provozním prostředím.

Máte-li velkou laboratoř, můžete jmenovat vedoucího laboratoře. Protože dovednosti potřebné k vedení laboratoře a k vedení testování jsou velmi odlišné, do obou rolí raději jmenujte různé osoby. Vedoucí laboratoře musí mít značné technické znalosti, zatímco vedoucí testování musí disponovat manažerskými a komunikačními dovednostmi.

Další informace o vytváření a správě testovací laboratoře a o vytváření plánu testování najdete v kapitole „Vytvoření testovací laboratoře systému Windows 2000“ v této knize.

Definování kritérií úspěchu a neúspěchu

Při vykonávání různých testů budou některé aplikace úspěšné a jiné neúspěšné. Musíte definovat postup říkající, kam mají účastníci testování zaznamenat problémy s aplikacemi a otázky, které je zapotřebí vyřešit.

Jakmile pracovníci testování dokončí testy určité aplikace, musí výsledky zadat do vašeho systému sledování a hlášení testování. Všechny podstatné problémy musíte samozřejmě seřadit podle priority, sledovat je a po vyřešení problémů aplikace opakovaně otestovat. Abyste však mohli sledovat postup testování, budete muset vědět, které aplikace jsou připravené a které nejsou. Plánujete-li sledovat postup podle toho, zda byly aplikace úspěšné nebo neúspěšné, musíte definovat kritéria pro každou používanou kategorii. Při definování kritérií úspěchu a neúspěchu se zamyslete nad otázkami podobnými těmto:

- Jak důležitý daný problém je? Ovlivňuje důležitou funkci nebo jen okrajovou?
- Jak je pravděpodobné, že se s tímto problémem někdo setká?
- Je možné nějakým způsobem se danému problému vyhnout?

Vytvoření časového plánu testování

Časový plán testování závisí na mnoha podmínkách, jako jsou tyto:

- Kolik testovacích pracovníků se bude projektu účastnit.
- Zda budou testovací pracovníci pracovat na tomto projektu neustále nebo jen částečně.
- Jaká je úroveň zkušeností testovacích pracovníků.
- Jaký je počet a složitost aplikací.

V časovém plánu vyhradte dostatek prostoru na řešení problémů a opakované testování neúspěšných aplikací. Stanovte hlavní a podružné cíle, abyste mohli sledovat postup a ujistit se, že plníte časový plán.

Testování aplikací

Společnost Microsoft vyvinula ve spolupráci se zákazníky a nezávislími prodejci softwaru (ISV) specifikaci Windows 2000 Application Specification. Aplikace napsané podle této specifikace nejsou jen kompatibilní se systémem Windows 2000, ale také využívají jeho nové technologie.

Specifikace Windows 2000 Application Specification, kterou si můžete nahrát z webového sídla Microsoft Developer Network (MSDN), má dvě součásti: jednu pro desktopové aplikace a jednu pro distribuované aplikace. Specifikace desktopových aplikací platí pro aplikace spouštěné na systému Windows 2000 Professional, ať už se jedná o samostatné programy nebo klientskou část distribuované aplikace. Specifikace distribuovaných aplikací platí pro aplikace pracující na systému Windows 2000 Server. Další informace o této specifikaci a možnost jejího nahrání najdete v odkazu Windows 2000 Application Specification stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Komerční aplikace, které splňují specifikaci Windows 2000 Application Specification, lze také certifikovat. Certifikované aplikace byly otestovány nezávislou testovací organizací a splňují určité požadavky. Aby mohla aplikace obdržet certifikaci, musí například používat nástroj Windows Installer. Komerční aplikace mohou odpovídat uvedené specifikaci, aniž by byly certifikované. V takovém případě aplikaci testuje prodejce a nikoli nezávislá testovací organizace.

Některé organizace činí ze splnění této specifikace kritérium výběru při koupi aplikací, které budou součástí projektu zavedení systému Windows 2000. Vyvíjíte-li aplikace interně, zvažte přidání specifikace do pokynů pro vývoj aplikací.

V současné době již bylo otestováno mnoho komerčních aplikací a bylo určeno, jak dobře podporují systém Windows 2000. Společnost Microsoft nabízí adresář aplikací systému Windows 2000, kde si můžete vyhledat stav aplikací, které používáte. Další informace o tom, které klientské a serverové produkty podporují Windows 2000, najdete v odkazu Directory of Windows 2000 Applications stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Adresář používá následující označení:

Certified (certifikována) Označuje, že aplikace byla testována nezávislou testovací společností a že využívá nové funkce systému Windows 2000.

Ready (připravena) Označuje, že podle výrobce byla testována kompatibilita aplikace a její podpora ve Windows 2000. Aplikace však nemusí využívat nové funkce Windows 2000.

Planned (plánována) Označuje, že cílem výrobce je, aby aplikace po úplném testování splnila kritéria kategorie Certified nebo Ready.

Vývoj strategií testování

Cílem testování aplikací je zajistit, že vše, co funguje na aktuální platformě, bude fungovat také na systému Windows 2000. Jestliže byla nějaká aplikace napsána pro předchozí verzi Windows, nemusí sice nejvýhodněji používat nové funkce systému Win-

dows 2000, ale její funkce budou v systému Windows 2000 pracovat stejně dobře, jako na vaší aktuální platformě.

Strategie pro komerční aplikace

V případě komerčních aplikací je prvním krokem spuštění instalačního programu systému Windows 2000 Professional v režimu kontroly inovace a zjištění možné nekompatibility. Když spustíte instalační program v tomto režimu, porovná instalovaný software se seznamem známých nekompatibilních aplikací a výsledky zaprotokoluje. Syntaxe příkazového řádku režimu kontroly inovace je:

winnt32 /checkupgradeonly

Tento nástroj vás sice může upozornit na možné problémy s kompatibilitou, týká se však jen malého procenta vašich aplikací a navíc se kontrolují jen aplikace instalované na daném počítači. Když nějaká aplikace není na seznamu nekompatibilních aplikací, neznamená to, že musí být kompatibilní. Další informace o instalačním programu najdete v kapitole „Automatizování instalace a inovace klientů“ v této knize.

Dalším krokem je prověření adresáře aplikací Windows 2000 a určení kompatibility aplikací, které používáte.

I když zjistíte, že určité aplikace již testoval někdo jiný, měli byste je otestovat ve svém prostředí. V takovém případě se při testování zaměřte na konkrétní způsoby, jakými aplikaci využívá vaše organizace. Otestujte například:

- konfigurace, které vaše organizace používá;
- nejčastěji používané funkce;
- kombinace aplikací používaných společně.

Oddíl „Tipy testování“ dále v této kapitole uvádí příklady způsobů testování funkce aplikací. Jestliže nebyly některé vámi používané komerční aplikace testovány na kompatibilitu jinými organizacemi, měli byste je otestovat důkladněji.

Nezapomeňte otestovat svůj antivirový software. Mnoho takových aplikací vyžaduje inovaci, což je dáno jejich způsoby používání filtrů systému souborů. Díky změnám v systému souborů NTFS nemusí mnoho filtrů systému souborů Windows NT 4.0 ve Windows 2000 pracovat.

Strategie pro vlastní aplikace

Používáte-li vlastní produkty nezávislých výrobců nebo vyvíjíte-li své aplikace interně, musíte vytvořit rozsáhlejší strategii testování, než jaká byla uvedena u komerčních aplikací.

Specifikace Windows 2000 Application Specification vám může pomoci i při testování aplikace, kterou jste sami nevyvinuli. Webové sídlo MSDN obsahuje verzi této specifikace, kterou si můžete nahrát, i plán testování podrobně popisující všechny testy společnosti Microsoft vykonávané při certifikaci aplikace systému Windows 2000. Tento plán testování pro vás může představovat nové myšlenky o funkčních oblastech a způsobech testování. Další informace o nahrání specifikace a plánu testování najdete v odkazu Application Specification Download stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Webové sídlo MSDN také obsahuje další důležité informace o testování, jako jsou dokumenty o důkladném testování a metody používané nezávislými testovacími organizacemi při testování funkcí aplikací, které jejich výrobci podrobí certifikačnímu procesu.

Tipy testování

Návrhy týkající se testování v tomto oddílu nejsou všezahrnující a neplatí pro všechny situace. Jsou tu proto, aby vám pomohly s vymýšlením možností testování.

Testování scénářů zavedení

Měli byste otestovat instalaci a spuštění aplikací pomocí scénářů, které plánujete použít během zavádění. Můžete třeba naplánovat zavádění instalováním na čisté počítače nebo inovací ze systému Windows 3.x nebo z dřívějších verzí systému Windows NT. Plánujete-li inovaci, můžete aplikace během inovace ponechat na počítači, nebo je můžete odinstalovat a nainstalovat zpět až po inovaci.

Zvažte také opakované zabalení aplikace pro nástroj Windows Installer nebo do formy souborů .zap, aby bylo možné aplikaci spravovat nástrojem instalace a správy softwaru IntelliMirror. Další informace o přebalení aplikací najdete v kapitole „Aplikování správy změn a konfigurací“ v této knize.

Vzhledem k rozdílům mezi Windows 3.x a Windows 2000 funguje instalace některých aplikací různě podle operačního systému, který používáte k instalaci. Když například nainstalujete nějakou aplikaci na počítač se systémem Windows 3.x a pak počítač inovujete na systém Windows 2000, aplikace nemusí fungovat stejně, jako kdybyste ji přímo nainstalovali na systém Windows 2000. V takovém případě může být nutné aplikaci odstranit a znovu ji nainstalovat po inovaci nebo získat potřebnou dynamickou knihovnu (DLL) migrace.

Knihovna DLL migrace umožňuje aplikaci, která byla původně instalována na systému Windows 3.x fungovat správně i po inovaci počítače na systém Windows 2000. Knihovny DLL migrace mohou řešit problémy s aplikacemi vykonáním těchto akcí:

- Náhradou nebo inovací souborů specifických pro Windows 3.x soubory kompatibilními s Windows 2000.
- Přesunem nastavení aplikace a uživatelů na správné místo v systému Windows 2000.
- Připojením klíčů registru specifických pro Windows 3.x k příslušným místům v systému Windows 2000.

Pro aplikace vyvinuté interně můžete vytvořit knihovny DLL migrace nebo je můžete získat od výrobců. Více informací o vytváření a testování knihoven DLL migrace získáte, když budete v knihovně MSDN Library vyhledávat klíčová slova „migration DLL“. Další informace o MSDN Library najdete v odkazu MSDN stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>. Některé knihovny DLL migrace jsou součástí Windows 2000.

Protože výsledky se mohou podle použité metody inovace lišit, je důležité testovat aplikace stejnými postupy a nástroji, které plánujete používat během postupného zavádění. Nemáte-li při testování aplikací tyto postupy a nástroje ještě k dispozici, otestujte alespoň scénář, který plánujete použít.

Scénář inovace

Plánujete-li inovovat počítače, použijte následující postup:

- Nainstalujte systém Windows 3.x nebo Windows NT 3.51 či novější.
- Nainstalujte aplikaci.
- Inovujte na systém Windows 2000.
- Aplikaci otestujte.

Jestliže aplikace pro Windows 3.x nefunguje správně, kontaktujte nezávislého výrobce a požadujte knihovnu DLL migrace. Jestliže nefunguje správně aplikace pro Windows NT, kontaktujte nezávislého výrobce a požadujte opravu nebo nový instalační program.

Scénář čisté instalace

Plánujete-li instalovat systém Windows 2000 na přeformátované počítače, postupujte takto:

- Nainstalujte Windows 2000.
- Nainstalujte aplikaci.
- Aplikaci otestujte.

Jestliže aplikace nefunguje správně, kontaktujte nezávislého výrobce a požadujte opravu nebo nový instalační program.

Testování instalování a odinstalování

Instalaci aplikace otestujte různými způsoby, například:

- Ukončete instalaci před jejím dokončením.
- Vyzkoušejte všechny možnosti instalace používané ve vašem prostředí.
- Umožňujte-li vaše organizace uživatelům instalovat si aplikace, otestujte instalaci jako správce i jako zkušený uživatel. Pak otestujte funkci aplikace.
- Zkuste aplikaci odinstalovat.
- Prověřte, že lze aplikaci nainstalovat jako správce a odinstalovat jako uživatel. Když je nějaký uživatel přihlášen jako obyčejný uživatel, musí dojít buď k úplnému odstranění aplikace, nebo to nesmí být vůbec možné.

Testování základních funkcí aplikace

Aplikace otestujte pomocí funkcí, konfigurací a aplikačních sad, které používáte ke splnění svých výrobních či obchodních úkolů. Můžete zkusit třeba následující typy testů:

- Přihlaste se jako uživatel a otestujte funkce nejdůležitější pro koncové uživatele. Otestujte specifické scénáře potřebné k vykonání obchodních či výrobních úkolů.
- Přihlaste se jako několik uživatelů, kteří jsou členy skupiny Users.
- Aplikujte na systém a aplikace zásady skupiny.
- Otestujte kombinace aplikací, jako jsou například standardní konfigurace počítačů.
- Nechte na počítači několik dnů spuštěných více aplikací bez jejich ukončení.
- Otestujte automatizované úkoly využívající jazyk Microsoft Visual Basic for Applications (VBA) v aplikacích Microsoft Office.
- Otestujte konzistentní podporu dlouhých názvů souborů. Do názvů zahrňte také tečky a proveďte odstraňování úvodních mezer.
- Pracujte s velkými grafickými soubory, například soubory většími než 1 MB.
- Vykonejte rozsáhlé úpravy dokumentů v textových editorech.
- Vykonejte rychlé vývojové sekvence úpravy, kompilace, úpravy a kompilace.
- Otestujte vlastní ovládací prvky OLE (OCX).
- Otestujte funkce dalších hardwarových zařízení, jako jsou skenery a zařízení Plug-and-Play.

- Plánujete-li zavést terminálové služby (Terminal Services), otestujte aplikace na serveru terminálových služeb. Vyzkoušejte provozování jedné aplikace a různých aplikací více uživateli najednou a ověřte správnou funkci uživatelských nastavení.

Chcete-li si nahrát ukázkový plán testování, podívejte se na odkaz Application Specification Download stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Přístup k datům

Pokuste se přistoupit k datům různými způsoby, jako:

- Přistupte k datům na serveru se spuštěnou aktuální verzí Windows i k serveru se systémem Windows 2000.
- Otestujte současné použití databáze včetně simultánního přístupu k záznamu a jeho aktualizaci.
- Vykonejte složité dotazy.

Testování tisku

Vytiskněte různé typy dokumentů na různých tiskárnách, jako například:

- Vytiskněte dokumenty s vloženými soubory několika zdrojových aplikací.
- Při tisku použijte dlouhé názvy souborů.

Použití nástrojů testování

Sady Windows 2000 Software Development Kit (SDK), Driver Development Kit (DDK) a *Microsoft Windows 2000 Server Resource Kit* obsahují nástroje testování a ladění aplikací.

- Nástroj Dependency Walker v sadě *Windows 2000 Server Resource Kit* rekurzivně prohledává závislé moduly, které požaduje nějaká aplikace. Tento nástroj detekuje chybějící soubory, neplatné soubory, nesoulad importu a exportu, chyby cyklických závislostí a moduly instalované na nesprávných počítačích. Další informace najdete v souboru nápovědy tohoto programu.
- Nástroj Apimon sady *Windows 2000 Server Resource Kit* sleduje všechna volání programovacího rozhraní aplikací (API) určité spuštěné aplikace, přičemž je počítá a zaznamenává jejich čas. Volitelně může také sledovat chyby stránkování. Apimon může hlásit tyto údaje:
 - Počet volání API a jejich časování.
 - Sledování volání API v pořadí, v jakém k nim došlo.

Obvyklé problémy kompatibility

Nové technologie a techniky v systému Windows 2000 mohou způsobovat chyby v aplikacích vyvinutých pro předchozí verze systému Windows. Průvodce Windows 2000 Compatibility Guide, kterého najdete na webovém sídle MSDN, obsahuje podrobné popisy mnoha změn, které mohou způsobovat problémy aplikací. Průvodce uspořádává problémy kompatibility do čtyř oblastí:

- Instalační program a instalace
- Obecná kompatibilita systému Windows 2000
- Stabilita aplikací
- Platforma Windows

Tento oddíl popisuje některé ze změn ve Windows 2000, které většinou působí aplikacím problémy. Aplikace vyvinuté pro předchozí verze systému Windows nemusí plně využívat nových funkcí, jako je Active Directory nebo IntelliMirror. Tento oddíl nepojednává o problémech vznikajících v situacích, kdy aplikace tyto nové funkce nepoužívají.

S problémy se můžete setkat v těchto oblastech:

Ochrana systémových souborů

Dřívější verze Windows umožňovaly aplikacím nahrazovat sdílené soubory během instalace. Když došlo k takovým změnám, uživatelé se často setkávali s problémy od chyb programů až po nestabilní operační systém.

System File Protection (SFP) je nová funkce v systému Windows 2000, která zabraňuje aplikacím v náhradě systémových souborů. Tato funkce prověřuje, že chráněné systémové soubory mají správnou verzi. Dojde-li k nahrazení souboru jeho nesprávnou verzí, systém Windows 2000 obnoví správnou verzi.

Robustní kontrola haldy

Systém Windows 2000 obsahuje několik vylepšení výkonu ve správci haldy. U aplikací, které nepoužívaly správně správu hromady, se nyní mohou naplno projevit jejich problémy se správou paměti. Mezi obvyklé problémy patří používání paměti po jejím uvolnění a předpoklad, že se po vyhrazení menší velikosti paměť neposune.

Výčet hardwarových zařízení

Změny v seznamu podporovaných hardwarových zařízení mohou způsobovat problémy aplikacím, které používají již nepodporovaná zařízení.

Výčet písem

Seznam písem se změnil. Protože došlo k přidání klíčů registru podpory internacionalizace, některé aplikace mohou zobrazovat více různých verzí písem.

Změněné klíče registru

Některé klíče registru byly přesunuty nebo odstraněny. Aplikace, které ke změnám v registru používají programovací rozhraní aplikací (API) Win32 by neměly mít žádné problémy. Problémy však mohou mít aplikace, které zapisují data do registru přímo.

Kontrola verze

Instalační programy aplikací, které nesprávně kontrolují verzi, budou mít problémy. Měli byste zjistit minimální verzi operačního systému, který vaše aplikace požaduje, a instalovat ji na danou nebo novější verzi, pokud tedy není vaše aplikace závislá na specifickém operačním systému nebo jeho konkrétní verzi.

Služba Windows Messaging Service

Aplikace, které očekávají poskytování služby Windows Messaging Service (WMS) operačním systémem, tuto službu nenajdou. Tuto službu musíte získat z webového sídla Windows Update.

Zabezpečení vstupu/výstupu souborů

Systém Windows 2000 zpřísnil zabezpečení vstupu a výstupu souborů. Aplikace používající filtry souborů, jako jsou například antivirové programy, mohou ztratit ve Windows 2000 značnou část svých funkcí.

Sledování výsledků testování

I když již třeba máte systém sledování nehod, kam zadáváte nekompatibilitu aplikací v okamžiku, kdy ji objevíte, k zaznamenávání stavu testování aplikací budete muset použít jiný způsob. Musíte být schopni nalézt informace o tom, které aplikace testem úspěšně prošly, které neprošly a které zatím nebyly testovány.

Vymyslete nějaký způsob jednoduchého a přesného zachytávání výsledků testů, abyste mohli v případě potřeby rychle vytvářet sestavy (hlášení). Při plánování svého přístupu k tomuto problému zvažte následující dvě otázky:

- Mechanismus zachytávání dat
- Kategorie zachytávaných dat

Volba systému zachytávání

Mechanismus vybraný pro zachytávání dat závisí na rozsahu vašeho testování, vašem rozpočtu a odborných znalostech. Můžete se rozhodnout pro nákup systému sledování testování a hlášení. Takové produkty prodává mnoho výrobců. Další informace o výrobcích prodávajících tyto produkty najdete v odkazu Test Tracking Systems stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/res-kit/webresources>. Můžete také zadat vyhledávání na Webu pomocí klíčových slov, jako jsou:

- „software testing tools“ (nástroje testování softwaru)
- „test management tools“ (nástroje správy testování)
- „automated testing tools“ (nástroje automatizovaného testování)
- „testing tools“ (testovací nástroje)

Ještě než se rozhodnete, seznámte se s možnostmi různých nástrojů a porovnejte náklady na získání již připravených řešení s náklady na vývoj vašeho vlastního řešení.

Rozhodnete-li se vyvinout svůj vlastní systém, doporučujeme vám zachytávat výsledky testů do databáze a nikoli do pracovního listu nebo textového dokumentu. Databáze vám nabízí větší flexibilitu při vytváření sestav a nejjednodušeji se spravuje se vzrůstajícím objemem dat. Webové rozhraní může zajistit jednoduchý přístup k databázi jak pro zadávání dat tak i pro zobrazování stavu.

Výhodou automatizovaných online řešení je, že můžete jednoduše zaznamenávat výsledky a vytvářet sestavy (hlášení). Nevýhodou jsou čas a zkušenosti potřebné k jejich vývoji. Použití klasického zaznamenávání na papíry vám nedoporučujeme, protože má velké nevýhody, jako je nedostupnost a obtížné vytváření rychlých a přesných sestav.

Mechanismus, který se rozhodnete použít (ať už jej vyvinete nebo koupíte), by měl splňovat tato kritéria:

- Možnost jednoduchého přesného zadávání dat.
- Jednoduchý přístup pro všechny, kteří potřebují data zadávat nebo si je zobrazovat.
- Možnost jednoduchého zálohování nebo duplikování.
- Možnost jednoduše data vybírat a řadit do různých sestav.
- Možnost zpracovávat velké objemy dat.
- Možnost podporovat více současně připojených uživatelů.
- Ochrana existujících zadání před změnami.

Testovací pracovníci potřebují přímočarý a snadno zapamatovatelný proces zaznamenávání dat během dokončování testů. Také je možné vytvořit odkaz na aplikaci nebo na webové sídlo testovacích počítačů.

Vyvinete-li na svém intranetu webové sídlo sběru dat, můžete takové sídlo použít jako komunikační centrum testování. Umístěte sem stavové sestavy, kontaktní jména, kalendář testovacích událostí, odkazy na související informace a další vhodné dokumenty.

Abyste mohli vytvořit mechanismus sběru dat, potřebujete prostředky k vývoji těchto položek:

- Webový nebo jiný aplikační kód aplikace zadávání dat
- Databáze a schéma
- Sestavy (hlášení) a dotazy
- Zabezpečení, je-li zapotřebí

Zachytávání dat

Jakmile určíte metodu sběru dat, musíte ještě určit, jaká data se budou sbírat. Rozhodně se vyplatí, když předem strávíte nějaký čas určením potřebných dat. Budete-li všechna potřebná data shromažďovat hned od začátku, můžete později podle potřeb vytvářet další sestavy.

Většinu potřebných informací jste již získali během inventarizace aplikací. Navíc budete o jednotlivých aplikacích pravděpodobně potřebovat následující informace:

- Jméno testovacího pracovníka a výrobní či obchodní jednotku
- Jméno vývojáře a výrobní či obchodní jednotku (v případě interního vývoje)
- Název produktu Windows 2000 (Server nebo Professional)
- Výsledky testu, jako:
 - úspěšný
 - neúspěšný
 - probíhá
 - neznámý
- Číslo přiřazené každému problému v systému sledování nehod
- Komentáře
- Označení data a času každého záznamu

Označení data a času představuje užitečný filtr při vytváření sestav o určitém časovém období.

Hlášení výsledků

Čím přesněji budete analyzovat data, která se budou sbírat, tím větší možnosti vytváření sestav se vám budou nabízet. Následující návrhy představují sestavy, které můžete shledat užitečnými:

- Seznam aplikací, které neuspěly v testech kompatibility.
Tato sestava vyžaduje následné řešení problémů a opakované testování aplikací.
- Celkový počet aplikací jednotlivých úrovní priority pro všechny provozní jednotky.
- Celkový počet neotestovaných aplikací pro všechny provozní jednotky.

Uvedte také procentuální část neotestovaných aplikací. Tuto sestavu můžete použít k určení, kdo postupuje rychle a kdo pomalu. Nepřehlížejte také možnost použití této sestavy jako pobídky pro skupiny, které se s testováním opoždují.

Budete-li vytvářet sestavu vyjadřující, zda aplikace uspěly nebo neuspěly, zamyslete se také nad tím, zda musíte zobrazovat relativní postup nebo skutečná čísla. Relativní postup lze zobrazit například pomocí barevných schémat nebo obrázků. Tím mohou vaši posluchači získat celkový přehled o postupu, aniž byste jim říkali přesná čísla, která mohou být matoucí. Potřebujete-li ukazovat postup ve skutečných číslech, můžete vymyslet nějaký způsob vyhodnocení nebo hlášení čísel na základě priority aplikací. Například sestava ukazující, že testem prošlo deset aplikací a jedna neprošla, nemusí představovat skutečný stav. Pokud těch deset aplikací bylo speciálními nástroji používaných jen občas několika uživateli a ta jediná neúspěšná aplikace byla důležitou aplikací potřebnou každodenně v provozním prostředí, tato sestava nedává správný obrázek.

Jestliže vaši testovací pracovníci posílají problémy na nějaké místo, například na webové sídlo, můžete vytvořit sestavu otevřených a uzavřených otázek.

Po každé testovací události a pravidelně podle potřeby vytvářejte a rozesílejte sestavy managementu a účastníkům testování. Máte-li pro projekt testování vyhrazené webové sídlo, můžete také umožnit vytváření online sestav.

Řešení nekompatibility aplikací

Když se setkáte s problémy nekompatibility aplikací, musíte je seřadit podle priorit a pak určit někoho k jejich vyřešení. Měli byste vytvořit plán přiřazování problémů. Například problémy s komerčními aplikacemi se řeší úplně jinak než problémy s aplikacemi, které jste vyvinuli interně. Přiřazení odpovídajícího personálu k prozkoumání a vyřešení problémů je zásadní podmínkou úspěchu celého testování aplikací. Řešení problémů může zahrnovat velké množství různých činností, jako je:

- vyhledávání známých problémů a jejich řešení na webových sídlech;
- požadování oprav, instalačních programů a knihoven DLL migrace od výrobce aplikace;
- kontaktování služeb podpory výrobků společnosti Microsoft;
- ladění interně vyvinutých aplikací.

Při vyhledávání příčiny problému najdete nejefektivnější řešení zvážením různých přístupů. Můžete například:

- problém vyřešit, pokud jste aplikaci vyvinuli;
- porádat výrobce a vyřešení problému, pokud jste aplikaci koupili;
- nahradit aplikaci novější verzí nebo aplikací;
- chybu ignorovat, pokud existuje způsob, jak obejít problém.

Ještě než začnete problém řešit jako nekompatibilitu s Windows 2000, vždy se ujistěte o tom, že k němu nedochází také na vaší aktuální platformě. Mezi zdroje vyhledávání problémů kompatibility se systémem Windows 2000 patří:

- Specifikace Windows 2000 Application Specification

Další informace o možnosti nahrání této specifikace najdete v odkazu Application Specification Download stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

- Průvodce Windows 2000 Compatibility Guide

Tento průvodce, který je přístupný na sítích MSDN a Technet, obsahuje cenné informace o diagnostikování problémů kompatibility.

- Síť Microsoft Technet

Tento prostředek obsahuje aktualizace produktů, různé dokumenty a další technické informace. Další informace o síti Technet najdete v odkazu Technet stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

- Adresář aplikací systému Windows 2000

Tento adresář zahrnuje podpůrné informace a odkazy na webová sídla prodejců. Další informace o tomto adresáři najdete v odkazu Directory of Windows 2000 Applications stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Seznam úkolů plánování testování aplikací

Tabulka 21.1 shrnuje úkoly, které musíte vykonat při plánování a testování kompatibility aplikací se systémem Windows 2000.

Tabulka 21.1 Seznam úkolů plánování testování aplikací

Úkol	Umístění v kapitole
Zinventarizujte aplikace potřebné pro vaše výrobní či obchodní úkoly.	Identifikování obchodních aplikací a určení jejich priorit
Zvažte omezení počtu používaných aplikací a vývoj standardů počítačů.	Identifikování obchodních aplikací a určení jejich priorit
Vytvořte systém určení priorit aplikací.	Identifikování obchodních aplikací a určení jejich priorit
Seřadte aplikace podle toho, jak důležité jsou pro vaši výrobu nebo obchod.	Identifikování obchodních aplikací a určení jejich priorit
Napište plán testování včetně metodologie testování, požadavků na laboratoř a prostředky a časového plánu.	Příprava plánu testování aplikací
Vytvořte systém sledování testování sloužící k zachytávání a hlášení výsledků testů.	Sledování výsledků testování
Zveřejněte metodologii testování.	Příprava plánu testování aplikací
Naplánujte testovací události.	Příprava plánu testování aplikací
Testujte aplikace a výsledky zaznamenávejte.	Testování aplikací
Vytvářejte sestavy postupu testování.	Sledování výsledků testování
Vyřešte nekompatibilitu aplikací.	Řešení nekompatibility aplikací

Další zdroje

- Další informace o testování a diagnostikování nekompatibility aplikací najdete v odkazu Microsoft Knowledge Base stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.
- Další informace o testování aplikací najdete v těchto knihách:
 - *Testing Computer Software*, kterou napsali Cem Kaner, Jack Falk and Hung Quoc Nguyen, 1993, New York, NY: Van Nostrand Reinhold
 - *Black-Box Testing: Techniques for Functional Testing of Software and Systems*, kterou napsal Boris Bizer, 1995, New York, NY: John Wiley & Sons
 - *Software Testing: A Craftsman's Approach*, kterou napsal Paul Jorgensen, 1995, Boca Raton, FL: CRC Press
 - *The Craft of Software Testing: Subsystem Testing Including Object-Based and Object-Oriented Testing*, kterou napsal Brian Marick, 1995, Englewood Cliffs, NJ: Prentice Hall

KAPITOLA 22

Definování strategie konektivity klientů

Smyslem této kapitoly je pomoci vám s určením strategie připojení konfigurací klientských počítačů k síti se systémem Microsoft Windows 2000 Server v podnikovém prostředí. S doporučeními popsanými v této kapitole by se měli seznámit osoby účastnící se logického návrhu podnikové sítě. Tato doporučení platí pro velké i malé organizace.

Abyste měli ze čtení této kapitoly co největší prospěch, musíte mít základní znalosti o klientech a sítích systému Windows. Také vám musí být jasné adresovací metody TCP/IP, metody vzdálené konektivity a služba Směrování a vzdálený přístup (Routing and Remote Access). Užitečné jsou také určité znalosti sítí a protokolů NetWare.

V této kapitole

Přehled konektivity klientů 651

Základní konektivita klientů 653

Pokročilá konektivita klientů 659

Metody vzdáleného připojení k síti 662

Seznam úkolů plánování konektivity klientů 670

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujícího dokumentu plánování:

- Strategie konektivity klientů pro konfigurace klientských počítačů

Související informace v sadě Resource Kit

- Další informace o protokolu TCP/IP systému Microsoft Windows 2000 najdete v knize *Microsoft Windows 2000 Server Sítě TCP/IP*.
- Další informace o službě Směrování a vzdálený přístup systému Windows 2000 najdete v knize *Microsoft Windows 2000 Server Internetworking*.

Přehled konektivity klientů

Sítě se v závislosti na své funkci liší velikostmi i typy. Způsob připojení klientů k síti záleží na jejich umístění. Příklady jsou:

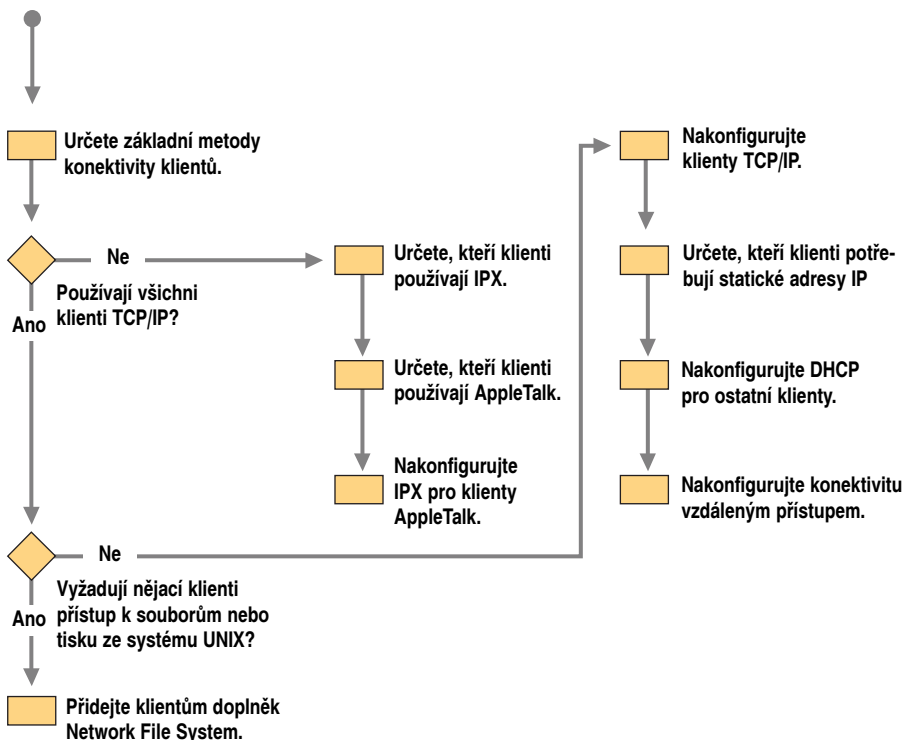
- Interní klienti jsou fyzicky umístěni v infrastruktuře ve společnosti. Interní klienti používají velké množství různých síťových médií, jako jsou například režim asynchronního přenosu (Asynchronous Transfer Mode – ATM), Ethernet nebo Token Ring.

- Externí klienti jsou od infrastruktury sítě společnosti vzdáleni a musí použít službu Směrování a vzdálený přístup nebo virtuální privátní síť.

Klienti musí být schopni připojit se k různým prostředkům. Tyto prostředky zahrnují souborové a tiskové servery, databázové servery jako je Microsoft SQL Server, servery Microsoft Exchange a interní webové servery.

Chcete-li zajistit spolehlivé a výkonné připojování klientů, musíte strategii konektivity připojování klientů systému Windows 2000 určit ještě před začátkem zavádění plánů konektivity. Základní proceduru určení strategie konektivity klientů ukazuje obrázek 22.1. Úkoly nemusíte vykonat v pořadí uvedeném na obrázku. Vývojový graf vám spíše jen nabízí seznam úkolů, které je zapotřebí vykonat, a naznačuje úkoly v jednom z možných pořadí jejich vykonání.

Začátek



Obrázek 22.1 Proces určení strategie konektivity klientů

Základní konektivita klientů

Když spojíte počítače se spuštěným systémem Microsoft Windows 2000 Professional do místní sítě (LAN), operační systém Windows 2000 detekuje síťové adaptéry a vytvoří pro vás připojení k místní síti. To se objeví jako všechny ostatní typy připojení ve složce Síťová a telefonická připojení (Network and Dial-up Connections), ke které se přistupuje za složky ovládacích panelů. Připojení k místní síti je ve výchozím stavu jediným typem připojení, který se automaticky aktivuje. Systém neaktivuje telefonická připojení, která vyžadují ruční konfiguraci s využitím Průvodce připojením k síti (Network Connection Wizard) umístěným ve složce Síťová a telefonická připojení ovládacích panelů.

Příklady připojení k LAN zahrnují Ethernet, Token Ring, kabelové modemy, digitální předplatitelskou linku (digital subscriber line – DSL), rozhraní Fiber Distributed Data Interface (FDDI), protokol IP přes ATM, rozhraní Infrared Data Association (IrDA), bezdrátové připojení a místní síť s emulací ATM. Emulované síť LAN vycházejí z ovladačů virtuálních adaptérů, jako je například protokol LAN Emulation Protocol.

Pokud v síti provedete nějaké změny, můžete nastavení existujícího připojení k místní síti upravit tak, aby zadaným změnám odpovídaly. Tyto změny mohou mít formu:

- protokolů, jako jsou změny statické adresy IP;
- konfigurace DNS nebo WINS;
- služeb.

V dialogovém okně **Stav** (Status) si můžete zobrazit informace o připojení k místní síti, jako je délka připojení, rychlost, množství přijatých a odeslaných dat a diagnostické nástroje dostupné pro dané připojení. Ikonu stavu připojení k místní síti si také můžete nechat zobrazovat na hlavním panelu systému Windows.

Nainstalujete-li na klienta nové zařízení LAN, po příštím spuštění systému Windows 2000 se ve složce Síťová a telefonická připojení (Network and Dial-up Connections) objeví ikona nového připojení k místní síti. Do notebooků můžete přidat kartu do slotu Personal Computer Memory Card International Association (PCMCIA) neboli kartu PC síťového adaptéru i při zapnutém počítači – ikona připojení k místní síti se do uvedené složky přidá okamžitě a není tedy nutné restartovat počítač.

Síťové součásti používané připojením k místní síti lze nakonfigurovat pomocí příkazu **Vlastnosti** (Properties) nabídky. Síťovými součástmi jsou klienti, služby a protokoly, které používáte ke komunikaci se servery na síti, jakmile se připojíte k serveru. Konfigurovatelnými součástmi a jejich funkcemi jsou:

- Služby, jako je například sdílení souborů a tiskáren.
- Protokoly, jako je například Transmission Control Protocol/Internet Protocol (TCP/IP).
- Klienti, jako je například Gateway and Client Services for NetWare.

Další informace o konfiguraci vlastností připojení k místní síti najdete v nápovědě systému Windows 2000 Professional Help.

Pomocí příkazu **Upřesnit nastavení** (Advanced Settings) nabídky připojení k místní síti ve složce Síťová a telefonická připojení můžete také nakonfigurovat nastavení pro více adaptérů LAN. Touto volbou lze změnit pořadí adaptérů používaných pro připojení a klienty, služby a protokoly přiřazené adaptéru.

Služby a protokoly systému Windows 2000

Standardním síťovým protokolem používaným systémem Windows 2000 je protokol TCP/IP. Aby mohli klienti přistupovat k souborovým a tiskovým prostředkům ze serverů NetWare nebo Macintosh, dodává společnost Microsoft buď protokol potřebný k zajištění konektivity na těchto sítích nebo kompatibilní protokol pro toto prostředí. Příkladem takového kompatibilního protokolu je NWLink, což je implementace protokolu IPX/SPX společnosti Novell vytvořená společností Microsoft.

Na klientské počítače, které potřebují přistupovat k prostředkům systémů Macintosh můžete nainstalovat službu Services for Macintosh, která zahrnuje protokol AppleTalk. Klienti systému Macintosh mohou také přistupovat k souborovým serverům pomocí TCP/IP.

Systém Windows 2000 se pokouší o vytvoření připojení k vzdáleným serverům pomocí síťových protokolů v pořadí připojení k místní síti zadaném uživatelem v dialogovém okně **Upřesnit nastavení** (Advanced Settings). Instalujte a povolte pouze protokoly, které potřebujete. Jestliže například potřebujete pouze TCP/IP, ale máte také nainstalovaný protokol IPX, vytváříte tím zbytečný síťový provoz IPX a SAP.

Síťoví klienti protokolu TCP/IP

TCP/IP je jedním z nejpoužívanějších síťových protokolů. Klienti na síti TCP/IP mohou mít adresy přiřazené staticky správcem sítě nebo dynamicky serverem protokolu Dynamic Host Configuration Protocol (DHCP).

Systém Windows 2000 používá novou službu DNS označovanou za dynamickou aktualizaci DNS. DNS se používá jako poskytovatel oboru názvů, ať už klient používá DHCP nebo statické adresy IP. Klienti Windows nyní již nemusí používat WINS, ale mohou jednoduše používat DNS. V předchozích verzích sítě systému Windows byl systém WINS používán ve spojení s DHCP a umožňoval hostitelům dynamicky registrovat jejich název systému NetBIOS a adresu IP v databázi WINS. Máte-li na síti nějaké klienty se systémem Microsoft Windows NT Workstation, Microsoft Windows 95, Microsoft Windows 98 nebo Microsoft Windows 3.1, musíte ještě používat WINS, protože tito klienti používají metodu názvu systému NetBIOS.

Když na své síti použijete Microsoft DNS, získáte tím určité výhody. Systém DNS:

- zajišťuje interoperabilitu s dalšími servery DNS, jako jsou Novell NDS a UNIX Bind;
- integruje se a je vyžadován pro podporu adresářové služby Active Directory;
- integruje se s dalšími síťovými službami, jako jsou WINS a DHCP;
- umožňuje klientům aktualizovat záznamy o prostředcích dynamickým registrováním jejich názvů DNS a adres IP;
- podporuje přírůstkové zónové přenosy mezi servery.
- podporuje nové typy záznamů prostředků, včetně záznamů Services Locator (SRV) a Asynchronous Transfer Mode Addresses (ATMA).

Ještě než si na systém nainstalujete Microsoft TCP/IP, určete, zda klient obdrží statickou nebo dynamickou adresu IP. Zjistěte, zda hostitelé na vaší síti používají DHCP, nebo jsou-li vaše adresy IP přiřazeny staticky.

Protokol DHCP

Použití protokolu Dynamic Host Configuration Protocol (DHCP – protokol dynamické konfigurace hostitele) umožňuje klientovi automaticky přijmout adresu IP. Tím se za-

braňuje chybám konfigurace zapříčiněným potřebou ručního zadání hodnot na každém počítači. Protokol DHCP také zabraňuje konfliktům adres, které vznikají v okamžiku, kdy je již dříve přiřazená adresa IP použita při konfigurování nového počítače na síti. Navíc proces obnovení pronájmu DHCP pomáhá zajistit v prostředích, kde je zapotřebí klientské konfigurace často aktualizovat (například v případě uživatelů s přenosnými počítači, kteří často mění své místo), aby k těmto změnám docházelo výkonně a automaticky. Zavedení protokolu DHCP v síti umožní také mnohem efektivnější použití a správu adresového prostoru vaší organizace, protože adresy, které již nejsou zařízeními používány, se opakovaně vkládají do fondu adres a přiřazují se dalším klientům. Chcete-li používat DHCP, stačí v dialogovém okně vlastností protokolu TCP/IP, které je dostupné z ikony připojení k místní síti na klientovi, jednoduše zvolit polohu **Získat adresu IP ze serveru DHCP automaticky** (Obtain an IP address automatically) přepínače. Tato volba je po instalaci klienta systému Windows 95, Windows 98, Windows NT nebo Windows 2000 Professional ve výchozím stavu vybrána, takže jestliže používáte DHCP, nemusíte ručně zadávat konfiguraci IP.

Výhody použití DHCP jsou:

- Nemusíte ručně měnit nastavení IP, když se sítí pohybuje nějaký klient, například cestující uživatel. Klientovi se automaticky přiřadí nová adresa IP bez ohledu na to, ke které podsíti se připojí. To platí za předpokladu, že z daných podsítí je dostupný nějaký server DHCP.
- Není zapotřebí ručně konfigurovat nastavení DNS nebo WINS. Tato nastavení mohou být předána klientovi serverem DHCP, pokud byl tedy server DHCP nastaven tak, aby klientům DHCP takové informace vydával. Chcete-li tuto možnost na klientovi povolit, jednoduše zvolte polohu **Získat adresu serveru DNS automaticky** (Obtain DNS server address automatically) přepínače. Další informace o DNS a WINS najdete v oddílu „Síťoví klienti protokolu TCP/IP“ této kapitoly.
- Neexistují žádné konflikty způsobené duplikovanými adresami IP.

Další informace o zavádění DHCP najdete v kapitole „Určení strategií konektivity sítě“ v této knize.

Statické adresy

Jestliže jsou vaše adresy IP přiřazeny staticky, máte k dispozici následující informace:

- Adresu IP a masku podsítě každého síťového adaptéru instalovaného na klientovi.
- Adresu IP výchozí brány.
- Zda se klient účastní DNS či WINS nebo ne.
- Pokud se klient účastní DNS, název domény DNS, jejíž součástí klient právě je, a adresy IP primárního a záložního serveru DNS.
- Jestliže se klient účastní WINS, adresy IP primárního a záložního serveru WINS.

Adresářová služba Active Directory

Systém Windows 2000 nyní podporuje službu Active Directory, avšak klienti systémů Windows 95 (a novějších) a Windows NT 4.0 potřebují doplňkový klientský software pro služby Active Directory. Klient nakonfigurovaný s Active Directory se může k síti přihlásit vyhledáním řadiče domény. Takový klient pak může plně využívat výhody funkcí adresářové služby Active Directory. Mezi tyto výhody patří:

- Okamžitý přístup k informacím o všech objektech na síti.
- Použití funkcí zabezpečení Active Directory prostřednictvím ověření přihlášení a řízení přístupu.

Poznámka Klient Active Directory pro systémy Windows 95 a Windows 98 je poskytován jako jeden inovační balíček ve složce Clients na disku CD-ROM systému Windows 2000 Server.

Síťoví klienti protokolu IPX

Klienti systému Windows mohou pomocí služby (klienta) Client Services for NetWare nebo Gateway Services for NetWare spolupracovat se servery NetWare.

Máte-li na síti servery, které používají operační systémy Novell NetWare, pak se mohou klienti Windows přes službu Client Services for NetWare přímo připojovat k serveru, nebo se mohou připojovat nepřímě k serveru se systémem Windows 2000, na kterém je spuštěna služba Gateway Services for NetWare.

Kroky potřebnými pro získání klientského přístupu k prostředkům NetWare jsou:

1. Nainstalujte klienta Client Services for NetWare. To vám umožní uskutečnit přímé připojení k prostředkům NetWare. Během instalace klienta Client Services for NetWare se také instaluje protokol NWLink systému NetBIOS. Jedná se o verzi společnosti Microsoft protokolu IPX, která podporuje konektivitu mezi systémy Windows 2000 Server a systémy NetWare 4.x a dřívějšími.
2. Připojte se ke svazkům NetWare. Po instalaci dříve uvedených klientů se můžete připojit ke svazku NetWare klepnutím na ikonu **Místa v síti** (My Network Places) na pracovní ploše.
3. Připojte se k souborovým a tiskovým prostředkům systému NetWare. Tiskárnu NetWare přidáte do klienta Windows 95 nebo novějšího tak, že si otevřete složku Tiskárny (Printers) z nabídky **Nastavení** (Settings) a budete postupovat podle instrukcí Průvodce instalací tiskárny (Printer Installation Wizard). V průvodci zadáte tiskárnu NetWare tím, že zapíšete jejich názvy v normálním formátu Universal Naming Convention (UNC).

Klient Gateway Services for NetWare

Klienta Gateway Services for NetWare můžete nainstalovat na server se systémem Windows 2000 a umožnit mu tak fungovat jako brána. Klienti se pak mohou připojovat k prostředkům NetWare pouze pomocí TCP/IP, aniž by bylo nutné spouštět NWLink. Na serveru běží klient Gateway Services for NetWare a NWLink, které zajišťují připojení klienta k serveru NetWare. Tento klient je součástí systému Windows 2000 Server.

Služba File and Print Services for NetWare

Tato služba je samostatný produkt a umožňuje serveru se systémem Windows 2000 poskytovat souborové a tiskové služby přímo serveru NetWare a kompatibilním klientským počítačům. Prostředky připojené přes tuto službu se klientům NetWare jeví jako jiné servery NetWare a klienti tak mohou získat přístup ke svazkům, souborům a tiskárnám na serveru. Pro klientský software NetWare nejsou zapotřebí žádné změny ani doplňky.

Klient Client Services for NetWare

Tento klient (služba) umožňuje klientským počítačům přímo se připojovat k souborovým a tiskovým prostředkům na serverech NetWare se spuštěným systémem NetWare 2.x, 3.x nebo 4.x. Klienta Client Services for NetWare lze použít k získání přístupu na servery se spuštěnou službou Novell Directory Services nebo s vazební databází se zabezpečením. Tato služba je součástí Windows 95, Windows 98, Windows NT a Windows 2000 Professional.

Klienti systému Windows na server systému Novell

Správci mají několik možností, jak umožnit klientům přístup k souborovým a tiskovým službám na serveru systému Novell:

Instalovat klienta Client Services for NetWare Jak bylo popsáno v oddílu „Síťoví klienti protokolu IPX“ dříve v této kapitole.

Poznámka Klient Client Services for NetWare pracuje pouze nad protokolem IPX/SPX. Pro zajištění interoperability se servery NetWare 5.0, na nichž je spuštěný pouze protokol TCP/IP, musíte použít klienta sítě Novell.

Instalovat na server Novell NetWare doplněk Common Internet File System Systém Windows 2000 Professional používá pro souborové a tiskové služby protokol Common Internet File System (CIFS). CIFS je vylepšenou verzí protokolu Microsoft Server Message Block (SMB). Jakmile je instalován modul snap-in protokolu CIFS, server NetWare reaguje jako server se systémem Windows 2000 na klienty Windows. I když všechny počítače na síti používají IPX, klienti Windows mohou přistupovat k souborovým a tiskovým službám na serveru se systémem Windows 2000 bez jakéhokoli doplňkového softwaru.

Klienti systému Windows ve smíšeném prostředí systémů Novell NetWare a Windows 2000 Server

I když všechny počítače na síti používají IPX, klienti stále mohou mít možnost přistupovat k souborovým a tiskovým službám na serveru Novell, pokud na něm běží NetWare Core Protocol a klienti Windows používají CIFS (standardně přes klienta sítě Microsoft). Máte několik možností povolení komunikace mezi klienty Windows a servery se systémy NetWare a Windows 2000:

Možnost 1: Instalace služby File and Print Services for NetWare Služba File and Print Services for NetWare umožňuje serveru se systémem Windows 2000 Server reagovat na všechny klienty jako server NetWare. Když se uživatel přihlásí k počítači se spuštěným systémem Windows 2000 Server, jeho rozhraní vypadá, jako by se přihlásil k serveru se systémem NetWare 3.x. Služba File and Print Services for NetWare, která je součástí služby kompatibilní s IPX/SPX nástroje NWLink, dovoluje systému Windows 2000 Server emulovat souborový a tiskový server NetWare tím, že používá stejné dialogy jako server NetWare. Souborové a tiskové služby systému Windows 2000 Server můžete spravovat pomocí nástrojů NetWare, a proto není zapotřebí pracovníky přeskolovat. Jestliže použijete službu File and Print Services for NetWare, nemusíte ani nijak měnit klienty NetWare. Například klientská aplikace používající protokoly a pojmenovávací konvence NetWare nepotřebuje žádné přesměrování ani překlad.

Poznámka Služba File and Print Services for NetWare funguje pouze na systémech Windows 2000 Server a Windows 2000 Advanced Server.

Možnost 2: Instalace klienta Gateway Services for NetWare Máte-li instalovaného klienta Gateway Services for NetWare, systém Windows 2000 Server se stane branou pro klienty systému Windows používající CIFS a komunikující se serverem NetWare a umožní uživatelům přístup ke všem prostředkům na daném serveru. Klienti se systémem Windows 95 a novějším mohou přistupovat k prostředkům NetWare pomocí TCP/IP, nativním síťovým komunikačním protokolem operačních systémů Windows 2000. Navíc klient Gateway Services for NetWare umožňuje klientům sítí Windows 2000 přistupovat k souborům na serveru NetWare bez přeměrovače klienta NetWare a zásobníku protokolu IPX/SPX (jako je NWLink). Tyto prvky omezují zatížení správy pro jednotlivé klienty a zlepšují výkon sítě. Klient Gateway Services for NetWare také podporuje navigaci Novell Directory Services, ověřování, tisk a přihlašovací skripty. Klient Gateway Services for NetWare umožňuje počítači se spuštěným systémem Windows 2000 Server fungovat jako server komunikační brány do sítě NetWare a opakovaně sdílet síťová připojení ze serveru NetWare.

Tisk na tiskárny systému NetWare

Kromě tradičních služeb sdílení tiskáren podporuje systém Windows 2000 Professional také službu Novell Distributed Print Services, což je vylepšená tisková architektura v systému NetWare 5, která integruje tiskové služby do služeb Novell Directory Services. Služba Novell Distributed Print Services také podporuje obousměrnou komunikaci s tiskárnou, správu tiskáren z jediného místa a automatickou instalaci správného ovladače tiskárny na klienta při prvním použití tiskárny.

Jakmile je na serveru NetWare nakonfigurována tiskárna služby Novell Distributed Print Services, můžete nainstalovat další tiskárnu následujícím postupem:

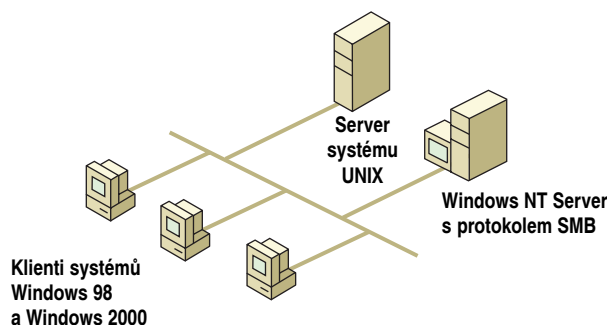
▼ **Chcete-li nainstalovat tiskárnu na server systému NetWare, postupujte takto:**

1. Vyhledejte instalovanou tiskárnu v položce **Místa v síti** (Network Places).
2. Klepněte pravým tlačítkem myši na ikonu tiskárny a pak zadejte příkaz **Připojit** (Connect).
3. Server nainstaluje a nakonfiguruje správný ovladač podle operačního systému počítače.

Součástí systému Windows 2000 Professional je podpora tisku pro NetWare verzí 2.x, 3.x a 4.x. Připojení k síťovým tiskárnám můžete vytvořit přímo nebo mapováním portu LPT na port UNC. Protože služba Novell Distributed Print Services vyžaduje Novell Directory Services, schopnost používat Novell Distributed Print Services vyžaduje klienta Novell NetWare.

Síťoví klienti systému UNIX

Aby mohly počítače vzájemně komunikovat, musí na nich pracovat stejné protokoly. Na obrázku 22.2 v celé síti běží provozní protokol TCP/IP. Nad vrstvou TCP/IP provozuje server systému UNIX aplikační protokol Network File System (NFS – standard systému UNIX pro souborové a tiskové služby) a operační systém Windows 2000 Server tu provozuje aplikační protokol CIFS.



Obrázek 22.2 Sít' systémů UNIX a Windows NT

Po ustanovení komunikace podporuje každý operační systém další schopnosti, jako je centralizovaná správa, vzdálený přístup a další funkce, které jsou buď integrované do operačního systému nebo jsou dostupné pomocí doplňkový produktů od společnosti Microsoft, prodejců systému UNIX nebo nezávislých výrobců softwaru.

Dále je uveden přehled dostupných možností integrování prostředí systému UNIX a Windows:

Přidejte doplněk NFS na klienty Jedním z nejobvyklejších způsobů zajištění interoperability je přidat na počítače schopnosti systému NFS, jako jsou například ty poskytované službou Services for UNIX.

Přidejte podporu protokolu CIFS na server systému UNIX Instalujte doplněk protokolu CIFS na server systému UNIX. Server systému UNIX pak bude reagovat jako server se systémem Windows 2000 na všechny klienty se systémem Windows.

Použijte bránu NFS se systémem Windows 2000 Server Instalací produktu brány NFS, jako je služba Services for UNIX, se server Windows 2000 stane branou pro klienty systému Windows používající protokol CIFS a komunikující se serverem systému UNIX. Uživatelé mohou přistupovat ke všem prostředkům na serveru systému UNIX, jako by šlo o standardní místo sdílení souborů systému Windows 2000 Server.

Použijte integrované klienty protokolů Telnet a File Transfer Protocol Systém Windows 2000 Server poskytuje jako své standardní součásti klienty protokolů Telnet a File Transfer Protocol (FTP). Pomocí těchto klientů mohou uživatelé systému Windows 2000 Professional vytvořit standardní relace v prostředí VT100 s libovolným systémem UNIX, který podporuje protokol Telnet, nebo mohou pro přenos souborů mezi systémy UNIX a Windows 2000 Professional používat protokol FTP.

Síťovní klienti protokolu AppleTalk

Chcete-li umožnit systémům Macintosh přístup k serverům Windows 2000 Server, můžete na dané servery instalovat službu Services for Macintosh. Takto nakonfigurovaný server se systémem Windows 2000 Server se objeví v zóně AppleTalk a umožní přístup stejným způsobem jako jiné systémy Macintosh.

Pokročilá konektivita klientů

Klienti, kteří používají jako médium na síti technologii ATM a kteří vyžadují vyšší úroveň konektivity, mohou použít podporu režimu asynchronního přenosu (Asynchronous

Transfer Mode – ATM) systému Windows 2000 a IP přes ATM. Tyto typy technologií zajistí klientům maximální šířku pásma ve vysoce zatížených síťových prostředích. Následující oddíly popisují uvedené technologie.

Režim asynchronního přenosu (ATM)

Vysokou rychlost a kvalitu služeb můžete přímo přinést klientům tím, že je připojíte na síť ATM. Při plánování strategie konektivity klientů k ATM rozhodněte, zda připojíte klienta přímo na ATM, nebo zda ponecháte existující infrastrukturu Ethernetu a použijete emulaci LAN (LANE). Jestliže bude klient používat existující infrastrukturu, bude dostávat také stávající síťový hardware Ethernetu. Pro připojení segmentů Ethernetu k jádru ATM sítě pak budete potřebovat LANE.

Přímo připojená síť ATM

Aby mohl klient používat přímo připojenou síť ATM, musí obsahovat kartu ATM kompatibilní se systémem Windows 2000. Tuto kompatibilitu můžete prověřit pomocí seznamu kompatibility hardwaru (Hardware Compatibility List – HCL). Další informace o HCL najdete v odkazu Microsoft Windows Hardware Compatibility List stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>. Jestliže daná síťová karta ATM nepodporuje detekci Plug-and-Play, pak si u výrobce vyžádejte instalační software. Jakmile systém detekuje kartu ATM, nakonfiguruje ji na emulaci LAN.

Síť IP/ATM

Síť IP/ATM nabízí klientům možnost získat přístup k vysokorychlostní síti a přitom stále používat jako svůj protokol TCP/IP. Síť IP/ATM používá k překladu adres IP na adresy ATM server ATM Address Resolution Protocol (ARP) a umožňuje tak přístup k serverům na síti ATM. Server Multicast Addresses Resolution (MARS) umožňuje překlad adres vícesměrového vysílání.

Sada protokolů sdružení Infrared Data Association

Systémy Windows 2000 Professional, Windows 98 a Windows 95 podporují sadu protokolů sdružení Infrared Data Association (IrDA). Tento protokol umožňuje uživatelům přenášet informace a sdílet prostředky, jako jsou například tiskárny, mezi počítači bez pomoci fyzických kabelů. Většina nových přenosných počítačů obsahuje hardware podpory IrDA.

Například dva uživatelé, kteří cestují s notebooky, mohou mezi sebou přenášet soubory vytvořením spojení IrDA a nikoli pomocí kabelů nebo disket. Spojení IrDA lze iniciovat umístěním přenosných počítačů blízko sebe. IrDA podporuje vzdálenosti kolem jednoho metru.

Protokol IrDA také umožňuje počítačům přistupovat k prostředkům připojeným ke druhému počítači. Potřebujete-li například vytisknout dokument z notebooku, můžete vytvořit spojení IrDA na počítač, který je připojený k tiskárně – místně nebo přes síť. Jakmile je takové spojení vytvořeno a máte-li potřebná oprávnění, můžete tisknout přes spojení IrDA. Některé tiskárny také protokol IrDA podporují přímo a umožňují tak uživatelům odesílat tiskové úlohy přímo na tiskárnu přes port IrDA počítače.

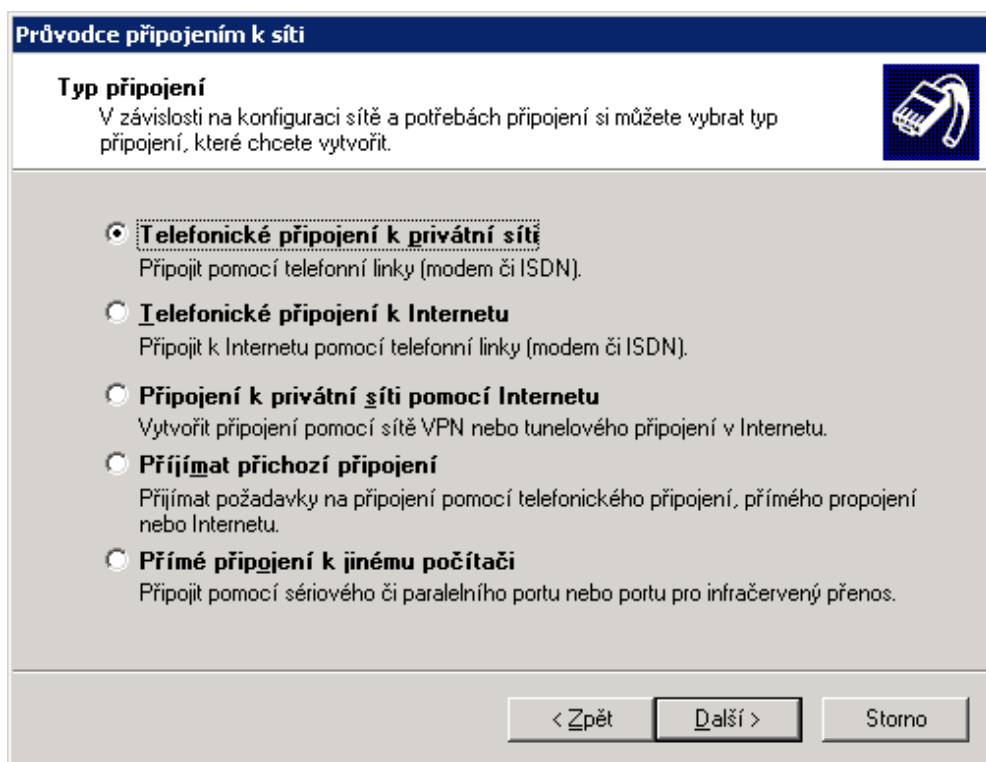
Systém Windows 2000 Professional také podporuje schopnost umožnit odesílání souborů pomocí IrDA jen vlastníkovi počítače. Uživatelé mohou také zadat místo, kde mu-

sí být dokumenty přijaty. Systém Windows 2000 Professional automaticky detekuje zařízení používající infračervenou komunikaci, jako jsou další počítače a fotoaparáty.

Klienti vzdáleného přístupu

Jeden ze způsobů, jak může společnost zvýšit svou produktivitu, nabízí služba Směrování a vzdálený přístup (Routing and Remote Access) systému Windows 2000. Jestliže se klienti nenacházejí v místě vašich kanceláří, tato služba jim může umožnit vzdálený přístup k prostředkům na interní síti a pomoci maximalizovat rychlost a zabezpečení. Systém Windows 2000 Professional uživateli značně zjednodušuje proces připojení ke vzdáleným sítím včetně virtuálních privátních sítí (VPN) a zjednodušuje také telefonická a infračervená připojení i přímá připojení kabelem.

S vytvářením nových typů připojení jediným nástrojem pomůže uživateli Průvodce připojením k síti (Network Connection Wizard). Nastavení připojení je také automatizováno, takže se eliminuje potřeba nahrávat si a instalovat další služby. Průvodce připojením k síti najdete na obrázku 22.3.



Obrázek 22.3 Průvodce připojením k síti

Telefonické připojení k privátní síti

Klienti, kteří nechtějí používat pro vzdálený přístup virtuální privátní síť (VPN), se mohou v zájmu získání přístupu k prostředkům přímo telefonicky připojit k serveru vzdáleného přístupu vaší společnosti. Výhodou této metody je, že se používá jednoduché

telefonické připojení a nepotřebujete služby poskytovatele připojení k Internetu (ISP). Nevýhodou této metody jsou případné poplatky za mezinárodní volání.

Virtuální privátní síť

Vzdálení klienti ve dnešních pokročilých sítích mohou přistupovat k prostředkům pomocí protokolů VPN. Systém Windows 2000 podporuje široce používaný protokol Point-to-Point Tunneling Protocol (PPTP), ale umožňuje také velmi bezpečné připojení pomocí protokolu Layer 2 Tunneling Protocol (L2TP) ve spojení se zabezpečeným protokolem IP (IPSec). Pomocí L2TP a IPSec lze vytvořit přes ISP vzdáleného klienta zabezpečené tunely, které umožní klientovi odesílat a přijímat data chráněná před narušením v prostředí Internetu.

Protokol IPSec data putující mezi dvěma počítači šifruje, čímž je na síti chrání před jejich neoprávněnou změnou a čtením. Nejprve musí správce definovat, jak si budou oba počítače vzájemně důvěřovat, a pak musí určit, jak počítače zabezpečí svůj provoz. Tato konfigurace je obsažena v zásadách protokolu IPSec, které správce vytváří a aplikuje na místní počítač nebo pomocí zásad skupiny v Active Directory. Vzhledem k obtížnosti konfigurování zásad protokolu IPSec společnost Microsoft zabudovala podporu IPSec do protokolu L2TP, takže stačí jen vytvořit připojení VPN pomocí L2TP ze vzdáleného počítače na server VPN. Další informace o protokolu IPSec najdete v knize *Microsoft Windows 2000 Server Síť TCP/IP*.

Abyste mohli používat protokol IPSec u internetových nebo síťových klientů, musí být na obou hostitelích, kteří si vyměňují data, instalován modul snap-in protokolu IPSec. Jestliže se vzdálený uživatel telefonicky připojuje přes svého místního poskytovatele připojení k Internetu (ISP), pak musí protokol IPSec běžet jak na tomto klientovi, tak i na serveru VPN, který klient volá. Potřebují-li si zabezpečeně vyměňovat data dva klienti v interní síti, na obou klientech také musí běžet protokol IPSec.

Metody vzdáleného připojení k síti

Existují různé metody vzdáleného připojení, které můžete používat v závislosti na typu infrastruktury, který vytváříte. Lze je kategorizovat podle velikosti a patří sem:

- síť Small Office/Home Office (SOHO – malá kancelář/domácí kancelář);
- síť střední velikosti, kterou mohou využívat středně velké až velké obchodní jednotky;
- velmi velká síť společnosti s několika tisíci klienty.

Sítě malé kanceláře

Sítě Small Office/Home Office (SOHO) se používají především v domácích kancelářích, které mohou být součástí větší společnosti, zůstávají se však mimo ni. Síť SOHO může využívat dvě technologie umožňující připojení mezi klienty na síti SOHO a Internetem, podnikovou síť nebo obou. Těmito technikami jsou Internet Connection Sharing (ICS) a překlad síťových adres (Network Address Translation – NAT).

Sítě SOHO jsou obvykle sítěmi typu peer-to-peer. Tento typ sítě je jediná podsíť používaná k pohodlnému spojování klientů, bez potřeby směrovačů, serverů DHCP a serverů WINS. To je ideální pro domácí kanceláře, kde uživatel potřebuje používat více počítačů a také potřebuje mezi počítači sdílet prostředky, jako jsou soubory, aplikace a tiskárny.

Následující oddíl vysvětluje výhody, požadavky a zavádění obou uvedených typů technologií.

Konektivita sítě SOHO

Síť SOHO potřebuje mít schopnost spravovat a organizovat svou vlastní interní síťovou strukturu a také se připojovat k Internetu a udržovat zabezpečené připojení.

Systém Windows 2000 nabízí síti SOHO možnost automaticky přiřazovat privátní adresy IP interním počítačům prostřednictvím funkce nazvané Automatic Private IP Addressing (APIPA). Adresy síti SOHO lze také přiřazovat během připojování k Internetu. K tomu dochází prostřednictvím služby označované za překlad síťových adres (Network Address Translation – NAT). Služba NAT umožňuje překlad privátních adres IP na veřejné adresy IP, které se používají v internetovém provozu. Tím je interní síť zabezpečená před Internetem a uživatel sítě SOHO přitom nemusí vynakládat žádný čas ani náhodu na získání a údržbu nějaké oblasti veřejných adres. Tabulka 22.1 představuje možné požadavky na implementaci sítě SOHO.

Tabulka 22.1 Návrh sítě SOHO

Síťová součást	Metoda
Systém Windows 2000 Server	Zajistěte, aby hardware serveru splňoval specifikace uvedené v seznamu HCL systému Windows 2000.
Médium LAN	Použijte nestíněný kroucený párový kabel 10BaseT či 100BaseT, rozbočovače 10BaseT či 100BaseT nebo síťové karty 10BaseT či 100BaseT. Požadavky na kompatibilitu síťového adaptéru najdete v seznamu HCL.
Konektivita k Internetu	Použijte ICS, NAT nebo trasované připojení k Internetu. Použijte POTS, ISDN, částečnou linku T1, kabelový modem nebo DSL.
Interní konektivita klientů	Použijte adresy IP služby Automatic Private IP Addressing (APIPA), adresy přiřazené ISP nebo statické adresy.
Síťové protokoly	TCP/INSTALAČNÍ PROGRAM

Sdílení připojení k Internetu

Internet Connection Sharing (ICS) je jednoduchý balíček, který se skládá z protokolu DHCP, služby překladu síťových adres (NAT) a systému DNS. ICS lze použít pro připojení vaší sítě SOHO k Internetu prostřednictvím jednoduché konfigurace s jediným krokem umožňující překládané připojení, které následně dovoluje všem počítačům na síti přistupovat k elektronické poště, webovým sídlům, sídlům FTP atd. ICS zajišťuje překlad síťových adres (viz následující oddíl), automatické adresování IP a služby překladu názvů všem počítačům na síti SOHO. ICS poskytuje:

- jediné zaškrtnuté políčko zaručující jednoduchou konfiguraci;
- jedinou veřejnou adresu IP;
- pevný rozsah adres pro hostitele SOHO;
- proxy-server DNS pro překlad názvů;
- jediné rozhraní SOHO pro síť peer-to-peer.

ICS můžete nakonfigurovat na novém nebo již existujícím připojení vzdáleného přístupu nebo síti LAN pomocí jediného políčka, které zaručuje sdílení připojení. Abyste mo-

hli použít ICS, musíte mít počítač se síťovým připojením k místnímu ISP a kartu síťového rozhraní nebo adaptér pro připojení k síti peer-to-peer. ICS je povoleno na připojení k místnímu ISP a svou adresu získává od ISP. Je-li na připojení povoleno ICS, síťový adaptér se také automaticky nakonfiguruje na statickou adresu IP s hodnotou 192.168.0.1, což je součást oblasti adres IP od 192.168.0.0 do 192.168.254.254. Počítače za systémem ICS také obdrží adresy IP z tohoto rozsahu.

Poznámka Uvědomte si, že po zavedení ICS není možná žádná další konfigurace služeb na síti, jako jsou DNS nebo adresování IP. Všechny tyto služby jsou implementovány systémem ICS.

Překlad síťových adres

Překlad síťových adres (Network Address Translation – NAT) se liší od ICS tím, že podobné funkce zajišťuje pružněji. Také vyžaduje více kroků nastavení. Jedním z hlavních rozdílů mezi NAT a ICS je, že NAT vyžaduje jako minimum systém Windows 2000 Server, zatímco ICS lze nakonfigurovat na systému Windows 2000 Professional nebo Windows 98 Second Edition. NAT se nahrává a konfiguruje ze Správce směrování a vzdáleného přístupu (Routing and Remote Access Manager) systému Windows 2000. NAT zajišťuje tyto funkce:

Ruční konfigurace Ta dovoluje uživateli všestrannější metodu konfigurování překládaných připojení vzdáleného přístupu.

Více veřejných adres IP NAT může využívat více rozsahů veřejných adres.

Konfigurovatelný rozsah adres NAT umožňuje ruční konfigurování adres IP a masek podsítě, zatímco ICS používá pevný rozsah adres IP. Pomocí vlastností NAT ve Správci směrování a vzdáleného přístupu lze nakonfigurovat libovolný rozsah adres IP. Mechanismus distribuování adres IP zajišťuje funkce přidělování DHCP stejným způsobem jako služba DHCP. NAT může také používat adresy IP distribuované ze serveru DHCP – stačí vybrat políčko automatického získání adresy IP ze serveru DHCP (**Automatically assign IP addresses by using DHCP**) v okně vlastností NAT.

DNS a proxy WINS Pomocí DNS nebo WINS lze zavést překládání názvů. To lze nakonfigurovat výběrem odpovídajících zaškrtnutých políček v okně vlastností NAT na kartě překladu názvů (**Name Resolution**).

Více síťových rozhraní Funkci NAT můžete distribuovat na více síťových rozhraní. Stačí přidat dané rozhraní do NAT ve Správci směrování a vzdáleného přístupu.

Sítě používající NAT mohou také inicializovat připojení VPN pomocí PPTP. To umožňuje malým podnikům nebo dokonce sítím SOHO, kde je služba NAT instalována, inicializovat zabezpečená připojení vzdáleného přístupu s podnikovou sítí.

Poznámka Nepoužívejte NAT na síti s dalšími řadiči domén systému Windows 2000 Server, servery DNS, branami, servery DHCP nebo se systémy s nakonfigurovanými statickými adresami IP, protože může docházet ke konfliktům s jinými službami.

Nepřipojujte NAT přímo k podnikové síti, protože ověřování protokolem Kerberos, IPSec a Internet Key Encryption (IKE) nebudou fungovat.

Automatické privátní adresování IP

Systémy Windows 2000 Server, Windows 2000 Professional a Windows 98 si mohou samy přiřadit nějakou adresu IP z rozsahu adres 169.254.0.0/16, když na síti nejsou detekovány žádné servery DHCP. Systémy Windows 3.11, Windows NT 3.51 a Windows NT 4.0 také mohou získat adresu IP z tohoto rozsahu, ale musí ji získat ze serveru APIPA. Službu APIPA lze nastavit na distribuování adres IP z tohoto rozsahu tak, že se jednoduše spustí Správce směrování a vzdáleného přístupu (Routing and Remote Access Manager), přidá se a nakonfiguruje NAT, přidá se rozhraní distribuující adresy IP a pak se nakonfiguruje rozsah adres IP ve vlastnostech NAT na dříve uvedený rozsah adres. Další informace o APIPA najdete v kapitole „Určení strategií konektivity sítě“ v této knize.

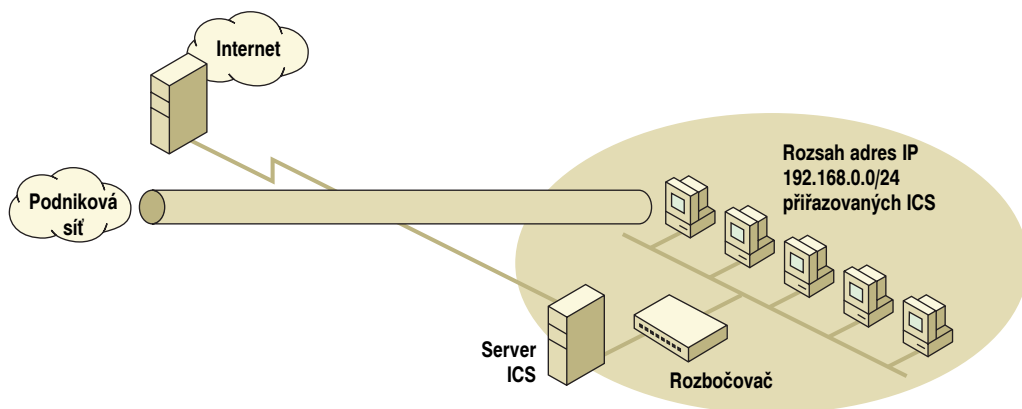
Poznámka Jedinými klienty, kteří jsou schopni účastnit se v APIPA, jsou klienti systémů Windows 98 a Windows 2000 Professional. Všechny ostatní systémy vyžadují server se spuštěnou službou Směrování a vzdálený přístup systému Windows 2000, která jim distribuuje adresy APIPA.

Příklady SOHO

V tomto oddílu najdete dva příklady ukazující, jak lze implementovat síť SOHO.

Příklad 1

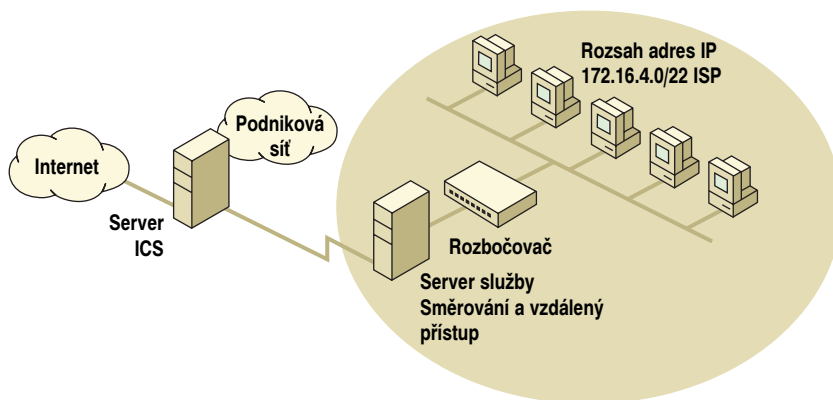
Toto je příklad, kde je na síti SOHO pět počítačů. Síť SOHO používá pro připojení k Internetu ICS a pomocí Internetu se připojuje k podnikové síti přes tunel PPTP. Rozsah adres IP používaných klienty se distribuuje počítačem ICS. Potřebuje-li některý z klientů připojení k podnikové síti, použije se na klientech nakonfigurovaný profil VPN a síť Internet se pak vytvoří tunel PPTP k podnikové síti. Tuto síť ukazuje obrázek 22.4.



Obrázek 22.4 Domácí síť

Příklad 2

Tento příklad je síť SOHO, kde klienti přistupují k podnikové síti přes server se spuštěnou službou Směrování a vzdálený přístup (Routing and Remote Access). Klienti na síti přistupují k Internetu přes podnikovou síť. Tuto síť znázorňuje obrázek 22.5.



Obrázek 22.5 Síť SOHO

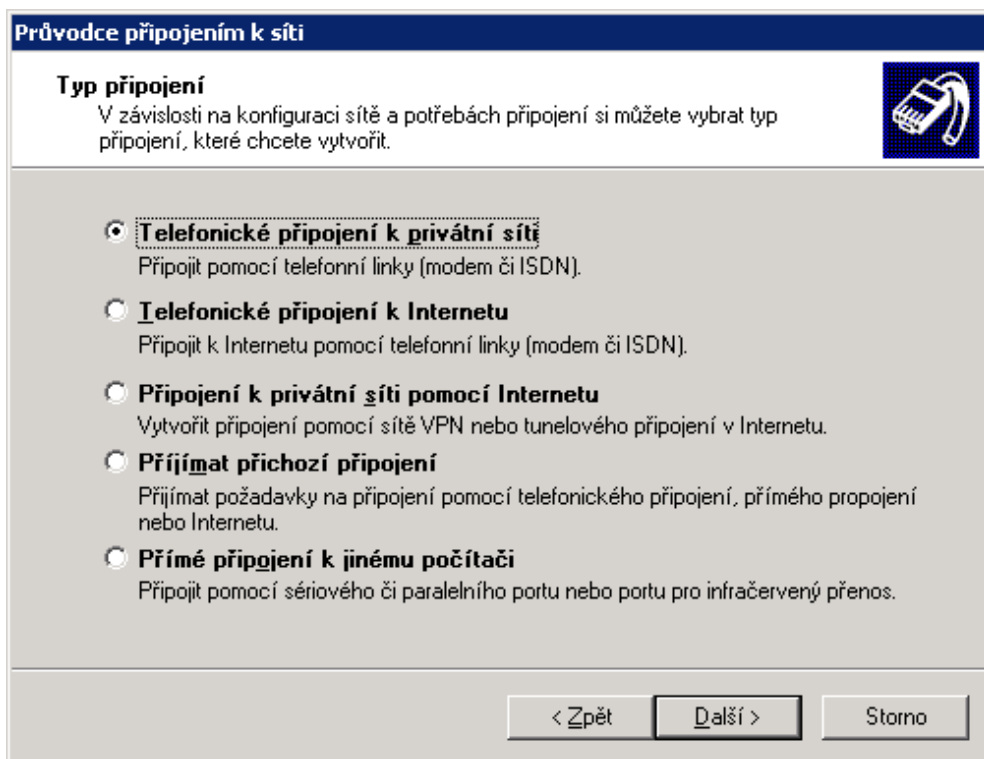
Střední až velké sítě

Střední až velké sítě vyžadují robustnější architekturu, jejíž součástí je více propojených podsítí a která může růst podle potřeb uživatelů.

Směrování a vzdálený přístup

Jednou ze služeb, která umožňuje společnosti zvýšit svou produktivitu, je služba Směrování a vzdálený přístup (Routing and Remote Access) systému Windows 2000. Jestliže se klienti nenacházejí v místě vašich kanceláří, tato služba jim umožní vzdálený přístup k prostředkům na interní síti. Služba také zajišťuje několik možností maximalizování rychlosti a zabezpečení. Systém Windows 2000 Professional uživatelům značně zjednodušuje proces připojení ke vzdáleným sítím včetně virtuálních privátních sítí (VPN) a zjednodušuje také telefonická a infračervená připojení i přímá připojení kabelem.

S vytvářením nových typů připojení jediným nástrojem pomůže uživatelům Průvodce připojením k síti (Network Connection Wizard). Nastavení připojení je také automatizováno, takže se eliminuje potřeba nahrávat si a instalovat další služby, což je krok nutný pro nastavení určitých typů vzdáleného připojení k síti v systému Windows 95. Průvodce připojením k síti najdete na obrázku 22.6.



Obrázek 22.6 Průvodce připojením k síti

Telefonické připojení k privátní síti

Klienti, kteří nechtějí používat pro vzdálený přístup virtuální privátní síť (VPN), se mohou v zájmu získání přístupu k prostředkům přímo telefonicky připojit k serveru vzdáleného přístupu vaší společnosti. Jediným požadavkem je nastavit oprávnění pro vzdálené klienty, které umožní uživatelům přístup. Nevýhodou této metody jsou případné poplatky za meziměstské volání hrazené uživatelem nebo společností.

Přímé telefonické spojení

Chtějí-li uživatelé přenášet soubory a odesílat a přijímat poštu, mohou se telefonicky přímo připojit k serverům vzdáleného přístupu své společnosti. Je to sice pohodlná, ale potenciálně nákladná možnost získání přístupu k síti. Poplatky za místní i meziměstské hovory mohou časem zvýšit náklady jak pro vzdáleného uživatele tak i pro podnik. Mezi dodatečné náklady patří také potřeba správy infrastruktury přímého telefonického připojování. V některých případech může být ekonomičtější nahradit služby přímého telefonického připojení použitím služby Internet Authentication Services (IAS) systému Windows 2000. Další informace o službě IAS najdete v kapitole „Určení strategií konektivity sítě“ v této knize.

Aby se mohl klient připojit k serveru vzdáleného přístupu společnosti, musí klient obdržet příslušná oprávnění pro podnikovou síť. Pak je zapotřebí vytvořit profil telefonického připojení na klientském počítači výběrem položky **Vytvořit nové připojení**

(Make New Connection) ve složce Síťová a telefonická připojení (Network and Dial-Up Connections), která je součástí ovládacích panelů.

Další možností přístupu uživatelů k jejich podnikovým účtům je použití VPN, jak je popsáno v následujícím oddílu.

Přes ISP pomocí virtuálních privátních sítí

Vzdálení klienti ve dnešních pokročilých sítích mohou přistupovat k prostředkům pomocí protokolů VPN. Systém Windows 2000 podporuje protokol PPTP, ale umožňuje také velmi bezpečné připojení pomocí protokolu L2TP ve spojení s protokolem IPSec. Pomocí L2TP a IPSec lze vytvořit přes ISP vzdáleného klienta zabezpečené tunely, které umožní klientovi odesílat a přijímat data chráněná před narušením v prostředí Internetu.

Protokol IPSec data putující mezi dvěma počítači šifruje, čímž je na síti chrání před jejich neoprávněnou změnou a čtením. Nejprve musí správce definovat, jak si budou oba počítače vzájemně důvěřovat, a pak musí určit, jak počítače zabezpečí svůj provoz. Tato konfigurace je obsažena v zásadách protokolu IPSec, které správce vytváří a aplikuje na místní počítač nebo pomocí zásad skupiny v Active Directory. Vzhledem k obtížnosti konfigurování zásad protokolu IPSec společnost Microsoft zabudovala podporu IPSec do protokolu L2TP, takže stačí jen vytvořit připojení VPN pomocí L2TP ze vzdáleného počítače na server VPN. Další informace o protokolu IPSec najdete v knize *Microsoft Windows 2000 Server Síť TCP/IP*.

Abyste mohli používat protokol IPSec u internetových nebo síťových klientů, musí být na obou hostitelích, kteří si vyměňují data, instalován modul snap-in protokolu IPSec. Jestliže se vzdálený uživatel telefonicky připojuje přes svého místního poskytovatele připojení k Internetu (ISP), pak musí protokol IPSec běžet jak na tomto klientovi, tak i na serveru VPN, který klient volá. Potřebují-li si zabezpečeně vyměňovat data dva klienti v interní síti, na obou klientech také musí běžet protokol IPSec.

Příklad střední až velké sítě

Střední až velká síť obsahuje stovky až tisíce počítačů a více podsítí. Technologie, které byly použity v sítích SOHO pro připojení k Internetu nebo k podnikové síti, vyžadují nyní více konfigurování, zároveň však mají více schopností. Tabulka 22.2 uvádí seznam různých technologií a jak se aplikují na jednotlivé typy sítí.

Tabulka 22.2 Síťové technologie

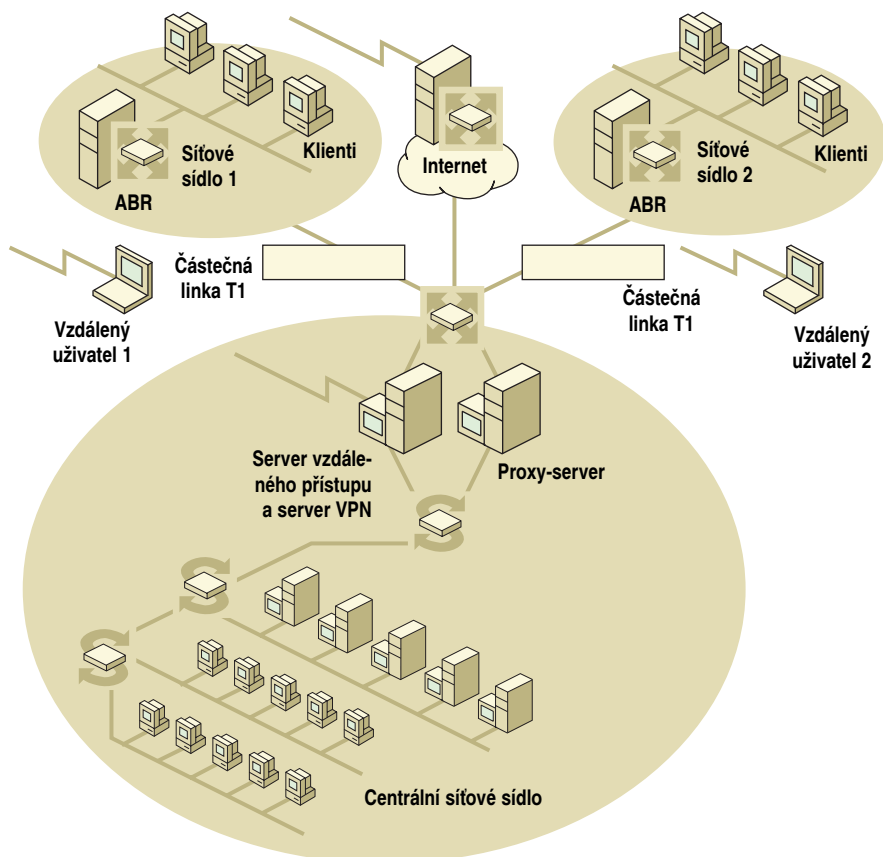
SOHO	Střední síť	Velká síť
Používá ICS, rozsah privátních adres IP 192.168.0.0/24.	Používá službu NAT nakonfigurovanou s příslušným rozsahem privátních adres IP.	Používá Microsoft Proxy Server pro připojení k Internetu a používá DHCP k alokování adres IP.
Využívá pouze PPTP.	Využívá pouze PPTP.	Používá oddělený server VPN umožňující tunelový provoz PPTP a L2TP/IPSec.
Využívá jen jedno rozhraní sítě.	Využívá více rozhraní sítě.	Servery proxy a VPN jsou připojeny ke směrovači s více síťovými rozhraními.
Používá k překladu názvů pouze DNS.	Používá k překladu názvů DNS, WINS nebo obě technologie.	Používá k překladu názvů DNS, WINS nebo obě technologie.

ICS výborně funguje na menších sítích SOHO, kde existuje jen jedna podsít' a jediné připojení k Internetu. Středně velké sítě mohou využívat pro připojení svých klientů k Internetu službu NAT, vzhledem k její schopnosti obsluhovat více podsítí a více rozsahů adres IP. Větší sítě potřebují proxy-server a server VPN, aby umožnily klientům přístup na Internet a tunelový provoz.

Velké sítě musí mít ve své infrastruktuře oblast nazývanou *demilitarizovaná zóna* (DMZ). Tato oblast je síť dovolující rozšíření Internetu do privátní sítě, která však zároveň udržuje zabezpečení na síti. Do této oblasti patří všechny servery, které mají nějaká rozhraní vystavená Internetu. Další informace o zónách DMZ najdete v kapitole „Určení strategií konektivity sítě“ v této knize.

V našem příkladě používá střední až velký podnik síť obsluhující 750 až 1000 zaměstnanců ve třech síťových sídlech. Sídla v síti jsou propojena linkami T1 a částečnými linkami T1. Podnik má určité vzdálené uživatele, kteří se telefonicky připojují, aby mohli přijímat soubory a elektronickou poštu, a každý zaměstnanec má svůj vlastní účet vzdáleného přístupu. Každé sídlo má také připojení k Internetu, přes které mohou zaměstnanci přistupovat z pracovních důvodů na Internet. Tato síť je v procesu přechodu ze systému NetWare na infrastrukturu Windows 2000 a velmi důležitá je možnost interoperability mezi klienty a servery v prostředích Windows 2000 i NetWare.

Obrázek 22.7 je zjednodušený diagram tohoto příkladu.



Obrázek 22.7 Střední až velká síť

Klienty v této síti jsou:

- Klienti Windows 98
- Klienti Windows 2000 Professional
- Klienti Windows 95
- Klienti Windows NT 4.0 Workstation
- Klienti NetWare

Protože tato síť je postupně migrována z NetWare na Windows 2000, většina zaměstnanců nadále vyžaduje přístup k serverům a tiskárnám NetWare. Někteří klienti Windows na části sítě, kde stále běží IPX, používají službu Client Services for NetWare a protokol NWLink. Jiní klienti Windows používají TCP/IP a přistupují k potřebným souborům a tiskárnám NetWare přes směrovače Windows 2000 se spuštěnou službou Gateway Services for NetWare. Vzdálení klienti přistupují k serverům se systémem Windows 2000 a serverům NetWare pomocí víceprotokolového připojení VPN a serveru vzdáleného přístupu umístěného v demilitarizované zóně (DMZ) centrálního síťového sídla. Klienti na této síti získávají své adresy IP ze serveru DHCP a přístup k Internetu probíhá přes proxy-server umístěný v DMZ. Další informace o návrhu středních až velkých sítí najdete v kapitole „Určení strategií konektivity sítí“ v této knize.

Seznam úkolů plánování konektivity klientů

Tabulka 22.3 shrnuje úkoly, které musíte vykonat při určování svých strategií konektivity klientů.

Tabulka 22.3 Seznam úkolů plánování konektivity klientů

Úkol	Umístění v kapitole
Určete použití potřebného protokolu.	Služby a protokoly systému Windows 2000
Nakonfigurujte klienty se statickými adresami IP.	Statické adresy
Nakonfigurujte možnosti DHCP.	Protokol DHCP
Nakonfigurujte klienty používající IPX.	Síťoví klienti protokolu IPX
Nakonfigurujte klienty používající AppleTalk.	Síťoví klienti protokolu AppleTalk
Učiňte rozhodnutí ohledně telefonického přístupu a přístupu přes VPN.	Střední až velké sítě

KAPITOLA 23

Definování standardů správy a konfigurace klientů

Mezi základní cíle zavádění informačních technologií (IT) do organizací patří zvýšení produktivity uživatelů a omezení nákladů souvisejících se správou klientských počítačů. Systémy Microsoft Windows 2000 Server a Microsoft Windows 2000 Professional poskytují více nových funkcí orientovaných na uživatele i správu, které může váš tým používání klientských a přenosných počítačů využít pro zvýšení produktivity uživatelů a správu nákladů na podporu klientů.

Tato kapitola vám pomůže identifikovat a implementovat uvedené prvky ve vaší organizaci. Navíc vás tato kapitola uvede do rozšířených možností správy poskytovaných zásadami skupiny (Group Policy) v systémech Windows 2000 Professional a Windows 2000 Server. Tyto informace vám pomohou vytvořit standardy správy a klientů vaší organizace, které budou daných možností využívat. Jestliže jste tak ještě neučinili, dokončete vyhodnocení klientského softwaru a hardwarové infrastruktury vaší organizace. Další informace najdete v kapitolách „Vytvoření testovací laboratoře systému Windows 2000“ a „Testování kompatibility aplikací se systémem Windows 2000“ v této knize. Také bude vhodné, když se seznámíte s cíly správy IT vaší organizace.

V této kapitole

Umožnění správy klientských systémů 672

Správa klientů pomocí zásad skupiny 680

Konfigurování hardwaru 693

Definování standardů uživatelského rozhraní 696

Seznam úkolů plánování klientských standardů 706

Cíle kapitoly

Tato kapitola vám pomůže vyvinout následující dokumenty plánování:

- Plán správy klientů
- Preferované konfigurace klientů

Související informace v sadě Resource Kit

- Další informace o použití zásad skupiny a vytváření souborů šablony pro správu (.adm) najdete v kapitole „Zásady skupiny“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.

- Další informace o použití funkcí Microsoft IntelliMirror v systému Windows 2000 najdete v kapitole „Aplikování správy změn a konfigurací“ v této knize.
- Další informace o instalačních službách a nástrojích najdete v kapitolách „Automatizování instalace a inovace klientů“ a „Zavádění systému Windows 2000 pomocí serveru Systems Management Server“ v této knize.
- Další informace o zavádění terminálových služeb najdete v kapitole „Zavádění terminálových služeb“ v této knize.
- Další informace o plánování funkcí zabezpečení systému Windows 2000 najdete v kapitole „Plánování distribuovaného zabezpečení“ v této knize.

Umožnění správy klientských systémů

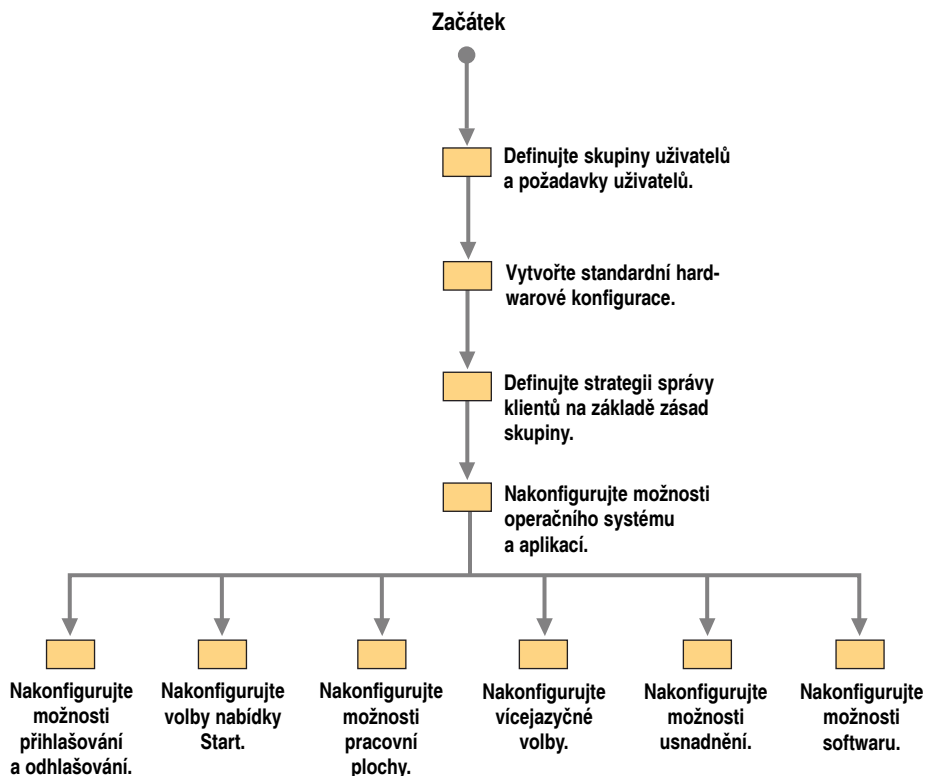
Správa a podpora klientských počítačů může být jednoduchá činnost nebo může jít o extrémně složitou aktivitu. Uživatelé ve velkých organizacích mají obvykle velmi různé znalosti práce s počítači. Používají různé aplikace a hardware a často pracují v široce distribuovaných lokacích. Stále rostoucí procento uživatelů pracuje mimo síťové sídlo a připojuje se k síti pomocí pomalých spojení. Řada studií identifikovala tyto vzory rozmanitého používání a nedostatek standardů konfigurace klientů jako nejvýznamnější faktory růstu nákladů na podporu IT.

Tato kapitola vám pomůže definovat základní standardy konfigurace klientů, které budou sloužit potřebám vašich uživatelů bez ohledu na místo jejich práce nebo toho co jejich práce vyžaduje. Navíc se naučíte používat zásady skupiny k lepší správě klientských počítačů se systémem Windows 2000.

Plánování standardů klientských počítačů vyžaduje technické i organizační znalosti. Musíte rozumět svému počítačovému prostředí a určit potřeby jak pro uživatele tak i pro organizaci. Musíte také rozhodnout, které možnosti systému Windows 2000 povolíte, a pak zdokumentovat změny potřebné ke splnění vašich cílů. Váš plán standardů klientských počítačů musí počítat s těmito prvky:

- Uživatelé a jejich požadavky na počítače.
- Aplikace a požadavky aplikací.
- Hardware a požadavky hardwaru.
- Váš aktuální a požadovaný model správy.
- Významné problémy podpory a jejich řešení.

Na základě výzkumu a pochopení nových funkcí podpory klientů v systémech Windows 2000 Server a Windows 2000 Professional můžete naplánovat standardy správy a konfigurace klientů. Obrázek 23.1 ukazuje proces plánování vytváření standardů správy a konfigurace klientů.



Obrázek 23.1 Přehled plánování správy a konfigurace klientů

Vytvoření klientských standardů zahrnuje více problémů, než je možné popsat v jediné kapitole. Tato kapitola popisuje následující možnosti správy a konfigurace klientů systému Windows 2000:

- Možnosti konfigurace hardwaru. Standardní volby hardwarové konfigurace mobilních i kancelářských počítačů potřebných k provozování systému Windows 2000.
- Možnosti správy. Zásady skupiny, základní prostředek systému Windows 2000 pro implementování voleb správy a konfigurace klientů.
- Možnosti operačního systému a aplikací. Operační systém a aplikace, které uživatelé potřebují pro svou práci. Sem patří také možnosti konfigurace nabídky Start a pracovní plochy dostupné v systému Windows 2000 včetně:
 - Vícejazyčné volby. Výběr mezi podporou více jazyků, která je součástí Windows 2000, nebo novou vícejazyčnou verzí systému Windows 2000.
 - Možnosti usnadnění. Funkce systému Windows 2000, které usnadňují používání počítačů osobám nějakým způsobem postiženým.

V jiných kapitolách této knihy jsou popsány následující možnosti správy a konfigurace klientů systému Windows 2000:

- Možnosti zabezpečení klientů jsou popsány v kapitole „Plánování distribuovaného zabezpečení“.
- Funkce správy klientů používající adresářovou službu Active Directory, správa uživatelských dat, instalace a údržba softwaru a správa uživatelských nastavení, které se společně označují termínem IntelliMirror, a také vzdálená instalace operačního systému, jsou popsány v kapitole „Aplikování správy změn a konfigurací“.
- Přístup k síti je popsán v kapitole „Definování strategie konektivity klientů“.

Jakmile dokončíte úkoly plánování popsané v této kapitole, přečtěte si a splňte úkoly plánování ve výše uvedených kapitolách. Tak dokončíte plánování standardů správy a konfigurace klientů.

Definování typů uživatelů

Velké organizace mají mnoho různých typů uživatelů. Následující výpis představuje některé z rozdílů, které ovlivňují uživatelské vzory používání počítačů:

- Organizační jednotka (OU), do které uživatel patří (jako je účetní oddělení, technické oddělení nebo marketing).
- Typ práce vykonávané uživatelem (například technická, exekutivní nebo v administrativě).
- Kde uživatelé vykonávají svou práci (jako například v kanceláři, ze vzdáleného místa nebo na sdíleném počítači).
- Stupeň autonomie, který uživatelé pro svou práci požadují.
- Množství a typ podpory vyžadované uživatelem.

Navíc je důležité uvědomit si, zda je uživatel:

Cestující Mnoho uživatelů se přesunuje od jednoho počítače k druhému. Cestující uživatelé si počítač obvykle při přesunu mezi různými místy neberou sebou, ale místo toho používají počítač v místě, kde právě pracují. Příklady cestujících uživatelů, kteří často pracují na různých místech, jsou recepční nebo pokladní v bance.

Mobilní Vzrůstající počet pracovníků pravidelně cestuje a vykonává svou práci na přenosném počítači. Při cestování jsou většinou odpojeni od sítě a často se také připojují k síti pomocí připojení s úzkou šířkou pásma. Do kategorie mobilních uživatelů často patří prodejci a konzultanti.

Vzdálený Vzdálení uživatelé se od mobilních uživatelů odlišují tím, že se obvykle k síti připojují z jednoho místa, například z pobočky nebo z domova, a často používají pomalé nebo zprostředkované síťové připojení.

Určený pro konkrétní úkoly Uživatelé, kteří potřebují počítač k vykonání specifické, omezené sady úkolů, jako je například zadávání objednávek. Uživatelé určenému pro konkrétní úkoly může dostávat počítač se spuštěnými terminálovými službami. Příklady uživatelů s konkrétními úkoly jsou recepční a pokladní v bankách.

Se speciálními znalostmi Uživatelé, jako jsou technici, právníci, grafičtí návrháři a programátoři, kteří na své počítače kladou největší požadavky a často požadují specializované aplikace a zvláštní konfigurace.

Jestliže jste tak zatím ještě neučinili, vytvořte tabulku podobnou té uvedené dále, s jejíž pomocí určíte typy uživatelů ve vaší organizaci (někteří uživatelé spadají do více kategorií).

Tabulka 23.1 Příklad tabulky typů uživatelů

Práce	Kategorie	Pracovní skupina	Umístění	Požadované aplikace	Požadovaná podpora	Množství autonomie
Hlavní finanční úředník	Uživatel se speciálními znalostmi	Finanční	Ředitelství	Nutné a volitelné	Normální	Vysoká
Manažer pobočky	Vzdálený uživatel se speciálními znalostmi	Marketing	Pobočka	Nutné a volitelné	Normální	Vysoká
Prodejce	Mobilní uživatel se speciálními znalostmi	Marketing	Mění se	Nutné a volitelné	Normální	Vysoká
Pracovník ve výrobě	Cestující pracovník s konkrétními úkoly	Výroba	Různá místa ve výrobní hale	Nutné	Vysoká	Nízká
Recepční	Cestující pracovník s konkrétními úkoly	Administrativa	Různá místa na ředitelství	Nutné	Vysoká	Nízká

Fakta o samotných uživateli nejsou informacemi dostačujícími pro vytvoření klientských standardů. Musíte dosáhnout hlubokého porozumění jejich potřebám a problémům, se kterými se mohou setkávat (například ztráta dat způsobená selháním počítače, stejný přístup k datům bez ohledu na to, kde se právě nacházejí, nebo udržování jejich dat v synchronizaci s daty ostatních uživatelů, i když jsou často odpojeni od sítě). Až po opravdu důkladném pochopení uživatelů a jejich potřeb práce s počítačem můžete vyvinout potřebné klientské standardy.

Vyhodnocení požadavků typů uživatelů

Jakmile pochopíte základní obchodní či výrobní požadavky uživatelů, musíte v zájmu dokončení klientských standardů vyhodnotit své aktuální a požadované prostředí. Proto proveďte tyto body:

- Požadavky softwaru
- Hardware počítačů
- Model správy
- Konfigurace počítačů

Následující oddíly představují reprezentativní sady požadavků pro „základní“ i „pokročilé“ uživatele. Základní požadavky, které jsou tu definované, se nejčastěji aplikují na zaměstnance s konkrétními úkoly. Pokročilé požadavky se obvykle aplikují na pracovníky se speciálními znalostmi. Další informace o tom, jak splnit potřeby základních a pokročilých uživatelů, najdete v kapitole „Aplikování správy změn a konfigurací“ v této knize. Uvedené profily jsou však obecné. Standardy ve vaší organizaci se budou li-

šit a podle potřeb vaší organizace může být také nutné vytvořit standardy pro další kategorie uživatelů.

Definování softwarových standardů

Velké organizace obvykle podporují stovky a někdy i tisíce různých softwarových aplikací a verzí softwarových aplikací včetně operačních systémů. Mnoho organizací může snížit náklady na klientské počítače implementováním základních softwarových standardů – to platí zejména pro funkce používané v celé organizaci, jako jsou elektronická pošta, zpracování textu a pracovní listy – a odstraněním zastaralého a zbytečného softwaru.

Chcete-li vyvinout standardy klientských aplikací, zabývejte se následujícími otázkami týkajícími se operačních systémů, obvyklých komerčních aplikací, jako je software zpracování textu, a obchodních aplikací, které byly vyvinuty interně pro zpracování takových úkolů, jako je správa klientů nebo plnění objednávek:

- Jaký software musí vaše organizace mít?
- Jaký software je zapotřebí pro konkrétní práci nebo provozní jednotku?
- Jaký software je pro organizaci, provozní jednotku, nebo pro pracovníky vykonávající určitý typ práce volitelný?
- Jak často se softwarové požadavky ve vaší organizaci mění?
- Kdo určuje používaný software – určuje se v celé organizaci nebo v jednotlivých pracovních skupinách?
- Jak se software upravuje?
- Jak se software distribuuje?
- Jak se software konfiguruje?
- Jak se instaluje nový klientský software?
- Jak se inovuje existující software?
- Jak se nový software vyhodnocuje nebo zkouší v pilotních programech?

Zároveň určete, jaký software se bude zavádět společně se systémem Windows 2000 a jak se bude zavádět. Software, který se nainstaluje společně s operačním systémem, lze zpřístupnit uživatelům dále podle potřeb.

Základní uživatelé

Základní uživatelé mohou vyžadovat standardizovanou konfiguraci operačního systému a minimální počet standardních aplikací ve společnosti, jako je podpora elektronické pošty a zpracování textu, společně se specifickými aplikacemi, které potřebují pro svou práci (například aplikace zadávání objednávky). Základním uživatelům však nebude umožněno instalovat volitelné aplikace a lze také zakázat složitější funkce aplikací, jako jsou například kontingenční tabulky v aplikacích pracovních listů.

Pokročilí uživatelé

Pokročilí uživatelé často požadují pokročilé funkce operačního systému, jako je schopnost vytvářet osobní místa sdílení na síti. Také obvykle vyžadují další volitelné aplikace a funkce, které si mohou podle potřeby nainstalovat. Můžete jim však zabránit v instalaci neschválených aplikací.

Poznámka Jakmile určíte, které aplikace jsou nutné a které volitelné, přečtěte si kapitoly „Aplikování správy změn a konfigurací“, „Automatizování instalace a inovace klientů“ a „Zavádění systému Windows 2000 pomocí serveru Systems Management Server“ v této knize, kde najdete instrukce týkající se instalace a správy těchto aplikací.

Definování hardwarových standardů

Aplikace, které vaši uživatelé potřebují ke své práci, určují hardwarové požadavky vaší společnosti. Plánování rozpočtu pro hardware však často představuje delší zaváděcí časy než plánování inovace softwaru. Proto plánujte pečlivě, aby byl dostatek času pro předání potřebného počítačového hardwaru uživatelům v okamžiku, kdy jej potřebují. Následující výčet uvádí některé otázky, které si můžete položit v souvislosti s klienty ve vaší organizaci:

- Jak rychlé jsou procesory ve vašich současných klientských kancelářských počítačích? Jak rychlé jsou procesory v přenosných počítačích?
- Jak rychlá je síťová konektivita vašich současných klientů (včetně přenosných počítačů, které jsou připojeny k síti nebo mají modem)?
- Jak velké množství paměti s náhodným přístupem (RAM) a kolik místa na pevném disku mají?
- Existují pro současné síťové adaptéry a další periferní zařízení ovladače určené pro systém Windows 2000?
- Jaké systémy souborů používají?
- Pracují na počítačích v současné době jiné operační systémy, které je zapotřebí inovovat, nebo musíte vykonat čisté instalace?
- Mohou současné počítače využít technologii vzdáleného spouštění? Mají síťové adaptéry kompatibilní se vzdáleným spouštěním? Mohou použít disketu vzdáleného spouštění?
- Budete k ukládání uživatelských dat a konfiguračních dat používat sdílená místa na síti?
- Kdo je zodpovědný za zálohování dat uživatelů?
- Jak do své organizace zavedete nové počítače? Jak aplikujete nový hardware? Instaluje výrobce originálního vybavení aplikace předběžně? Odstraňujete z nového hardwaru nějaký předem instalovaný software a pak jej znovu instalujete podle svých standardů?
- Jak nahradíte porouchaný hardware? Dojde-li k selhání pevného disku, jak jej nahradíte? Jak nahradíte nebo obnovíte operační systém? Jak nahradíte nebo obnovíte aplikace? Jak nahradíte nebo obnovíte uživatelská data?
- Kladete na data na pevném disku nějaké požadavky týkající se zabezpečení? Používáte nějakou formu šifrování dat?
- Mají vaše počítače více konfigurací? Má například přenosný počítač jednu sadu hardwarových funkcí v okamžiku, kdy je v doku (včetně síťového adaptéru), a jiný hardwarový profil v okamžiku, kdy není v doku (a používá místo síťové karty vysoko rychlostní modem)?
- Jakou dobu strávíte řešením hardwarového problému, než nahradíte počítač a obnovíte na něm standardní prostředí operačního systému a aplikací?

Pro každou třídu uživatelů v organizaci definujte standardní typ počítače, který splňuje aktuální potřeby a předpokládané potřeby minimálně po následující dva roky. Navíc se pokuste snížit počet různých podporovaných hardwarových konfigurací, protože tím zvýšíte své schopnosti podporovat uživatele a také omezíte náklady na podporu klientů.

Další informace o možnostech inovace a čisté instalace najdete v kapitolách „Automatizování instalace a inovace klientů“ a „Zavádění systému Windows 2000 pomocí serveru Systems Management Server“ v této knize. Další informace o vzdálené instalaci operačního systému a složkách režimu offline najdete v kapitole „Aplikování správy změn a konfigurací“ v této knize.

Protože jen málo organizací si může dovolit koupit nejnovějších, výkonných a univerzálních počítačů pro všechny zaměstnance, ukazují pokyny v tabulce 23.2, jak můžete vyrovnat počítačový hardware s potřebami vašich skupin uživatelů.

Tabulka 23.3 Ukázková strategie přidělování počítačů

Pokud počítač:	Přiřadte jej:	Také zvažte:
Nesplňuje minimální hardwarové požadavky systému Windows 2000	Uživatelům s konkrétními úkoly	Použití terminálových služeb s tímto hardwarem
Splňuje minimální hardwarové požadavky systému Windows 2000	Základním uživatelům (včetně cestujících uživatelů a uživatelů s konkrétními úkoly)	Poskytnutí trvalého síťového připojení základním uživatelům
Překračuje minimální hardwarové požadavky systému Windows 2000	Pokročilým uživatelům (včetně mobilních uživatelů a uživatelů se speciálními znalostmi)	

Definování významných problémů technické podpory

Když porozumíte aktuálním problémům podpory, pomůže vám to zlepšit klientské standardy správy a konfigurace a snížit náklady na podporu. Následující otázky vám pomohou určit, jaké zásady správy budou vaší organizaci přinášet největší hodnoty:

- Jakých je vašich deset nejvýznamnějších problémů podpory?

Vytvořte jejich seznam a vyvíjte akční plány na omezení jejich výskytu.

- Jak často uživatelé „narušují“ svou konfiguraci tím, že se pokusí změnit nastavení (například ovladače grafické karty) a další konfigurační volby?

Je-li častost problémů s konfigurací nepřijatelně vysoká, můžete omezit možnosti uživatelů nastavovat konfiguraci operačního systému.

- Jak často uživatelé „narušují“ svou konfiguraci tím, že se pokusí nesprávně přidat nebo odebrat aplikace?

Je-li častost tohoto problému nepřijatelně vysoká, můžete omezit možnosti uživatelů instalovat a odebírat aplikace.

- Instalují uživatelé na své počítače neautorizovaný software?

Je-li to ve vaší organizaci problém, vytvořte zásady vaší společnosti určující, zda je povoleno používání neautorizovaného softwaru. Když povolíte uživatelům přinášet

do organizace neautorizovaný software, definujte typy povoleného softwaru a pravidla licencování, kterých se musí uživatelé držet.

- Byla zabezpečena data na klientech? Musejí být zabezpečena?

Většina organizací definuje prostředky zabezpečení dat společnosti. Úroveň zabezpečení se liší podle typu daných dat (například finanční data nebo obchodní tajemství vyžadují jednu úroveň zabezpečení a oznámení pro veřejnost vyžadují zase jinou úroveň). Můžete také definovat, kdo podle typu dat zodpovídá za zabezpečení (například uživatelé nebo oddělení IT).

- Mají uživatelé možnost pracovat se svým počítačem jako místní správce?

Jestliže měli v minulosti uživatelé možnost fungovat jako místní správci, pak je instalace nového operačního systému perfektní příležitostí změnit nebo doladit oprávnění tak, aby efektivněji plnily potřeby správy vaší organizace.

- Jakou dobu se pracovníci vašeho oddělení technické podpory snaží vyřešit problém narušené konfigurace, než znovu nainstalují nebo resetují základní konfiguraci?

Nemáte-li časové limity technické podpory pro narušené konfigurace, zvažte jejich zavedení. Také vyhodnoťte funkce systému Windows 2000, které lze použít k zálohování dat uživatelů a instalaci nebo opakované instalaci operačního systému a aplikací. Tyto nové funkce mohou ovlivnit dobu vyřešení problému. Je-li například jednodušší přeinstalovat počítač a obnovit data, než vyhledávat problém v narušené konfiguraci, můžete výrazně snížit délku průměrného řešení problému.

Vaše odpovědi na tyto a další otázky o technické podpoře vám pomohou určit, které funkce a konfigurace systému Windows 2000 musíte implementovat. Dále v této kapitole je popsáno mnoho reprezentativních konfigurací a možností řízení.

Odpovědi na uvedené otázky související s technickou podporou vám také pomohou vyhodnotit efektivitu vašeho současného modelu správy a standardů. Mezery a nedostatky ve službách technické podpory klientů lze často vyřešit zavedením vylepšeného modelu správy. Následující oddíl vám pomůže vyhodnotit váš stávající model správy.

Definování modelu správy a standardů

Dosud byly manažeři IT omezeni v tom, že nemohli delegovat úkoly správy IT způsobem, který by jejich organizaci vyhovoval nejlépe. Systém Windows 2000 poskytuje výrazně zlepšenou podporu řízení klientů a delegování úkolů správy.

Odráží váš model správy IT aktuální strukturu vaší organizace? Je-li váš model správy IT již zastaralý, musíte přehodnotit všechny důležité úlohy IT a místa jejich vykonávání, aby je bylo možné delegovat a vykonávat efektivněji. Některé z otázek, na které si musíte odpovědět, jsou uvedeny zde:

- Kdo vytváří a mění účty uživatelů a počítačů? Kolik uživatelských a počítačových účtů je vytvořeno nebo upraveno každý měsíc?

V mnoha organizacích, které rychle rostly, nemůže již jedinec nebo ani tým pravidelně aktualizovat informace o uživateli a počítači. Naopak organizace, které se sloučily nebo prošly akvizicí, mohou mít několik jednotlivců nebo týmů, které nadbytečně vykonávají stejné úkoly. Budete muset určit nejefektivnější způsob delegování těchto úkolů IT – na úrovni domény, na úrovni organizační jednotky nebo na úrovni síťového sídla.

- Kdo vytváří softwarové standardy? Kdo zodpovídá za zavádění softwaru?
Nemá-li vaše organizace softwarové standardy, migrace na nový operační systém může být vhodnou příležitostí k zavedení takových pravidel, která umožní uživatelům efektivněji komunikovat a sdílet informace. Můžete také zjistit, že mnoho oddělení nebo organizačních jednotek má jedinečné požadavky na aplikace. Při definování aplikačních standardů musíte postihnout centralizované i decentralizované požadavky vaší organizace.
- Kdo zadává nebo aktualizuje hesla? Jaké jsou vaše požadavky na hesla a ověřování?
Mnoho organizací deleguje oprávnění měnit hesla týmu technické podpory. Na druhou stranu samotné požadavky na hesla jsou pravděpodobně nastaveny na vyšší úrovni v organizaci a pro celou organizaci často platí jediná sada požadavků na ověřování.
- Kdo zálohuje servery? Kdo zálohuje data uživatelů? Jak často se zálohování vykonává? Jak často obnovujete data ze zálohy?
V mnoha organizacích se zálohuje pouze servery a uživatelé si musí svá data zálohovat sami – což činí nepravidelně nebo nečiní vůbec. Nezajišťuje-li vaše organizace zálohování dat uživatelů, zvažte vytvoření míst sdílení na serverech pro uživatele a vydání požadavku, aby si uživatelé ukládali důležitá data na tato sdílená místa, která je možno pravidelně zálohovat.
- Má vaše organizace dohody o úrovni služeb nebo jiné explicitní cíle služeb? Jaké jsou explicitní cíle služeb nebo kritéria úspěchu ve vaší organizaci?
Stále větší počet organizací sestavuje explicitní cíle služeb nebo podepisuje dohody o úrovni služeb, na jejichž základě je možné dosáhnout kvantifikovatelných výsledků. Do plánu správy klientů systému Windows 2000 zahrňte existující nebo nové servisní síle. Nastavení explicitních cílů vám pomůže doladit a dotvarovat plány správy klientů tak, aby splnily potřeby vaší organizace.

Shrnutí vašich cílů správy a konfigurace

Než budete pokračovat, shrňte existující plán podpory klientů ve vaší organizaci a standardy podpory, které chcete přijmout.

Také shrňte existující model správy klientů ve vaší organizaci a model správy, který chcete implementovat pomocí funkcí a schopností poskytovaných systémem Windows 2000.

Správa klientů pomocí zásad skupiny

Způsob použití zásad skupiny (Group Policy) ke správě klientů je určen servisními standardy a cíly, které jste ustanovili.

Ve vysoce spravovaném prostředí může vaše dohoda o úrovni služeb zahrnovat instrukce pro zajištění rychlého řešení problémů (například reagování do 15 minut), rychlé výměny zařízení v případě selhání a časté (pravděpodobně každodenní) zálohování dat. Vysoce spravovaná podpora bude navíc zahrnovat pokročilé prvky, jako jsou uživatelská a počítačová prostředí vycházející ze zásad skupiny, instalace a údržba softwaru, složky režimu offline a vlastní skripty procesů přihlašování, odhlašování, spouštění a vypínání.

Méně spravovaná prostředí budou mít pravděpodobně delší čas zavádění podpory a náhrady vybavení a budou poskytovat jenom část služeb nabízených vysoce spravovaným prostředím.

Uživatelé v nespravovaném prostředí si sami řeší své problémy, nahrazují vlastní vybavení, zálohují si svá data a jen minimálně využívají funkce vycházející ze zásad skupiny. Následující oddíly popisují různé úrovně a kvality podpory, kterých lze dosáhnout pomocí systémových zásad systému Microsoft Windows NT verze 4.0, místních zásad skupiny systému Windows 2000 Professional a zásad skupiny vycházejících ze služby Active Directory systému Windows 2000. S těmito znalostmi budete schopni delegovat řízení klíčových úkolů podpory klientů na nejefektivnější úrovni ve vaší organizaci.

Porovnání systémových zásad systému Windows NT 4.0 a zásad skupiny systému Windows 2000

V systému Windows NT 4.0 uvedla společnost Microsoft nástroj Editor systémových zásad (System Policy Editor), který se používal k zadání uživatelských a počítačových konfigurací, jež byly uloženy v registru Windows NT. Pomocí Editoru systémových zásad jste mohli vytvořit systémové zásady sloužící k řízení pracovního prostředí uživatelů a zadat vynucování nastavení konfigurace systémů na všech počítačích se systémem Windows NT 4.0 Workstation nebo Windows NT 4.0 Server.

V systému Windows NT 4.0 (a Microsoft Windows 95 a Microsoft Windows 98) existuje 72 nastavení zásad. Tato nastavení jsou:

- omezena na nastavování hodnot položek v registru na základě souborů .adm;
- aplikovaná na domény;
- dále řízena členstvím uživatelů ve skupinách se zabezpečením;
- nezabezpečená;
- trvale existující v uživatelských profilech, dokud nejsou specifikované zásady zrušeny nebo uživatel neupraví registr;
- používána především k zamknutí počítačů;
- rozšiřitelná výhradně prostřednictvím souborů .adm.

V systému Windows 2000 jsou nastavení zásad skupiny (Group Policy) hlavní metodou, kterou správce umožňuje centralizovanou správu změn a konfigurace. Zásady skupiny lze použít k vytvoření specifických desktopových konfigurací pro určitou skupinu uživatelů a počítačů. Toho se dosahuje úpravou zásad skupiny pomocí modulu snap-in Zásady skupiny (Group Policy) konzoly Microsoft Management Console (MMC). Modul snap-in Zásady skupiny nahrazuje Editor systémových zásad systému Windows NT 4.0 a dává vám větší kontrolu nad konfiguračními nastaveními skupin počítačů a uživatelů.

S více než 100 nastaveními souvisejícími se zabezpečením a více než 450 nastaveními vycházejícími z registru vám zásady skupiny systému Windows 2000 poskytují široký rozsah možností správy počítačového prostředí uživatelů. Zásady skupiny systému Windows 2000:

- mohou vycházet ze služby Active Directory nebo mohou být definovány místně;
- mohou být rozšířeny pomocí konzole Microsoft Management Console (MMC) nebo souborů .adm;
- jsou zabezpečené;

- nezanechávají nastavení v profilech uživatelů po změně efektivních zásad;
- mohou být aplikovány na uživatele nebo počítače v zadaném kontejneru Active Directory (sídla, domény a organizační jednotky);
- mohou být dále řízeny členstvím uživatele nebo počítače ve skupinách se zabezpečením;
- lze používat ke konfigurování mnoha typů nastavení zabezpečení (další informace o nastavení zabezpečení najdete v kapitole „Plánování distribuovaného zabezpečení“ v této knize);
- lze použít k aplikování přihlašovacích, odhlašovacích, spouštěcích a vypínacích skriptů;
- lze používat k instalování a údržbě softwaru;
- lze používat k přesměrování složek (jako jsou Dokumenty [My Documents] a Aplikační data [Application Data]).
- lze používat k údržbě programu Microsoft Internet Explorer.

Vytvořená nastavení zásad skupiny jsou obsažena v objektech zásad skupiny, které jsou svázány s vybranými sídly, doménami a organizačními jednotkami Active Directory. Zásady skupiny používají při vytváření, ukládání a přiřazování nastavení zásad přístup, při němž je ve středu dění dokument. Stejně jako si Microsoft Word ukládá informace do souborů .doc, zásady skupiny ukládají nastavení do objektů zásad skupiny.

Navíc máte možnost přesně nastavit použití zásad skupiny na počítače a uživatele ve vaší společnosti tím, že k filtrování objektů zásad skupiny použijete skupiny se zabezpečením. To zajišťuje rychlejší zpracování zásad skupiny.

Aplikování zásad systému Windows NT 4.0 na systém Windows 2000

Přesun klientů a serverů systému Windows NT 4.0 na systém Windows 2000 změní chování zásad. Svou strategii migrace založte na tom, zda jsou objekty účtů uživatelů a objekty účtů počítačů umístěny na serveru se systémem Windows NT 4.0 Server nebo na serveru se systémem Windows 2000 Server se službou Active Directory. Tabulka 23.3 předpokládá přítomnost klienta se systémem Windows 2000. Všichni klienti, kteří obdrží systémové zásady systému Windows NT 4.0, je získají ze sdíleného místa Netlogon přihlašovacího serveru uživatele.

Tabulka 23.3 Očekávaná chování serverových operačních systémů

Prostředí	Umístění objektu Account	Co ovlivňuje klienta
Čistý systém Windows NT 4.0	Počítač: Windows NT 4.0	Při spuštění počítače: Místní zásady skupiny počítače (pouze při změně). Kdykoli se uživatel přihlásí: Systémové zásady počítače.
	Aktualizace počítače	Před stiskem Ctrl+Alt+Delete: Pouze místní zásady skupiny počítače. Po přihlášení uživatele: Místní zásady skupiny počítače a systémové zásady počítače.
	Uživatel: Windows NT 4.0	Když se uživatel přihlásí: Systémové zásady uživatele. Jestliže se změní místní zásady skupiny: Místní zásady skupiny uživatele a systémové zásady uživatele.

Kombinované (migrace)	Aktualizace uživatele	Místní zásady skupiny uživatele a systémové zásady uživatele.
	Počítač: Windows NT 4.0	Při spuštění počítače: Místní zásady skupiny počítače (pouze při změně). Kdykoli se uživatel přihlásí: Systémové zásady počítače.
	Aktualizace počítače	Před stiskem Ctrl+Alt+Delete: Pouze místní zásady skupiny počítače. Po přihlášení uživatele: Místní zásady skupiny počítače a systémové zásady počítače.
Kombinované (migrace)	Uživatel: Windows 2000	Když se uživatel přihlásí: Zásady skupiny se zpracují po systémových zásadách počítače.
	Aktualizace uživatele	Zásady skupiny uživatele.
	Počítač: Windows 2000	Během spouštění systému: Zásady skupiny.
	Aktualizace počítače	Zásady skupiny počítače.
	Uživatel: Windows NT 4.0	Když se uživatel přihlásí: Systémové zásady uživatele. Jestliže se změní místní zásady skupiny: Místní zásady skupiny uživatele a systémové zásady uživatele.
Systém Windows 2000	Aktualizace uživatele	Místní zásady skupiny uživatele a systémové zásady uživatele.
	Počítač: Windows 2000	Během spouštění počítače a když se uživatel přihlásí: Zásady skupiny.
	Uživatel: Windows 2000	
Bez služby Active Directory	Místní	Pouze místní zásady skupiny.

Poznámka Když existuje objekt účtu počítače v doméně systému Windows NT 4.0 a objekt účtu uživatele existuje v doméně systému Windows 2000, po přihlášení uživatele se zpracují systémové zásady počítače. Toho lze dosáhnout použitím souboru NTConfig.pol ze sdíleného místa Netlogon řadiče domény systému Windows 2000, který se používá k ověření uživatele, a nikoli pomocí řadiče domény se systémem Windows NT 4.0. Doporučujeme vám opustit tento režim kombinovaného zpracování a co nejdříve vstoupit do režimu čistého systému Windows 2000.

Neexistují žádné možnosti změnit toto chování. Chcete-li zjednodušit správu ve vaší organizaci, zvažte co nejrychlejší náhradu systémových zásad systému Windows NT 4.0 zásadami skupiny systému Windows 2000.

Delegování správy klientů pomocí služby Active Directory

Správa klientů systému Windows 2000 je umožněna do plné míry v prostředí zahrnujícím systémy Windows 2000 Professional a Windows 2000 Server a oborů názvů Active Directory.

Nastavení zásad skupiny jsou přiřazena kontejneru služby Active Directory – doméně, sídlu nebo organizační jednotce (OU). Nastavení zásad skupiny, která konfiguruje ve spojení se strukturou Active Directory vaší organizace, vám umožňují definovat klientské standardy tak široce (pro celou organizaci) nebo tak úzce (pro členy jediné pracovní skupiny, pracovní funkce nebo umístění), jak potřebujete. Úroveň, ve které jsou nastavení zásad skupiny implementována, musí být v souladu s modelem správy vaší organizace, který byl definován společně s modelem Active Directory a domén.

Třebaže tým IT, který má za úkol vytvořit a implementovat klientské standardy, se v minulosti obvykle neúčastnil plánování doménového oboru názvů, rozhodně vám doporučujeme, abyste tak učinili, pokud plánujete používat obor názvů Active Directory. Čím dříve v procesu plánování tým doménového oboru názvů pochopí vaše potřeby a cíle správy klientů, tím je pravděpodobnější, že výsledný návrh oboru názvů vaší organizace zlepší vaše možnosti spravovat a podporovat potřeby uživatelů.

Upozornění Pokud jste ještě nevyvinuli obor názvů Active Directory, týmy správy klientů musí spolupracovat s týmem adresáře a oborů názvů, aby mohly být v organizaci stanoveny klientské standardy, definována nastavení zásad skupiny a vykonány úkoly správy na té neefektivnější úrovni.

Dobře navržený obor názvů Active Directory umožňuje relativně jednoduše implementovat určité klientské standardy, jako je podniková elektronická pošta, na úrovni domény nebo organizační jednotky. To také umožňuje delegování možností spravovat specifické úlohy klientů na jiných úrovních, jako je přidávání a odstraňování uživatelů, změna konfigurací počítačů nebo implementování aplikací pro pracovní skupiny.

Můžete například definovat zabezpečené a základní (elektronická pošta, zpracování textu atd.) aplikační standardy na úrovni domény pro celý podnik. Může však být nevýhodné mít na podnikové úrovni správce pro přidávání a odstraňování uživatelů, když je možné asistentovi správce na úrovni sídla nebo OU předat omezená oprávnění vykonávat tyto časté avšak rutinní změny.

Podobně nemusí být správce na úrovni domény nejlepší osobou pro změnu hesel, když uživatelé volají v okamžiku potřeby změny hesla obvykle nejprve technika z oddělení podpory na úrovni sídla nebo OU. Pomocí zásad skupiny systému Windows 2000 můžete delegovat úlohy související s hesly osobám technické podpory, aniž byste jim umožňovali přístup k nastavením, která nemají měnit.

Jako součást plánu správy klientů:

- identifikujte všechny úkoly správy související s klienty, jako jsou: nastavení nového počítače, nastavení účtu uživatele, převody a odstranění, instalace a inovace softwaru, řešení problémů a definování standardů konfigurace klientů;
- zjistěte, kde v organizaci se tyto úkoly v současné době provádějí;
- určete, na jaké úrovni v organizaci je zapotřebí tyto úkoly provádět.

Další informace o vztahu zásad skupiny (Group Policy) ke struktuře služby Active Directory najdete v kapitole „Návrh struktury služby Active Directory“ v této knize.

Delegování správy zásad skupiny

Organizace zavádějící službu Active Directory mohou také delegovat řízení částí této adresářové služby a tak delegovat odpovědnost za mnoho úkolů správy klientů popsaných dříve v této kapitole. Tento oddíl vysvětluje, jak vám mohou zásady skupiny umožnit delegovat úkoly správy na úrovních sídla, domény a OU.

Delegování správy přes zásady skupiny zahrnuje následující tři úkoly, které lze vykonat společně nebo samostatně, jak vaše situace vyžaduje:

- Správa odkazů zásad skupin pro sídlo, doménu nebo OU.
- Vytváření objektů zásad skupiny.
- Úprava objektů zásad skupiny.

Správa odkazů zásad skupiny pro sídlo, doménu nebo OU

Ve výchozím stavu mohou zásady skupiny pro sídla, domény a OU konfigurovat pouze členové skupin Domain Administrators a Enterprise Administrators. Karta **Zásady skupiny** (Group Policy) okna vlastností sídla, domény nebo OU vám umožňuje zadat, které objekty zásad skupiny jsou propojeny na sídlo, doménu nebo OU.

Služba Active Directory podporuje nastavení zabezpečení podle jednotlivých vlastností. To znamená, že můžete uživateli, který není správcem, přidělit oprávnění pro čtení a zápis ke specifickým vlastnostem. Jestliže v tomto případě byl uživateli, kteří nejsou správci, delegován úkol správy odkazů zásad skupiny, mohou spravovat objekty zásad skupiny propojené s daným sídlem, doménou nebo OU. Chcete-li dát uživateli tuto možnost, použijte Průvodce vytvoření delegování (New Delegation Wizard).

Vytváření objektů zásad skupiny

Ve výchozím stavu mohou objekty zásad skupiny vytvářet pouze členové skupiny Domain Administrators, Enterprise Administrators a Group Policy Creator Owners. Jestliže chce správce domény umožnit uživateli, který není správcem, nebo nějaké skupině vytvářet objekty zásad skupiny, daný uživatel nebo skupina může být přidána do skupiny se zabezpečením Group Policy Creator Owners. Když uživatel, který není správcem, ale je členem skupiny Group Policy Creator Owners, vytvoří nějaký objekt zásad skupiny, daný uživatel se stane tvůrcem a vlastníkem daného objektu zásad skupiny a může objekt upravovat. Členství ve skupině Group Policy Creator Owners dává uživateli, kteří nejsou správci, plnou kontrolu pouze nad těmi objekty zásad skupiny, které uživatel vytvoří, nebo těmi, které jsou uživateli explicitně delegovány.

Úprava objektů zásad skupiny

Ve výchozím stavu umožňují objekty zásad skupiny plné řízení členům skupin Domain Administrators, Enterprise Administrators a Group Policy Creator Owners, přičemž není nastaven atribut aplikování zásad skupiny. To znamená, že tito členové mohou upravovat daný objekt zásad skupiny, ale zásady obsažené v daném objektu zásad skupiny se na ně neaplikují.

Standardně mají přístup pro čtení k objektu zásad skupiny členové skupiny Authenticated Users, přičemž atribut aplikování zásad skupiny je nastaven. To znamená, že dané zásady skupiny je ovlivňují.

Členové skupiny Domain Administrators a Enterprise Administrators jsou také členy skupiny Authenticated Users, a proto jsou členové výše uvedených skupin také standardně ovlivněny objekty zásad skupiny, pokud je explicitně nevyjmete.

Když objekt zásad skupiny vytvoří uživatel, který není správcem, daná osoba se stane tvůrcem a vlastníkem (Creator Owner) objektu zásad skupiny. Když objekt zásad skupiny vytvoří nějaký správce, stane se tvůrcem a vlastníkem daného objektu zásad skupiny skupina Domain Administrators.

Aby mohl uživatel upravit objekt zásad skupiny, musí k němu mít přístup pro čtení i zápis. Aby mohl upravit objekt zásad skupiny, musí být uživatel:

- členem skupin Domain Administrators nebo Enterprise Administrators;
- členem skupiny Group Policy Creator Owners a musel daný objekt zásad skupiny dříve vytvořit;
- uživatel s delegovaným přístupem k danému objektu zásad skupiny, tedy správce nebo uživatel, kterému je delegován přístup někým s potřebnými oprávněními pomocí karty **Zabezpečení** (Security) okna vlastností objektu zásad skupiny.

Vytváření konzol MMC zásad skupiny pro delegování zásad skupiny

Zásady skupiny lze delegovat vytvořením a uložením konzol snap-in zásad skupiny (souborů .msc) a následným zadáním, kteří uživatelé a skupiny mají oprávnění pro přístup k danému objektu zásad skupiny nebo do kontejneru Active Directory. Oprávnění objektu zásad skupiny lze definovat pomocí karty **Zabezpečení** (Security) okna vlastností objektu zásad skupiny; tato oprávnění povolují nebo odpírají zadaným skupinám přístup k objektu zásad skupiny.

Tento typ delegování je ještě vylepšen nastaveními zásad dostupnými v konzole MMC. V uzlu **Šablony pro správu** (Administrative Templates) pod položkou **Součástí systému Windows** (Windows Components) v konzole **Microsoft Management Console** je k dispozici několik zásad. Tyto zásady umožňují správci definovat, které moduly snap-in konzoly MMC může a nemůže daný uživatel spustit. Definice zásad mohou být inkluzivní, takže umožňují spouštění pouze určité sady modulů snap-in, nebo mohou být exkluzivní, takže neumožňují spouštění sady modulů snap-in.

Speciální možnosti implementování zásad skupiny

Když budete zásady skupiny aplikovat rozvážně, můžete zlepšit reakční časy sítě, i když začnete používat datově náročnější přesměrování složek a možnosti instalace softwaru. Zásady skupiny aplikujte konzervativně, zejména ze začátku, a pečlivě otestujte všechny navrhované změny, abyste se ujistili, že nedochází ke snížení výkonu sítě.

Navíc vám řada možností implementace umožňuje vyladit aplikování zásad skupiny, aniž by bylo nutné vytvářet další objekty zásad skupiny. Dále jsou uvedeny některé z dostupných možností:

- Možnosti filtrování skupin se zabezpečením
- Možnost nepřepisování (vynucování) objektu zásad skupiny
- Možnost blokování dědění zásad organizační jednotkou
- Možnosti zpracování duplicitních zásad
- Možnosti zpracování přes pomalé připojení
- Možnosti periodické aktualizace
- Možnosti synchronního a asynchronního zpracování

Všechny tyto možnosti jsou krátce popsány v následujících oddílech.

Možnosti filtrování skupin se zabezpečením

Pomocí skupin se zabezpečením systému Windows 2000 můžete přesně určit, které skupiny uživatelů a počítačů určitý objekt zásad skupiny ovlivňuje. To znamená, že můžete filtrovat efekt, jaký má libovolný objekt zásad skupiny na členy zadaných skupin se zabezpečením. K tomu použijte kartu **Zabezpečení** (Security) okna vlastností daného objektu zásad skupiny.

Například na základě úrovně autonomie vhodné pro vaše uživatele přiřadíte různé typy uživatelů do skupin uživatelů systému Windows 2000. Systém Windows 2000 nabízí tyto výchozí skupiny uživatelů, které jsou podobné (nikoli však shodné) výchozím skupinám v systémech Microsoft Windows NT verze 3.51 a Windows NT 4.0:

- **Administrators.** Členové mohou plně spravovat počítač nebo doménu.
- **Backup Operators.** Členové mohou při zálohování souborů obejít zabezpečení souborů.
- **Power Users.** Členové mohou upravovat počítač a instalovat programy, nemohou však číst soubory patřící jiným uživatelům. Mohou také sdílet adresáře a tiskárny.
- **Users.** Členové mohou vytvářet a ukládat dokumenty, nemohou však bez oprávnění správce instalovat programy a nemohou zadávat potenciálně nebezpečné změny do systémových souborů a nastavení systému.
- **Guests.** Členům je zaručen krátkodobý přístup k počítači nebo doméně. Tato kategorie může zahrnovat speciální oprávnění příslušná výrobcům nebo kontraktörům. Účet Guest může být také standardně zakázán.

Poznámka Systém Windows 2000 umožňuje správcům přesněji řídit uživatele, než jak to bylo možné v systému Windows NT 4.0. Proto výchozí oprávnění aplikovaná na členy skupiny Users v systému Windows NT 3.51 a 4.0 nyní platí pro členy skupiny Power Users a výchozí oprávnění aplikovaná na členy skupiny Restricted Users v systému Windows NT 3.51 a 4.0 nyní platí pro členy skupiny Users.

V tabulce 23.1 je možné přidat do skupiny Power Users hlavního finančního úředníka, manažera pobočky a prodejce, zatímco recepční a pracovník ve výrobě budou patřit do skupiny Users. Na základě úkolů vykonávaných členy organizace můžete vytvořit další skupiny a určit úroveň oprávnění, kterou mají ke změně svých vlastních i jiných počítačů, a konfiguraci, kterou jim chcete přiřadit. Můžete například skupinu Users dále rozdělit podle oddělení ve vaší organizaci (prodej, lidské zdroje, technické oddělení atd.), abyste mohli vytvořit a zavést příslušné standardní konfigurace pro všechny zaměstnance vykonávající shodné úkoly. To může výrazně zjednodušit proces správy uživatelů s různými požadavky na konfiguraci a oprávnění.

Chcete-li zabránit aplikování nastavení zásad objektu zásad skupiny na zadanou skupinu, musíte z dané skupiny odstranit položku řízení aplikování přístupu zásad skupiny.

U skupin obsahující uživatele, kteří nejsou správci, musíte také odstranit položku řízení přístupu ke čtení, protože data jsou viditelná všem s přístupem pro čtení.

Další informace o nastavení a používání skupin se zabezpečením najdete v kapitole „Plánování distribuovaného zabezpečení“ v této knize.

Možnosti nepřepisování (vynucování) a blokování zásad

Existují také volby umožňující vám vynutit si nastavení obsažená v určitém objektu zásad skupiny, takže objekty zásad skupiny v kontejnerech Active Directory na nižší úrovni nemohou takové zásady obejít či přepsat. Jestliže jste například definovali určitý objekt zásad skupiny na úrovni domény a zadali jste vynucování (enforce) tohoto objektu zásad skupiny (nepřepisování – no override), nastavení zásad obsažená v daném objektu zásad skupiny platí pro všechny organizační jednotky v doméně. To znamená, že kontejnery nižší úrovně (OU) nemohou přepsat dané doménové zásady skupiny.

Je také možné zablokovat dědění zásad skupiny z nadřazených (rodičovských) kontejnerů Active Directory. Určíte-li například „zásadu blokování dědění“ pro OU, zabráníte tím aplikování objektů zásad skupiny zadaných v kontejnerech Active Directory na vyšší úrovni (jako je OU vyšší úrovně nebo doména). Před možností blokování zásad má však vždy přednost možnost nepřepisování (vynucování).

Možnost duplicitních zásad

Zásady skupiny se aplikují na uživatele nebo počítač podle toho, kde se daný objekt uživatele nebo počítače nachází v adresáři Active Directory. Můžete však potřebovat aplikovat zásady skupiny na uživatele na základě fyzického umístění objektu počítače a nikoli podle logického umístění objektu uživatele v organizaci – například v knihovně nebo když se uživatel z jedné OU přihlásí na počítač v jiné OU. Funkce duplicitních zásad skupiny dává správci možnost aplikovat nastavení zásad skupiny uživatele podle počítače, na který se uživatel přihlásí.

Možnost duplicitních zásad lze například nastavit, když si nepřejete, aby se aplikace přiřazené nebo publikované uživatelům OU marketingu instalovaly v okamžiku, kdy se ti to uživatelé přihlásí na počítače v OU serverů. Prostřednictvím funkce podpory duplicitních zásad skupiny můžete zadat dva další způsoby převzetí seznamu objektů zásad skupiny pro všechny uživatele počítačů v OU serverů:

Režim sloučení V režimu sloučení se během přihlašovacího procesu normálně zpracuje seznam objektů zásad skupiny uživatele pomocí funkce GetGPOList rozhraní Application Programming Interface (API) a pak se znovu zavolá funkce GetGPOList rozhraní API pomocí umístění počítače v Active Directory. Následně se seznam objektů zásad skupiny počítače přidá na konec objektů zásad skupiny uživatele. Objekty zásad skupiny počítače tak budou mít přednost před objekty zásad skupiny uživatele.

Režim nahrazení V tomto režimu se objekty zásad skupiny platící pro uživatele nezpracují. Použijí se pouze objekty zásad skupiny platící pro objekt počítače.

Cesta k tomuto nastavení je: Konfigurace počítače\Šablony pro správu\System\Zásady skupiny (Computer Configuration\Administrative Templates\System\Group Policy). Název zásad je: Režim zpracování duplicitních zásad skupiny uživatele (User Group Policy loopback processing mode).

Zpracování přes pomalé připojení

Mnoho uživatelů, jako jsou ti s přenosnými počítači a ti, kteří pracují mimo prostory společnosti nebo v pobočkách, se občas připojuje k síti přes pomalá spojení. Řadu nastavení zásad skupiny lze nakonfigurovat tak, aby pracovaly, pouze je-li k dispozici odpovídající síťové připojení. Mezi tyto zásady skupiny patří:

- Instalace a údržba softwaru
- Skripty
- Diskové kvóty

- Zabezpečený protokol IP
- Zásady obnovení systému DFS
- Údržba programu Internet Explorer

Cesta k nastavení zásad pomalého připojení je: Konfigurace počítače\Šablony pro správu\System\Zásady skupiny (Computer Configuration\Administrative Templates\System\Group Policy). Každá uvedená možnost zásad skupiny má zásadu zpracování umožňující změnit chování na pomalém připojení.

Jakmile zásady skupiny zjistí pomalé připojení, aplikují následující výchozí nastavení, pokud nejsou změněna:

- Nastavení zabezpečení: Zapnuto (a nelze je vypnout).
- Šablony pro správu: Zapnuto (a nelze je vypnout).
- Instalace a údržba softwaru: Vypnuto.
- Skripty: Vypnuto.
- Přesměrování složek: Vypnuto.
- Údržba programu Internet Explorer: Vypnuto.

Pro všechny položky s výjimkou Šablony pro správu (Administrative Templates) a Nastavení zabezpečení (Security Settings) existuje zásada zapnutí a vypnutí tohoto nastavení. Další informace o konfigurování počítačů s pomalým síťovým připojením najdete v oddílu „Řízení konfigurace pomocí zásad skupiny“ dále v této kapitole.

Zpracování periodické aktualizace

Můžete také zadat periodické zpracování zásad skupiny. Standardně k tomu dochází každých 90 minut s náhodnou odchylkou 30 minut. Tato odchylka je náhodná doba přidaná k intervalu aktualizace, která zabraňuje tomu, aby všichni klienti požadovali zásady skupiny najednou. Slouží k odstranění zbytečných špičkových zatížení na síti například 90 minut poté, co větší počet uživatelů zapne své počítače a přihlásí se ve stejný okamžik. Rychlost aktualizace můžete podle potřeby změnit a použít například menší hodnoty v testovacích a demonstračních prostředích nebo větší intervaly podle potřeby.

Existují dvě nastavení zásad, která vám umožňují změnit interval aktualizování a která se nacházejí v: Konfigurace počítače\Šablony pro správu\System\Zásady skupiny (Computer Configuration\Administrative Templates\System\Group Policy). Jedno nastavení zásad je pro řadiče domény a druhé pro všechny ostatní počítače (včetně dalších serverů). Tato nastavení zásad jsou pojmenována: Interval aktualizace zásad skupiny pro ... (Group Policy refresh interval for...).

Synchronní a asynchronní zpracování

Zpracování zásad skupiny je standardně synchronní jak pro nastavení zásad počítačů tak i uživatelů. V případě zpracování počítačů se uživatelé nemohou přihlásit, dokud nejsou aktualizována všechna nastavení zásad skupiny počítače. V případě zpracování uživatelů nemají uživatelé přístup k pracovní ploše, dokud nejsou aktualizována všechna nastavení zásad skupiny uživatele. Tato pravidla zpracování zajišťují nejbezpečnější operaci.

Existují nastavení zásad skupiny jak pro zpracování zásad skupiny počítače tak i uživatele, která umožňují asynchronní zpracování. Instruuji systém v tom smyslu, aby bez čekání na dokončení aktualizací zásad skupiny pokračoval ve zobrazení výzvy k přihlášení (nastavení počítače) nebo pracovní plochy (nastavení uživatele).

Výsledkem asynchronního zpracování je, že se dialogové okno přihlášení nebo rozhraní systému Windows může objevit dříve, než došlo k aplikování všech nastavení zásad skupiny.

Zadáte-li asynchronní zpracování a uživatel dokáže dokončit proces přihlášení a začít pracovat na počítači ještě před zpracováním všech nastavení počítače nebo uživatele, můžete uživateli způsobit značné problémy. Jestliže například uživatel začne pracovat v aplikaci, která se upravuje, proces může selhat nebo může být uživatel po zpracování nastavení počítače a uživatele svědkem nežádoucích událostí.

Používání klientských rozšíření

Některé součásti zásad skupiny obsahují klientská rozšíření (knihovny .dll), které zodpovídají za implementování zásad skupiny na klientském počítači.

Klientská rozšíření se nahrávají podle potřeby, když klient zpracovává zásady. Klient nejprve obdrží seznam objektů zásad skupiny. Dále projde všemi klientskými rozšířeními a určí, zda mají jednotlivá klientská rozšíření nějaká data v některém z objektů zásad skupiny. Má-li nějaké klientské rozšíření data v určitém objektu zásad skupiny, toto klientské rozšíření se zavolá se seznamem objektů zásad skupiny, které musí zpracovat. Nemá-li určité klientské rozšíření žádná nastavení v žádném z objektů zásad skupiny, nezavolá se.

Pro každé klientské rozšíření zásad skupiny existují nastavení zásad počítače. Každé zásady obsahují nejvýše tři možnosti (zaškrťovací políčka). Některá klientská rozšíření obsahují pouze dvě možnosti zásad počítače, protože třetí možnost nelze na dané rozšíření aplikovat.

Následující oddíly popisují možnosti klientského zpracování zásad skupiny.

Umožnit zpracování přes pomalá síťová připojení

Když se klientské rozšíření zaregistruje v operačním systému, nastaví hodnoty v registru určující, zda musí být zavoláno při aplikování zásad přes pomalé připojení. Některá rozšíření (jako je například instalace a údržba softwaru) přesunují velká množství dat, takže zpracování přes pomalé připojení může výrazně ovlivnit výkon (zvažte čas potřebný k instalování velké aplikace přes modemové spojení 28,8 kilobitů za sekundu [kb/s]).

Správce může nastavit rychlost připojení, která se považuje za pomalou. Jestliže správce rozhodne, že dané klientské rozšíření musí pracovat i na pomalém připojení bez ohledu na množství dat, může také tuto zásadu povolit. Cesta k tomuto nastavení je: Konfigurace počítače\Šablony pro správu\Systém\Zásady skupiny (Computer Configuration\Administrative Templates\System\Group Policy).

Neaplikovat během periodického zpracování na pozadí

Zásady počítače se aplikují během spouštění a pak znovu na pozadí přibližně každých 90 minut. Zásady uživatele se aplikují při přihlašování uživatele a pak přibližně každých 90 minut.

Některá rozšíření mohou zpracovat zásady pouze při prvním spuštění, protože je riskantní zpracovávat zásady na pozadí. Například u instalace a údržby softwaru je bezpečné zpracovávat změny aplikací jen během spouštění počítače nebo v procesu přihlašování uživatele. Jinak se může stát uživateli, který používá nějakou aplikaci, že dojde k jejímu odinstalování a instalaci nové verze v době, kdy se s ní pokouší pracovat.

Některá rozšíření umožňují změnu svého výchozího chování. Možnost **Zakázat aktualizace zásad skupiny na pozadí** (Do not apply during periodic background proces-

sing) lze použít k přepsání tohoto výchozího chování a přinutit rozšíření pracovat nebo nepracovat na požadí.

Zpracovat, i když nedošlo ke změně objektů zásady skupiny

Standardně platí, když nedošlo ke změně objektů zásad skupiny na serveru, není nutné opakovaně zásady aplikovat na klienty, protože ti již potřebná nastavení obsahují. Jsou-li však uživatelé správci svých počítačů, mohou nastavení zásad změnit. V tomto případě může být rozumné opakovaně tato nastavení aplikovat během procesu přihlašování nebo během cyklu periodické aktualizace, aby se tak počítač vrátil do požadovaného stavu.

Například předpokládejme, že jste pomocí zásad skupiny definovali specifickou sadu možností zabezpečení pro určitý soubor. Pak se přihlásí uživatel (s oprávněními správy) a tato nastavení změní. Můžete nastavit zásady tak, aby se zpracovaly zásady skupiny, i když nedošlo ke změně objektů zásad skupiny – zabezpečení se tak bude opakovaně aplikovat po každém spuštění nebo přihlašování. To platí také pro aplikace. Zásady skupiny instalují aplikaci, ale cílový uživatel může aplikaci odinstalovat nebo odstranit její ikonu. Volba **Zpracovat i nezměněné objekty zásad skupiny** (Process even if the Group Policy objects have not changed) dává správci možnost vynutit obnovení aplikace při dalším přihlášení uživatele.

Porovnání samostatných funkcí správy s funkcemi správy využívajícími službu Active Directory

Tabulka 23.4 shrnuje funkce správy dostupné v systému Windows 2000 Professional ve spojení se službou Active Directory a v systému Windows 2000 Professional bez použití služby Active Directory.

Tabulka 23.4 Porovnání funkcí správy systému Windows 2000 Professional a služby Active Directory

Funkce správy	Systém Windows 2000 Professional	Systém Windows 2000 Professional se systémem Windows 2000 Server, službou Active Directory a zásadami skupiny
Šablony pro správu (nastavení v registru)	X	X
Nastavení zabezpečení	X	X
Instalace a údržba softwaru (přirazení a publikování)	–	X
Vzdálená instalace	–	X
Bezobslužná instalace	X	X
Sysprep	X	X
Skripty	X	X
Přesměrování složky	–	X
Údržba programu Internet Explorer	X	X
Profily uživatelů	X	X
Cestovní profily uživatelů	–	X

Všechny moduly snap-in zásad skupiny, které lze použít na místním počítači, lze použít také v případě, kdy se zásady skupiny zaměřují na nějaký kontejner služby Active Directory.

Následující činnosti však vyžadují systém Windows 2000 Server, infrastrukturu Active Directory a klienta se spuštěným systémem Windows 2000:

- Instalace a údržba softwaru, tedy schopnost centrálně spravovat software pro skupiny uživatelů a počítačů.
- Správa uživatelských dat a nastavení včetně přesměrování složek, což umožňuje přesměrování speciálních složek na síť.
- Vzdálená instalace operačního systému.

Další informace o možnostech změn a konfigurací najdete v kapitole „Aplikování správy změn a konfigurací“ v této knize.

Používáte-li zpočátku místní zásady skupiny, a pak učiníte počítač členem domény s implementovanou službou Active Directory a zásadami skupiny, nejprve se zpracují místní zásady skupiny a dále pak doménové zásady skupiny. Nastane-li konflikt mezi doménovými a místními zásadami skupiny, doménové zásady budou mít přednost. Jestliže však počítač následně opustí doménu, znovu se aplikují místní zásady.



Důležité rozhodnutí Jestliže před inovací serverů na systém Windows 2000 Server inovujete klienty na systém Windows 2000 Professional a předpokládáte pozdější přechod na spravované prostředí Active Directory, musíte pečlivě naplánovat strategii zásad skupiny, aby uživatelé nemohli upravit své počítače ještě před zavedením důraznějších prvků řízení. Jestliže například zavedete systém Windows 2000 Professional do nespravovaného prostředí a později chcete tyto počítače přesunout do spravované domény se službou Active Directory, bude vhodnější znovu nainstalovat operační systém a aplikace. Tak zajistíte, že nedošlo k zadání neoprávněných změn konfigurace systému.

Používání zásad skupiny na samostatných počítačích

I když vám to nedoporučujeme, mohou nastat situace, kdy budete potřebovat aplikovat zásady skupiny na samostatné počítače.

Na samostatném počítači se systémem Windows 2000 Professional jsou objekty místních zásad skupiny umístěny v adresáři \\%SystemRoot%\System32\GroupPolicy. Je-li modul snap-in zaměřen na místní počítač, můžete používat následující prvky:

- Nastavení zabezpečení. Definovat lze jen nastavení zabezpečení místního počítače, nikoli domény nebo sítě.
- Šablony pro správu, které vám umožňují nastavit více než 450 možností chování operačního systému.
- Skripty. Skripty lze použít k automatizování spouštění a vypínání počítače i k přihlašování a odhlašování uživatelů.

Dále jsou uvedeny příklady pravidel, které lze vynutit prostřednictvím místních zásad skupiny:

- Uživatelé tohoto počítače nemohou používat příkaz Spustit (Run).
- Antivirový program se spustí po každém restartování počítače.
- Společné skupiny programů v nabídce tlačítka Start se skryjí.

Abyste mohli spravovat zásady skupiny na místních počítačích, musíte mít na daných počítačích práva správce. K modulu snap-in Zásady skupiny (Group Policy) zaměřenému na místní počítače můžete přistoupit následujícím postupem:

▼ **Chcete-li přistoupit k modulům snap-in Zásady skupiny (Group Policy), postupujte takto:**

1. Z nabídky tlačítka **Start** zadejte příkaz **Spustit** (Run), zapište **MMC** a pak stiskněte tlačítko **OK**.
2. V nabídce **Konzola** (Console) okna konzoly MMC klepněte na příkaz **Přidat nebo odebrat modul snap-in** (Add/Remove Snap-in).
3. Na kartě **Samostatný** (Stand-alone) stiskněte tlačítko **Přidat** (Add).
4. V dialogovém okně **Přidat samostatný modul snap-in** (Add Snap-in) klepněte na položku **Zásady skupiny** (Group Policy) a pak stiskněte tlačítko **Přidat**.
5. Jakmile se objeví dialogové okno **Vyberte objekt zásad skupiny** (Select Group Policy Object), vyberte položku **Místní počítač** (Local Computer), která vám umožní upravovat místní objekt zásad skupiny.
6. Stiskněte tlačítko **Dokončit** (Finish).
7. Stiskněte tlačítko **Zavřít** (Close).
8. Stiskněte tlačítko **OK**. Otevře se modul snap-in Zásady skupiny (Group Policy) zaměřený na místní objekt zásad skupiny.

Tato procedura také umožňuje otevření modulu snap-in Zásady skupiny (Group Policy) na vzdáleném počítači. V kroku 5 stiskněte tlačítko **Procházet** (Browse) a pak vyberte požadovaný počítač.

Poznámka Místní zásady skupiny vám neumožňují používat filtrování zabezpečení ani více sad objektů zásad skupiny (jako je tomu v případě objektů zásad skupiny založených na Active Directory). Můžete však nastavit seznamy řízení zabezpečeného přístupu (Discretionary Access Control List – DACL) ve složce %SystemRoot%\System32\GroupPolicy tak, aby zadané skupiny byly nebo nebyly ovlivněny nastaveními obsaženými v objektu místních zásad skupiny. Tato možnost je užitečná, když potřebujete řídit a spravovat počítače používané například v prostředí kiosků, které nejsou připojeny k místní síti. Na rozdíl od zásad skupiny spravovaných z Active Directory se tu používá pouze atribut pro čtení, což umožňuje objektu místních zásad skupiny ovlivňovat normální uživatele, nikoli však místní správce. Místní správce může nejprve zadat požadovaná nastavení zásad a pak nastavit seznamy DACL na adresář objektu místních zásad skupiny, takže správci jako skupina již nebudou mít přístup ke čtení. Aby mohl správce zadat následně změny objektu místních zásad skupiny, musí nejprve převzít vlastnictví adresáře, čímž získá přístup pro čtení, zadat změny a pak znovu odstranit přístup pro čtení.

Konfigurování hardwaru

Nyní byste již měli vědět, které z kancelářských počítačů, pracovních stanic a přenosných počítačů a periferních zařízení splňují minimální požadavky systému Windows 2000.



Důležité rozhodnutí Ještě než spustíte proces inovování systémů, přesvědčte se, že váš aktuální systém základních vstupů a výstupů (basic input/output system – BIOS) podporuje systém Windows 2000 nebo že je k dispozici aktualizace systému BIOS kompatibilní se systémem Windows 2000.

Jestliže ověříte, že váš systém splňuje požadavky systému Windows 2000, většina činností konfigurování hardwaru systému Windows 2000 proběhne během instalačního procesu automaticky. Existuje však několik důležitých problémů s konfigurací hardwaru, kterými se musí váš plán konfigurace klientů zabývat. Ty jsou uvedeny dále.

Podpora systému souborů

Společnost Microsoft vám doporučuje, abyste naformátovali všechny oddíly systému Windows 2000, ke kterým nemusí přistupovat klienti s jinými operačními systémy, systémem souborů NTFS. V případě selhání systému používá systém NTFS k obnovení konzistentnosti systému souborů informace ze svého souboru protokolu a kontrolní body. Navíc systém NTFS:

- podporuje všechny funkce operačního systému Windows 2000;
- umožňuje kompresi a dekompresi souborů;
- zajišťuje větší rychlosti přístupu tím, že minimalizuje počet přístupů na disk potřebný k vyhledání souboru;
- nabízí vyšší zabezpečení souborů a složek.

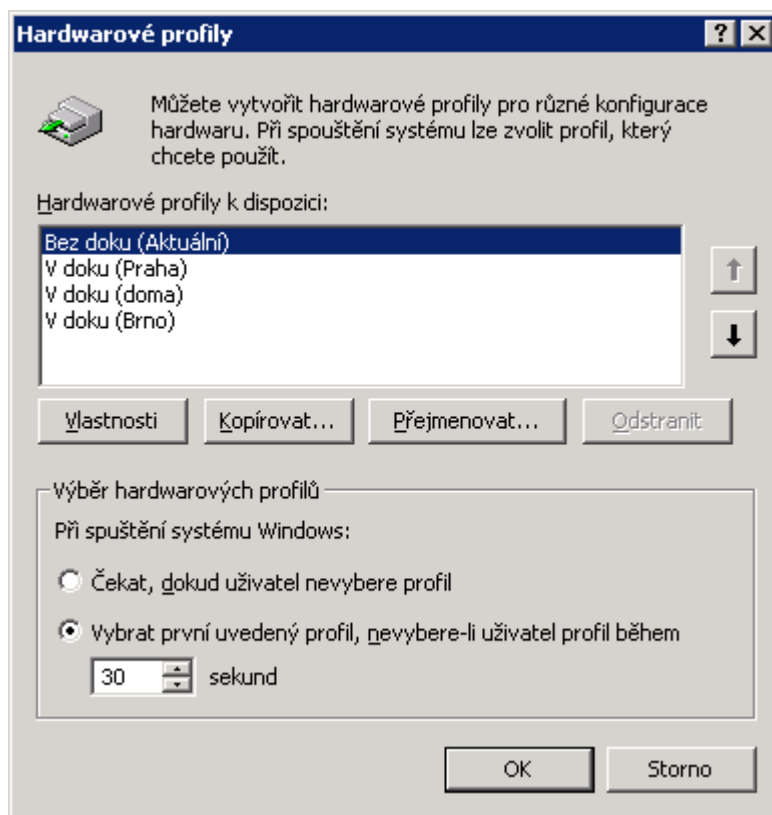
Na svazcích NTFS můžete pomocí zásad skupiny určit následující možnosti oprávnění souborů – No Access (žádný přístup), List (seznam), Read (čtení), Add (přidávání), Add and Read (přidávání a čtení), Change (změna), Full Control (plné řízení), Special Directory Access (speciální přístup k adresářům) a Special File Access (speciální přístup k souborům). Pomocí zásad skupiny můžete také zadat, kteří uživatelé a skupiny mají přístup k těmto svazkům a jakou úroveň přístupu mají.

Tyto dodatečné možnosti zabezpečení souborů umožňují organizacím nakonfigurovat přísnější kontrolu přístupu k souborům než v systémech Windows 95 a Windows NT 4.0 Workstation. Jestliže uživatelé ukládají citlivé informace na přenosný počítač, mohou tyto soubory a složky zašifrovat. Dojde-li ke zcizení přenosného počítače, šifrovaný systém souborů (Encrypting File System – EFS) Windows 2000 ochrání své soubory a složky i v případě, kdy si zloděj nainstaluje systém Windows 2000 Professional. Nezapomeňte však zajistit, aby měl správce i koncový uživatel dostatečná práva pro přístup k šifrovaným souborům a složkám.

Hardwarové profily

Jak již bylo řečeno dříve, většina činností konfigurace hardwaru je automatizována. Některé pokročilejší konfigurace jsou však zapotřebí pro starší modely přenosných počítačů, které se často používají v docích i samostatně nebo se přesunují z primárního připojení k síti do režimu offline a pak se opakovaně připojují k síti druhým, třetím nebo dokonce i čtvrtým typem síťového připojení.

Protože mnoho uživatelů mobilních počítačů není dostatečně zběhlých v rychlé konfiguraci hardwarových profilů, můžete hardwarové profily pro tato různá prostředí nakonfigurovat sami nebo proškolit uživatele v takové úpravě jejich počítačů, která jim umožní připojit se k síti. Příklad najdete na obrázku 23.2.



Obrázek 23.2 Přenosný počítač s více hardwarovými profily

Hardwarové profily nakonfigurujte pro více počítačů najednou, pouze jsou-li přenosné počítače, konfigurační možnosti a periferní zařízení naprosto identické. Je také možné nakonfigurovat některá hardwarová nastavení a koncové uživatele zároveň proškolit v konfigurování, aby mohli některé úkoly vykonávat sami.

Definování standardů uživatelského rozhraní

Jak již bylo v této kapitole uvedeno, každá organizace má jedinečné požadavky uživatelů na počítače. Systém Windows 2000 vám umožňuje vytvořit standardní operační prostředí včetně standardů uživatelského rozhraní (user interface – UI) na základě potřeb vaší organizace.

Ať už se rozhodnete používat výchozí nastavení systému Windows 2000 nebo zavedete své vlastní preference UI, doporučujeme vám vyhodnotit konfigurační možnosti systému Windows 2000 podle následujících kritérií:

- Je možné snadno se je naučit?
- Je jejich používání výhodné?
- Lze si je snadno zapamatovat?
- Pomohou odstranit některé z problémů řešených technickou podporou?
- Snižují počet chyb uživatelů?

I když jen málo organizací se musí těmito otázkami zabývat do takové hloubky, jako výrobci softwaru, například společnost Microsoft, následující techniky vám mohou pomoci s nakonfigurováním systému Windows 2000 tak, aby nejlépe naplňoval potřeby vašich uživatelů:

- Svolání skupin. Svolejte skupiny uživatelů a diskutujte s nimi o tom, co se jim líbí a nelíbí na konfiguracích jejich počítačů a jaké změny pomohou zvýšit jejich produktivitu.
- Výzkum sledováním. Sledujte uživatele při práci na počítačích.
- Externí výzkum. Promluvte si se správci v jiných organizacích a zeptejte se, jaké zkušenosti nasbírali.
- Názory expertů. Prostudujte si výzkumné zprávy o návrhu uživatelského rozhraní a zvýšení produktivity uživatelů.

Následující oddíly popisují mnoho možností UI v systému Windows 2000, které lze pomocí zásad skupiny nakonfigurovat. Konfigurační volby nenastavené správcem se stávají částí profilů uživatelů, které si mohou nakonfigurovat podle libosti. Vytvoříte-li následně zásady skupiny ovlivňující takovou konfigurační možnost, mají zásady skupiny přednost. Nastavení zásad skupiny mají vždy přednost před konfiguracemi UI zadanými uživateli, které jsou uloženy v profilech uživatelů.

Základní uživatelé

Základní uživatelé mají méně zkušeností s počítači než pokročilí uživatelé, a proto oddělení IT nakonfiguruje jejich systémy v zájmu maximalizace jejich produktivity a minimalizování možnosti škodlivých změn v jejich systému. Příkaz **Spustit** (Run) a ovládací panely jsou zakázány, aby byly implementovány pouze změny zadané správcem prostřednictvím zásad skupiny. Uživatelům jsou k dispozici pouze síťová připojení přiřazená správcem. Uživatelé také nemohou přidávat ani odstraňovat aplikace neschválené správcem.

Pokročilí uživatelé

Pokročilí uživatelé jsou obvykle zkušenější, často provozují náročné aplikace vyžadující speciální konfigurační volby nebo jsou odpojeni od sítě, a proto potřebují mít k dispozici větší možnosti správy svých systémů. Musí jim však být dostupné stejné nutné

volby a funkce přihlašování a odhlašování, jako jsou například vícejazyčné volby a možnosti usnadnění.

Řízení konfigurace pomocí zásad skupiny

Pomocí zásad skupiny lze řídit mnoho nastavení pracovní plochy a konfiguračních možností, jako:

- Úprava procesů přihlašování a odhlašování
- Úprava pracovní plochy
- Úprava mnoha součástí operačního systému

Následující oddíly popisují konfigurační možnosti v každé z uvedených kategorií. Jsou jen reprezentativními příklady a nikoli vyčerpávajícím seznamem. Uvědomte si, že je tu více než 550 různých nastavení zásad skupiny a nejlepším způsobem, jak si prohlédnout všechny různé možnosti, je prostudovat nainstalovanou verzi systému Windows 2000. Další informace o nastavení zásad skupiny najdete v kapitole „Zásady skupiny“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.

Při čtení zbývajících částí této kapitoly a následné práci s Windows 2000 i všimněte možností, které mohou být ve vaší organizaci využitelné. Jakmile budete mít seznam kompletní, můžete začít upravovat objekty zásad skupiny podle svých potřeb. Úplný seznam možností a nastavení zásad skupiny byste také měli zahrnout do svého plánu konfigurace klientů.

Úprava procesů přihlašování a odhlašování

Systém Windows 2000 poskytuje mnoho různých způsobů úpravy procesů přihlašování a odhlašování. Můžete například zadat, že se po každém přihlášení nebo odhlášení uživatele má spustit nějaký diagnostický nebo antivirový program.

Tabulka 23.5 uvádí některé z možností přihlášení a odhlášení, které pro vás mohou být užitečné.

Tabulka 23.5 Ukázka možností zásad skupiny přihlašování a odhlašování

Zásada	Popis
Spouštět starší přihlašovací skripty skrytě (Run legacy logon scripts hidden)	Systém Windows 2000 standardně postupně zobrazuje v příkazovém okně instrukce v přihlašovacích skriptech napsaných pro systém Windows NT 4.0 a dřívější (nezobrazuje přihlašovací skripty napsané pro Windows 2000). Povolení této zásady zabrání zobrazování přihlašovacích skriptů napsaných pro systém Windows NT 4.0 a dřívější.
Přidat příkaz Odhlásit uživatele do nabídky Start (Add Logoff to the Start Menu)	Přidá do nabídky Start příkaz „Odhlásit <jméno_uživatele>“ a zabrání uživatelům v jeho odstranění.
Při ukončení neukládat nastavení (Do not save settings at exit)	Zruší změny zadané na pracovní ploše uživateli během jejich poslední relace.
Při přihlášení nezobrazovat úvodní obrazovku (Do not display welcome screen at logon)	Skryje uvítací obrazovku Začínáme se systémem Windows 2000 (Getting Started with Windows 2000), která se zobrazuje v systému Windows 2000 Professional při každém přihlášení uživatele.

Omezení změn na pracovní ploše

Zásady skupiny vám mohou pomoci zabránit uživatelům v zadávání potenciálně kontraproduktivních změn na svých počítačích. Mohou vám také umožnit optimalizovat pracovní plochu pro určité úkoly vykonávané ve vaší organizaci. Tabulka 23.6 uvádí některé zásady, které můžete použít k úpravě pracovní plochy.

Poznámka Mnoho organizací si přeje vytvořit své vlastní konfigurace softwaru prohlížeče Internetu a intranetu. Další informace o úpravě a správě programu Internet Explorer 5 najdete v odkazu Microsoft Internet Explorer Administration Kit (IEAK) stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/res-kit/webresources>. Systém Windows 2000 obsahuje modul snap-in zásad skupiny umožňující konfigurovat a spravovat Internet Explorer 5. Tento modul se nazývá Údržba aplikace Internet Explorer (Internet Explorer Maintenance).

Tabulka 23.6 Ukázkové možnosti vlastní pracovní plochy

Zásada	Popis
Zabránit uživatelům změnit cestu ke složce Dokumenty (Prohibit user from changing My Documents path)	Zabrání uživatelům ve změně cesty ke složce Dokumenty (My Documents).
Zakázat Ovládací panely (Disable Control Panel)	Zakáže všechny programy ovládacích panelů.
Skrýt možnost Přidat program z disku CD-ROM nebo z diskety (Hide the Add a program from CD-ROM or floppy disk option)	Odstraní ze stránky Přidat nové programy (Add New Programs) položku Přidat program z disku CD-ROM nebo z diskety (Add a program from CD-ROM or floppy disk).
Skrýt určené panely v Ovládacích panelech (Hide specified Control Panel programs)	Skrýje určené položky a složky ovládacích panelů.
Zakázat změny systému Active Desktop (Prohibit changes to the Active Desktop)	Umožňuje vám vynutit si standardní pracovní plochu tím, že zabráníte uživateli povolit či zakázat systém Active Desktop nebo změnit jeho konfiguraci.
Tapeta systému Active Desktop (Active Desktop wallpaper)	Určuje tapetu pozadí pracovní plochy zobrazenou na pracovních plochách všech uživatelů.
Interpretace století pro rok 2000 (Century Interpretation for Year 2000) (System)	Určuje poslední rok, pro který jsou dvě číslce interpretovány jako rok ve 21. století.
Skrýt tyto jednotky v okně Tento počítač (Hide these specified drives in My Computer)	Odstraní ikony představující vybrané pevné jednotky z okna Tento počítač (My Computer), Průzkumník Windows (Windows Explorer) a okna Místa v síti (My Network Places). Písmena jednotek představující vybrané jednotky se neobjeví ani v dialogovém okně Otevřít (Open).
Název programu spořiče obrazovky (Desktop screen saver executable name)	Určuje spořič obrazovky používaný na počítači.

Zakázat příkazový řádek (Disable the command prompt)	Zabrání uživatelům ve spuštění interaktivního příkazového řádku, programu Cmd.exe. Tato zásada také určuje, zda je možné na počítači spouštět dávkové soubory (.bat, .cmd).
Zakázat nástroje pro úpravu registru (Disable registry editing tools)	Zakazuje editory registru systému Windows, programy Regedt32.exe a Regedit.exe.

Omezení změn v nabídce Start

Ve vaší organizaci může být zapotřebí řídit, jaké funkce nabídky **Start** jsou povoleny. Zásady skupiny vám umožňují zakázat možnosti, které nemají být dostupné, a vytvořit optimalizovanou nabídku **Start** odpovídající potřebám vaší organizace a jejím uživatelům. Několik příkladů najdete v tabulce 23.7.

Tabulka 23.7 Reprezentativní možnosti nabídky Start

Zásada	Popis
Zakázat a odebrat propojení na server WWW Windows Update (Disable and remove links to Windows Update)	Odstraní hypertextový odkaz na server Windows Update . Tato zásada odstraňuje hypertextový odkaz Windows Update z nabídky Start i z nabídky Nástroje (Tools) Internet Exploreru.
Odebrat příkaz Spustit z nabídky Start (Remove Run command from Start Menu)	Odstraní příkaz Spustit (Run) z nabídky Start a také odstraní příkaz Nová úloha (New Task) ze Správce úloh. Ani uživatelé s rozšířenými klávesnicemi si již nemohou zobrazit dialogové okno Spustit (Run) pomocí speciální klávesové zkratky.
Přidat příkaz Odhlásit uživatele do nabídky Start (Add Logoff to the Start Menu)	Přidá do nabídky Start příkaz „Odhlásit <jméno_uživatele>“ a zabrání uživatelům v jeho odstranění.
Zakázat přetahování místních nabídek nabídky Start myši (Disable drag-and-drop shortcut menus on the Start menu)	Zabrání uživatelům ve změně uspořádání nebo odstranění položek nabídky Start pomocí přetažení myši. Zároveň odstraňuje místní nabídky z nabídky Start .
Při určování cíle zástupců prostředí nepoužívat metody založené na sledování (Do not use the search-based method when resolving shell shortcuts)	Zabraňuje systému ve vykonávání zevrubného vyhledávání cílové jednotky při určování zástupce.
Nespouštět určené aplikace systému Windows (Do not run specified Windows-based applications)	Zabrání systému Windows ve spuštění programů zadaných touto zásadou.

Poznámka Upravená nabídka **Start**, kterou poskytnete uživatelům, může být uložena místně, nebo může být uložena na síťovém serveru.

Konfigurace možností pro vzdálené uživatele

Stále větší počet uživatelů s přenosnými počítači činí v mnoha organizacích správu těchto počítačů velmi důležitou. Strategie popsané v tabulce 23.8 mohou být užitečné pro správu dat uživatelů, kteří k síti přistupují vzdáleně.

Tabulka 23.8 Možnosti přenosných a vzdálených počítačů

Strategie	Popis
Omezte použití zásad skupiny	Zásady skupiny nelze vypnout ani na pomalých připojeních. (Dávejte si pozor na aplikování extrémně omezujících nastavení zásad skupiny nebo takových nastavení, která nahrávají na přenosné počítače nebo domácí počítače uživatelů velké množství dat. Zvažte přihlašovací skripty a výchozí čas vypršení s hodnotou 600 sekund.)
Automaticky detekujte pomalá síťová připojení	Umožňuje vám nastavit úroveň toho, co je považováno za pomalé připojení. Pak lze definovat určité aktivity náročné na šířku pásma, k nimž nesmí docházet při detekování pomalého připojení.
Určete síťové soubory a složky, které budou vždy k dispozici offline	Umožňuje vám zadat síťové soubory a složky, které jsou vždy k dispozici pro použití offline.
Zakažte možnost zpřístupnění offline	Zabrání uživatelům ve zpřístupnění určitých souborů a složek.

Přidání vícejazyčných možností

Stále více organizací vstupuje na nové trhy a po celém světě existují velké počty uživatelů hovořící mnoha různými jazyky. Vícejazyční uživatelé existují prakticky v každé střední a velké organizaci v každé zemi a regionu.

To představuje pro správce IT nové problémy, jako jsou:

- Podpora uživatelů, kteří hovoří jinými jazyky a kteří raději pracují a jejichž práce s počítačem je efektivnější v jiném jazyku, než se v kanceláři nejčastěji používá. Pro zajištění optimální produktivity je zapotřebí nakonfigurovat rozložení klávesnice, pořadí řazení, formáty data, peněžní formáty, soubory nápovědy a podobná lokalizovaná nastavení.
- Nakonfigurování operačních systémů na všechny možné kombinace jazyků situaci dále komplikuje a zvyšuje náklady na zavádění a podporu. Osoby technické podpory nemohou jednoduše řešit a opravovat problémy v prostředí s více verzemi operačního systému.
- Existuje-li v organizaci více lokalizovaných verzí operačního systému, musí se po každém zveřejnění otestovat a zavést stejný počet servisních balíčků.

Systém Windows 2000 zlepšuje podporu mezinárodního a vícejazyčného používání počítačů prostřednictvím kódování znaků systémem Unicode a rozhraní API podpory národních jazyků (National Language Support – NLS), vícejazyčnými rozhraními API a soubory prostředků systému Windows. Tato vícejazyčná technologie umožňuje systému Windows 2000 podporovat zadávání a zobrazování jazyků používaných ve více než 100 oblastech světa, bez ohledu na to, kterou ze 24 lokalizovaných verzí systému Windows 2000 používáte.

Navíc společnost Microsoft nabízí samostatnou vícejazyčnou verzi systému Windows 2000 (MultiLanguage Version), která rozšiřuje podporu rodného jazyka v systému Windows 2000 tím, že umožňuje změnu jazyka rozhraní podle jednotlivých uživatelů.

Poznámka Vícejazyčná verze systému Windows 2000 je k dispozici pouze zákazníkům s dohodami Microsoft Open License Program, Select a Enterprise. Další informace o těchto programech najdete v odkazu Licensing Programs for Enterprises stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Vícejazyčná verze umožňuje správcům:

- Minimalizovat počet instalačních balíčků systémů Windows 2000 Server a Windows 2000 Professional zavedených v síti.
- Podporovat cestující uživatele, kteří hovoří jinými jazyky, než kterými se mluví ve vzdálených kancelářích, jež navštěvují.
- Vykonávat úkoly správy v jednom jazyku a používat stejný počítač, klávesnici a monitor k vykonávání dalších úkolů v jiném jazyku bez nutnosti restartovat počítač.
- Přidávat na počítače se systémy Windows 2000 Server a Windows 2000 Professional nebo z nich odstraňovat více jazyků uživatelského rozhraní podle potřeby.

Vícejazyčná verze nemění jazyk používaný v aplikacích, mění pouze jazyk používaný v nabídkách, dialogových oknech a souborech nápovědy systému Windows 2000. Podobný vícejazyčný balíček Microsoft Office 2000 MultiLanguage Pack umožňuje organizacím zjednodušit možnosti zavádění sady Office 2000.

Úvahy o volbě vícejazyčné verze

Vícejazyčná verze systému Windows 2000 poskytuje mezinárodním a vícejazyčným uživatelům mnoho možností. Tabulka 23.9 vám pomůže vybrat jazykové možnosti vhodné pro vaši organizaci.

Tabulka 23.9 Vícejazyčné funkce a výhody podle verze

Funkce	Jednojazyčná verze	Vícejazyčná verze
Vícejazyčné funkce pro uživatele	Plně lokalizované uživatelské rozhraní zahrnuje nabídky, soubory nápovědy, dialogová okna a názvy složek. Uživatelé mohou data zadávat, zobrazovat a tisknout ve více než 60 jazycích.	Uživatelé si mohou přepnout uživatelské rozhraní na libovolný jazyk, kterému dávají přednost. Mohou také data zadávat, zobrazovat a tisknout ve více než 60 jazycích.
Vícejazyčné funkce pro profesionály IT	Ideální, není-li zapotřebí výrazně podporovat více než jednu jazykovou verzi ve vašem prostředí. Uživatelé si mohou zobrazovat a upravovat dokumenty v jiných jazycích.	Ideální, potřebujete-li zavést a podporovat více jazyků ve svém prostředí. Například k zavádění servisního balíčku je zapotřebí jen jedna jeho verze. Také ideální, potřebujete-li na jednom počítači podporovat více uživatelů hovořících různými jazyky.

Inovace na vícejazyčnou verzi systému Windows 2000

Na vícejazyčnou verzi (MultiLanguage Version) lze inovovat pouze z mezinárodních anglických verzí systému Windows. Chcete-li nahradit verzi Windows 2000 MultiLanguage Version jakékoli jiné jazykové verze systému Windows, musíte vykonat čistou instalaci vícejazyčné verze.

Při plánování inovace na vícejazyčnou verzi si musíte být vědomi dalších existujících omezení verzí. Údaje o kompatibilitě najdete v tabulce 23.10.

Tabulka 23.10 Možnosti inovace na vícejazyčnou verzi

	Windows 2000 Professional Multi- Language Version	Windows 2000 Server MultiLan- guage Version	Windows 2000 Advanced Server MultiLanguage Version
Windows 3.x	–	–	–
Windows for Workgroups	–	–	–
Windows NT 3.51 Workstation	X	–	–
Windows NT 4.0 Workstation	X	–	–
Windows 95	X	–	–
Windows 98	X	–	–
Windows 2000 Professional	X	–	–
Windows NT 3.51 Server	–	X	X
Windows NT 4.0 Server	–	X	X
Windows 2000 Server	–	X	–
Windows NT 4.0 Terminal Server	–	X	X
Windows NT 4.0 Enterprise Edition	–	–	X
Windows 2000 Advanced Server	–	–	X

Plánování instalace vícejazyčné verze systému Windows 2000

Úspěšného zavedení systému Windows 2000 MultiLanguage Version dosáhnete, když se zamyslíte nad následujícími prvky:

- Jaké soubory a jazykové skupiny vícejazyčné verze potřebujete?
- Kolik diskového prostoru tyto soubory jazyků požadují?
- Jaký instalační proces bude nejlepší?
- Jak budete tyto soubory zavádět?
- Budete instalovat z disku CD-ROM nebo se sdíleného místa na síti?

Soubory a jazykové skupiny vícejazyčné verze

Pro podporu určitého jazyka uživatelského rozhraní v systému Windows 2000 MultiLanguage Version jsou zapotřebí dvě rozdílné kolekce jazykových souborů:

- Jazykové skupiny, které obsahují všechna potřebná písmena a další soubory nezbytné ke zpracování a zobrazení konkrétní skupiny jazyků.
- Soubory vícejazyčné verze, které zajišťují jazykový obsah uživatelského rozhraní a systému nápovědy.

Ke každému instalovanému jazyku uživatelského rozhraní vyžaduje systém Windows 2000 MultiLanguage Version také instalaci odpovídající jazykové skupiny. Chcete-li například používat německé uživatelské rozhraní, musíte si nejprve nainstalovat jazykovou skupinu Západní Evropa a Spojené státy (Western Europe and United States).

Instalovat a odstraňovat jazykové skupiny Windows 2000 lze během vykonávání instalačního programu i později pomocí ovládacího panelu Místní nastavení (Regional Options). Instalace a odstranění souborů vícejazyčné verze je proces oddělený od instalace jazykových skupin.

Diskový prostor

Každá další jazyková skupina, kterou budete chtít podporovat na jednom počítači, vyžaduje dodatečný prostor na disku. Tabulka 23.11 ukazuje přibližná množství prostoru potřebná pro jednotlivé jazykové skupiny.

Tabulka 23.11 Přibližný diskový prostor požadovaný pro jazykové skupiny

Jazyková skupina	Požadovaný prostor v megabajtech (přibližně)
Arabština (Arabic)	1,6
Arménština (Armenian)	11,5
Pobaltské státy (Baltic)	1
Střední Evropa (Central European)	1,2
Cyrilice (Cyrillic)	1,2
Gruzínština (Georgian)	5,8
Řečtina (Greek)	1
Hebrejština (Hebrew)	1,4
Indie (Indic)	0,25
Japonština (Japanese)	58
Korejština (Korean)	29,4
Zjednodušená čínština (Simplified Chinese)	32,5
Thajsko (Thai)	3,9
Tradiční čínština (Traditional Chinese)	13,5
Turečtina (Turkic)	0,9
Vietnamština (Vietnamese)	0,5
Západní Evropa a Spojené státy (Western Europe and United States)	10,1

Poznámka Řada souborů (zejména písma a rozložení klávesnic) je sdílena několika jazykovými skupinami. Když tedy nainstalujete více jazykových skupin, celkový požadovaný prostor může být o něco menší, než je součet hodnot z tabulky.

Navíc ponechte až 45 MB volného diskového prostoru pro instalaci souborů vícejazyčné verze pro každý vybraný jazyk uživatelského rozhraní.

Instalace

Instalace systému Windows 2000 MultiLanguage Version se skládá ze dvou kroků:

1. Instalace systému Windows 2000
2. Instalace souborů vícejazyčné verze

Jestliže potřebné jazykové skupiny nainstalujete již při vykonávání instalačního programu systému Windows 2000, ještě než začnete instalovat odpovídající soubory vícejazyčné verze, nebudete muset během instalace vícejazyčné verze vyměňovat disky CD-ROM v mechanice.

Výchozí jazyk uživatelského rozhraní (jazyk standardně aplikovaný na všechny nové účty uživatelů vytvořené na počítači) je určen během instalace vícejazyčné verze. Výchozí jazyk uživatelského rozhraní můžete změnit a jazyky uživatelského rozhraní můžete přidávat nebo odstraňovat pomocí souboru Muisetup.exe.

Poznámka Přidávání a odstraňování jazyků pomocí souboru Muisetup.exe ovlivňuje pouze soubory vícejazyčné verze. Chcete-li přidat nebo odstranit soubory patřící jazykovým skupinám, použijte ovládací panel Místní nastavení (Regional Options).

Další informace a automatizování instalace systému Windows 2000 najdete v kapitolách „Automatizování instalace a inovace serveru“ a „Zavádění systému Windows 2000 pomocí serveru Systems Management Server“ v této knize.

Správa jazyků uživatelského rozhraní pomocí zásad skupiny

Když ve vaší organizaci použijete k omezení počtu klientských konfigurací vícejazyčnou verzi (MultiLanguage Version), výrazně se zjednoduší úkol správy klientů. Jestliže však každému uživateli umožníte měnit jazyk uživatelského rozhraní (UI) na počítači, může se celé prostředí zbytečně komplikovat. Z tohoto důvodu je vhodné omezit možnosti některých uživatelů měnit jazyk UI. Toho lze dosáhnout pomocí zásad skupiny v uzlu **Konfigurace uživatele** (User Configuration) modulu snap-in Zásady skupiny (Group Policy).

Také si uvědomte, že když aplikujete vícejazyčné zásady na místní počítač prostřednictvím zásad skupiny, místní objekt zásad skupiny ovlivní všechny uživatele na daném počítači, protože místní objekty zásad skupiny nelze filtrovat podle jednotlivých uživatelů.

Další informace o systému Windows 2000 MultiLanguage Version najdete v odkazu Windows 2000 Professional Multilanguage Support stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Zajištění větší přístupnosti systémů

Uživatelské rozhraní počítače je nejdůležitější pro osoby se speciálními potřebami. Jedním z cílů vašeho plánování musí být zajištění rovnocenného přístupu k počítačovému softwaru pro všechny uživatele, včetně osob s postiženími zraku, sluchu, pohyblivosti či rozpoznávání.

Nezahrnujte všechny uživatele s vadami rozpoznávání do jediné kategorie; jejich potřeby se liší přinejmenším stejně, ne-li ještě více, jako potřeby jiných typů uživatelů. Zvažte různorodost otázek uživatelského rozhraní, kterým čelí lidé s těmito postiženími:

- **Zrak.** Zahrnuje slepotu, omezené vidění a barvoslepost.
- **Sluch.** Zahrnuje hluchotu nebo částečnou ztrátu sluchu.
- **Pohyblivost.** Zahrnuje ochrnutí páteře, třas, záchvaty epilepsie, ztrátu údů nebo prstů a paralýzu. Za osoby s postiženou pohyblivostí lze považovat také osoby se zánětem šlach v prstech a dalšími nemocemi způsobenými opakovaným namáháním.
- **Rozpoznávání.** Sem patří omezení možnosti učení, jako je dyslexie a ztráta paměti, Downův syndrom a jazyková postižení, jako je negramotnost a neznalost jazyka.

Konfigurování funkcí usnadnění systému Windows 2000

Podle specifických potřeb jednotlivých osob mohou mít různí uživatelé problémy s odlišnými aspekty systému Windows 2000. Tabulka 23.12 popisuje několik obecných úvah o konfigurování systému Windows 2000 i specifické nové a inovované funkce zpřístupnění v systému Windows 2000.

Tabulka 23.12 Funkce usnadnění v systému Windows 2000

Funkce	Definice
Správce nástrojů (Utility Manager)	Správce nástrojů zlepšuje přístup k aplikacím usnadnění na počítači a zjednodušuje proces konfigurování těchto voleb.
Průvodce funkcemi usnadnění (Accessibility Wizard)	Průvodce funkcemi usnadnění usnadňuje zadání obvykle používaných funkcí usnadnění přímým určením typu postižení a nikoli zadáváním různých číselných hodnot.
Klávesnice na obrazovce (On-Screen Keyboard)	Klávesnice na obrazovce umožňuje omezený přístup uživatelům s postižením pohyblivosti.
Narrator (se zabudovanou funkcí převodu textu na řeč)	Narrator je syntetizovaný nástroj převodu anglického textu do řeči s omezenými funkcemi sloužící uživatelům s lehčími vadami zraku. Narrator čte nahlas text zobrazený na monitoru.
Lupa (Magnifier)	Lupa je základní nástroj zvětšování obrazovky, který v samostatném okně ukazuje část zobrazení.
Lépe viditelné ukazatele myši	Nové velké, největší, bílé a černé ukazatele myši. Invertované ukazatele navíc mění svou barvu na barvu kontrastní k pozadí.
Barevná schémata s vysokým kontrastem	Rozšířená knihovna barevných schémat může pomoci uživatelům se špatným zrakem, kteří potřebují větší stupeň kontrastu mezi popředím a pozadím.
Systémová oblast hlavního panelu	Stavové ikony funkcí usnadnění v systémové oblasti hlavního panelu ukazují uživateli, zda jsou určité často používané filtry klávesnice aktivní.
Standard Synchronized Accessible Media Interchange (SAMI)	Umožňuje používat textování multimediálních produktů.

Použití zařízení jiných výrobců

I když nástroje usnadnění v systému Windows 2000 zajišťují řadu funkcí pro uživatele se speciálními potřebami, většina postižených uživatelů potřebuje každodenně další nástroje. Novinkou v systému Windows 2000 je rozhraní API nazvané Microsoft Active Accessibility (MSAA), které umožňuje pomůckám usnadnění spolupracovat s prvky uživatelského rozhraní, jako jsou panely nástrojů, nabídky, text a grafika.

Příklady doplňkového hardwaru jsou menší nebo větší klávesnice, zařízení sledující pohyb očí a systémy řízené dechem. Další je kategorie komunikačních zařízení, která byla původně vyvinuta k řízení řečového syntezátoru pro osoby, jež nemohou mluvit.

Vaši uživatelé mohou být s těmito výrobky seznámeni a mohou vám říci, které by rádi měli na svých počítačích. Další informace o hardwaru a softwaru pro osoby s posti-

ženími najdete v odkazu Microsoft Accessibility stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Vyladění konfigurace usnadnění pomocí zásad skupiny

Pro postižené uživatele může být užitečná řada konfiguračních možností, které jsou přístupné pomocí zásad skupiny. Konfigurační možnosti uživatelského rozhraní konzultujte s někým, kdo zná potřeby postižených lidí (takové zkušenosti má obvykle někdo z oddělení lidských zdrojů), a počítače nakonfigurujte pro postižené lidi.

Také při plánování pokročilé správy změn a konfigurace (viz kapitola „Aplikování správy změn a konfigurací“ v této knize) se zamyslete nad hodnotou, jakou mají tyto funkce pro postižené osoby, které třeba najednou nemusí pracovat už jen na jediném počítači, který byl nakonfigurován přesně podle jejich potřeb.

Seznam úkolů plánování klientských standardů

Tabulka 23.13 shrnuje úkoly, které musíte vykonat při přípravě standardů správy a konfigurace klientů pro systém Windows 2000.

Tabulka 23.13 Seznam úkolů plánování klientských konfigurací

Úkol	Umístění v kapitole
Definujte strategii správy klientů.	Definování modelu správy a standardů
Definujte požadavky klientů na aplikace podle jejich práce.	Definování softwarových standardů
Definujte omezení konfigurace klientů podle jejich práce.	Definování typů uživatelů
Konfigurujte hardware klientů (přenosných a kancelářských počítačů) schválený ke spouštění systému Windows 2000.	Konfigurování hardwaru
Konfigurujte základní možnosti	Umožnění správy klientských systémů uživatelského rozhraní systému Windows 2000.
Zadejte možnosti přihlášení a odhlášení.	Řízení konfigurace pomocí zásad skupiny
Zadejte možnosti nabídky Start.	Řízení konfigurace pomocí zásad skupiny
Zadejte možnosti pracovní plochy.	Řízení konfigurace pomocí zásad skupiny
Zadejte vícejazyčné možnosti.	Přidání vícejazyčných možností
Zadejte možnosti usnadnění	Zajištění větší přístupnosti systémů
Konfigurujte aplikace podle požadavků klientů a instrukcí správy.	Definování softwarových standardů
Použijte nutné aplikace.	Definování softwarových standardů
Použijte volitelné aplikace.	Definování softwarových standardů

KAPITOLA 24

Aplikování správy změn a konfigurací

Konfigurace klientských počítačů a způsoby používání přenosných i kancelářských počítačů jsou stále komplikovanější. Složitější jsou také řešení a služby, které musí oddělení informačních technologií (IT) poskytovat uživatelům. Systém Microsoft Windows 2000 nabízí řadu pokročilých funkcí správy změn a konfigurací, které vám umožňují zpřístupnit nastavení, dokumenty a software uživatelům, i když jsou na jiném počítači. Navíc tyto funkce podporující adresářovou službu Active Directory umožňují poskytnout uživateli prakticky totožnou náhradu v případě selhání pevného disku nebo jiné součásti počítače.

V této kapitole jsou načrtnuty kroky plánování potřebné k implementování funkcí pokročilé správy klientů systému Windows 2000, které se obecně označují za funkce IntelliMirror. Také se dozvíte, jak můžete do svého plánu podpory klientů zahrnout vzdálenou instalaci operačního systému. Ještě než začnete číst tuto kapitolu, pochopte a dokončete kroky plánování určené v kapitolách „Definování standardů správy a konfigurace klientů“ a „Návrh struktury služby Active Directory“.

V této kapitole

Vyhodnocení správy změn a konfigurací 708

Umožnění funkce vzdálené instalace 714

Zlepšení správy softwaru pomocí zásad skupiny 720

Převedení uživatelských dat a nastavení na síť 731

Výběr možností správy změn a konfigurací vaší organizace 737

Seznam úkolů plánování správy změn a konfigurací 743

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujících dokumentů plánování:

- Plán implementace funkcí IntelliMirror
- Plán implementace vzdálené instalace operačního systému

Související informace v sadě Resource Kit

- Další informace o základních možnostech konfigurace klientů a správě klientů systému Windows 2000 pomocí zásad skupiny najdete v kapitole „Definování standardů správy a konfigurace klientů“ v této knize.

- Další informace o použití serveru Systems Management Server najdete v kapitole „Zavádění systému Windows 2000 pomocí serveru Systems Management Server“ v této knize.
- Další informace o testování a pilotních programech technologií systému Windows 2000 najdete v kapitolách „Vytvoření testovací laboratoře systému Windows 2000“ a „Vykonání pilotního programu systému Windows 2000“ v této knize.

Vyhodnocení správy změn a konfigurací

Když mají uživatelé nějaké problémy se svými počítači – jako je software, který nefunguje, chybějící soubory nebo chybná funkce hardwaru – technik z oddělení IT musí často osobně jít k danému počítači a diagnostikovat a vyřešit problém. Když se to znásobí stovkami a tisíci klientských počítačů a navíc se přidá vzrůstající počet počítačů, které jsou často odpojeny od sítě, a počítače využívané více uživateli, jedná se o nejnákladnější problémy podpory, kterým správci sítí čelí.

Systém Windows 2000 poskytuje různé technologie správy změn a konfigurací, které mohou oddělení IT pomoci omezit množství práce a náklady spojené se správou a podporou klientských počítačů. Jestliže jako základ použijete standardy správy a konfigurace vytvořené v kapitole „Definování standardů správy a konfigurace klientů“, můžete omezit množství práce a času potřebného k výměně počítačů povolením následujících uživatelských služeb podporujících Active Directory:

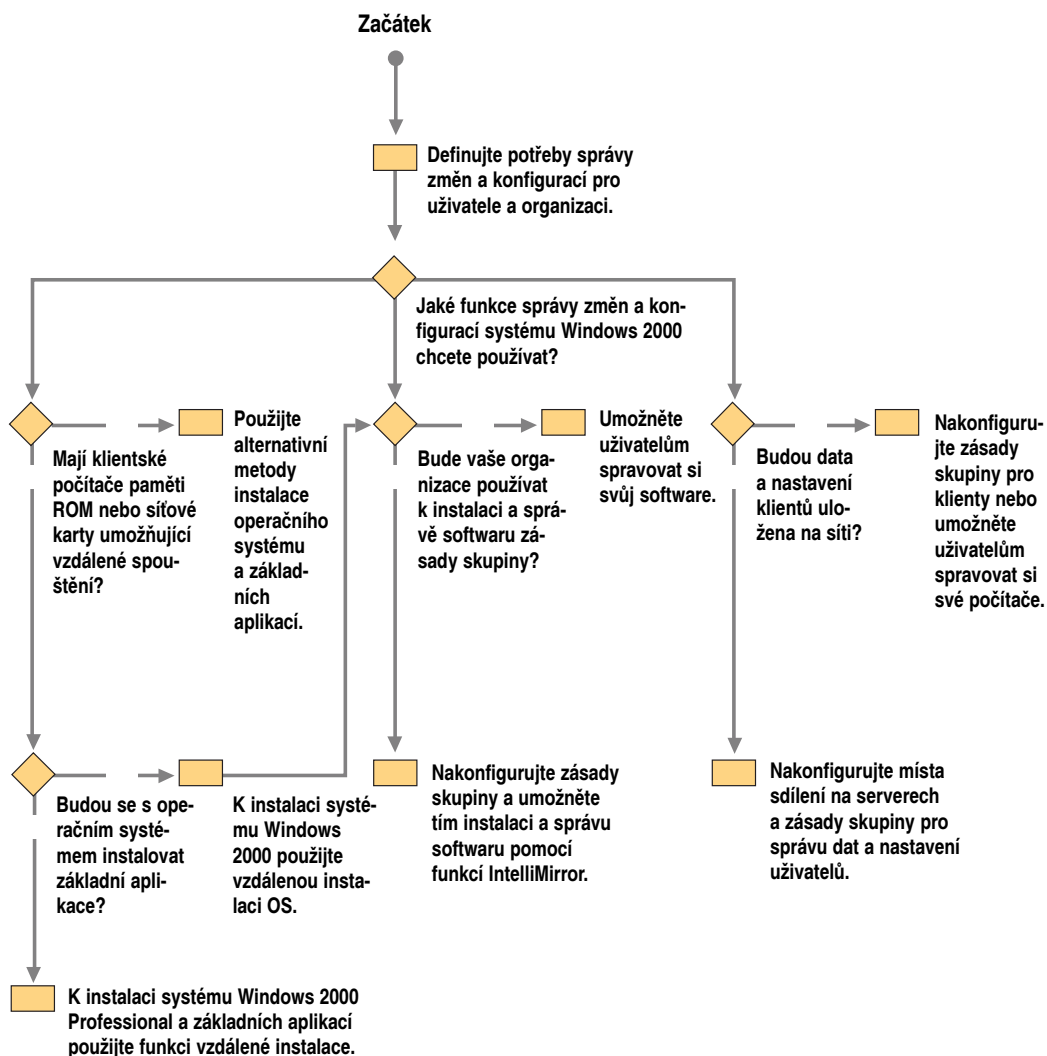
Vzdálená instalace operačního systému Umožňuje správcům zjednodušit a snížit náklady na konfigurování a uvádění do provozu nových či náhradních klientských počítačů. Navíc vzdálená instalace operačního systému zlepšuje schopnost oddělení IT rychle obnovit systém, na kterém selhaly jak předem nakonfigurovaný operační systém tak i základní aplikace.

Instalace a údržba softwaru Umožňuje správcům určit sadu aplikací, které budou uživateli nebo skupině uživatelů vždy dostupné. Není-li požadovaná aplikace ještě instalovaná na počítači v okamžiku, kdy je zapotřebí, automaticky se nainstaluje. Podobně potřebuje-li aplikace opravit (například kvůli chybnému nebo náhodně odstraněnému souboru), inovovat nebo odstranit, lze to také zařídit automaticky.

Správa nastavení uživatelů Zatímco kapitola „Definování standardů správy a konfigurace klientů“ ilustrovala, jak můžete upravit a řídit uživatelské rozhraní, v této kapitole se dozvíte, jak implementovat cestovní profily uživatelů. Pomocí cestovních profilů uživatelů se uživatelská nastavení (i další nastavení zásad skupiny platící pro daného uživatele) zkopírují na jakýkoli počítač v síti, ke kterému se uživatel přihlásí.

Správa dat uživatelů Umožňuje uživatelům přesunout se na libovolný počítač se systémem Windows 2000 Professional na síti a stále mít přístup ke svým datům. Navíc převede-li uživatel síťové prostředky do režimu offline, po opakovaném připojení uživatele k síti se tyto prostředky synchronizují.

Poslední tři možnosti jsou seskupeny pod názvem IntelliMirror. Funkce IntelliMirror společně s funkcí vzdálené instalace vytvářejí správu změn a konfigurací systému Windows 2000, která může výrazně omezit množství práce a času potřebného k výměně počítačů. Obrázek 24.1 ukazuje proces plánování těchto funkcí.



Obrázek 24.1 kroky plánování funkce IntelliMirror a vzdálené instalace OS

Technologie používané k umožnění správy změn a konfigurací

Funkce IntelliMirror a vzdálená instalace nejsou naprosto nezávislé technologie v systému Windows 2000. Tyto možnosti využívají mnoha jiných technologií systému Windows 2000, které už pravděpodobně zavádíte. Tabulka 24.1 uvádí technologie potřebné k implementování funkcí IntelliMirror a vzdálené instalace.

Tabulka 24.1 Technologie používané k umožnění funkcí IntelliMirror a vzdálené instalace

Funkce	Používaná technologie
Správa uživatelských nastavení	Active Directory Zásady skupiny Složky offline Cestovní profily uživatelů
Správa uživatelských dat	Active Directory Zásady skupiny Složky offline Správce synchronizace Diskové kvóty Cestovní profily uživatelů
Instalace a údržba softwaru	Active Directory Zásady skupiny Služba Windows Installer Přidat nebo odebrat programy Distribuovaný systém souborů (DFS)
Služby vzdálené instalace	Active Directory Zásady skupiny Služby vzdálené instalace (RIS) Pracovní stanice podporující vzdálenou instalaci

Vzdálenou instalaci operačního systému a správu dat uživatele, správu nastavení uživatele a instalaci a údržbu softwaru pomocí funkcí IntelliMirror můžete aplikovat individuálně nebo v libovolné kombinaci dvou či tří prvků. Jestliže implementujete všechny čtyři funkce, vytvoříte integrované řešení správy změn a konfigurací zaručující rychlou a téměř přesnou automatizovanou náhradu počítače v případě selhání vybavení.

Poznámka Náhrada je popsána jako „téměř přesná“, protože někteří uživatelé si mohou ukládat data na nevhodná místa, což zabrání replikaci takových souborů na serveru. Navíc je obtížné spravovat extrémně velké soubory, jako jsou některé soubory poštovních schránek nebo databází, což může být zapříčiněno šířkou přenosového pásma sítě, diskovým prostorem serveru a synchronizačním časem vyžadovaným k udržování aktuálních kopií jak na serveru tak i na klientském počítači.

Identifikování potřeb a příležitostí správy změn a konfigurací

Funkce správy změn a konfigurací systému Windows 2000 vám pomohou vyřešit mnoho otázek správy. V následujícím výčtu jsou uvedeny typické situace, kdy organizace používají funkce IntelliMirror a vzdálené instalace.

- Konfigurování počítače k novému pronájmu
- Instalování a správa softwaru
- Zálohování podnikových dat
- Zotavení po selhání počítače

Tyto problémy se mohou týkat všech pokročilých i základních typů uživatelů (mobilních, cestujících, vzdálených, s konkrétními úkoly i se speciálními znalostmi), které by-

ly popsány v kapitole „Definování standardů správy a konfigurace klientů“. Jako základ plánu implementace funkcí IntelliMirror a vzdálené instalace použijte plány preferované konfigurace klientů a správy klientů. Plány implementace funkcí IntelliMirror a vzdálené instalace rozšíří výše uvedené plány a pomohou vám naplnit potřeby správy a klientů, které jste určili dříve v plánování zavedení systému Windows 2000.

Základní potřebné informace

Při plánování funkcí IntelliMirror a vzdálené instalace jsou velmi důležité zejména následující informace:

- Jak rychle bude vaše organizace migrovat na systémy Windows 2000 Professional a Windows 2000 Server?

Funkce IntelliMirror a vzdálené instalace jsou dostupné pouze klientům se systémy Windows 2000 Professional běžícími v infrastruktuře systému Windows 2000 Server se službou Active Directory.

Poznámka Klienti terminálových služeb systému Windows 2000 mohou také využívat funkce IntelliMirror a vzdálené instalace. Plní klienti terminálových služeb se nemohou účastnit instalování a údržby softwaru, protože potřebné aplikace musí být instalovány na klientovi terminálových služeb. Klienti terminálových služeb (Terminal Services) pracující v režimu správy mohou používat funkce instalace a údržby softwaru. Další informace o terminálových službách najdete v kapitole „Zavádění terminálových služeb“ v této knize.

- Splňují existující klientské počítače požadavky vzdálené instalace na paměť ROM a prostředí vzdáleného spouštění (PXE)?

Funkce IntelliMirror nevyžadují rychlejší procesory nebo více paměti, než je zapotřebí k provozování systémů Windows 2000 Server a Windows 2000 Professional. Chcete-li však používat vzdálenou instalaci, klienti musí mít podporovanou síťovou kartu nebo paměť ROM vzdáleného spouštění verze .99b nebo novější.

- Jaké jsou potřeby vašich uživatelů? Přesunují se mezi různými místy? Používají více počítačů? Jsou často odpojeni od sítě? Mají stabilní nebo neustále měněné požadavky na aplikace?

Vaším cílem by mělo být zajistit přesně ty funkce správy, které uživatelé potřebují, a nezavádět jich ani více ani méně. Další informace o sladění funkcí IntelliMirror a vzdálené instalace s potřebami uživatelů najdete v oddílu „Výběr možností správy změn a konfigurací vaší organizace“ dále v této kapitole.

- Jak rychlá jsou síťová propojení ve vaší organizaci? Jsou uživatelé často připojeni přes pomalá připojení? Máte dostatečnou kapacitu sítě, abyste mohli podporovat takové funkce, jako je automatizovaná instalace a inovace softwaru?

Své plány funkcí IntelliMirror a vzdálené instalace budete muset otestovat a prověřit v pilotních programech ve všech předpokládaných vzorech používání – jen tak určíte, kolik serverů a jaká kapacita sítě bude zapotřebí k implementování vašich plánů změn a konfigurací.

- Jak chcete spravovat účty počítačů? Vytvoří si uživatelé, kteří si instalují systém Windows 2000 Professional, své vlastní účty počítačů a upraví si svá nastavení operačního systému? Nebo nějaký pracovník oddělení IT nastaví počítače předběžným definováním těchto účtů a nastavení?

Funkce vzdálené instalace podporuje prostřednictvím kombinace nastavení zásad skupiny a zabezpečení jak alternativy správy uživatelem tak i správy oddělením IT.

- Jsou klientské počítače spravovány přísně nebo volně? Jaké jsou vaše nejnákladnější problémy správy klientů? Lze tyto problémy vyřešit nebo omezit pomocí technologií správy změn a konfigurací? Jak často inovujete existující aplikace nebo distribuujete nové aplikace?

Jestliže jste ještě nezískali data související s těmito otázkami, přečtěte si kapitolu „Definování standardů správy a konfigurace klientů“.

- Byla ve vaší organizaci zavedena služba Active Directory a struktura domén? Jaké jsou důvody související se správou a logické důvody zavedení služby Active Directory a struktury domén ve vaší organizaci? Používají se ve vaší organizaci také služby Dynamic Host Configuration Protocol (DHCP) a Domain Name Server (DNS)?

Další informace o dokončení těchto částí vaší infrastruktury IT najdete v kapitole „Návrh struktury služby Active Directory“, kde najdete důležité informace plánování, které vám pomohou vytvořit solidní základy pro plány správy změn a konfigurací.

Doplnění funkcí IntelliMirror pomocí serveru Systems Management Server

Mnoho organizací se složitými prostředímí doplní funkce IntelliMirror a vzdálené instalace nástroji pokročilé správy změn a konfigurací poskytovanými programem Systems Management Server 2.0. Tyto nástroje zahrnují:

Nástroje plánování Program Systems Management Server používá k získávání a nahrávání podrobných inventárních informací o softwaru a hardwaru (jako je měření používání aplikací) do skladiště systému Microsoft SQL Server technologií Windows Management Instrumentation (WMI) a skenery softwaru. Tato sada nástrojů plánování vám může pomoci pochopit konfiguraci vašeho prostředí, dokončit audit a kontroly kompatibility, sledovat a omezovat použití aplikací a plánovat takové operace, jako jsou zavádění nového softwaru a inovace.

Nástroje zavedení Pomocí serveru Systems Management Server můžete časově naplánovat a synchronizovat zavádění softwaru na počítače se systémem Windows, kam patří také systémy Windows 3.x, Windows NT 3.51/4.0 a Windows 2000. Taková distribuce je plně integrována s inventářem a umožňuje tak přesné zacílení a zároveň vytváření podrobných sestav stavu postupu a úspěchu každého naplánovaného zavedení. Pomocí serveru Systems Management Server můžete distribuovat a instalovat software na pozadí na jeden, deset nebo i tisíc počítačů, i když k nim nejsou přihlášení žádní uživatelé. Server Systems Management Server může také zavádět software používající novou technologii a balíčky nástroje Windows Installer.

Diagnostické nástroje Server Systems Management Server nabízí řadu pokročilých nástrojů vzdálené diagnostiky, které vám pomohou spravovat kancelářské počítače a servery, aniž byste k nim museli chodit. Sem patří nástroje, jako je vzdálené řízení a vzdálené restartování, sledování sítě s funkcemi pracujícími v reálném čase i později vyhodnocujícími zachycená data, které analyzují podmínky a výkon sítě, a serverový nástroj HealthMon, který zobrazuje důležité informace o výkonu v systémech Windows 2000 Server a Microsoft BackOffice.

To, zda budete používat funkce IntelliMirror a program Systems Management Server odděleně nebo dohromady, závisí na složitosti vašeho prostředí. Tabulka 24.2 ukazuje

řešení správy společnosti Microsoft, která mohou být pro organizace různých složitostí z hlediska nákladů nejvýhodnější.

Tabulka 24.2 Doporučení řešení správy změn a konfigurací

	Jednoduchá místní síť (LAN)/ jednoduchá síť více LAN s rychlými propojeními	Složitá síť více LAN/systémy více síťových sídel
Pouze systémy založené na Windows 2000	IntelliMirror Vzdálená instalace	IntelliMirror Vzdálená instalace Systems Management Server
Kombinovaná prostředí Windows včetně systémů založených na Windows 2000	IntelliMirror Vzdálená instalace Systems Management Server	IntelliMirror Vzdálená instalace Systems Management Server
Windows 3.x, Windows NT 3.51/4.0	Systems Management Server	Systems Management Server

Tabulka 24.3 ukazuje, jak lze funkce IntelliMirror a vzdálené instalace a server Systems Management Server zkombinovat do efektivního řešení správy změn a konfigurace.

Tabulka 24.3 Možnosti efektivní správy změn a konfigurací

	Vzdálená instalace OS	IntelliMirror	Systems Management Server
Instalace obrazů počítačů se systémem Windows 2000.	X	–	–
Umožnění, aby data, software a nastavení následovaly uživatele.	–	X	–
Základní zotavení po havárii pro systémy založené na Windows 2000	X	X	–
Správa prostředí, která nevy- cházejí ze systému Windows 2000.	–	–	X
Inventář, pokročilé zavádění, řešení problémů a diagnos- tické nástroje	–	–	X
Zevrubná správa změn a konfigurací	X	X	X

Informace v uvedených tabulkách použijte společně s porozuměním problémů správy klientů ve vaší organizaci k výběru nejvhodnějších funkcí pro vaši organizaci.

Další informace o použití serveru Systems Management Server ve spojení se systémem Windows 2000 najdete v kapitolách „Analýza infrastruktury sítě pomocí serveru Systems Management Server“ a „Zavádění systému Windows 2000 pomocí serveru Systems Management Server“ v této knize. Podrobné technické informace o serveru Systems Management Server najdete v knize *Microsoft Systems Management Server Resource Kit*.

Plánování vylepšené podpory klientů pomocí funkcí IntelliMirror

Zbytek této kapitoly vás provede kroky zlepšení podpory klientů nakonfigurováním a vyřešením kritických problémů v zavádění funkcí IntelliMirror a vzdálené instalace.

Jestliže vaše standardy správy klientů zahrnují ukládání uživatelských dat a nastavení na síťový server, budete muset v zájmu naplnění tohoto cíle vytvořit ještě před začátkem zavádění klientů základní obraz (bitovou kopii) klienta a infrastruktury sítě (konkrétně sdílená místa na serveru a nastavení zásad skupiny).

Volba metod zavádění klientů má dvě části:

- Zavádění základního operačního systému
- Zavádění aplikací

Stejně jako u alternativních metod zavádění, jakými jsou použití nástroje Sysprep nebo serveru Systems Management Server, můžete k zavádění základních aplikací spolu se systémem Windows 2000 Professional použít vzdálenou instalaci. To znamená, že musíte svou strategii zavádění aplikací pečlivě naplánovat, a určit:

- které aplikace budou zavedeny s operačním systémem pomocí funkce vzdálené instalace OS;
- které aplikace budou zavedeny pomocí funkce instalace a správy softwaru po instalaci operačního systému;
- jak budete podporovat opakovanou instalaci nebo opravu aplikací, které byly původně instalovány pomocí funkce vzdálené instalace.

Instalování základní sady aplikací již v procesu vzdálené instalace OS může zjednodušit proces konfigurace počítače podle standardů vaší organizace. Tím se však neeliminuje potřeba podporovat instalaci na počítače, na kterých je již instalován systém Windows 2000 Professional. Proto aplikace, které nejsou instalovány zároveň se systémem Windows 2000 v procesu vzdálené instalace OS, budou také muset být zahrnuty ve vašem plánu instalace a údržby softwaru pomocí funkcí IntelliMirror.

Následující oddíly se zabývají klíčovými problémy plánování a pomohou vám použít funkci vzdálené instalace, instalaci a údržbu softwaru pomocí funkcí IntelliMirror a správu uživatelských dat a nastavení pomocí funkcí IntelliMirror ve vaší organizaci. Poslední oddíl nazvaný „Souhrn“ uvádí doporučení, jak mohou některé organizace s různými typy požadavků implementovat funkce IntelliMirror a vzdálené instalace.

Umožnění funkce vzdálené instalace

Funkce vzdálené instalace OS systému Windows 2000 poskytuje počítačům prostředky pro připojení k síťovému serveru Windows 2000 během počáteční sekvence spouštění a následně umožňuje serveru nainstalovat na klientský počítač systém Windows 2000 Professional. Funkce vzdálené instalace vám jako správci dovoluje nakonfigurovat systém Windows 2000 a všechny aplikace, které chcete instalovat společně s operačním systémem, jen jednou pro skupinu uživatelů a pak tuto konfiguraci aplikovat při instalování operačního systému na jednotlivé klientské počítače. Z hlediska uživatelů bude výsledkem zjednodušená a časově méně náročná instalace a konfigurace jejich počítačů a rychlejší návrat k práci v případě selhání hardwaru.

Tabulka 24.4 ukazuje technologie Windows 2000 potřebné k tomu, abyste mohli používat funkci vzdálené instalace OS.

**Tabulka 24.4 Technologie systému Windows 2000
potřebné k používání funkce vzdálené instalace**

Technologie	Účel
Protokol Dynamic Host Configuration Protocol (DHCP)	Ještě před kontaktováním serveru se spuštěnou službou RIS přiřazuje adresu IP klientovi, kterého lze vzdáleně spouštět.
Systém Domain Name Server (DNS)	Překládá názvy počítačů z adres TCP/IP.
Zásady skupiny (Group Policy)	Definuje uživatele a počítače, na kterých bude možno (nebo naopak nebude možno) přijímat zadanou konfiguraci.
Adresářová služba Active Directory	Vyhledává klientské počítače a servery RIS a ukládá objekty zásad skupiny definující, k jakým prostředkům uživatel nebo počítač může či nemůže přistupovat.
Služby vzdálené instalace (Remote Installation Services – RIS)	Spravují a distribuují soubory obrazů (bitových kopií) systému Windows 2000 Professional na klienty s možností vzdáleného spouštění.

Jestliže jste ještě nenainstalovali a nenakonfigurovali součásti DNS, DHCP a Active Directory, přečtěte si kapitolu „Definování struktury služby Active Directory“ v této knize, která vám pomůže s dokončením kroků plánování jejich zavedení. Pak můžete pokračovat ve čtení této kapitoly. Také byste měli rozumět krokům plánování zásad skupiny načrtnutým v kapitole „Definování standardů správy a konfigurace klientů“. Zbývající část tohoto oddílu se zaměří na plánování související s různými součástmi služby RIS a na to, jak je nakonfigurovat pro efektivní zavádění.

Definování požadavků uživatelů

Všichni uživatelé, bez ohledu na jejich úroveň nebo požadavky práce s počítačem, potřebují výkonnou a rychlou možnost instalace nového operačního systému a základních aplikací v případě selhání jejich systému nebo obdržení nového počítače. Abyste snížili čas a náklady související s předběžnou konfigurací nových systémů pro uživatele, musíte zodpovědět následující otázky:

Jaká je nejlepší metoda instalace operačního systému pro tyto uživatele?

V malých pobočkách nebo v domácích kancelářích, kde není dostatek uživatelů ospravedlňující instalaci serveru RIS nebo kde uživatelé cestují a nemají širokopásmové připojení k síťovému serveru, bude asi nejlepší použít disk CD-ROM nebo jinou metodu místní instalace operačního systému. V případě uživatelů, kteří sice mají širokopásmové síťové připojení, ale jejichž počítače nemají síťovou kartu nebo paměť ROM odpovídající standardu vzdáleného spouštění, bude další vhodnou možností zkopírování obrazu (bitové kopie) uloženého na síti nebo ruční instalace (další informace najdete v kapitole „Automatizování instalace a inovace klientů“ v této knize). Chcete-li zajistit ve všech ostatních případech čistou a známou konfiguraci systému Windows 2000 Professional, použijte funkci vzdálené instalace.

Jakou volnost mají mít uživatelé při výběru volitelných součástí operačního systému nebo alternativních obrazů operačního systému?

Následující oddíly popisují řadu volitelných nastavení, která můžete použít ke konfiguraci obrazů (bitových kopií) vzdálené instalace. Ve většině případů budete muset uživatelům s menšími znalostmi nebo orientovanými na konkrétní úkoly během instalace operačního systému nabídnout jen málo volitelných možností nebo dokonce nenabízet žádné možnosti. Pokročilejší uživatelé s rozsáhlejšími znalostmi mohou během instalace systému Windows 2000 Professional požadovat další volby.

Použití funkce vzdálené instalace

Proces vzdálené instalace OS je z hlediska koncových uživatelů poměrně přímočarý, protože většinu práce vykoná vaše oddělení IT zavedením následujících konfigurací:

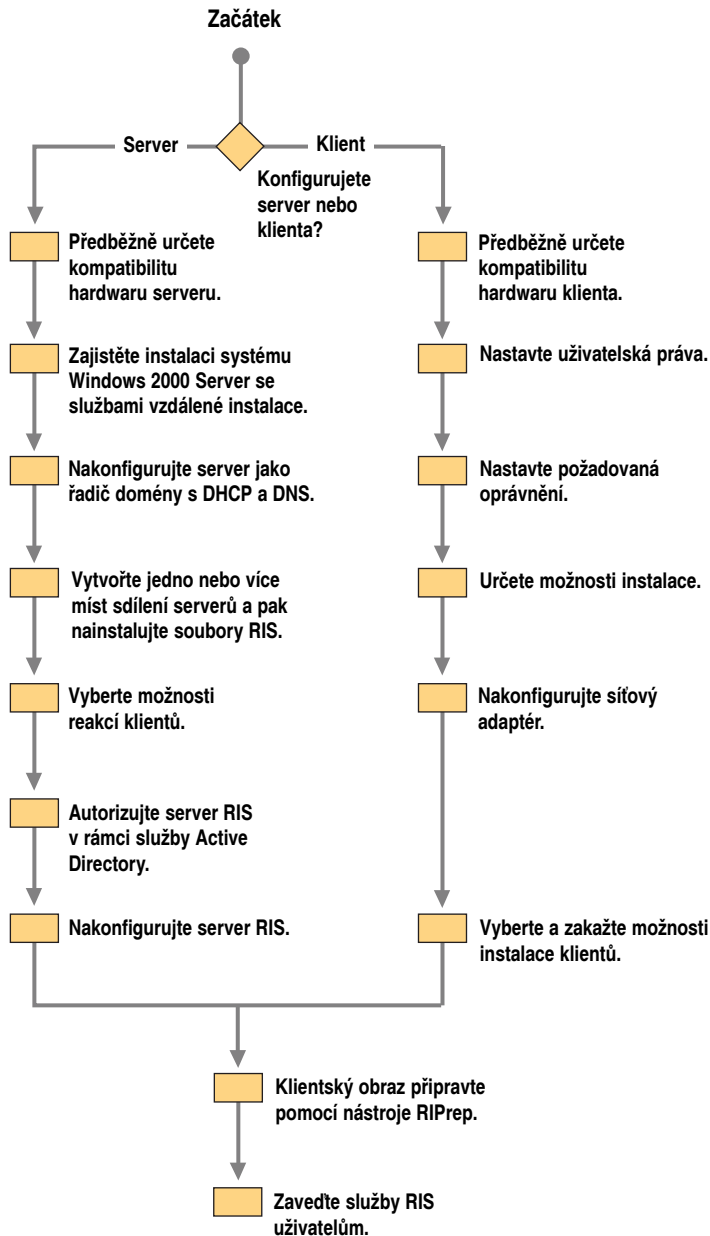
- Definování konfigurace operačního systému pro jednotlivé skupiny uživatelů.
- Omezení uživatelů na co nejmenší potřebný počet konfigurací operačního systému.
- Provádění uživatele úspěšnou instalací operačního systému předběžným určením instalačních voleb, které bude moci uživatel změnit (pokud vůbec nějaké).

Se vzdálenou instalací OS souvisí pět hlavních komponent služby RIS:

- **Průvodce instalací služeb vzdálené instalace (RISetup.exe).** Používá se k nastavení serveru služby RIS.
- **Správce služeb vzdálené instalace.** Používá se ke konfigurování nastavení zásad skupiny souvisejících se službami RIS.
- **Průvodce přípravou vzdálené instalace (RIPrep.exe).** Používá se k vytvoření obrazů (bitových kopií) operačních systémů a jejich instalaci na server RIS. Chcete-li instalovat s operačním systémem také nějakou aplikaci, můžete příslušné obrazy aplikace také vytvořit nástrojem RIPrep.
- **Spouštěcí disketa vzdálené instalace (RBFGE.exe).** Používá se k vytvoření spouštěcí diskety, která je zapotřebí k instalaci operačních systémů pomocí služby RIS na určité klientské počítače.
- **Průvodce instalací klienta (OSChooser.exe).** Používá se klientských počítačích k výběru obrazu RIS, který si uživatel nainstaluje.

Všechny počítače splňující specifikace PC98 verze 0.6 a novější obsahují paměť ROM prostředí vzdáleného spouštění (PXE) sloužící ke vzdálené instalaci OS. U existujících počítačů, které neobsahují paměť ROM PXE, můžete použít nástroj vytvoření spouštěcí diskety vzdálené instalace, kterou použijete k inicializaci procesu RIS. Spouštěcí disketu služby RIS lze použít ve spojení s řadou různých podporovaných síťových karet standardu Peripheral Component Interconnect (PCI). Další informace najdete v seznamu Hardware Compatibility List (HCL) na CD operačního systému Windows 2000 a v odkazu Microsoft Windows Hardware Compatibility List stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Obrázek 24.2 ukazuje hlavní kroky konfigurování funkce vzdálené instalace OS. Následující oddíly popisují klíčové problémy plánování, kterým se musíte věnovat při použití nástroje RISetup.exe, modulu snap-in Správce služeb vzdálené instalace (Remote Installation Services Administrator) a nástroje RIPrep.exe.

**Obrázek 24.2 Kroky plánování zavedení služeb RIS**

Konfigurování služeb vzdálené instalace

Služby vzdálené instalace (Remote Installation Services – RIS) jsou volitelnou součástí, kterou můžete nainstalovat při instalaci systému Windows 2000 Server. Většina procesu instalace je sice automatizovaná, existuje tu však několik základních a pokročilých nastavení, která můžete nakonfigurovat během instalace služby RIS ještě před nabídnutím této služby uživatelům.

Služba RIS není standardně nakonfigurována na obsluhu klientských počítačů ihned po své instalaci. Chcete-li, můžete přijmout všechna výchozí nastavení konfigurace RIS a začít nabízet instalační obrazy uživatelům na základě těchto voleb. Většina organizací si však službu RIS upraví tak, aby lépe splňovala požadavky jejich oddělení IT a provozní potřeby.

Chcete-li nakonfigurovat nastavení RIS jak pro server RIS tak i pro klientský počítač, budete muset použít modul snap-in Uživatelé a počítače služby Active Directory (Active Directory Users and Computers) konzoly Microsoft Management Console (MMC). Možnosti konfigurace serveru určují, jak bude určitý server RIS reagovat na klientské počítače požadující jeho služby. Klientské možnosti vám pomohou definovat, jak se obraz (bitová kopie) RIS nainstaluje na klientský počítač.

Mezi hlavní konfigurační možnosti, které lze nastavit pomocí modulu snap-in Uživatelé a počítače služby Active Directory (Active Directory Users and Computers), patří:

Definovat formát automatického pojmenovávání klientských počítačů Umožňuje vám určit, zda bude název počítače (který se generuje automaticky) vycházet ze jména uživatele, příjmení uživatele, za nímž bude následovat jméno uživatele, nebo zda se bude používat vlastní pojmenovávací formát specifický pro vaši organizaci. Výchozí je jméno uživatele.

Definovat výchozí umístění ve službě Active Directory pro vytváření všech objektů účtů počítačů Můžete vybrat výchozí kontejnery nebo organizační jednotky (OU) Active Directory, nebo můžete vytvořit novou OU služby Active Directory speciálně pro klienty RIS. Výchozím nastavením je kontejner Computers (počítače).

Před zavedením služby umístit klientské počítače do Active Directory Tato možnost vám dovoluje definovat, které účty klientských počítačů v Active Directory mohou používat funkci vzdálené instalace. Abyste mohli tuto volbu použít, musíte určit název klientského počítače, výchozí umístění v Active Directory, globálně jednoznačný identifikátor (GUID) klientského počítače a volitelně (pro účely vyrovnávání zatížení) také, který server RIS bude podporovat specifické klienty. Výchozím nastavením nejsou žádní předem zavádění klienti.

Nabídnout nástroje pro správu a údržbu od nezávislých výrobců Umožňuje správcům a (povolíte-li to) koncovým uživatelům přistupovat k předinstalačním nástrojům správy a řešení problémů od nezávislých výrobců softwaru. Takové systémy mohou například inovovat systém BIOS počítače, kontrolovat nepřítomnost virů, vykonávat diagnostiku počítače nebo inventarizovat systém ještě před instalací operačního systému. Výchozím nastavením jsou žádné instalované nástroje.

Přidat další obrazy operačních systémů ve formátu CD nebo RiPrep Tato volba vám dovoluje přidat na existující servery RIS v podniku nové verze operačních systémů či obrazy RiPrep nebo k existujícím obrazům (bitovým kopiím) operačních systémů přiřadit různé šablony bezobslužné instalace. Tuto možnost lze například použít k nastavení více obrazů RiPrep, z nichž každý lze pak zpřístupnit pouze příslušným uživatelům v organizaci. Výchozím nastavením je bitová kopie systému Windows 2000 na disku CD.

Vzdáleně konfigurovat servery RIS z pracovních stanic systému Windows 2000 Professional

Povolením této volby můžete vzdáleně spravovat mnoho možností RIS na libovolném serveru RIS v doméně nebo podniku. Výchozí nastavení je nedostupné, což znamená, že většinu zde popsaných konfiguračních možností lze zadat také z počítače se spuštěným systémem Windows 2000 Professional, na kterém je povoleno vykonávání úkolů správy.

Podporovat společnou existenci instalačních serverů od různých výrobců Tato možnost podporuje organizace, které používají na stejné fyzické síti jiné servery vzdálené instalace a spouštění, než systém Windows 2000. Tato volba se obvykle používá ve spojení s dříve popsanou možností předběžného zavádění, takže služba RIS nekoliduje s již existujícími servery vzdáleného spouštění, které používají stejné protokoly vzdáleného spouštění. Výchozím nastavením je zakázáno.

Existují tři další konfigurační možnosti, které lze definovat mimo okno vlastností serveru RIS. Tyto volby jsou určeny jak pomocí nastavení zásad skupiny tak i nastavením specifických popisovačů zabezpečení neboli seznamů řízení přístupu (ACL) na obrazech operačních systémů, které chcete před uživateli chránit:

Definovat dostupné možnosti instalace klientů Tato volba používá zásady skupiny k omezení instalačních možností pro skupinu uživatelů. Například nebudete chtít, aby měli určití uživatelé přístup k nabídce nástrojů údržby a řešení problémů nebo k možnosti vlastní instalace. Výchozím nastavením je zpřístupnění automatické instalace všem uživatelům. Žádné další instalační volby nejsou dostupné.

Definovat dostupné možnosti instalace operačního systému Tato možnost používá popisovače zabezpečení k určení uživatelů, kteří mají mít přístup k obrazům operačního systému dostupným na serveru RIS. Tuto funkci lze používat pro navigování uživatelů k bezobslužné instalaci operačního systému odpovídající jejich roli v organizaci. Standardně jsou všechny obrazy dostupné všem uživatelům.

Autorizovat servery RIS v zájmu ochrany před cizími servery Tato volba zabráňuje neautorizovaným serverům RIS obsluhovat klienty na síti organizace. Musíte určit, které servery RIS mohou poskytovat instalace klientům s možností vzdáleného spouštění. Toto nastavení nelze nijak změnit.

Příprava obrazů klientských operačních systémů

Služba RIS podporuje dva typy obrazů (bitových kopií) operačního systému: obrazy na CD a obrazy RIPrep. V nejjednodušším případě můžete uživatelům nabídnout přímo instalaci operačního systému z disku CD, která nainstaluje systém Windows 2000 Professional v bezobslužném režimu.

Chcete-li nakonfigurovat vlastní instalace systému Windows 2000 Professional, aniž byste vytvářeli samostatné obrazy pro každý typ klientského počítače a každou hardwarovou součást instalovanou na daném počítači, můžete používat službu RIS, která pomocí vylepšené podpory zařízení Plug-and-Play systému Windows 2000 detekuje rozdíly mezi zdrojovým počítačem a cílovými počítači v okamžiku instalace.

Poznámka Jestliže ovladače vrstvy abstrakce hardwaru (HAL) vašich klientských počítačů nejsou stejné, nebude možné konfigurovat vlastní instalace systému Windows 2000 Professional bez vytvoření samostatného obrazu pro každý typ klientského počítače a každou hardwarovou součást instalovanou na daném počítači. Většina počítačů třídy pracovních stanic a kancelářských počítačů nevyžaduje zvláštní ovladače HAL – jinak je tomu u počítačů serverové třídy. Ovladače HAL se většinou liší na klientských počítačích podporujících rozhraní Advanced Configuration Power Interface (ACPI) a počítačích, které rozhraní ACPI nepodporují.

Nástroj RIPrep lze použít k přípravě existujícího obrazu systému Windows 2000 Professional včetně všech místně instalovaných aplikací a konfiguračních nastavení a k replikování tohoto obrazu na síťový server RIS. Když do svých obrazů RIS zahrnete také základní sadu aplikací, dramaticky tím snížíte množství práce nutné k nastavení klientského počítače. Další informace o zabalení aplikací v zájmu zavádění pomocí služby RIS a funkcí IntelliMirror najdete v oddílu „Zlepšení správy softwaru pomocí zásad skupiny“ dále v této kapitole.

Možnosti instalace klientů

Abyste mohli spustit nástroj RIPrep, musíte zodpovědět několik základních otázek, jako je například umístění serveru, kam se obraz uloží. Po zodpovězení těchto otázek nakonfiguruje průvodce nástroje RIPrep obraz do obecného stavu tak, že z něj odstraní všechny prvky specifické pro daný počítač, jako je například jednoznačný identifikátor zabezpečení (SID) počítače, a pak jej replikuje na server RIS.

Zásady skupiny lze při nastavování RIS použít ke konfiguraci následujících možností instalace klientů:

Automatická instalace Všichni uživatelé mají přístup k možnosti automatické instalace. Zajistíte-li zároveň přístup k jedinému obrazu operačního systému, instalace operačního systému se spustí okamžitě po přihlášení uživatele, aniž by uživatel musel zodpovídat nějaké otázky. Rozhodnete-li se nabídnout uživatelům více typů instalací operačního systému, omezte tento počet na tři až pět možností, abyste minimalizovali možné nejasnosti a zajistili jste, že uživatelé si vyberou operační systém, který nejlépe odpovídá jejich potřebám a rolím v organizaci.

Vlastní instalace Možnost vlastní instalace vám nebo personálu technické podpory umožňuje nastavit počítač pro někoho jiného v organizaci. Dosahuje se toho tím, že je vám umožněno přepsat pravidla řídící automatické pojmenovávání počítačů a místo, kde se vytvoří účet počítače. Je tomu tak proto, že nemusí být vhodné pojmenovat počítač nebo umístit jeho účet podle nastavení zásad skupiny platících pro daného správce nebo osobu technické podpory. Tuto volbu lze použít k předběžné instalaci klientského počítače nebo musí-li někdo z oddělení IT či technické podpory fyzicky navštívit koncového uživatele při nastavování nebo opakované instalaci jeho počítače.

Opakovaně spustit předchozí instalaci Touto možností se můžete vyhnout nutnosti, aby klienti opakovaně odpovídali na otázky o instalovaném operačním systému. Jestliže byl uživatel již například dotazován na název organizace, název oddělení či používané grafické rozlišení, možnost restartování zajistí, že nemusí při opakování nepodařené instalace na uvedené otázky znovu odpovídat. Tato volba nerestartuje instalaci v okamžiku selhání. Také se nepokusí vyřešit problémy, ke kterým došlo v předchozím pokusu o instalaci.

Údržba a řešení problémů Tato volba poskytuje přístup k hardwarovým a softwarovým nástrojům od jiných výrobců, jako jsou inovace systému BIOS a antivirové programy. Budete-li umožňovat přístup k instalačním nástrojům, povolte přístup pouze k takovým nástrojům, které nemohou poškodit počítač nebo způsobit další problémy.

Zlepšení správy softwaru pomocí zásad skupiny

Typická velká organizace podporuje stovky a někdy i tisíce programů. Tento počet může být ještě výrazně vyšší, započítáte-li jako samostatné programy v inventáři všechny různé verze, opravy a šablony.

Protože mnoho organizací nemá výkonné prostředky pro správu svých portfolií softwaru, nedaří se jim pravidelně inovovat aplikační software. Když se pak rozhodnou opustit zastaralý software nebo zavést nové aplikace, taková změna může být extrémně rušivá.

Systém Windows 2000 vám může pomoci se zjednodušením procesů správy softwaru v následujících oblastech:

- **Příprava.** Jaký software chcete spravovat? Jak chcete naformátovat daný software pro distribuci a instalaci?
- **Distribuce.** Odkud chcete daný software spravovat?
- **Zacílení.** Kdo bude daný software přijímat?
- **Instalace.** Jak se bude daný software instalovat na počítač?

Obrázek 24.3 ukazuje hlavní otázky plánování související s jednotlivými fázemi.

Tyto úkoly plánování musíte splnit i u aplikací, které byly instalovány společně se systémem Windows 2000 Professional. Uvedenými kroky plánování budete muset také projít při zavádění, inovaci a údržbě aplikací na existujících počítačích.

Příprava softwaru na distribuci

V kapitolách „Testování kompatibility aplikací se systémem Windows 2000“ a „Definování standardů správy a konfigurace klientů“ jste byli požádáni o vyhodnocení kompatibility aplikací ve vaší organizaci se systémem Windows 2000 a jejich rozdělení do kategorií nutných a volitelných:

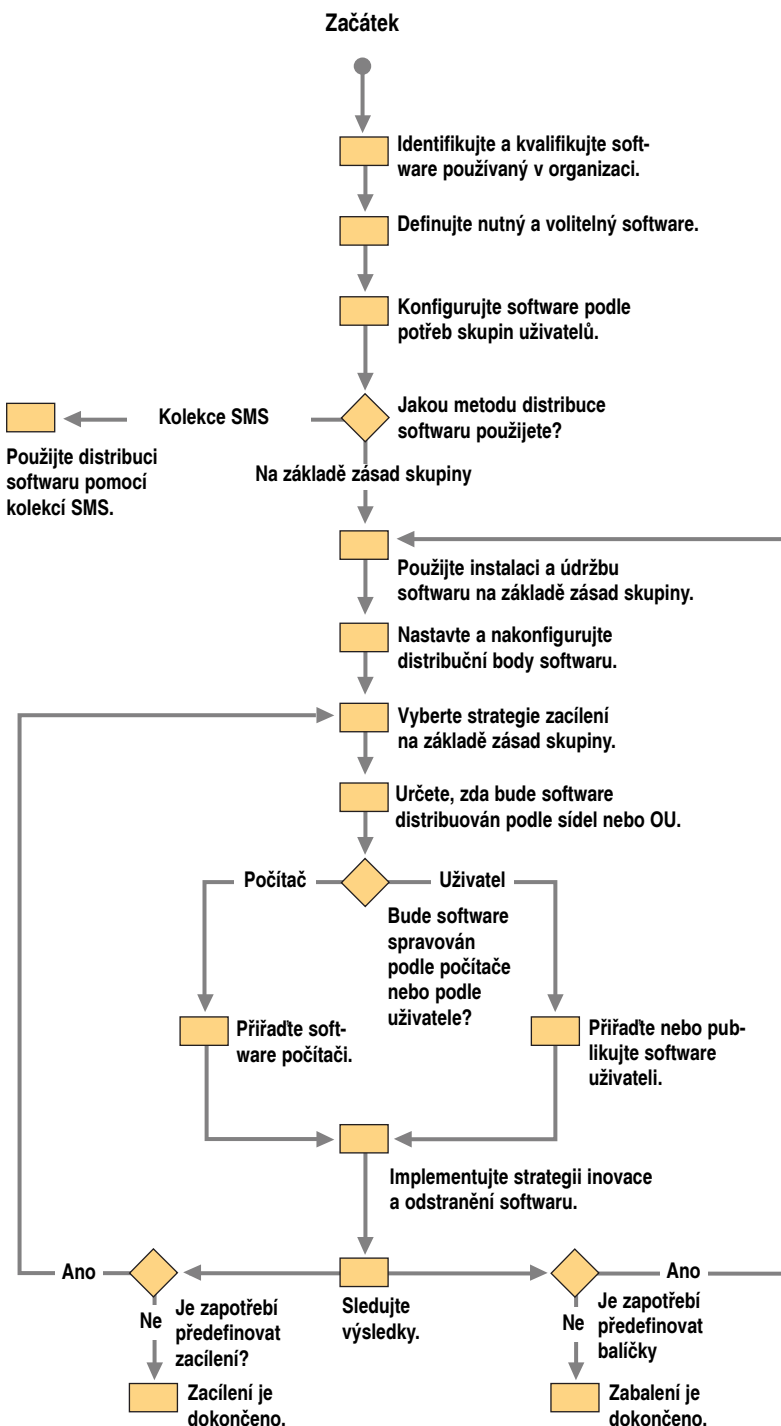
- pro organizaci jako celek;
- pro skupiny uživatelů v organizaci.

Než budete moci požívat k distribuování softwarových aplikací funkce IntelliMirror, musíte se přesvědčit o jejich správném nakonfigurování pro zavedení se systémem Windows 2000.

Aplikace pracující s nástrojem Windows Installer využijí funkce podpory aplikací systému Windows 2000 neefektivněji. Windows Installer je nová instalační služba, která se skládá z těchto částí:

Instalační služba, která se nachází v operačním systému V minulosti obsahovala každá aplikace svůj vlastní spustitelný instalační program nebo skript. Proto musela každá aplikace zajistit splnění příslušných pravidel instalace (jako jsou například pravidla uvádění verzí souborů). Vývojáři instalačních rutin měli navíc k dispozici jen málo doporučených instalačních postupů. Výsledkem bylo, že instalace (nebo odebrání) určité aplikace často poškodila existující aplikace na počítači. Služba Windows Installer zaručuje implementování nejdůležitějších pravidel instalace přímo operačním systémem. Aby byla tato pravidla naplněna, stačí když se aplikace samy popíší ve standardním formátu služby Windows Installer.

Standardní formát správy součástí Služba Windows Installer se na všechny aplikace dívá jako na logické stavební bloky: součásti, funkce a produkty. Součásti jsou kolekce souborů, klíčů registru a dalších prostředků, které se společně instalují nebo odstraňují. Je-li nějaká součást označena k instalaci nebo odstranění, nainstalují se nebo odstraní všechny prostředky v dané součásti. Funkce jsou části aplikace, které může uživatel vybrat k instalaci, a obvykle představují funkční prvky samotné aplikace. Když uživatel zvolí vlastní instalaci, funkcím zhruba odpovídají části aplikace, které může vybrat k in-



Obrázek 24.3 Klíčové otázky plánování zavádění softwaru pomocí funkcí IntelliMirror

stalaci. Produkt služby Windows Installer představuje jediný výrobek, jako například Microsoft Office. Produkty se skládají z jedné nebo více funkcí instalační služby Windows Installer. Každý produkt je popsán pro službu Windows Installer ve formě jediného souboru balíčku (.msi) nástroje Windows Installer.

Rozhraní API správy pro aplikace a nástroje Rozhraní programování aplikací (API) služby Windows Installer umožňuje nástrojům a aplikacím vytvářet výčty produktů, funkcí a součástí nainstalovaných na počítači, instalovat a konfigurovat produkty a funkce služby Windows Installer a určovat cestu ke specifickým součástem služby Windows Installer instalovaným na počítači. Aplikace, které umějí využívat službu Windows Installer, získávají výhody podpory cestujících uživatelů, instalace na požádání a přizpůsobivost prostředků při běhu.

Aplikace, které nativně využívají technologii Windows Installer, budou podporovat tyto prvky:

- **Instalace funkcí v okamžiku potřeby.** To vám umožňuje distribuovat jen část volitelných funkcí aplikace. Když se pak uživatel pokusí použít odinstalovaný prvek (například kontrolu gramatiky nebo knihovnu klipartů), daný prvek se ihned nainstaluje. Tím se šetří diskový prostor potřebný pro málokdy používané funkce aplikace, které jsou však zároveň přístupné uživatelům, kteří s nimi občas pracují.
- **Opravení funkcí.** Dojde-li k poškození nebo náhodnému odstranění důležitých aplikačních souborů, služba Windows Installer identifikuje potřebné soubory a automaticky je znovu nainstaluje.
- **Instalace s vyššími privilegii.** Uživatelé nemusí být správci na místním počítači, aby mohli instalovat software pomocí funkcí instalace a údržby softwaru IntelliMirror. Stačí, když budou členy skupiny Users nebo Power Users.

Poznámka Mnoho výrobců softwaru a interních vývojových skupin inovuje své aplikace tak, aby využívaly schopností služby Windows Installer. Další informace o specifikaci aplikací pro systém Windows 2000 najdete v odkazu MSDN stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Když není vytváření nativních aplikací možné

Není vždy možné vytvářet nativní aplikace pro systém Windows 2000. Můžete mít třeba starší aplikace, pro něž nemáte prostředky potřebné k vytvoření nativních balíčků služby Windows Installer. Když však takové aplikace znovu zabalíte pro systém Windows 2000, budete moci využívat výhody služby Windows Installer.

Soubory lze znovu zabalit pomocí nástrojů zabalení, jako je například program WinInstall LE, což je součást systému Windows 2000 Server.

Změny mezi originální aplikací a obrazem (bitovou kopií) upravené aplikace se pak převedou do balíčku služby Windows Installer.

Znovu zabalené soubory vám umožní využívat některé funkce služby Windows Installer. Znamená to, že je lze inzerovat a opravovat a instalovat s vyššími privilegii. (Inzerování a další možnosti distribuování jsou popsány v oddílu „Možnosti správy softwaru“ dále v této kapitole.) Znovu zabalená aplikace však nebude využívat architekturu služby Windows Installer, což znamená, že se nainstaluje, jako by měl produkt jen jednu (rozsáhlou) funkci.

Správa starších aplikací

Uživatelům můžete využitím existujících instalačních programů zpřístupnit také další aplikace. K tomu budete potřebovat textový editor, například Poznámkový blok, ve kterém vytvoříte soubor ZAP (.zap). Soubory ZAP, které se podobají souborům INI, jsou umístěny ve stejné složce bodu distribuce softwaru, jako je originální instalační program, na který se odkazují. Jelikož publikujete existující instalační program, uživatel nezíská nic víc, než skutečně tento program. Jestliže instalační program například nepodporuje čisté a úplné odstranění daného softwaru, pak se pouhým publikováním existujícího instalačního programu nezlepší možnosti odstranění aplikace. Budete-li spravovat soubory softwaru pomocí souborů ZAP, aplikace se objeví v ovládacím panelu Přidat nebo odebrat programy (Add/Remove Programs) a uživatelé budou moci aplikaci instalovat z tohoto místa.

Poznámka Aby bylo možné dokončit tento typ instalace, uživatel bude potřebovat stejná oprávnění správy, jaká jsou požadována starší aplikací.

Další informace o správě starších aplikací najdete v kapitole „Správa softwaru“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.

Používání transformací

V minulosti museli správci, kteří chtěli upravit chování instalace, znovu zabalit aplikaci přímou změnou instalačního skriptu. Jen tak mohli dosáhnout požadovaných výsledků. Pokud podobné změny vyžadovalo mnoho různých instalačních skriptů, museli tuto činnost zopakovat v každém skriptu zvlášť.

V systému Windows 2000 již nemusíte upravovat balíčky služby Windows Installer, chcete-li upravit instalaci pro vaši organizaci. Můžete místo toho vytvořit transformaci a tu pak použít pro upravení (modifikování) balíčku. Transformace služby Windows Installer upravuje soubor balíčku služby Windows Installer v okamžiku zavádění, a proto dynamicky ovlivňuje chování instalace.

Balíčky služby Windows Installer můžete transformovat nebo upravit tak, aby umožňovaly různé změny. Transformaci lze například použít k instalaci vybraných funkcí na předem zadané místo, takže se uživatelé nemusejí rozhodovat, jaké prvky si mají nainstalovat a kam si je mají nainstalovat. Transformaci lze použít také ke změně cesty zadané součástí, pokud tedy daná součást v upravovaném balíčku existuje.

Zatímco existující instalační programy obvykle nabízejí uživateli jen logickou možnost „instalovat“ nebo „neinstalovat“ danou funkci, funkce služby Windows Installer lze nastavit do jednoho ze čtyř stavů:

- **Instalovat na místní pevný disk.** Soubory se zkopírují na pevný disk místního počítače.
- **Instalovat pro spouštění ze zdroje.** Soubory se ponechají ve zdrojovém místě (obvykle sdílené místo sítě nebo disk CD). Aplikace přistupuje k souborům na zdroji.
- **Inzerovat soubory.** Soubory jsou ponechány na zdroji, lze je však při prvním použití instalovat na váš pevný disk.
- **Neinstalovat.** Soubory se nekopírují.

Transformace musí být uloženy na stejných místech sdílení na síti, jako jsou balíčky služby Windows Installer, které upravují. Transformace (modifikace) se aplikují při zavádění a nelze je aplikovat na již instalovanou aplikaci.

Distribuce softwaru

Po opravení softwaru (tedy po vytvoření softwaru v příslušném formátu balíčku a zadání úprav a transformací) můžete přesunout vlastní soubory softwaru včetně balíčku a všech transformací na řadu sdílených síťových míst v celé vaší organizaci. Obvykle jsou distribuční body umístěny po celé organizaci, aby mohli lidé vždy získat software z distribučního bodu, který nabízí z jejich hlediska spolehlivé vysokorychlostní připojení.

Instalace a údržba softwaru systému Windows 2000 se netýká přímo fáze distribuce. Bude záležitostí vašeho týmu zavádění otestovat plány distribuce softwaru a zajistit, aby vaše šířka pásma v síti a umístění instalačních serverů odpovídalo očekávaným nárokům ve vaší organizaci.

Ke správě fáze distribuce však můžete také použít další služby systému Windows 2000, jako například distribuovaný systém souborů (DFS). Další informace o plánování a zavádění svazků DFS najdete v kapitole „Určení strategií správy úložišť systému Windows 2000“ v této knize.

Zacílení softwaru

Správci IT musí instalovat aplikace v celé organizaci na základě toho, jak uživatelé vykonávají svou práci. Protože požadavky na software uživatelů i jejich zkušenosti práce s počítači se liší, oddělení IT musí typicky distribuovat kombinaci:

- univerzálních aplikací, jako je zpracování elektronické pošty a textu, které používají všichni uživatelé;
- aplikací pro specifické činnosti, které potřebují uživatelé vykonávající speciální úkoly nebo patří do specifických oddělení a divizí;
- volitelných aplikací, které si uživatelé mohou instalovat podle potřeby.

V tomto okamžiku plánování zavedení byste měli být schopni určit:

- kteří uživatelé mají obdržet určité aplikace;
- která nastavení zásad skupiny pro správu aplikací musí být nastavena na úrovni síťového sídla, na úrovni domény a na úrovni organizační jednotky (OU).

Poznámka Snažte se vyhnout spravování jedné aplikace, jako je například Microsoft Word, v různých objektech zásad skupiny, které se mohou aplikovat na stejnou osobu.

Abyste mohli definovat své cíle pomocí zásad skupiny, potřebujete použít moduly snap-in Zásady skupiny (Group Policy) a Instalace softwaru (Software Installation). Pomocí modulu snap-in Zásady skupiny (Group Policy) můžete vytvořit nový objekt zásad skupiny nebo upravit již existující objekt a software přiřadit nebo publikovat uživatelům či počítačům.

Modul snap-in Instalace softwaru (Software Installation) vytváří skript inzerování aplikace a tento skript ukládá na příslušná místa v Active Directory a objektu zásad skupiny.

Další informace o použití zásad skupiny společně se síťovými sídly a organizačními jednotkami najdete v kapitole „Návrh struktury služby Active Directory“ v této knize. Další informace o použití zásad skupiny při implementování standardů klientských konfigurací najdete v kapitole „Definování standardů správy a konfigurace klientů“ v této knize.

Možnosti správy softwaru

Zavádění softwaru na základě zásad skupiny slouží ke zjednodušení procesu správy softwaru po celou jeho životnost. Správu a údržbu softwaru můžete používat k přiřazování a publikování aplikací, k inovaci zavedených aplikací, k instalaci servisních balíčků a k odstranění již nepotřebných aplikací. Všechny tyto úkoly lze vykonat bez zásahu uživatele. Zásady skupiny systému Windows 2000 vám umožňují distribuovat aplikace na základě tří kritérií:

Přiřazení aplikací uživatelům Když přiřadíte aplikace uživatelům, daná aplikace se vždy objeví v nabídce tlačítka **Start** daného uživatele, bez ohledu na to, k jakému počítači se uživatel přihlásí. Když uživatel spustí přiřazenou aplikaci, která není instalovaná na místním počítači, aplikace se nejprve nainstaluje a pak spustí. Jestliže uživatel odstraní přiřazenou aplikaci, její zástupce se znovu objeví v nabídce tlačítka **Start**. Obecně platí, že byste uživatelům měli přiřadit všechny nutné aplikace (univerzální a určené ke konkrétní práci).

Přiřazení aplikací počítačům Na rozdíl od aplikací přiřazených uživatelům se aplikace přiřazené počítačům instalují při následujícím spouštění počítače. Jestliže počítač používá několik lidí, kteří pracují se stejnou aplikací, pak je daná aplikace kandidátem na přiřazení počítači. Příkladem softwaru, který je možno přiřadit počítači, je antivirový software licencovaný na síťovém sídle. Aplikace přiřadte počítačům také v případě, že jsou dané aplikace zapotřebí, jen pokud uživatelé používají konkrétní počítač (například počítač v knihovně).

Publikování aplikací Když aplikace publikujete, neobjevují se v nabídce tlačítka **Start**. Musí být instalovány ručně pomocí ovládacího panelu Přidat nebo odebrat programy (Add/Remove Programs). Panel Přidat nebo odebrat programy převezme seznam publikovaných aplikací od služby Active Directory. Uživatelé mohou publikované aplikace ze svých počítačů odstranit – aplikace se na jejich počítači nebudou opakovaně inzerovat. Aplikaci publikujte, když ji sice nepožadují všichni uživatelé v síťovém sídle, doméně nebo organizační jednotce, ale některým může být užitečná. Starší aplikace nelze přiřadit uživateli nebo počítači, lze je pouze publikovat.

Poznámka Chcete-li, aby vždy došlo k instalaci aplikace nebo byla její instalace kdykoli možná bez ohledu na akce uživatele, přiřadte daný software buď uživateli nebo počítači. Publikování váže danou aplikaci k uživateli nebo počítači méně pevně, než přiřazení aplikace.

Přiřazené nebo publikované aplikace lze také instalovat, když uživatel poklepe na dokument, jehož přípona názvu souboru je přidružena k dané aplikaci. Tabulka 24.5 uvádí dodatečné informace o rozdílech mezi přiřazováním aplikací uživatelům, přiřazováním aplikací počítačům a publikováním aplikací.

Tabulka 24.5 Rozdíly v chování mezi přiřazenými a publikovanými aplikacemi

	Přiřazené uživateli	Přiřazené počítači	Publikované
Kdy je daný software po zavedení dostupný pro instalaci?	Po dalším přihlášení.	Po dalším spuštění nebo restartu počítače.	Po dalším přihlášení.
Odkud si uživatel daný software obvykle nainstaluje?	Nabídka tlačítka Start nebo zástupce na pracovní ploše.	Software je již instalován.	Ovládací panel Přidat nebo odebrat programy (Add/Remove Programs).
Jestliže daný software není instalován a uživatel otevře soubor přidružený k danému softwaru, nainstaluje se tento program?	Ano.	Software je již instalován.	Ano.
Může uživatel daný software odstranit pomocí ovládacího panelu Přidat nebo odebrat programy?	Ano a software bude okamžitě dostupný pro další instalaci.	Ne. Software může odstranit jen místní správce.	Ano a může znovu zadat jeho instalaci z ovládacího panelu Přidat nebo odebrat programy.
Jaké instalační soubory jsou podporovány?	Balíčky instalační služby Windows Installer.	Balíčky instalační služby Windows Installer.	Balíčky instalační služby Windows Installer a starší aplikace.

Vlastní kroky přiřazení nebo publikování softwaru jsou si podobné. Správce zadává obě tyto možnosti z modulu snap-in Instalace softwaru (Software Installation). Konkrétní úlohy jsou popsány v souboru nápovědy tohoto modulu snap-in.

Aplikace se obvykle přiřazují ve vysoce spravovaných organizacích, zejména kde jsou problémem náklady na podporu a kde počítače sdílí více uživatelů. V méně spravovaných organizacích se aplikace častěji publikují než přiřazují.

Podpora cestujících uživatelů

V mnoha organizacích se určití lidé přesunují při své práci mezi různými místy, jako je tomu například v případě recepčního, který pravidelně zastupuje jiného recepčního. Třebaže se tito uživatelé přihlašují k různým počítačům, mají vždy k dispozici vysoko rychlostní připojení nebo spojení na LAN.

Instalace a údržba softwaru systému Windows 2000 může zlepšit podporu oddělení IT cestujícím uživatelům tím, že se na libovolný jimi používaný počítač nainstaluje jakákoli aplikace v okamžiku, kdy ji potřebují. Podobně platí, že dojde-li k odstranění dříve publikované aplikace, znovu se odstraní po přihlášení uživatele a nezáleží na tom, jaký počítač používá.

Těmto uživatelům můžete software přiřadit. I když se pak přesunou na jiný počítač, stále uvidí své aplikace. Jejich zásady skupiny však nakonfigurujte tak, aby se daná aplikace instalovala, pouze pokud se ji uživatel skutečně pokusí spustit.

Podpora sdílených počítačů

V mnoha organizacích lidé sdílejí počítače. Máte-li počítače ve výrobní hale, školící místnosti nebo v laboratoři, pravděpodobně podporujete sdílené počítače.

V takových případech můžete software přiřadit počítačům a nikoli uživatelům. To vám umožní spravovat software výkonněji a jestliže jej uživatel odstraní, automaticky se znovu nainstaluje při restartu počítače.

V takových prostředích se sdílenými počítači zvažte použití funkce vzdálené instalace. Když pak budete muset znovu vybudovat celé prostředí, dosáhnete toho velmi výkonně.

Podpora mobilních pracovníků

Stále větší procento zaměstnanců, jako jsou prodejci a konzultanti, při své práci neustále cestuje. Tito lidé se zpravidla přihlašují na stále stejný počítač a někdy se připojují k síti přes vysokorychlostní linky a jindy zase přes pomalé telefonické připojení. Instalace a údržba softwaru se standardně neaplikuje přes pomalé připojení. To platí, ať už by mělo jít o čistou instalaci nebo inovaci. Další informace o konfigurování zásad skupiny pro pomalá připojení najdete v kapitole „Definování standardů správy a konfigurace klientů“ v této knize.

Takovým uživatelům můžete software publikovat a zajistit, aby se veškeré úpravy softwaru instalovaly místně na počítač uživatele (a nenechat tedy funkci pro instalaci při prvním použití nebo ji spouštět ze sítě).

Můžete také zařídit, aby měli mobilní pracovníci určitý software při cestování k dispozici na místním médiu. Jestliže například mobilní profesionál často pořádá prezentace, bude pravděpodobně vhodné dát mu CD sady Microsoft Office, aby si mohl kdykoli a kdekoli instalovat nebo opravit důležité soubory.

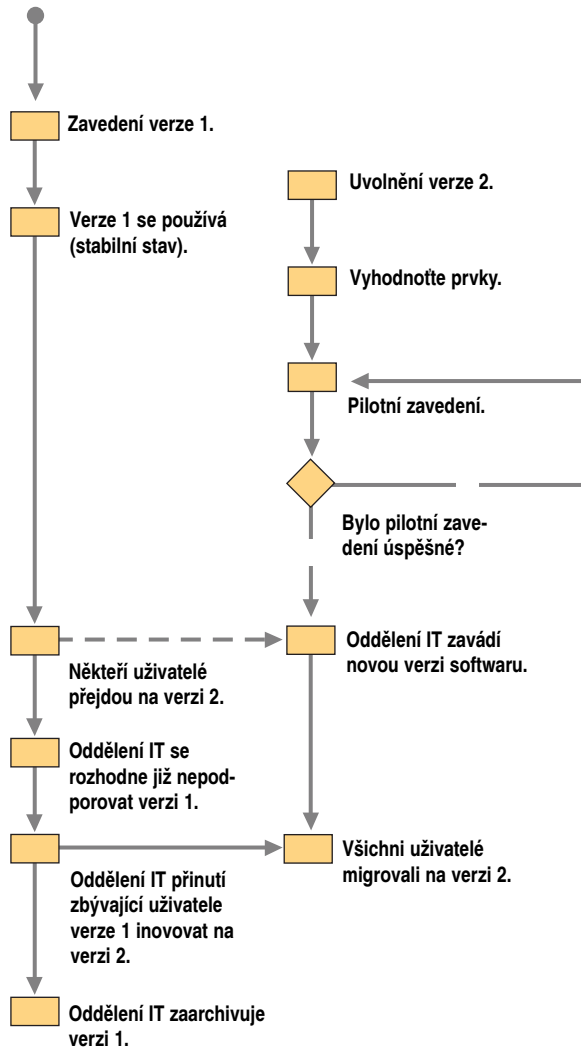
Správa softwaru funkcemi IntelliMirror

Správci musí být schopni spravovat software v celém jeho životním cyklu. Instalace a údržba softwaru funkcemi IntelliMirror byla vytvořena s ohledem na následující životní cyklus softwaru:

1. Životní cyklus softwaru začíná jeho prvním zavedením. Uživatelé se softwarem naučili pracovat a produktivně jej používají. Protože se jedná o stabilní a známý stav, správci by chtěli v tomto stavu zůstat.
2. Díky změně výrobních či obchodních požadavků nebo dostupnosti nové, vylepšené verze daného softwaru, se musíte zamyslet nad zavedením nové verze. Vyhodnotíte nové funkce a zavedete je pečlivě vybrané skupině uživatelů během pilotního programu. Při pilotním testování bude většina uživatelů nadále používat starší verzi.
3. Jestliže byl pilotní program úspěšný, personál oddělení IT bude postupně zavádět nový software do zbytku organizace. Ohledně starší verze máte dvě možnosti:
 - Vynutit si inovaci na novou verzi.
 - Ponechat existující verzi k dispozici, ale nadále ji nepodporovat.
4. Nakonec budou všichni uživatelé používat novou verzi a bude existovat jen málo důvodů (pokud vůbec nějaké) pro další dostupnost starší aplikace. V tomto okamžiku ji pravděpodobně odstraníte z místa distribuce softwaru, zálohujete ji a archivujete pro případ potřeby jejího použití v budoucnosti.

Tento proces ukazuje obrázek 24.4.

Začátek

**Obrázek 24.4 Životní cyklus softwaru**

Tento životní cyklus zahrnuje následující úkoly správy softwaru:

- Instalace
- Úprava
- Inovace
- Oprava
- Odstranění

Prozatím se toto pojednání o instalaci a údržbě softwaru funkcemi IntelliMirror soustředilo prakticky výhradně na instalaci. Následující oddíly se zabývají úpravou, inovací a odstraněním.

Opravení existujícího softwaru

Výrobci softwaru často poskytují opravy (záplaty) řešící některé velmi konkrétní problémy v jejich aplikacích. Budete muset určit, zda vaše organizace potřebuje nějakou takovou opravu.

Rozhodnete-li se zavést opravu pomocí systému Windows 2000, můžete soubory opravy zkopírovat na bod distribuce softwaru a nahradit jím starší soubory. Výrobce softwaru, který danou opravu distribuuje, by měl dodat buď nový balíček služby Windows Installer (soubor .msi) nebo opravu služby Windows Installer (soubor .msp). Balíčkem instalační služby Windows Installer můžete jednoduše nahradit existující balíček. Alternativně můžete inovovat existující balíček opravou služby Windows Installer.

Přiřazený nebo publikovaný balíček pak opakovaně zavedete pomocí modulu snap-in Instalace softwaru (Software Installation). Opravené nebo inovované soubory se tak zkopírují na počítače uživatelů, kteří si daný software nainstalovali.

Servisní balíčky obvykle obsahují několik oprav, které byly testovány společně. Proto se servisní balíčky distribuují méně často než opravy, ale častěji než plné inovace.

Poznámka Jestliže servisní balíček inovuje pouze malý počet souborů, distribuujte a spravujte jej, jako by šlo o opravu. Pokud servisní balíček aktualizuje více souborů, distribuujte a spravujte jej, jako by šlo o inovaci.

Inovace existujícího softwaru

Existují dva typy inovací v síťovém prostředí:

- **Povinné inovace, ke kterým dochází okamžitě.** To znamená, že všichni uživatelé používající existující verzi dané aplikace se okamžitě inovují na novou verzi a uživatelé, kteří si daný software nikdy nenainstalovali, si mohou nainstalovat jen inovovanou verzi.
- **Nepovinné inovace, ke kterým nedochází okamžitě.** Existující uživatelé si mohou určit, zda budou inovovat, a noví uživatelé se mohou rozhodnout, kterou verzi si nainstalují.

Zpočátku můžete zpřístupnit nové inovace na základě nepovinné inovace, aby uživatelé mohli inovovat, až když budou chtít. Později se můžete rozhodnout, že se nepovinná inovace má stát povinnou.

Balíčky služby Windows Installer vycházejí z konceptu označovaného za „deklarovaný vztah inovace“, v němž jeden balíček ví, které další balíčky může inovovat. K vytvoření takového deklarovaného vztahu inovace můžete použít modul snap-in Instalace softwaru (Software Installation). Například jeden balíček sady Microsoft Word 2000 může inovovat Microsoft Word 6.0 a Microsoft Word 7.0.

Tento deklarovaný vztah inovace vyžaduje nativně vytvořené a nikoli jen opakovaně zabalené aplikace. To znamená, že budete muset ručně vytvořit vztahy inovace pro opakovaně zabalené aplikace.

Nový balíček aplikace (ať už byl vytvořen nativně nebo znovu zabalen) nemusí být schopen inovovat aplikaci, která nebyla vytvořena nativně. V některých případech bu-

deté muset použít k odstranění existující aplikace nástroje instalace a údržby softwaru a aplikaci pak nahradit inovací.

Může být také nemožné úplně odstranit opakovaně zabalenou aplikaci. Některé součásti, jako například zástupci na pracovní ploše, budou muset být odstraněny ručně, i když nejsou ani sdílené, ani zapotřebí. Postupně se však bude objevovat stále více aplikací s nativně vytvořenými balíčky a inovace budou schopny zajistit migraci existující aplikace na novou aplikaci.

Odstranění softwaru

Prakticky každý software není již v určitém okamžiku zapotřebí a vy se musíte rozhodnout, co s ním. Můžete prostě přestat zajišťovat jeho podporu, i když uživatelé budou nadále používat tuto zastaralou aplikaci. Bude pak na uživateli, aby takovou aplikaci odstranili, když ji již nebudou využívat. Na druhou stranu noví uživatelé si tuto verzi nebudou moci nainstalovat ani z ovládacího panelu Přidat nebo odebrat programy (Add/Remove Programs), ani z nabídky tlačítka **Start** a ani pokusem o otevření přířazeného dokumentu.

Alternativně si můžete vynutit odstranění daného softwaru z počítačů uživatelů. Chcete-li odstranit nějaký software, vyberte daný balíček v modulu snap-in Instalace softwaru (Software Installation). Pak zadejte příkaz **Odstranit** (Remove) místní nabídky. Odstranění softwaru si můžete vynutit při dalším přihlášení uživatele (v případě publikovaného nebo uživateli přiřazeného softwaru) nebo při dalším restartu počítače (v případě softwaru přiřazeného počítači). Software se odstraní, pokud se uživatel, který nemusí být v kanceláři ale třeba na dovolené, přihlásí alespoň jednou během následujícího roku.

Převedení uživatelských dat a nastavení na síť

Správa dat uživatelů a správa nastavení uživatelů umožňují, aby data a nastavení následovaly uživatele, ať už je připojen k síti nebo není, a bez ohledu na to, který počítač používá. Přístup uživatele k datům a jeho osobnímu prostředí můžete zlepšit tak, že dané informace uložíte na síťových serverech i na synchronizovaných místech offline na místním pevném disku.

K implementování správy dat a správy nastavení uživatelů se používá mnoho stejných technologií. Některé organizace mohou zavést správu dat a správu nastavení odděleně, jiné organizace mohou je mohou naplánovat a zavést společně. Následující oddíly popisují uživatelská data a nastavení společně.

K centrální správě uživatelských dat a nastavení jsou zapotřebí dále uvedené technologie:

Služba Active Directory Poskytuje infrastrukturu pro používání a správu zásad skupiny.

Zásady skupiny (Group Policy) Umožňuje správcům upravit a řídit prvky systému Windows 2000 sloužící uživatelům a počítačům, jako je pracovní plocha, přístup k síti a program Microsoft Internet Explorer.

Cestovní profily uživatelů Umožňuje, aby uživatelé následovaly jeho osobní nastavení a konfigurace pracovní plochy (včetně úprav nabídky tlačítka **Start** a obsahu složky Dokumenty) i na jiné počítače. To uživatelům dovolí pracovat ve známém prostředí bez ohledu na konkrétní počítač, který právě používají.

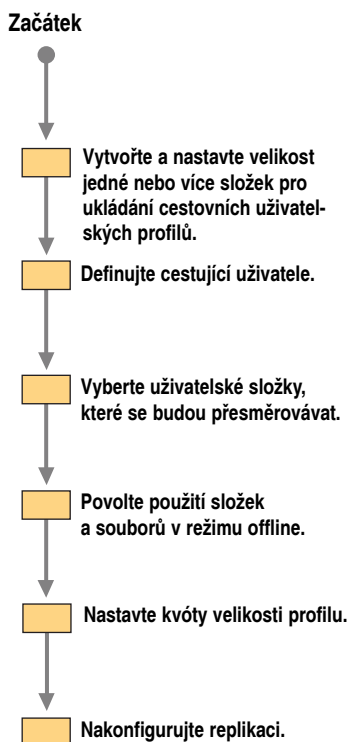
Přesměrování složky Používá zásady skupiny k přesměrování osobních složek (Dokumenty, Data aplikací, Nabídka Start a Plocha) na síťový server. Je-li přesměrována osobní složka, uloží se na síti a uživateli je dostupná bez ohledu na to, ke kterému počítači se přihlásí.

Složky (nebo soubory) offline Umožňují uživatelům udržovat dvě kopie dokumentu – jednu uloženou v místě sdílení souborů na síti a druhou na počítači uživatele. Když se uživatel přihlašuje nebo odhlašuje, systém Windows 2000 obě kopie dokumentu synchronizuje.

Diskové kvóty Omezuje množství informací, které si může uživatel uložit na zadaný svazek systému NTFS. Protože většina technologií funkcí IntelliMirror používá ukládání uživatelských dat na síť a nikoli na místní pevné disky, diskové kvóty mohou být zapotřebí k zajištění dostatečného diskového prostoru na síti.

Nastavení zabezpečení Umožňuje nastavit seznamy řízení zabezpečeného přístupu (DACL) na soubory a složky.

Obrázek 24.5 ukazuje klíčové kroky plánování, které musíte splnit při zavádění správy uživatelských dat a nastavení.



Obrázek 24.5 Proces plánování správy uživatelských dat a nastavení

V následujících oddílech se dozvíte něco o dodatečných technologiích potřebných ke správě uživatelských dat a nastavení:

- Cestovní profily uživatelů
- Přesměrování složek
- Soubory (nebo složky) offline
- Správce synchronizace
- Diskové kvóty

Zavedení cestovních uživatelských profilů

Cestovní uživatelské profily umožňují zajistit uživatelům známé a snadno použitelné prostředí. Na rozdíl od místního profilu, který je uložen na jediném počítači se systémem Windows 2000 Professional, je cestovní profil uložen na sdíleném místě sítě, což znamená, že k němu lze přistoupit z libovolného počítače se systémem Windows 2000 na síti.

Ať už je profil uživatele místní nebo cestovní, obsahuje řadu složek včetně (nikoli však pouze) složky Data aplikací (Application Data), Plocha (Desktop), Oblíbené položky (Favorites), Dokumenty (My Documents) a Nabídka Start (Start Menu).

Implementace cestovních uživatelských profilů v systému Windows 2000 se obecně podobá implementaci v systému Windows NT 4.0. Další informace o podobnostech a rozdílech najdete v kapitole „Úvod do správy počítačů“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.

▼ Chcete-li vytvořit cestovní profil uživatele, postupujte takto:

1. Vytvořte sdílené místo na síti, kam se budou ukládat profily uživatelů na serveru.
2. Nakonfigurujte tuto složku jako sdílenou složku.
3. Otevřete si modul snap-in Uživatelé a počítače služby Active Directory (Active Directory Users and Computers) a přesuňte se na specifický uzel, kde jsou uloženy vlastnosti uživatele.
4. Klepněte pravým tlačítkem myši na jméno uživatele a pak z místní nabídky zadejte příkaz **Vlastnosti** (Properties).
5. Zobrazte si kartu **Profil** (Profile).
6. Jako cestu k profilu zadejte cestu ke sdílenému místu na síti, kam se budou ukládat profily uživatelů. Například pro uživatele, jehož jméno je MarieK vytvoří síťová cesta \\Sdílení\Profil\MarieK adresář pojmenovaný MarieK ve sdíleném místě Profil na serveru používaném k ukládání uživatelských profilů.

Cestovat budou pouze položky uložené na síti. To znamená, že další položky, jako jsou sporič obrazovky a tapeta pracovní plochy, nebudou dostupné, pokud jejich kopie nebudou uloženy na každém počítači, ke kterému se daný uživatel přihlašuje.

Pokyny pro nastavení cestovních uživatelských profilů

Cestovní uživatelské profily mají své výhody i nevýhody. Výhodnou je, že jak osobní nastavení tak i dokumenty mohou následovat uživatele na různé počítače. Potenciálně nevýhodnou je množství provozu v síti, který to může představovat. Budete muset otestovat podrobné scénáře použití a určit vhodnou úroveň podpory cestování ve vaší organizaci. Nedoporučuje se používat cestovní profily pro vzdálené uživatele, kteří k síti přistupují přes pomalá spojení, jako jsou například telefonní linky.

Přesměrování složek

Osobní složky, kam patří i složky Dokumenty (My Documents) a Obrázky (My Pictures), lze přesměrovat pomocí zásad skupiny. Složky, které byly přesměrovány, budou dostupné uživatelům bez ohledu na to, ke kterému počítači se přihlašují. Také se správcům jednodušeji spravují a zálohují.

Uživatelé se přesměrovaná složka jeví jako místně uložená osobní složka a také tak funguje. Přesměrované složky se na rozdíl od složek vytvářejících cestovní profil uživatele nekopírují při přihlášení nebo odhlášení uživatele přes síť. Přesměrované složky mohou poskytnout uživatelům snadný přístup k jejich dokumentům, aniž by přitom byly kladeny vysoké nároky na síť.

Chcete-li přesměrovat složky, vytvořte v konzole Zásady skupiny (Group Policy) nový objekt zásad skupiny a pak rozbalte položky **Konfigurace uživatele** (User Configuration), **Nastavení systému Windows** (Windows Settings) a **Přesměrování složek** (Folder Redirection). Uvidíte ikony pěti osobních složek, které lze přesměrovat – Data aplikací (Application Data), Plocha (Desktop), Dokumenty (My Documents), Obrázky (My Pictures) a Nabídka Start (Start Menu). Chcete-li přesměrovat některou z těchto složek, klepněte pravým tlačítkem myši na její název, zadejte příkaz **Vlastnosti** (Properties) a pak vyberte jednu z následujících možností:

Základní Přesměrovat složky všech uživatelů na stejné místo sdílení v síti. Všechny složky ovlivněné tímto objektem zásad skupiny se uloží na stejné místo sdílení v síti.

Pokročilé Přesměrovat osobní složky na základě členství uživatelů ve skupinách se zabezpečením systému Windows 2000. Složky se přesměrují na různá místa sdílení v síti podle členství ve skupinách se zabezpečením. Například složky patřící uživatelům ve skupině Účtování mohou být přesměrovány na server Finance, zatímco složky patřící uživatelům ve skupině Prodej budou přesměrovány na server Marketing.

Po výběru základního nebo pokročilého nastavení musíte zadat jako umístění cílové složky název sdílené síťové složky, například: `\\Server\Složek\SložkyDokumenty\JménoUživatele`

Po zadání umístění cílové složky si zobrazte kartu **Nastavení** (Settings), nakonfigurujte na ní obsažené požadované volby a přesměrování složky dokončete stiskem tlačítka **Dokončit** (Finish).

Poznámka Předem nevytvářejte adresář definovaný jako *JménoUživatele*. Přesměrování složky nastaví na složku příslušné seznamy DACL.

Pokyny pro konfiguraci přesměrování složek

Přesměrováním složek můžete dokumenty zpřístupnit uživatelům podle potřeby. Dostupnost takových dokumentů můžete ještě zlepšit, když je zahrnete do svého časového plánu zálohování serveru.

Produkují-li cestovní uživatelské profily ve vaší organizaci příliš mnoho síťového provozu, zvažte přesměrování jen vybraných osobních složek, aby uživatele mezi různými počítači následovaly alespoň dokumenty, když už ne osobní nastavení.

Konfigurace synchronizování souborů offline

Většina organizací používá zálohovací procesy, zejména pro kritická data. V některých případech k vykonávání tohoto důležitého úkolu používají programy, jako je Systems Management Server, nebo výrobky jiných společností.

V mnoha případech jsou kritické datové soubory nebo složky souborů sdíleny mezi více uživateli, jako je tomu například u cestujících prodejců. Udržování aktuálních kopií všech těchto souborů či složek může být pro oddělení IT vážný problém.

Systém Windows 2000 nabízí nástroj Správce synchronizace (Synchronization Manager), který usnadňuje zajištění aktuálnosti kritických souborů a složek na klientských počítačích a síťových serverech a průběžné zálohování důležitých dat podle časového plánu.

Správce synchronizace je cenný zejména pro vzdálené nebo cestující uživatele, kteří se k síti připojují přerušovaně. Pomocí Správce synchronizace můžete řídit, kdy se soubory offline uživatelů synchronizují se soubory na síti. Tento proces je pro uživatele transparentní, protože ke svým souborům přistupují naprosto stejným způsobem, ať už jsou offline nebo online. Tím je zajištěno, že mají k dispozici nejnovější informace ze sítě, když je potřebují, a zároveň se minimalizují možná vyrušení, ke kterým by mohlo docházet při ztrátě dat na jejich místním počítači.

Správce synchronizace porovnává položky na síti s těmi, které uživatel otevřel nebo opravil při práci offline, a nejnovější verzi zpřístupní jak místnímu počítači tak i síti. Mezi položkami, které můžete synchronizovat, jsou jednotlivé soubory, celé složky a webové stránky offline. Správce synchronizace může automaticky synchronizovat informace, které jsou dostupné offline:

- kdykoli se uživatel přihlásí k síti nebo se odhlásí od sítě nebo v obou případech;
- v zadaných intervalech když je počítač nevyužitý, ale stále připojený k síti;
- v naplánovaných časech.

Kombinaci těchto a dalších možností lze použít pro soubory offline z různých sdílených zdrojů.

Správci mohou libovolnou sdílenou složku na síti označit tak, že má být dostupná i pro použití offline.

▼ Chcete-li umožnit použití offline nějaké sdílené složky, postupujte takto:

1. V Průzkumníku Windows klepněte pravým tlačítkem myši na složku, kterou chcete sdílet.
2. Klepněte na příkaz **Sdílení** (Sharing) a pak stiskněte tlačítko **Mezipaměť** (Caching).
3. Vyberte položku **Povolit použití mezipaměti pro soubory v této sdílené složce** (Allow caching of files in this shared folder), vyberte jednu z následujících možností a stiskněte tlačítko **OK**:
 - **Ruční ukládání dokumentů do mezipaměti (Manual caching for documents).** Uživatelé musí ručně zadat dokumenty, které se mají ukládat. Všechny vybrané soubory se budou automaticky ukládat.
 - **Automatické ukládání dokumentů do mezipaměti (Automatic caching for documents).** Ukládat bude možné celý obsah složky. Skutečně se však uloží pouze soubory, které uživatel otevřel. Výsledkem je menší síťový provoz než při ručním ukládání, kdy se ukládají všechny vybrané soubory, ať už byly otevřeny nebo ne.

- **Automatické ukládání programů do mezipaměti (Automatic caching for programs).** Omezuje síťový provoz, protože síťové verze dokumentů nebo programů se ukládají jen jednou; poté se používají kopie offline. Toto nastavení je určeno pro složky obsahující dokumenty, které jsou určeny pouze pro čtení, nebo aplikace, které jsou určeny ke spouštění ze sítě.

Pokyny pro konfiguraci souborů offline

Zásady skupiny vám poskytují mnoho možností správy složek offline ve vaší organizaci.

Nejprve můžete určit pomocí příkazů **Sdílení** a **Mezipaměť** (Sharing a Caching) určité složky, zda budou na určitém klientském počítači k dispozici dané složky offline. Při sdílení složky je výchozí režim mezipaměti nastaven na **Ruční ukládání dokumentů do mezipaměti**. Chcete-li uživatelům zabránit v ukládání složky do mezipaměti, zrušte zaškrtnutí políčka **Povolit použití mezipaměti pro soubory v této sdílené složce**.

Podobně můžete použít volbu neukládání souborů do mezipaměti (**Files not cached**) k určení určitých typů souborů (podle přípony), které se nebudou ukládat do mezipaměti. Tuto možnost lze použít například k zákazu přenášení velkých multimediálních souborů .avi tam a zpět přes síť.

Pomocí volby zákazu konfigurace synchronizace při odhlašování uživatelem (**Disable user configuration of logoff synchronization**) můžete zabránit uživateli v ruční změně výše popsaných možností synchronizace.

Další dvě možnosti, automatické synchronizace při odhlašování (**Automatic synchronization at logoff**) a zákazu synchronizace složek a souborů uživatelem (**Disable user synchronization of folders and files**), vám umožňují řídit, kdy dochází k synchronizaci, a nikoli které soubory se synchronizují. První volba určuje typ synchronizace (rychlá nebo úplná) vykonávané při odhlašování. Rychlá synchronizace synchronizuje soubory jednotlivě vybrané uživatelem. Plná synchronizace zároveň automaticky synchronizuje všechny soubory v mezipaměti. Možnost zákazu synchronizace složek a souborů uživatelem vám umožňuje určit, že k synchronizaci bude docházet pouze při vašem přihlašování a odhlašování.

Nastavení diskových kvót

Přestože ukládání dokumentů a profilů uživatelů na síti má své výhody, stačí jen několik uživatelů, kteří mohou snadno spotřebovat veškerý dostupný diskový prostor na serveru. Aby k tomu nemohlo dojít, můžete nakonfigurovat diskové kvóty, čímž zároveň vyrovnáte potřeby uživatelů na prostor k ukládání s náklady na přidání dalšího prostoru.

Diskové kvóty lze vytvářet podle jednotlivých uživatelů na jednotlivých svazcích. Jestliže profil nějakého uživatele překročí nastavenou velikost souboru, uživatel se nebude moci od počítače odhlásit, dokud neomezí velikost daného souboru. Kvóty jednotlivých uživatelů na jednotlivých svazcích mají dvě klíčové výhody:

- Když nastavíte kvóty na svazku, tyto kvóty platí pouze pro daný svazek. Jestliže si uživatelé ukládají soubory na více svazků systému souborů NTFS, můžete na každém svazku nakonfigurovat jiné kvóty.
- Kvóty se připisují osobě, která soubor vlastní. Proto jsou hranice vlastnictví jasně vyznačeny, i když nějaký uživatel sdílí určité své soubory s jinými uživateli.

Pokyny pro nastavení diskových kvót

Je důležité, abyste zajistili dostatek prostoru pro oprávněné požadavky uživatelů na ukládání souborů a abyste nenutili společnost zbytečně přidávat servery pro soubory, které mohou uživatelé poslat na sdílené místo na síti. Neptejte se přímo uživatelů, kolik diskového prostoru potřebují, ale raději sami na základě počátečních pilotních zavedení zjistěte smysluplná data ukazující, jaký diskový prostor uživatelé skutečně požadují.

Pamatujte, že všichni uživatelé nemají stejné požadavky na diskový prostor. Například vývojáři softwaru vyžadují větší diskový prostor v síti než jiní uživatelé. Finanční a techničtí uživatelé představují další dvě skupiny uživatelů, které mají často větší počet rozsáhlejších souborů než ostatní uživatelé.

Chcete-li nastavit efektivní diskové kvóty ve vaší organizaci, ještě před zavedením přísných kvót se seznámte s legitimními požadavky uživatelů.

Informace o nastavení a používání diskových kvót najdete v kapitole „Určení strategií správy úložišť systému Windows 2000“ v této knize.

Výběr možností správy změn a konfigurací vaší organizace

Chcete-li připravit plán implementace změn a konfigurací, budete muset rozhodnout, které funkce zajišťují největší výhody pro jednotlivé skupiny uživatelů, a jak je zapotřebí tyto funkce nakonfigurovat.

Přemýšlejte o výše popsaných možnostech správy změn a konfigurací jako o současech, které můžete zavést, aby se zlepšily služby uživatelům. Některé stavební bloky mohou zajistit typickým organizacím základní podporu, jiné zase poskytují pokročilejší podporu.

Chcete-li dokončit plán funkcí IntelliMirror a vzdálené instalace:

- definujte, které funkce se budou používat pro základní správu změn a konfigurací a které pro pokročilou správu změn a konfigurací;
- definujte, jak nejlépe naplní základní a pokročilé možnosti správy změn a konfigurací potřeby typů uživatelů ve vaší organizaci;
- shrňte, jak bude správa změn a konfigurací naplňovat potřeby vaší organizace.

Následující oddíly jsou příklady možných implementací funkcí IntelliMirror a vzdálené instalace v plánu změn a konfigurací. V závislosti na vašich potřebách mohou být některé možnosti označené v dalších oddílech za pokročilé ve skutečnosti pro vaši organizaci základní, zatímco jiné možnosti označené za základní mohou být v jiné organizaci považovány za pokročilé. Budete muset definovat základní a pokročilé požadavky a implementace pro svou organizaci.

Přehled základních a pokročilých možností

Následující možnosti použití mohou obsluhovat základní požadavky na správu uživatelských dat:

- Poskytněte uživatelům soukromá místa sdílení na síti a připojte jejich složky Dokumenty (My Documents) k tomuto sdílenému místu.

- Jako součást tohoto místa sdílení zahrňte také pracovní plochu, aby se dokumenty ukládané na plochu uložily také na dané místo sdílení na síti.
- Poskytněte uživatelům veřejná místa sdílení na síti. Takové místo sdílení může sloužit jedinému uživateli nebo pracovní skupině.
- Na sdílená místa, zejména na místa jednotlivých uživatelů, zaveďte kvóty.
- Pro sdílená místa, zejména pro místa jednotlivých uživatelů, zajistěte služby zálohování a obnovení.
- Povolte složky offline na sdílených místech zahrnujících soukromá data.
- Povolte použití Správce synchronizace (Synchronization Manager) pro obvyklé typy dat.

Při zavádění pokročilé správy uživatelských dat se zamyslete nad implementací následujících funkcí:

- Pro uživatele používající více počítačů implementujte cestovní uživatelské profily.
- Zajistěte, aby došlo k vyprázdnění cestovního uživatelského profilu a mezipaměti poté, co cestující uživatel opustí nějaký počítač.

V rámci základní správy nastavení zvažte poskytnutí těchto možností:

- Ustanovte základní zásady řízení pracovní plochy nebo prostředí.
- Ustanovte základní zásady řízení zabezpečení (viz kapitola „Plánování distribuovaného zabezpečení“ v této knize).
- Definujte přihlašovací skripty.
- Na jednoho uživatele nebo počítač neaplikujte více než pět či šest objektů zásad skupiny. (Další informace o použití a aplikování zásad skupiny při správě clientských konfigurací najdete v kapitole „Definování standardů správy a konfigurace klientů“ v této knize.)
- Definujte standardní uživatelský profil pro nové uživatele s cestovními profily. Tento výchozí profil existuje na serveru a kopíruje se na počítač při prvním přihlášení uživatele.

V rámci pokročilé správy nastavení zvažte poskytnutí těchto možností:

- Nakonfigurujte zásady skupiny na přísné omezení přístupu k místům uložení systémových souborů.
- Nakonfigurujte zásady skupiny, které zabrání uživatelům ve spouštění neschváleného softwaru.

V rámci základní instalace a údržby softwaru zvažte použití těchto možností:

- Umožněte uživatelům používat po celý životní cyklus aplikace ovládací panel Přidat nebo odebrat programy (Add/Remove Programs).
- Zabraňte uživatelům v instalování softwaru pomocí disku CD.
- Publikujte existující aplikace používající službu Windows Installer ve formě „částečné instalace/instalace na požádání“.
- K úpravě chování balíčku používejte transformace.
- Publikujte nebo přiřazujte inovace operačního systému.
- K inovaci aplikací používejte zásady skupiny.

V rámci pokročilé instalace a údržby softwaru zvažte použití těchto možností:

- Vytvořte distribuční body podporující systém DFS.
- Distribuční body DFS spravujte pomocí serveru Systems Management Server.

Následující oddíly ukazují plány správy změn a konfigurací pro několik různých typů uživatelů.

Naplnění potřeb technických uživatelů

Techničtí uživatelé, jako jsou například vývojáři, často musí být správci svých vlastních počítačů. Obvykle jsou spokojeni, když jim oddělení IT poskytuje služby správy, ale přitom mají možnost řídit svůj vlastní počítač.

Těmto uživatelům může správa změn a konfigurací systému Windows 2000 zjednodušit instalaci počítačů a minimalizovat možnost ztráty osobních dat.

Následující základní a pokročilé možnosti ilustrují, jak může být správa změn a konfigurací aplikována na technické uživatele:

- **Základní správa uživatelských dat.** Můžete aplikovat všechny aspekty. Přesměrujte složku Dokumenty (My Documents), zejména v případě uživatelů přenosných počítačů. Nepřesměřovávejte pracovní plochu. Povolte složky offline na sdíleném místě Dokumenty.
- **Pokročilá správa uživatelských dat.** Někteří techničtí uživatelé mohou chtít používat cestovní uživatelské profily. Zároveň budou chtít ponechat oprávnění místní správy.
- **Základní správa nastavení.** Na jejich konfigurace zaveďte co nejmenší počet omezení.
- **Pokročilá správa nastavení.** Žádná.
- **Základní instalace a údržba softwaru.** Můžete aplikovat všechny aspekty. Publikované aplikace a funkce vzdálené instalace nabízejí mnoho výhod, aniž by zbavovaly technické uživatele řízení.
- **Pokročilá instalace a údržba softwaru.** Nic nepřipražujte ani nezavádějte žádnou formu řízení.
- **Pokročilá funkce vzdálené instalace.** Umožněte přístup k pokročilým instalačním možnostem. Je-li to nutné, zpřístupněte uživateli všechny možné instalační obrazy (bitové kopie).

Naplnění potřeb stacionárních profesionálních uživatelů

Stacionární profesionální uživatelé obvykle ocení určité služby správy, pokud nabízejí nějakou hodnotu a neodebírají jim příliš velkou část řízení.

Těmto uživatelům poskytují funkce vzdálené instalace a IntelliMirror nejjednodušší možnou metodu nastavení jejich počítačů, zálohování dat a nejlepší kombinaci funkcí pro nejobvyklejší použití.

Následující základní a pokročilé plány ilustrují, jak může být správa změn a konfigurací aplikována na stacionární profesionální uživatele:

- **Základní správa uživatelských dat.** Můžete aplikovat všechny aspekty. Lze přesměrovat pracovní plochu. Pro tuto skupinu je také výhodné zřídit místní soukromé úložiště.
- **Pokročilá správa uživatelských dat.** Někteří uživatelé mohou chtít používat cestovní uživatelské profily. Pro vyšší řídicí pracovníky bude také vhodné zavést šifro-

vaný systém souborů. Uvědomte si však, že zašifrované soubory a složky nelze zahrnout do cestovního uživatelského profilu. Zašifrované soubory a složky však lze přesměrovat.

- **Základní správa nastavení.** Lze tolerovat menší počet omezení. Tito uživatelé nemohou fungovat jako místní správci.
- **Pokročilá správa nastavení.** Je v pořádku, budete-li řídit stav počítače a přístup k němu. To však bude často vyžadovat vytvoření místní složky Dokumenty (My Documents), jsou-li síťové kvóty nízké.
- **Základní instalace a údržba softwaru.** Aplikujte všechny aspekty včetně publikování aplikací. Pro volitelné funkce použijte instalaci na požádání.
- **Pokročilá instalace a údržba softwaru.** Přiřazení aplikací používejte jen výjimečně.
- **Základní funkce vzdálené instalace.** Proces co nejvýše zjednodušte omezením možností instalací a dostupných obrazů (bitových kopií).

Naplnění potřeb cestujících profesionálních uživatelů

Cestující profesionální uživatelé se velmi podobají stacionárním profesionálům a třebaže používají více počítačů, také mají obvykle nějaký hlavní počítač.

Těmto uživatelům musí být k dispozici nenáročné funkce podpory cestování, které by neměly představovat žádné dodatečné náklady nad rámec stacionárního používání.

Následující plán ilustruje, jak může být základní a pokročilá správa změn a konfigurací aplikována na cestující profesionální uživatele:

- **Základní správa uživatelských dat.** Můžete aplikovat všechny aspekty. Pro tuto skupinu je důležité zřídit místní soukromé úložiště. Pracovní plocha by měla být přesměrována.
- **Pokročilá správa uživatelských dat.** Je nutné zavést cestovní uživatelské profily. Pro vyšší řídící pracovníky bude také vhodné zavést šifrovaný systém souborů. Uvědomte si však, že zašifrované soubory a složky nelze zahrnout do cestovního uživatelského profilu. Zašifrované soubory a složky však lze přesměrovat.
- **Základní správa nastavení.** Lze tolerovat menší počet omezení. Tito uživatelé nejsou místními správci.
- **Pokročilá správa nastavení.** Je v pořádku, budete-li řídit stav počítače a přístup k němu. To však bude často vyžadovat vytvoření místní složky Dokumenty (My Documents), jsou-li síťové kvóty nízké.
- **Základní instalace a údržba softwaru.** Můžete aplikovat všechny aspekty. Lze také použít publikování aplikací, ale pouze pokud je možné aplikace spouštět ze sítě, aby se aplikace nemusely instalovat na místní počítač. Pro volitelné funkce použijte instalaci na požádání.
- **Pokročilá instalace a údržba softwaru.** Přiřazení aplikací používejte jen výjimečně. Aplikace přiřazujte pouze uživatelům a nikoli počítačům.
- **Základní funkce vzdálené instalace.** Úplně odstraňte veškerý přístup uživatelů k možnostem vzdálené instalace, aby mohly instalace vykonávat pouze osoby správy nebo technické podpory. Alternativně mohou být možnosti vzdálené instalace omezeny tak, aby byla instalace úplně automatická.

Naplnění potřeb mobilních profesionálních uživatelů

Mobilní uživatelé budou s výhodou používat nové funkce systému Windows 2000, jako je Správce synchronizace (Synchronization Manager), šifrovaný systém souborů, ukládání dat do mezipaměti na straně klienta a technologie Plug-and-Play.

Tito uživatelé obvykle používají notebook i hlavní desktopový počítač.

Následující položky ilustrují, jak může být správa změn a konfigurací aplikována na mobilní profesionální uživatele:

- **Základní správa uživatelských dat.** Můžete aplikovat všechny aspekty. Pracovní plocha by neměla být přesměrována. Pro tuto skupinu je důležité zřídit místní soukromé úložiště. Ideální volbou pro tuto skupinu jsou také přesměrované a offline složky.
- **Pokročilá správa uživatelských dat.** Cestovní uživatelské profily se normálně používají. Má-li však uživatel jen jeden počítač, pak není cestovní uživatelský profil zapotřebí, snad jen pro účely zajištění ochrany dat. Také bude vhodné zavést šifrovaný systém souborů.
- **Základní správa nastavení.** Lze tolerovat menší počet omezení. Tito uživatelé nejsou místními správci.
- **Pokročilá správa nastavení.** Uživatelé mají často větší kontrolu nad notebooky, což je dáno jejich vzdáleností od správců.
- **Základní instalace a údržba softwaru.** Můžete aplikovat všechny aspekty. Lze také použít publikování aplikací, ale pouze pokud je možné aplikace instalovat místně. Pro volitelné funkce nepoužívejte instalaci na požádání.
- **Pokročilá instalace a údržba softwaru.** Aplikace můžete přiřazovat, ale pouze pokud se budou instalovat místně. Umožněte uživatelům instalovat z místního zdroje, jako je jednotka CD, kdy jsou odpojeni od bodů distribuce softwaru.
- **Pokročilé funkce vzdálené instalace.** Funkce vzdálené instalace podporuje přenosné počítače, pouze když jsou připojeny k síti přes dokovací stanici obsahující paměť ROM vzdáleného přístupu nebo obsahují podporovanou síťovou kartu. U uživatelů, kteří dok vůbec nepoužívají nebo je používají jen výjimečně, takže není možné používat funkci vzdálené instalace, zvažte aplikování alternativních řešení a procedur opakované instalace operačního systému.

Naplnění potřeb uživatelů s konkrétními úkoly

Uživatelé s konkrétními úkoly obvykle nemají žádný počítač, který by mohli považovat za svůj. Když se od počítače odhlásí, neměly by po nich zůstat žádné datové soubory nastavení počítače. Tito uživatelé nemohou instalovat žádné aplikace, vytvářet soubory mimo svá sdílená místa na síti nebo měnit správcem nakonfigurovaný stav místního počítače. V některých případech mohou být takové počítače klienty terminálových služeb (Terminal Services) systému Windows.

Následující položky ilustrují, jak může být správa změn a konfigurací aplikována na uživatele s konkrétními úkoly:

- **Základní správa uživatelských dat.** V prostředích, která nejsou ve stylu kiosků, můžete aplikovat všechny aspekty. Pracovní plocha je přesměrována. Nejsou tu žádná místní úložiště. V případě kiosků se po odhlášení uživatele odstraňují místní profily.

- **Pokročilá správa uživatelských dat.** Cestovní uživatelské profily se používají, pouze pokud se nejedná o prostředí kiosků. Na počítači by neměla zůstat žádná data.
- **Základní správa nastavení.** Pracovní plocha je přesměrována. Nastavení počítače jsou přísně řízena.
- **Pokročilá správa nastavení.** Pracovní plocha je přesměrována. Nastavení počítače jsou přísně řízena.
- **Základní instalace a údržba softwaru.** Většina aplikací se instaluje podle počítače (a nikoli podle uživatele). Je-li zapotřebí používat aplikace přiřazené uživateli, měly by se spouštět ze sítě.
- **Pokročilá instalace a údržba softwaru.** Aplikace jsou pouze přiřazeny. Zakažte instalaci softwaru ze všech jiných míst než ze sítě.
- **Základní funkce vzdálené instalace.** Úplně odstraňte veškerý přístup uživatelů k možnostem vzdálené instalace, aby mohly instalace vykonávat pouze osoby správy nebo technické podpory. Alternativně mohou být možnosti instalace omezeny tak, aby byla instalace operačního systému úplně automatická.

Souhrn

Tabulka 24.6 ukazuje příklad strategie správy změn a konfigurací pro velkou organizaci s více typy uživatelů.

Tabulka 24.6 Ukázková strategie správy změn a konfigurací

Klasifikace uživatele	Správa uživatelských dat	Správa uživatelských nastavení	Instalace a údržba softwaru	Vzdálená instalace OS
Technický	Základní	Základní (bez zamknutí)	Základní	Pokročilá
Stacionární profesionál	Základní	Základní	Pokročilá	Základní
Cestující profesionál	Pokročilá	Základní	Pokročilá	Základní
Mobilní profesionál	Pokročilá	Základní	Pokročilá	Pokročilá
Uživatel s konkrétními úkoly	Pokročilá	Pokročilá	Pokročilá	Základní

Pro správu uživatelských dat použijte tyto pokyny:

- Základní správa uživatelských dat může být užitečná ve společnostech, které spravují klientské počítače pouze na střední úrovni.
- Pokročilá správa uživatelských dat závisí na typech uživatelů, zejména ve vysoce spravovaných prostředích a je-li zaručena vysoká úroveň služeb (například pro vysoké řídící pracovníky).

Pro správu uživatelských nastavení byly aplikovány tyto zásady:

- Základní správa nastavení bude používána převážně v organizacích se středně spravovanými klientskými počítači a nejčastěji se bude aplikovat na vysoce spravované klientské počítače. Nejvíce se bude používat pro personál administrativy.
- Pokročilá správa nastavení se bude používat především ve vysoce spravovaných prostředích, kde jsou problémem náklady na podporu, jako jsou školy, nemocnice a výrobní haly.

Pro instalaci a údržbu softwaru byly aplikovány tyto zásady:

- Základní instalace a údržba softwaru se stane standardní praxí, zejména pokud jde o publikování softwaru v organizaci.
- Pokročilá instalace a údržba softwaru se bude používat převážně ve vysoce spravovaných prostředích, kde jsou problémem náklady na podporu, jako jsou kiosky, školy, nemocnice a výrobní haly.

Pro vzdálenou instalaci operačního systému byly aplikovány tyto zásady:

- Základní vzdálená instalace operačního systému se bude používat, když jsou možnosti uživatelů omezené nebo vysoce automatizované. Mají-li uživatelé možnost vykonávat vzdálené instalace, měli by jen inicializovat vzdálenou instalaci při spouštění systému a pak zadat své jméno a heslo.
- Pokročilá vzdálená instalace operačního systému se bude používat, když si může uživatel vybrat, který obraz operačního systému se nainstaluje a jak se nainstaluje, nebo když speciální podmínky ospravedlňují potřebu zavedení dalších voleb pro uživatele vykonávající instalaci.

Seznam úkolů plánování správy změn a konfigurací

Tabulka 24.7 shrnuje úkoly, které musíte splnit při vytváření plánu správy změn a konfigurací systému Windows 2000.

Tabulka 24.7 Seznam úkolů plánování správy změn a konfigurací

Úkol	Umístění v kapitole
Definujte potřeby správy změn a konfigurací pro uživatele a organizaci.	Vyhodnocení správy změn a konfigurací
Vyhodnoťte a vyberte potřebné funkce správy změn a konfigurací systému Windows 2000.	Vyhodnocení správy změn a konfigurací
Naplánujte použití funkce vzdálené instalace k instalaci systému Windows 2000.	Umožnění funkce vzdálené instalace
Nakonfigurujte zásady skupiny umožňující instalaci a správu softwaru funkcemi IntelliMirror.	Zlepšení správy softwaru pomocí zásad skupiny
Nakonfigurujte sdílená místa na serveru a zásady skupiny pro správu uživatelských dat.	Převedení uživatelských dat a nastavení na síť
Nakonfigurujte sdílená místa na serveru a zásady skupiny pro správu uživatelských nastavení.	Převedení uživatelských dat a nastavení na síť

KAPITOLA 25

Automatizování instalace a inovace klientů

Nyní jste připraveni vyvinout a vykonat automatizovanou instalaci systému Windows 2000 Professional a přidružených aplikací. To je základní požadavek uskutečnění všech fází zavedení – testování, pilotních programů i vlastního postupného zavádění do výrobního procesu. V této kapitole najdete popis dostupných metod automatizované instalace včetně požadavků na přípravu a ukázkových konfigurací. Doporučujeme, aby se s touto kapitolou seznámili zejména síťoví technici účastníci se návrhu procesu instalace a správci systému účastníci se instalace systému Windows 2000 a přidružených aplikací.

Instalace systému Windows 2000 Professional může být buď čistá na počítače, na nichž není instalována žádná verze operačního systému dřívějšího než Windows 2000, nebo čistá instalace či inovace na počítačích, na kterých v současné době běží systémy Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows NT Workstation verze 3.51 nebo Microsoft Windows NT Workstation verze 4.0. Při určování, zda vykonáte čistou instalaci nebo inovaci musíte vyřešit důležité otázky plánování, jak je popisuje kapitola „Přehled plánování“ v této knize.

V této kapitole

Rozhodnutí mezi inovací a čistou instalací 746

Příprava instalace 748

Automatizování instalace klientských aplikací 762

Automatizování instalace systému Windows 2000 Professional 766

Příklady konfigurace instalace 783

Seznam úkolů plánování instalace 787

Cíle kapitoly

Tato kapitola vám pomůže s vývojem následujícího dokumentu plánování:

- Plán automatizované instalace

Související informace v sadě Resource Kit

- Další informace o plánování najdete v kapitole „Přehled plánování“ v této knize.
- Chcete-li získat dodatečné informace o automatizování instalací serverů, podívejte se do kapitoly „Automatizování instalace a inovace serveru“ v této knize.

- Další informace o správě klientských počítačů najdete v kapitole „Definování standardů správy a konfigurace klientů“ v této knize.
- Další informace o parametrech bezobslužné instalace, na něž se tato kapitola odvolává, najdete v dokumentu „Microsoft Windows 2000 Guide to Unattended Setup“ (Unattend.doc) na CD operačního systému Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.
- Další informace o bezobslužné instalaci a ukázkové soubory odpovědí najdete v příloze „Příklady souborů odpovědí pro bezobslužnou instalaci“ v této knize.

Rozhodnutí mezi inovací a čistou instalací

V podnikovém prostředí není z hlediska nákladů výhodné instalovat systém Windows 2000 pomocí standardního interaktivního instalačního programu na každém jednotlivém počítači. Výrazného snížení celkových nákladů na vlastnictví (total cost of ownership – TCO) dosáhnete automatizovanými instalacemi systému Windows 2000 Professional na více počítačů.



Důležité rozhodnutí Před zautomatizováním instalace systému Windows 2000 Professional musíte rozhodnout, zda půjde o inovaci ze systému Windows NT nebo o čistou instalaci.

Následující dvě položky vám pomohou určit, zda je lepší vykonat inovaci nebo čistou instalaci.

- Jestliže již vaše organizace implementovala nějaký operační systém Windows a vaše oddělení informačních technologií (IT) je spravováno centrálně, bude lepší vykonat inovaci. Plánujete-li vytvoření nějakého spravovaného prostředí, ale zatím takové ve své organizaci nemáte, pak bude lepší zadat čistou instalaci, aby bylo možné během instalace implementovat standardní konfigurace.
- Plánujete-li používat již existující hardware a softwarové aplikace, pak budete muset učinit inovaci. Jestliže však předpokládáte koupi nového hardwaru a instalaci nových softwarových aplikací, budete muset zadat čistou instalaci.

Řešení kritických problémů

Plánujete-li instalovat systém Windows 2000 Professional na počítače, na nichž ještě není instalován žádný dřívější operační systém Windows, je zřejmé, že půjde o čistou instalaci. Jestliže na počítačích již běží systém Windows 95, Windows 98, Windows NT Workstation 3.51 nebo Windows NT Workstation 4.0, budete muset určit, zda je z hlediska nákladů výhodnější inovovat existující operační systém nebo vykonat čistou instalaci.

Typické problémy plánování shrnuje tabulka 25.1.

Tabulka 25.1 Problémy plánování, které musí být vyřešeny před inovací nebo instalací

Problém	Úkol
Cíle organizace	Určete hlavní cíle své organizace.
Regionální potřeby	Identifikujte specifické regionální potřeby a určete, zda jsou součástí vašeho podniku také zahraniční pobočky nebo společnosti.
Skupiny uživatelů	Analyzujte skupiny uživatelů včetně jejich specifických kategorií a potřeb, znalost problematiky počítačů a zkušenosti uživatelů, požadavky na zabezpečení a umístění uživatelů a jejich problémy se síťovým propojením včetně rychlosti propojení.
Potřeby aplikací	Určete, které produkty budou předběžně instalovány na všech počítačích, které produkty budou inzerovány jenom určitým uživatelům a které produkty se budou distribuovat specifickým kategoriím uživatelů.
Strategie počítačů/uživatelů	Vyhodnoťte aktuální nastavení uživatelů a úložišť dat, určete požadavky migrování uživatelských nastavení a vyhodnoťte nutné, cestovní a místní profily.
Hardware	Zinventarizujte existující hardware a stanovte potřeby nového hardwaru. Před inovací nebo instalací určete minimální požadavky na hardware. Naplánujte budoucí potřeby počítačů. Určete, jak se budou počítače pohybovat organizací. Zjistěte, zda lze všechny počítače spustit z kompaktních disků.
Rizikové a problémové oblasti	Určete potencionální rizika včetně nekompatibility aplikací se systémem Windows 2000, problémy s časovým plánem, více síťovými lokacemi, necentralizovaným rozpočtem nebo dopad možných budoucích slučování.
Očekávání růstu	Určete očekávaný růst v období projektu po jednom roce, třech a pěti letech. Vezměte v úvahu také plánovaná sloučení, nová síťová sídla, země atd.
Síťové záležitosti	Zjistěte, zda mají vzdálená síťová místa servery zavádění aplikací. Určete, jak se inovují servery mimo centrální sídlo.
Správa softwaru	Rozhodněte, zda již funguje nějaký systém správy softwaru, například server Microsoft Systems Management Server, v němž lze zavádění naplánuvat.
Konektivita	Určete, zda je možné servery a propojení mezi nimi nastavit tak, aby mohly distribuovat velké balíčky všem uživatelům ve společnosti.

Volba metody instalace

Po vyřešení důležitých problémů plánování můžete vybrat metody použité k automatizování instalací. Tabulka 25.2 uvádí metody automatizovaných instalací a popisuje, zda je lze použít k inovaci, k čisté instalaci, nebo v obou případech.

Tabulka 25.2 Metody automatizované instalace

Metoda	Verze systému Windows 2000	Inovace	Čistá instalace
Syspart	Server a Professional	Ne	Ano
Sysprep	Server a Professional	Ne	Ano
SMS	Server a Professional	Ano	Ano
Spustitelné CD	Server a Professional	Ne	Ano
Vzdálená instalace operačního systému	Professional	Ne	Ano

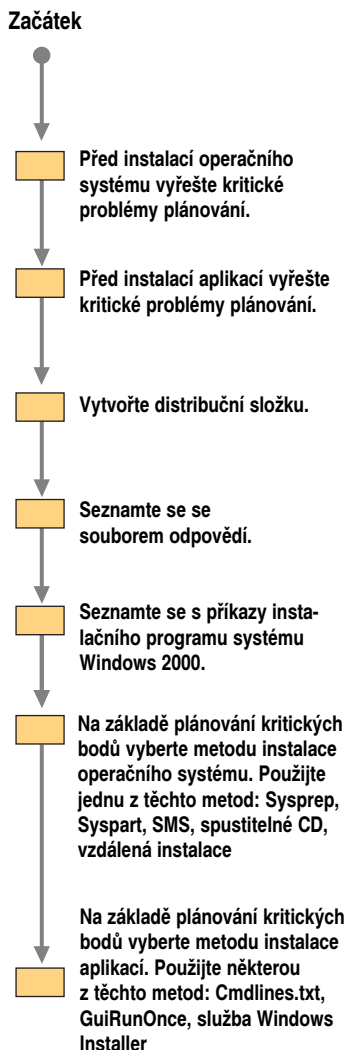
Příprava instalace

Během přípravy na čistou instalaci systému Windows 2000 Professional musíte učinit toto:

- Vytvořit distribuční složku.
- Pochopit použití souboru odpovědí.
- Pochopit příkazy instalačního programu systému Windows 2000.

Poznámka Principy vykonání automatizované instalace popsané v tomto oddílu platí pro čisté instalace i inovace. Nejobvyklejší je vykonat čistou instalaci.

Obrázek 25.1 je vývojový graf instalačního procesu.



Obrázek 25.1 Vývojový graf automatizované instalace

Vytváření distribučních složek

Chcete-li instalovat systém Windows 2000 Professional na více počítačů v síti, musíte vytvořit alespoň jednu sadu distribučních složek. Distribuční složky se obvykle nacházejí na serveru, kam se počítače mohou připojit a odkud si mohou spuštěním souboru Winnt.exe nebo Winnt32.exe na cílovém počítači nainstalovat systém Windows 2000. Jednu sadu distribučních složek lze používat pro různé implementace systému s různými soubory odpovědí. I když budete jako metodu instalace používat vytváření obrazů (bitových kopií) disku, počáteční použití distribučních složek zajistí konzistentní implementaci pro různé typy systémů. Kromě toho můžete používat distribuční složky k aktualizaci budoucích obrazů změnou souborů v distribučních složkách nebo změnou

souborů odpovědí a vytvořením nových obrazů a nemusíte tedy začínat znovu od začátku.

Chcete-li vyrovnat zatížení serverů a urychlit fázi kopírování instalačního programu systému Windows 2000 u počítačů se spuštěnými systémy Microsoft Windows 95, Windows 98, Windows NT nebo Windows 2000, vytvořte distribuční složky na více serverech. Soubor Winnt32.exe pak můžete spustit až s osmi umístěními zdrojových souborů. Další informace o příkazech instalačního programu najdete v oddílu „Přehled příkazů instalačního programu systému Windows 2000“ dále v této kapitole.

Poznámka V této kapitole označuje termín „Windows NT“ jak systém Microsoft Windows NT 3.51 tak i systém Microsoft Windows NT 4.0.

Distribuční složky obsahují instalační soubory systému Windows 2000 Professional a další ovladače zařízení a soubory potřebné k instalaci.

S automatizováním procesu vytvoření distribuční složky vám pomůže Správce instalace (Setup Manager), nástroj nacházející se na CD systému Windows 2000 Professional CD. Další informace o Správci instalace najdete v oddílu „Vytvoření souboru odpovědí“ dále v této kapitole.

Poznámka V této kapitole je „instalační program systému Windows 2000“ také zkráceně označován za „instalační program“.

▼ **Chcete-li vytvořit distribuční složku, postupujte takto:**

1. Připojte se k síťovému serveru, na němž chcete distribuční složku vytvořit.
2. Vytvořte ve sdílené oblasti síťového serveru složku \i386.

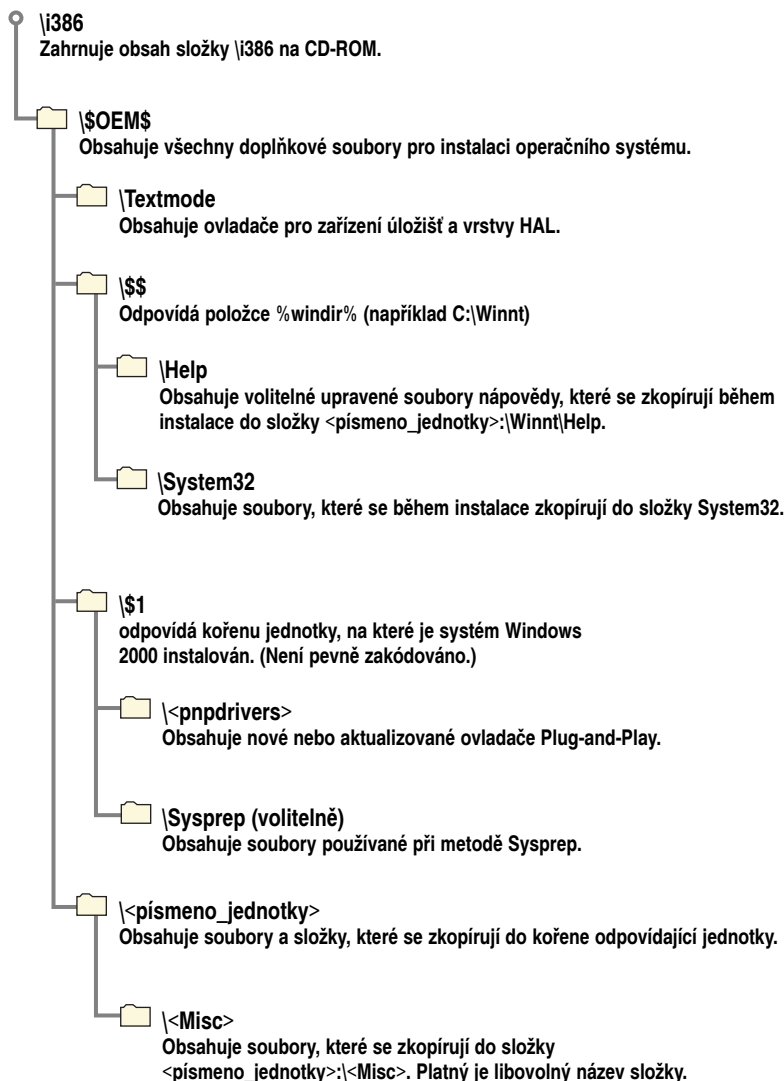
Chcete-li odlišit různé sdílené distribuce různých verzí systému Windows 2000 (mezi Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server a jednou pro Microsoft Windows 2000 Advanced Server), můžete vybrat jiný název této složky. Plánujete-li používat lokalizované jazykové verze systému Windows 2000 v zahraničních pobočkách, můžete vytvořit samostatné sdílené distribuce pro jednotlivé lokalizované verze.

3. Zkopírujte obsah složky \i386 z CD systému Windows 2000 Professional do právě vytvořené složky.
4. V právě vytvořené složce vytvořte podsložku nazvanou \ \$OEM\$.

Podsložka \ \$OEM\$ zajišťuje potřebnou strukturu složek pro doplňkové soubory kopírované během instalace na cílový počítač. Mezi tyto soubory patří ovladače, nástroje, aplikace a všechny další soubory potřebné k zavedení systému Windows 2000 Professional ve vaší organizaci.

Vytvoření struktury distribuční složky

Ukázka struktury distribuční složky je uvedena na obrázku 25.2.

**Obrázek 25.2 Příklad struktury distribuční složky**

\i386

Toto je distribuční složka obsahující všechny soubory potřebné k instalaci systému Windows 2000. Tuto složku vytvoříte v kořenu sdílené jednotky tak, že zkopírujete obsah složky \i386 na CD systému Windows 2000 Professional do distribuční složky.

\SOEM\$

Podsložku \SOEM\$ vytvoříte v distribuční složce přímo pod složkou \i386. Během instalace můžete do podsložky \SOEM\$ automaticky zkopírovat adresáře, standardní soubory ve formátu 8.3 a další nástroje vyžadované vašim procesem automatizované instalace.

Pokud v souboru odpovědí použijete klíč OEMFILESPATH, můžete pak vytvořit podsložku \ \$OEM\$ i mimo distribuční složku. Soubor odpovědí je popsán v oddílu „Přehled souboru odpovědí“ dále v této kapitole. Dodatečné informace o parametrech a syntaxi souboru odpovědí najdete v dokumentu „Microsoft Windows 2000 Guide to Unattended Setup“ (Unattend.doc) na CD operačního systému Microsoft Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

Podsložka \ \$OEM\$ může obsahovat volitelný soubor Cmdlines.txt, v němž je uveden seznam příkazů spuštěných během té části instalačního programu, která pracuje v grafickém uživatelském rozhraní (Graphical User Interface – GUI). Tyto příkazy lze použít k instalování dalších nástrojů, které mají být součástí vaší instalace. Další informace o souboru Cmdlines.txt najdete v oddílu „Použití souboru Cmdlines.txt“ dále v této kapitole.

Jestliže instalační program najde v kořenu distribučního bodu podsložku \ \$OEM\$, zkopíruje všechny soubory v tomto adresáři do dočasného adresáře, který se vytváří v textové části instalačního programu.

Poznámka V této kapitole označujeme část instalačního programu s grafickým rozhraním za „grafický režim“ a část instalačního programu s textovým rozhraním za „textový režim“.

\ \$OEM\$\Textmode

Podsložka \ \$OEM\$\Textmode obsahuje nové nebo aktualizované soubory instalace ovladačů zařízení hromadného ukládání dat a vrstev abstrakce hardwaru (HAL). Tyto soubory mohou zahrnovat OEM vrstvy HAL, ovladače zařízení SCSI a soubor Txtsetup.oem, který řídí nahrávání a instalaci těchto komponent.

Nezapomeňte na soubor Txtsetup.oem. Všechny soubory umístěné v podsložce \ \$OEM\$\Textmode (vrstvy HAL, ovladače a Txtsetup.oem) musí být uvedeny v oddílu [OEMBootFiles] souboru odpovědí.

\ \$OEM\$\\$\$

Podsložka \ \$OEM\$\\$\$ odpovídá proměnným prostředí %systemroot% a %windir%. Tato podsložka obsahuje další soubory, které chcete zkopírovat do různých podsložek instalačního adresáře Windows 2000. Struktura této podsložky musí odpovídat standardní struktuře instalace systému Windows 2000, přičemž \ \$OEM\$\\$\$ odpovídá %systemroot% nebo %windir% (například C:\Winnt), \ \$OEM\$\\$\System32 odpovídá %windir%\System32 atd. Každá podsložka musí obsahovat soubory, jež se zkopírují do odpovídající složky na cílovém počítači.

\ \$OEM\$\\$1

Podsložka \ \$OEM\\$1 je v systému Windows 2000 novinkou a ukazuje na jednotku, kam se systém nainstaluje. Označení **\$1** odpovídá systémové proměnné %systemdrive%. Instalujete-li například systém Windows 2000 na jednotku D, \ \$OEM\\$1 ukazuje na jednotku D.

\ \$OEM\\$1\Pnpdrivers

Podsložka \ \$OEM\\$1\Pnpdrivers je v systému Windows 2000 novinkou a umožňuje vám do distribučních složek umístit nové nebo aktualizované ovladače zařízení

Plug-and-Play. Tyto složky se zkopírují na místo %systemdrive%\Pnpdrivers na cílovém počítači. Když do svého souboru odpovědí přidáte parametr OemPnPDriversPath, řeknete tak systému Windows, aby hledal (během instalace i po ní) nové a aktualizované ovladače zařízení Plug-and-Play nejen ve složkách původních součástí systému, ale také ve vámi vytvořených složkách. Parametr *Pnpdrivers* můžete nahradit názvem s osmi nebo méně znaky.

\\$OEM\$\\$1\Sysprep

Podsložka \\$OEM\\$1\Sysprep je volitelná. Tato podsložka obsahuje soubory, které jsou zapotřebí ke spuštění nástroje Sysprep. Tyto soubory jsou popsány v oddílu „Duplikování disků pomocí nástroje Sysprep“ dále v této kapitole.

\\$OEM\$\Pismoeno_jednotky

V textovém režimu se struktura jednotlivých podsložek \\$OEM\$\Pismoeno_jednotky zkopíruje do kořene odpovídající jednotky na cílovém počítači. Například soubory umístěné do podsložky \\$OEM\$\D se zkopírují do kořene jednotky D. Je také možné vytvářet podsložky v rámci těchto podsložek. Například po zadání \\$OEM\$\E\Misc vytvoří instalační program na disku E podsložku \Misc.

Soubory, které je zapotřebí přejmenovat, musí být uvedeny v souboru \$\$Rename.txt. Další informace o přejmenovávání souborů najdete v oddílu „Převod délky názvu souboru pomocí souboru \$\$Rename.txt“ dále v této kapitole. Pamatujte, že soubory v distribučních složkách musí mít krátké názvy (formátu 8.3).

Instalace zařízení hromadného ukládání dat

V systému Windows 2000 technologie Plug-and-Play detekuje a instaluje většinu hardwarových zařízení, které je možné později během instalace nahrát. Zařízení pro hromadné ukládání dat, například pevné disky, však musí být řádně nainstalovány, aby byla v grafickém režimu dostupná plná podpora technologie Plug-and-Play.

Poznámka Zařízení nemusíte zadávat, pokud je systém Windows 2000 již podporuje.

Chcete-li nainstalovat zařízení SCSI v textovém režimu, tedy ještě před plným zpřístupněním technologie Plug-and-Play, musíte vytvořit soubor Txtsetup.oem popisující, jak má instalační program nainstalovat příslušné zařízení SCSI.

Důležité Před použitím aktualizovaných ovladačů ověřte, že jsou podepsány. Nejsou-li podepsány, instalační program nebude dokončen. Stav podepsání jednotlivých ovladačů zjistíte ve Správci zařízení (Device Manager). Můžete také spustit Sigverif.exe a vytvořit tak v podsložce %windir% soubor Sigverif.txt. Soubor Sigverif.txt uvádí stav podepsání všech ovladačů v systému.

▼ Chcete-li instalovat zařízení hromadného ukládání dat, postupujte takto:

1. V podsložce \\$OEM\\$ distribuční složky vytvořte podsložku \Textmode.
2. Do podsložky \Textmode zkopírujte následující soubory, které získáte od výrobce daného zařízení (nahraďte slovo *Ovladač* příslušným názvem ovladače):
 - *Ovladač.sys*
 - *Ovladač.dll*
 - *Ovladač.inf*
 - *Txtsetup.oem*

Poznámka Součástí některých ovladačů, například ovladačů miniportů SCSI, nemusí být soubor .dll.

3. V souboru odpovědí vytvořte oddíl [MassStorageDrivers] a do tohoto oddílu запиšte položky ovladačů, které chcete zahrnout. Příkladem možného zápisu v oddílu [MassStorageDrivers] může být:

```
„Adaptec 2940...“ = „OEM“
```

Informace o tomto oddílu najdete v souboru Txtsetup.oem, který vám dodá výrobce hardwaru.

Další informace o parametrech a syntaxi souboru odpovědí najdete v dokumentu „Microsoft Windows 2000 Guide to Unattended Setup“ (Unattend.doc) na CD operačního systému Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumník. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

4. V souboru odpovědí vytvořte oddíl [OEMBootFiles] a do tohoto oddílu запиšte seznam souborů složky \$OEM\$\Textmode, například:

```
[OEMBootFiles]
Ovladač.sys
Ovladač.dll
Ovladač.inf
Txtsetup.oem
```

kde *Ovladač* je název ovladače.

5. Vyhovuje-li vaše zařízení hromadného ukládání dat standardu Plug-and-Play, bude mít v souboru Txtsetup.oem oddíl nazvaný [HardwareIds.Scsi.yyyyy]. Není-li v souboru vašeho zařízení tento oddíl, budete jej muset vytvořit a pak do něj zapsat následující zadání:

```
id = „xxxxx“, „yyyyy“
```

kde *xxxxx* představuje identifikační číslo (id) zařízení a *yyyyy* představuje službu přiřazenou k zařízení.

Chcete-li tedy například instalovat ovladač Symc810, jehož identifikátor zařízení je PCI\VEN_1000&DEV_0001, zajistěte, aby soubor Txtsetup.oem obsahoval následující dodatečný oddíl:

```
[HardwareIds.scsi.symc810]
id = „PCI\VEN_1000&DEV_0001“, „symc810“
```

Instalace vrstev abstrakce hardwaru

Chcete-li zadat instalaci vrstev abstrakce hardwaru (hardware abstraction layer – HAL), potřebujete soubor Txtsetup.oem a soubory HAL, které vám dodá výrobce zařízení. Instalujete-li ovladače zařízení hromadného ukládání dat, musíte použít stejný soubor Txtsetup.oem. Použit může být jen jeden soubor Txtsetup.oem, pokud tedy potřebujete instalovat vrstvy HAL i ovladače zařízení hromadného ukládání dat, musíte všechna zadání zkombinovat do jednoho souboru.

Jestliže chcete využít ovladače jiných výrobců, musíte také příslušným způsobem upravit soubor odpovědí. Další informace o parametrech a syntaxi souboru odpovědí najdete v dokumentu „Microsoft Windows 2000 Guide to Unattended Setup“ (Unattend.doc) na CD operačního systému Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

▼ **Chcete-li instalovat vrstvu HAL, postupujte takto:**

1. Pokud jste tak ještě neučinili, vytvořte ve složce \%OEM\$ podsložku \Textmode.
2. Zkopírujte soubory, které jste získali od prodejce zařízení, do podsložky \Textmode.
3. V souboru odpovědí upravte oddíl [Unattend] vrstev HAL a přidejte sem ovladače, které chcete nainstalovat, například:

```
[Unattend]
Computertype = „PopisHAL“, OEM
```

Informace o položce *PopisHAL* získáte v oddílu [Computer] souboru Txtsetup.oem od poskytovatele ovladače.

4. V souboru odpovědí vytvořte oddíl [OEMBootFiles] a zadejte sem názvy souborů ve složce \%OEM%\Textmode.

Instalace zařízení Plug-and-Play

Následující procedura ukazuje, jak se instalují zařízení Plug-and-Play, pokud se nejedná ani o zařízení hromadného ukládání ani o vrstvy HAL a zároveň nejsou obsažena na CD operačního systému Windows 2000.

▼ **Chcete-li nainstalovat zařízení Plug-and-Play, postupujte takto:**

1. V distribuční složce vytvořte podsložku pro speciální ovladače zařízení Plug-and-Play a jejich soubory .inf. Můžete například vytvořit složku nazvanou PnPDrvs:

```
%OEM%\$1\PnPDrvs
```

2. Přidáním následujícího řádku do souboru odpovědí přidáte potřebnou cestu na seznam prohledávaných jednotek:

```
OEMPnPDriversPath = „PnPDrvs“
```

Máte-li ve složce PnPDrvs podsložky, musíte zadat cestu ke každé podsložce. Tyto cesty musí být odděleny středníky.

Chcete-li jednoduše spravovat složky tak, aby do nich bylo možné ukládat ovladače zařízení i v budoucnosti, vytvořte složky pro všechny potenciální ovladače zařízení. Když tyto složky rozdělíte do podsložek, můžete ovladače zařízení uchovávat podle typu zařízení a nemusíte mít všechny ovladače zařízení v jediné složce. Doporučujeme vám vytvořit složky Audio, Modem, Síť, Tisk, Video a Ostatní. Složka Ostatní vám bude umožňovat ukládat ovladače nových hardwarových zařízení, která třeba ještě nejsou známá.

Například obsahuje-li složka PnPDrvs podsložky Audio, Modem a Síť, soubor odpovědí musí obsahovat následující řádek:

```
OEMPnPDriversPath = „PnPDrvs\Audio;PnPDrvs\Modem;PnPDrvs\Síť“
```

Převod délky názvu souboru pomocí souboru \$\$Rename.txt

Soubor \$\$Rename.txt určuje změnu krátkých názvů souborů na dlouhé názvy souborů během instalace. Soubor \$\$Rename.txt uvádí všechny soubory v určité složce, které je zapotřebí přejmenovat. Každá složka obsahující krátké názvy souborů, které je zapotřebí přejmenovat, musí obsahovat svou vlastní verzi souboru \$\$Rename.txt.

Chcete-li používat soubor \$\$Rename.txt, vložte tento soubor do složky obsahující soubory, které se musí převést. Syntaxe souboru \$\$Rename.txt je následující:

```
[název_oddílu_1]
krátký_název_1 = „dlouhý_název_1“
krátký_název_2 = „dlouhý_název_2“

krátký_název_x = „dlouhý_název_x“
```

```
[název_oddílu_2]
krátký_název_1 = „dlouhý_název_1“
krátký_název_2 = „dlouhý_název_2“
```

```
krátký_název_x = „dlouhý_název_x“
```

Parametry jsou definované takto:

- ***název_oddílu_x*** Cesta k podsložce obsahující dané soubory. Oddíl nemusí být pojmenovaný nebo může mít za název zpětné lomítko (\), což znamená, že oddíl obsahuje názvy souborů nebo podsložek v kořenu jednotky.
- ***krátký_název_x*** Název souboru nebo podsložky v dané podsložce, která se bude přejmenovávat. Tento název *nesmí* být uzavřen v uvozovkách.
- ***dlouhý_název_x*** Nový název souboru nebo podsložky. Obsahuje-li tento název mezery nebo čárky, musí být uzavřen v uvozovkách.

Tip Používáte-li ke spuštění instalace systém MS-DOS a vaše nástroje systému DOS nedokáží kopírovat složky s cestami delšími než 64 znaků, můžete složky pojmenovat krátkými názvy a později je prostřednictvím souboru \$\$Rename.txt přejmenovat.

Přehled souboru odpovědí

Soubor odpovědí je upravený skript, který odpovídá na otázky instalačního programu místo uživatele. CD systému Windows 2000 Professional obsahuje ukázkový soubor odpovědí, který si můžete upravit a používat. Soubor odpovědí se obvykle nazývá Unattend.txt, můžete jej však přejmenovat. (Platnými názvy souboru odpovědí jsou například Comp1.txt, Install.txt a Setup.txt za předpokladu, že jsou tyto názvy správně použity v příkazu **setup**.) Přejmenování souboru odpovědí vám umožňuje vytvořit a používat více souborů odpovědí, potřebujete-li v různých částech své organizace používat různé skripty ovládané instalace. Soubory odpovědí využívají také další programy, například Sysprep, který pracuje s volitelným souborem Sysprep.inf.

Soubor odpovědí říká instalačnímu programu, jak pracovat s distribučními složkami a soubory, které jste vytvořili. Například v oddílu [Unattend] souboru odpovědí je položka „OEMPreinstall“ říkající instalačnímu programu, aby zkopíroval podsložky \$OEM\$ z distribučních složek na cílový počítač.

Soubor odpovědí obsahuje několik volitelných oddílů, které můžete upravit a zadat tak informace o požadavcích vaší instalace. Soubor odpovědí předá instalačnímu programu odpovědi na všechny otázky, které jsou vám kladeny během standardní interaktivní instalace systému Windows 2000. Dokument Unattend.doc obsahuje podrobné informace o klíčích a hodnotách souboru odpovědí. Další informace o oddílech souboru odpovědí a jejich parametrech najdete v dokumentu „Microsoft Windows 2000 Guide to Unattended Setup“ (Unattend.doc) na CD operačního systému Microsoft Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

Chcete-li dosáhnout bezobslužné instalace systému Windows 2000 Professional, musíte vytvořit soubor odpovědí a při spuštění instalačního programu metodou spustitelného CD nebo spuštěním souborů Winnt.exe či Winnt32.exe tento soubor určit. Příkladem spuštění instalace programem Winnt.exe může být:

```
Winnt /S:Z:\I386 /U:Z:\unattend.txt
```

Všimněte si přepínače **/U**: příkazového řádku, který při použití příkazu **Winnt** určuje bezobslužnou instalaci (v případě spuštění instalačního programu pomocí souboru **Winnt32** se pro zadání bezobslužné instalace používá parametr **/unattend**). Další informace o souborech Winnt.exe a Winnt32.exe najdete v oddílu „Přehled příkazů instalačního programu systému Windows 2000“ dále v této kapitole.

Vytvoření souboru odpovědí

Soubor odpovědí je upravený skript, jehož pomocí můžete spouštět bezobslužnou instalaci systému Windows 2000 Professional. Soubor odpovědí lze vytvořit dvěma způsoby: pomocí Správce instalace (Setup Manager) nebo jeho ručním zápisem.

Vytvoření souboru odpovědí pomocí Správce instalace

S vytvářením a úpravou souboru odpovědí vám může pomoci aplikace Správce instalace (Setup Manager), kterou najdete na CD operačního systému Windows 2000 v souboru Deploy.cab ve složce \Support\Tools. Prostřednictvím Správce instalace můžete dodat procesu vytváření nebo aktualizace souboru odpovědí konzistentnost.

Další informace o oddílech souboru odpovědí a jejich parametrech najdete v dokumentu „Microsoft Windows 2000 Guide to Unattended Setup“ (Unattend.doc) na CD operačního systému Microsoft Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

Správce instalace lze použít k následujícím činnostem (výsledky jsou pak vygenerovány jako parametry souboru odpovědí):

- Určení platformy souboru odpovědí (Microsoft Windows 2000 Professional, Windows 2000 Server, vzdálená instalace operačního systému nebo nástroj Sysprep).
- Určení úrovně automatizace bezobslužného režimu instalačního programu. (Tyto úrovně zahrnují „Poskytnout výchozí nastavení“ (Provide Defaults), „Plně automatická instalace“ (Fully Automated), „Skrýt stránky“ (Hide Pages), „Umožnit pouze čtení“ (Read Only) a „Obsluhovat pomocí grafického rozhraní“ (GUI-mode Setup).)
- Určení výchozích informací o uživateli.

- Definování možností názvu počítače včetně vytvoření /UDF pro přístup k souboru platných názvů počítačů.
- Konfigurování nastavení sítě.
- Vytvoření distribučních složek.
- Přidání vlastních souborů loga a pozadí.
- Přidání souborů do distribučních složek.
- Přidání příkazů do oddílu [GuiRunOnce].
- Vytvoření souborů Cmdlines.txt.
- Určení kódových stránek.
- Specifikování regionálních nastavení.
- Specifikování časového pásma.
- Specifikování informací TAPI.

Správce instalace nedokáže vykonat tyto funkce:

- Určení systémových součástí, například Internet Information Services.
- Vytvoření souborů Txtsetup.oem.
- Vytvoření podsložek v distribuční složce.

Tabulka 25.3 popisuje některé obvyklejší specifikace souboru odpovědí vytvoření Správcem instalace.

Tabulka 25.3 Specifikace souboru odpovědí vytvořené Správcem instalace

Parametr	Smysl
Instalační cesta	Určuje požadovanou cestu na cílovém počítači, kam se nainstaluje systém Windows 2000 Professional.
Možnost inovace	Určuje, zda půjde o inovaci ze systému Windows 95 či Windows 98, Windows NT nebo Windows 2000.
Název cílového počítače	Určuje název uživatele, název organizace a název počítače aplikovaný na cílový počítač.
Identifikátor produktu	Zadáva identifikační číslo produktu získané z dokumentace.
Skupina nebo doména	Určuje název pracovní skupiny nebo domény, do které počítač patří.
Časové pásmo	Zadáva počítači časové pásmo.
Informace o síťové konfiguraci	Zadáva typ síťového adaptéru (karty) a konfiguraci síťovými protokoly.

Ruční vytvoření souboru odpovědí

Chcete-li vytvořit soubor odpovědí ručně, použijte nějaký textový editor, například Poznámkový blok. Obecně lze říci, že se soubor odpovědí skládá ze záhlaví oddílů, parametrů a hodnot těchto parametrů. Většina záhlaví oddílů je sice předdefinovaná, můžete však nadefinovat další záhlaví oddílů. Jestliže vaše instalace nepotřebuje všechny parametry, nemusíte je zadávat.

Neplatné parametry mají za následek chyby nebo nekorektní chování po instalaci.

Formát souborů odpovědí je následující:

```
[oddíl11]
:
: Oddíl obsahuje klíče a odpovídající
: hodnoty daných klíčů/parametrů.
: Klíče a hodnoty jsou odděleny znaky ' = '.
: Hodnoty obsahující mezery obvykle musí být
: uzavřeny v uvozovkách „“ .
:
klíč = hodnota
.
.
.
[oddíl12]
klíč = hodnota
.
.
.
```

Nastavení hesel pomocí souboru odpovědí

Použijete-li při instalaci soubor odpovědí, můžete nastavit parametry těchto příkazů hesel:

- AdminPassword
- UserPassword
- DefaultPassword
- DomainAdminPassword
- AdministratorPassword
- Password

Definice těchto příkazů najdete v dokumentu „Microsoft Windows 2000 Guide to Unattended Setup“ (Unattend.doc) na CD operačního systému Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

Navíc ukázkové soubory odpovědí používající některé z těchto parametrů najdete v příloze „Příklady souborů odpovědí pro bezobslužnou instalaci“ v této knize.

Poznámka Hesla jsou omezena na 127 znaků. Zadáte-li heslo obsahující více než 127 znaků, nebudete se moci do systému přihlásit, protože heslo bude neplatné.

Po dokončení instalace zůstane na počítači soubor odpovědí se všemi použitými nastaveními, všechny informace o heslech se z jeho místní kopie však odstraní, aby nebylo narušeno zabezpečení.

Upozornění Během instalace však soubor existuje na pevném disku. Je-li pro vás zabezpečení prvořadé, nepřidávejte do souboru odpovědí vytvořeného pro bezobslužnou instalaci informace o heslech.

Místní soubor odpovědí vám umožňuje automaticky nastavovat volitelné součásti spouštěním příkazů obsahujících parametry již zadané v původním souboru odpovědí

použitím při instalaci. Tyto součásti mohou zahrnovat konfiguraci serveru jako řadiče domény, jako serveru klastru nebo povolovat službu Message Queuing.

Rozšiřování oddílů pevného disku

Instalaci můžete začít na malém oddílu disku (kolem 1 GB na větším disku) a zadat, aby se daný oddíl během procesu instalace systému Windows 2000 rozšířil. Toho docílíte použitím parametru `ExtendOemPartition` v souboru odpovědí. Parametr `ExtendOemPartition` funguje pouze na oddílech systému NTFS a lze jej použít jak ve standardním souboru odpovědí tak i v souboru odpovědí používaném při instalacích nástrojem Sysprep.

Další informace o nástroji Sysprep s souboru `Sysprep.inf` najdete v oddílu „Duplikování disků pomocí nástroje Sysprep“ dále v této kapitole.

Poznámka Parametr `ExtendOemPartition` funguje na aktivním systémovém oddílu. Ne funguje na jiných oddílech stejného disku nebo na jiných discích počítače. Navíc použijete-li zadání `ExtendOemPartition=1`, oddíl se rozšíří o veškerý zbývajících prostor na disku a poslední cylinder nechá prázdný. To je záměr sloužící k tomu, abyste mohli používat dynamické svazky.

Použijete-li `ExtendOemPartition` během instalace na oddílu systému File Allocation Table (FAT), musíte v oddílu `[Unattended]` souboru odpovědí ještě zadat `File System=ConvertNTFS`, aby se nejprve oddíl převedl na systém NTFS. Další informace o použití parametru `ExtendOemPartition` při instalaci pomocí nástroje Sysprep najdete v oddílu „Rozšiřování diskových oddílů pomocí nástroje Sysprep“ dále v této kapitole.

Další informace o použití `ExtendOemPartition` najdete v dokumentu „Microsoft Windows 2000 Guide to Unattended Setup“ (`Unattend.doc`) na CD operačního systému Windows 2000. Soubor `Unattend.doc` je součástí souboru `Deploy.cab` ve složce `\Support\Tools`. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

Přehled příkazů instalačního programu systému Windows 2000

Chcete-li nainstalovat systém Windows 2000, musíte spustit příslušný instalační program, buď `Winnt.exe` nebo `Winnt32.exe`. V této kapitole označujeme oba soubory `Winnt.exe` a `Winnt32.exe` společným názvem „instalační program“. Typ instalačního programu, který musíte spustit, se určuje takto:

- V případě čisté instalace na počítače se systémem MS-DOS nebo Microsoft Windows 3.x spusťte soubor `Winnt.exe` z příkazového řádku systému MS-DOS.
- V případě čisté instalace nebo aktualizace systému Windows NT, Windows 95 nebo Windows 98 spusťte soubor `Winnt32.exe`.

Uvědomte si také, že můžete spustit standardní interaktivní instalaci ze spouštěcích disket, které jsou součástí CD systému Windows 2000 Professional.

Upozornění Jestliže před instalací systému Windows 2000 inovujete nějaké aplikace na počítači, musíte jej před spuštěním instalačního programu nechat restartovat.

Další informace o metodách instalace najdete v oddílu „Automatizování instalace systému Windows 2000 Professional“ dále v této kapitole.

Winnt.exe

Příkaz Winnt.exe má včetně parametrů automatizované instalace tento tvar:

```
winnt [/S[:cesta_zdroje]] [/T[:dočasná_jednotka]] /U[:soubor_odpovědí]
[/R[x]:složka] [/E:příkaz]
```

Definici parametrů a syntaxi příkazu najdete v příloze „Příkazy instalačního programu“ v této knize.

V případě diskových jednotek s více oddíly nainstaluje instalační program Winnt.exe systém Windows 2000 do aktivního oddílu, pokud tento oddíl obsahuje dostatečné množství prostoru. Jinak instalační program vyhledá jiné oddíly, které obsahují dostatečné množství prostoru, a vyzve vás k zadání požadovaného oddílu. Při automatizovaných instalacích lze tuto výzvu odstranit spuštěním instalačního programu s parametrem **/T**, který automaticky ukáže na požadovaný oddíl, například:

```
winnt [/unattend] [[:<cesta>\answer.txt] [/T[:d]]
```

Winnt32.exe

Příkaz Winnt32.exe má včetně parametrů automatizované instalace tento tvar:

```
winnt32 [/s:cesta_zdroje] [/tempdrive:písmeno_jednotky]
[/unattend[čísló]][:soubor_odpovědí] [/copydir:název_složky]
[/copysource:název_složky] [/cmd:příkazový_řádek]
[/debug[úroveň]][:název_souboru] [/udf:id[,soubor_UDB]]
[/syspart:písmeno_jednotky] [/noreboot] [/makelocalsource] [/checkupgradeonly]
[/m:název_složky]
```

Definici parametrů a syntaxi příkazu najdete v příloze B „Příkazy instalačního programu“ v této knize.

V případě diskových jednotek s více oddíly nainstaluje instalační program Winnt.exe systém Windows 2000 do aktivního oddílu, pokud tento oddíl obsahuje dostatečné množství prostoru. Jinak instalační program vyhledá jiné oddíly, které obsahují dostatečné množství prostoru, a vyzve vás k zadání požadovaného oddílu. Při automatizovaných instalacích lze tuto výzvu odstranit spuštěním instalačního programu s parametrem **/tempdrive**, který automaticky ukáže na požadovaný oddíl, například:

```
winnt32 [/unattend] [[:<cesta>\answer.txt] [/tempdrive:d]]
```

Systém Windows 2000 může použít až osm přepínačů **/s** ukazujících na další distribuční servery jako zdroje instalace na cílový počítač. Tato funkce pomáhá urychlit fázi kopírování souborů instalačního programu na cílový počítač a zajišťuje také další možnosti vyrovnávání zatížení distribučních serverů, z nichž lze instalační program spustit, například:

```
<cesta k distribuční složce 1>\winnt32 [/unattend] [[:<cesta>\answer.txt]
[/s:<cesta k distribuční složce 2>] [/s:<cesta k distribuční složce 3>]
[/s:<cesta k distribuční složce 4>]
```

Tabulka 13.4 ukazuje příkazy instalačního programu a jejich použití v systému Windows 2000.

Tabulka 25.4 Použití příkazů instalačního programu

Příkaz instalačního programu	Verze systému Windows 2000	Inovace	Čistá instalace
Winnt.exe	Server a Professional	Ne	Ano
Winnt32.exe	Server a Professional	Ano	Ano

Automatizování instalace klientských aplikací

Po vyřešení kritických problémů plánování se můžete rozhodnout, jak budete automatizovat instalaci klientských aplikací. Ve většině případů bude zapotřebí použít funkce bezobslužné instalace dané aplikace.

Můžete si vybrat z těchto možností:

- Cmdlines.txt
- Spuštění instalačního programu aplikace nebo dávkového souboru z oddílu [GuiRunOnce] souboru odpovědí.
- Instalační služba Windows Installer

Použití souboru Cmdlines.txt

Soubor Cmdlines.txt obsahuje příkazy, které grafický režim vykoná při instalaci volitelných součástí, například aplikací, které se musí instalovat ihned po instalaci systému Windows 2000 Professional. Plánujete-li použít soubor Cmdlines.txt, musíte jej umístit do podsložky \ \$OEM\$ distribuční složky. Používáte-li nástroj Sysprep, umístíte soubor Cmdlines.txt do podsložky \ \$OEM\$ \ \$1 \ Sysprep.

Soubor Cmdlines.txt použijte v těchto situacích:

- Instalujete z podsložky \ \$OEM\$ distribuční složky.
- Instalovaná aplikace má některou z následujících vlastností:
 - Nekonfiguruje se sama pro více uživatelů, například sada Microsoft Office 95.
 - Je vytvořena pro instalaci jedním uživatelem a replikování informací jednotlivých uživatelů.

Syntaxe souboru Cmdlines.txt je následující:

```
[Commands]
„příkaz_1“
„příkaz_2“
.
.
„příkaz_x“
```

Parametry jsou definované takto:

- „příkaz_1“, „příkaz_2“, ... „příkaz_x“ představují příkazy, které chcete spustit (a jejich pořadí) v okamžiku, kdy grafický režim zavolá soubor Cmdlines.txt. Všimněte si, že všechny příkazy musí být v uvozovkách.

Při použití souboru Cmdlines.txt pamatujte na následující:

- Jsou-li příkazy souboru Cmdlines.txt vykonány během instalace, není k systému přihlášený žádný uživatel a není zaručeno síťové spojení. Proto se informace o jednot-

livých uživatelích zapíše do registru výchozího uživatele a všichni dále vytvoření uživatelé také obdrží tyto informace.

- Soubor Cmdlines.txt vyžaduje, abyste umístili soubory potřebné ke spuštění aplikace nebo nástroje do adresářů, ke kterým se během instalačního procesu přistupuje, což znamená, že tyto soubory musí být na pevném disku.

Použití oddílu [GuiRunOnce] souboru odpovědí

Oddíl [GuiRunOnce] souboru odpovědí obsahuje seznam příkazů, které se vykonají při prvním přihlášení uživatele na počítač po skončení instalačního programu. Chcete-li tedy například zajistit automatické spuštění instalace nějaké aplikace, můžete do oddílu [GuiRunOnce] zadat následující řádek:

```
[GuiRunOnce]
..%systemdrive%\slož_apl\inst_apl -quiet"
```

Plánujete-li inicializaci instalace pomocí oddílu [GuiRunOnce], musíte vzít v úvahu ještě následující faktory:

Požaduje-li aplikace restartování, zjistěte, zda lze restartování nějakým způsobem potlačit.

To je velmi důležité, protože po každém restartu systému jsou ztracena všechna předchozí zadání v oddílu [GuiRunOnce]. Jestliže bude systém restartovat před dokončením zadání dříve určených v oddílu [GuiRunOnce], zbývající položky se nespustí. Neexistuje-li v aplikaci žádná možnost potlačení restartu, můžete se pokusit zabalit danou aplikaci do balíčku programu Windows Installer. Tuto funkci zajišťují nástroje jiných výrobců.

Součástí systému Windows 2000 je WinINSTALL LE (Limited Edition), nástroj přebalíčkování pro službu Windows Installer. WinINSTALL LE vám umožňuje snadno přebalit aplikace vzniklé před zavedením nástroje Windows Installer do balíčků, které lze distribuovat pomocí nástroje Windows Installer. Další informace o programu WinINSTALL LE najdete ve složce \Valueadd\3rdparty\Mgmt\Winstle na CD systému Windows 2000.

Další informace o balíčkování programu Windows Installer najdete v oddílu „Použití instalační služby Windows Installer“ v této knize.

Důležité Jestliže instalujete nějakou aplikaci na více jazykově lokalizovaných verzí systému Windows 2000, doporučujeme vám vyzkoušet přebalenou aplikaci na lokalizovaných verzích a ujistit se, že kopíruje soubory na správná místa a řádně zapisuje požadované položky registru.

Vyžaduje-li aplikace ke své instalaci prostředí Průzkumníka Windows, pak nebude oddíl [GuiRunOnce] fungovat, protože v době vykonání příkazů Run a RunOnce není ještě toto prostředí nahráno.

Kontaktujte výrobce aplikace a zjistěte, zda je k dispozici nějaká aktualizace nebo oprava, která může tyto situace instalace aplikace řešit. Není-li nic takového k dispozici, můžete aplikaci přebalit do balíčku nástroje Windows Installer nebo použít jiné prostředky distribuce.

Aplikace používající stejný typ instalačního mechanismu nemusí fungovat správně, není-li použit příkaz /wait.

K tomu může dojít, když běží instalace aplikace a ta spustí další proces. Pokud ještě pracuje instalační rutina, pak může inicializace jiného procesu a zavření aktivního procesu způsobit spuštění další rutiny uvedené v položkách RunOnce registru. Protože běží více instancí instalačního mechanismu, druhá aplikace obvykle skončí chybou. Příklad řízení takové situace pomocí dávkového souboru najdete v oddílu „Řízení instalace více aplikací pomocí dávkového souboru“ dále v této kapitole.

Použití programů instalace aplikace

Upřednostňovanou metodou předběžné instalace aplikace je použití instalační rutiny, která je součástí dané aplikace. Toho můžete využít, pokud je instalovaná aplikace schopna po zadání přepínače **/q** nebo **/s** příkazového řádku běžet v *tichém* režimu (bez intervence uživatele). Seznam parametrů příkazového řádku podporovaných instalačním mechanismem najdete v nápovědě k aplikaci nebo v její dokumentaci.

Dále je uveden příklad řádku, který můžete vložit do oddílu [GuiRunOnce] a iniciovat tak bezobslužnou instalaci aplikace s využitím jejího vlastního instalačního programu.

```
<cesta k instalačnímu programu>\Setup.exe /q
```

Parametry instalačního programu se v jednotlivých aplikacích liší. Například parametr **/I** obsažený v některých aplikacích je užitečný, když chcete v zájmu sledování instalace vytvořit soubor protokolu. Některé aplikace mají příkazy, které jim zabrání v automatickém restartování. To vám pomůže řídit instalaci aplikací s minimálním počtem restartů.

Před zadáním předběžné instalace nějaké aplikace od jejího výrobce zajistěte všechny potřebné instrukce, nástroje a nejlepší postupy.

Důležité Bez ohledu na metodu instalování musíte splnit všechny licenční požadavky dané aplikace.

Řízení instalace více aplikací pomocí dávkového souboru

Chcete-li řídit způsob instalace více aplikací, můžete vytvořit dávkový soubor obsahující jednotlivé instalační příkazy a používající příkaz **Start** s přepínačem **/wait** příkazového řádku. Tato metoda zaručí, že se vaše aplikace nainstalují postupně a že jednotlivé aplikace bude plně nainstalovány, než dojde ke spuštění instalační rutiny následující aplikace. Dávkový soubor se pak spustí z oddílu [GuiRunOnce].

Následující procedura vysvětluje, jak vytvořit dávkový soubor, jak aplikaci nainstalovat a nakonec jak po dokončení instalace odstranit všechny odkazy daný dávkový soubor.

▼ Chcete-li nainstalovat aplikaci pomocí dávkového souboru, postupujte takto:

1. Vytvořte dávkový soubor obsahující řádky podobající se následujícímu příkladu:

```
Start /wait <cesta k první aplikaci>\Setup <parametry příkazového řádku>
Start /wait <cesta k druhé aplikaci>\Setup <parametry příkazového řádku>
Exit
```

kde:

- **<cesta>** je cesta ke spustitelnému souboru spouštějícímu instalaci. Tato cesta musí být během instalace k dispozici.

- *Setup* je název spustitelného souboru spouštějícího instalaci.
 - *<parametry příkazového řádku>* jsou nějaké dostupné parametry tichého režimu dané aplikace, kterou chcete instalovat.
4. Zkopírujte dávkový soubor do distribučních složek nebo na jiné místo přístupné během instalace.
 5. Je-li název dávkového souboru *<filename>.bat*, vložte do oddílu [GuiRunOnce] souboru odpovědi řádek, který daný soubor spustí, jak ukazuje následující příklad. Tento příklad předpokládá, že byl dávkový soubor zkopírován do složky Sysprep na místním pevném disku, i když může být umístěn na libovolném místě, kam má instalační program přístup.

```
[GuiRunOnce]
„%systemdrive%\sysprep\<filename>.bat“=“<cesta-1>\<příkaz-1>.exe“
„<cesta-n>\<příkaz-n>.exe“
„%systemdrive%\sysprep\sysprep.exe -quiet“
```

kde:

- *<cesta-1>\<příkaz-1.exe>* a *<cesta-n>\<příkaz-n.exe>* jsou plně zadané cesty k dalším instalačním či konfiguračním nástrojům jiných aplikací, nebo nástrojů. Může jít také o cestu k jinému dávkovému souboru. Tyto cesty musí být během instalace dostupné.

Použití instalační služby Windows Installer

Služba Windows Installer je součástí systému Windows 2000, která standardizuje způsob instalace aplikací na více počítačů.

Když instalujete aplikace bez služby Windows Installer, musí mít každá aplikace svůj vlastní spustitelný instalační program nebo skript. Každá aplikací musí sama zajistit dodržení příslušných pravidel instalace (například pravidla pro vytváření verzí souborů). To je dáno tím, že instalační program aplikace není integrální součástí vývoje operačního systému, takže neexistují žádná centrální instalační pravidla.

Služba Windows Installer implementuje všechna potřebná pravidla instalace přímo v samotném operačním systému. Aby aplikace odpovídaly tomuto formátu, musí být popsány standardním formátem označovaným za balíček služby Windows Installer. Datový soubor obsahující formátovací informace se označuje za soubor balíčku služby Windows Installer a má příponu .msi. Služba Windows Installer používá k instalaci aplikace soubor balíčku služby Windows Installer.

Terminologie služby Windows Installer

K popisu instalačního procesu využívajícího technologii Windows Installer se používají následující termíny:

Prostředek. Soubor, zadání v registru, zástupce nebo jiný prvek, který instalátor přenáší na počítač.

Součást. Kolekce souborů, položek v registru a dalších prostředků, které se instalují nebo odstraňují jako jednotka. Po výběru nějaké součásti k instalaci nebo odstranění se nainstalují nebo odstraní všechny prostředky v dané součásti.

Funkce. Části aplikace, které si uživatel může nainstalovat. Funkce obvykle odpovídají funkčním prvkům samotné aplikace.

Produkt. Jediný produkt, jako například Microsoft Office. Produkty obsahují jednu nebo více funkcí.

Soubor balíčku služby Windows Installer

Soubor balíčku má databázový formát optimalizovaný pro zajištění výkonné instalace. Tento soubor obecně popisuje vztah mezi funkcemi, součástmi a prostředky určitého produktu.

Soubor balíčku služby Windows Installer se obvykle nachází společně se soubory produktu v kořenové složce disku CD produktu nebo jeho obrazu (bitové kopii) na síti. Soubory produktu mohou mít formu zkomprimovaných souborů, které se pak označují za kabinety (mají příponu .cab). Každý produkt má svůj vlastní soubor balíčku. V okamžiku instalace si služba Windows Installer otevře daný soubor balíčku produktu a pomocí informací v balíčku určí všechny instalační operace, které musí být ve spojení s daným produktem vykonány.

Automatizování instalace systému Windows 2000 Professional

V podnikovém prostředí není z hlediska nákladů efektivní instalovat systém Windows 2000 pomocí standardního interaktivního instalačního programu na každém jednotlivém počítači. Výrazného snížení celkových nákladů na vlastnictví (total cost of ownership – TCO) dosáhnete automatizovanými instalacemi systému Windows 2000 Professional na více počítačů.

Automatizovat lze instalaci těchto součástí:

- Jádra operačního systému Windows 2000 Professional.
- Standardních výrobních aplikací, jako je Microsoft Office 2000 a dalších aplikací, které nepracují jako služby.
- Podporu dalších jazyků v systému Windows 2000 Professional pomocí instalace různých jazykových balíčků.
- Servisních balíčků pro systém Windows 2000 Professional.

Automatizovaná instalace systému Windows 2000 Professional zahrnuje spuštění instalačního programu se souborem odpovědí. Instalační program může proběhnout bezobslužně. Bezobslužná instalace zahrnuje tyto kroky:

- Vytvoření souboru odpovědí.
- Určení a implementace procesu konfigurace informací pro jednotlivé počítače.
- Přípravu na instalaci dalších souborů pomocí balíčků služby Windows Installer.
- Určení a implementace procesu automatizace vybrané metody distribuce, například použití síťového distribučního bodu nebo duplikování pevného disku.

Nové možnosti automatizované instalace

Automatizovaná instalace systému Windows 2000 nabízí několik nových voleb souboru odpovědí řídících, co a jak se má spustit. Další informace o parametrech a syntaxi souboru odpovědí najdete v dokumentu „Microsoft Windows 2000 Guide to Unattended Setup“ (Unattend.doc) na CD operačního systému Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Win-

dows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

Flexibilní práce v síti V systému Windows 2000 máte k dispozici flexibilní síťové konfigurace pro jednotlivé počítače včetně dodatečné podpory protokolů, služeb a klientů. Nyní je možné nastavit pořadí vázání, jednoduše zadat výchozí informace a instalovat více síťových karet v jednom systému. Aby byla instalace a konfigurace ještě jednodušší, systém Windows 2000 může automaticky zkopírovat a nainstalovat ovladače síťových zařízení. Systém Windows 2000 standardně instaluje pro všechny síťové adaptéry v systému výchozí komponenty, není-li tedy v souboru odpovědí řečeno jinak. Mezi výchozí síťové komponenty patří Klient sítě Microsoft (Client for Microsoft Networks), protokol TCP/IP, Sdílení souborů a tiskáren v sítích Microsoft (File and Printer Sharing for Microsoft Networks) a zavedení protokolu Dynamic Host Configuration Protocol (DHCP).

Možnost automatického přihlášení Soubor odpovědí si můžete upravit a umožnit počítači automatické přihlášení k účtu správce při prvním spuštění (nebo po zadaný počet spuštění) systému po dokončení instalace systému Windows 2000. Potřebujete-li, aby se systém Windows 2000 automaticky několikrát přihlásil, aby bylo možné vykonat úlohy zadané položkami [GuiRunOnce], budete muset vytvořit v souboru odpovědí neprázdné heslo správce (AdminPassword). Pomocí AutoAdminLogonCount pak lze zadat, kolikrát se má systém automaticky přihlásit v zájmu dokončení zadaných úloh. Použijete-li prázdné heslo, instalační program se bude moci přihlásit k systému jen jednou. Při dalších restartech bude nutné zadat oprávnění nějakým jiným způsobem. Smyslem tohoto opatření je snížit riziko narušení zabezpečení. Uvědomte si však, že zadání oprávnění správce do textového souboru vždy znamená ohrožení zabezpečení v případě, že uživatel získá k tomuto souboru přístup.

Automatické vykonávání příkazů Oddíl [GuiRunOnce] souboru odpovědí obsahuje seznam příkazů, které se mají postupně vykonat jako součást instalačního programu po dokončení grafického režimu. Pomocí oddílu [GuiRunOnce] lze specifikovat seznam instalovaných aplikací, nástrojů konfigurace systému a dalších nástrojů, jež se mají spustit při prvním přihlášení k instalovanému počítači.

Zjednodušené zadávání časové zóny V souboru odpovědí lze jednodušeji a s menším počtem chyb než v systému Windows NT zadat časové pásmo počítače. Protože jsou tu uvedeny možné časové zóny, chyby jsou méně časté, jelikož nyní již nemusíte zadávat celý řetězec časové zóny.

Vylepšená místní a jazyková nastavení V souboru odpovědí lze zadat místní nastavení systému a uživatelů, metodu klávesnice a vstupů a instalovanou podporu jazyků. Správce instalace (Setup Manager) tento proces ještě více zjednodušuje, protože vám nastavení instalace systému nabízí v grafickém rozhraní průvodce.

Jednodušší předběžná instalace zařízení Protože se zavádí podpora technologie Plug-and-Play, klíče OemPnPDriversPath a nová struktura sdílení distribučních bodů, předběžné instalování zařízení nyní spočívá v jednoduchém přidání ovladačů do nějaké složky na sdíleném distribučním místě a určení klíče OemPnPDriversPath.

Metody automatizované instalace

Automatizovanou instalaci systému Windows 2000 Professional lze spustit několika metodami. Vybraná metoda závisí na výsledku vašeho kritického plánování, které bylo popsáno dříve v této kapitole.

Mezi metody automatizované instalace na klientských počítačích patří:

- Použití nástroje Syspart na počítačích s rozdílným hardwarem.
- Použití nástroje Sysprep k duplikování disků.
- Použití serveru Systems Management Server.
- Použití spustitelného CD.
- Použití vzdálené instalace operačního systému.

Poznámka Funkce vzdálené instalace operačního systému automaticky instaluje systém Windows 2000 Professional a aplikace na klientské počítače z určeného souboru Služby vzdálené instalace (Remote Installation Service – RIS). RIS je volitelná komponenta, která je součástí systému Windows 2000 Server.

Tabulka 25.5 popisuje situace, kdy se používají různé metody automatizované instalace.

Tabulka 25.5 kdy se používají metody automatizované instalace

Metoda	Použití
Syspart	Nástroj Syspart se používá pro čistou instalaci na počítače s rozdílným hardwarem.
Sysprep	Nástroj Sysprep se používá, mají-li hlavní a cílový počítač stejný hardware, což zahrnuje také ovladače HAL a zařízení hromadného ukládání dat.
Systems Management Server	Server Systems Management Server se používá ke spravovaným inovacím programu Windows 2000 Professional na více systémů, zejména jsou-li geograficky rozptýleny.
Spustitelné CD	Metoda spustitelného CD se používá u počítačů, jejichž systém základních vstupů a výstupů (BIOS) umožňuje spuštění z CD.
Vzdálená instalace operačního systému	Vzdálená instalace obrazu (bitové kopie) systému Windows 2000 Professional se používá na podporovaných počítačích v zájmu eliminace nutnosti osobně navštívit každý instalovaný počítač.

Použití nástroje Syspart na počítačích s rozdílným hardwarem

Nástroj Syspart se spouští volitelným parametrem programu Winnt32.exe. Metodu Syspart můžete použít, když nemají hlavní počítač a počítač, na který instalujete systém Windows 2000 Professional podobný hardware. Tato metoda také omezuje čas zavedení odstraněním kroku kopírování souborů instalačního programu.

Syspart vyžaduje použití dvou fyzických disků, přičemž na cílovém pevném disku musí být primární oddíl.

Požadujete-li podobnou instalaci a konfiguraci operačního systému na typech hardwaru, kde se liší ovladače HAL nebo zařízení hromadného ukládání dat, můžete pomocí nástroje Syspart vytvořit hlavní sadu souborů s potřebnými konfiguračními informacemi a podporou ovladačů, které pak lze zkopírovat. Tyto obrazy lze následně použít na nepodobných systémech, kde se řádně detekuje hardware a konzistentně nakonfiguru-

je operační systém. Obsahuje-li vaše prostředí více typů systémů závislých na hardwaru, můžete použít nástroj Syspart k vytvoření hlavního obrazu jednotlivých typů. Nainstalujete systém Windows 2000 na jeden z počítačů každého typu a pomocí nástroje Sysprep pak vytvoříte obrazy použité na zbývajících počítačích stejného typu. Další informace o nástroji Sysprep najdete v oddílu „Duplikování disků pomocí nástroje Sysprep“ dále v této kapitole.

Ještě než začnete, vyberte počítač, který bude považován za referenční. Na referenčním počítači musí být instalován systém Windows NT nebo Windows 2000.

▼ **Chcete-li nainstalovat systém Windows 2000 Professional pomocí nástroje Syspart, postupujte takto:**

1. Spustíte referenční počítač a připojíte se k distribuční složce.
2. Spustíte instalační program.

Stiskněte tlačítko **Start**, zadejte příkaz **Spustit** (Run) a pak zapište:

```
winnt32 /unattend:unattend.txt /s:zdroj_instalace /syspart:druhá_jednotka  
/tempdrive:druhá_jednotka /noreboot
```

Důležité Úspěšná instalace nástrojem Syspart je podmíněna použitím parametru */tempdrive*. Při použití přepínače */tempdrive* příkazového řádku se ujistěte, že máte na svém druhém oddílu dostatek volného diskového prostoru k instalaci systému Windows 2000 Professional i aplikací. Geometrie disku, který plánujete použít jako cíl nástroje Syspart, musí být stejná jako geometrie disku na počítači, na který budete duplikovat.

Parametry */syspart* a */tempdrive* musí ukazovat na stejný oddíl druhého pevného disku. K instalaci systému Windows 2000 Professional musí dojít na primárním oddílu druhého pevného disku.

Upozornění Syspart automaticky označí jednotky za aktivní a výchozí spouštěcí zařízení. Proto před opakovaným zapnutím počítače jednotku vyjměte.

Mezi související definice patří:

Unattend.txt Soubor odpovědí používaný při bezobslužné instalaci, který poskytuje odpovědi na některé nebo všechny výzvy, na něž uživatel obvykle během instalace reaguje. Použití souboru odpovědí je při vytváření hlavního obrazu (bitové kopie) volitelné.

zdroj_instalace Umístění souborů systému Windows 2000 Professional. Chcete-li instalovat z více zdrojů současně, zadejte více přepínačů */s* příkazového řádku.

druhá_jednotka Volitelná druhá jednotka, na kterou předběžně nainstalujete systém Windows 2000 a aplikace.

Duplikování disků pomocí nástroje Sysprep

Duplikování disků je dobrou volbou, potřebujete-li nainstalovat identickou konfiguraci na více počítačů. Na hlavní počítač nainstalujete systém Windows 2000 a aplikace, které chcete mít instalované na všech cílových počítačích. Pak spustíte Sysprep a přenesete obraz na ostatní počítače. Sysprep připraví pevný disk na hlavním počítači, aby jej bylo možné duplikovat na ostatní počítače, a pak spustí proces kopírování disků od

nezávislého výrobce softwaru. Tato metoda dramaticky zkracuje čas zavedení v porovnání se standardními nebo skriptovými instalacemi.

Chcete-li použít Sysprep, váš hlavní a cílové počítače musí mít identické ovladače vrstvy HAL, podpory ACPI a zařízení hromadného ukládání dat. Systém Windows 2000 automaticky detekuje zařízení Plug-and-Play a Sysprep opakovaně detekuje a vyhodnocuje zařízení na systému v okamžiku startu počítače po proběhnutí nástroje Sysprep. To znamená, že zařízení Plug-and-Play, jako jsou síťové karty, modemy, grafické karty a zvukové karty, nemusejí být na cílových počítačích stejné jako na hlavním počítači. Hlavní výhodou instalace pomocí nástroje Sysprep je rychlost. Z obrazu disku lze udělat balíček a zkomprimovat jej a jako součást obrazu se vytvoří jen soubory potřebné pro danou konfiguraci. Na dalších systémech se vytvoří další potřebné ovladače Plug-and-Play. Obraz disku lze zkopírovat také na CD a tímto způsobem jej distribuovat do sídel s pomalým připojením.

Poznámka Protože hlavní a cílové počítače musí mít stejné ovladače HAL, podpory ACPI a zařízení hromadného ukládání dat, někdy může být nutné mít ve svém prostředí několik obrazů.

Důležité Během duplikování disku se u výrobce svého softwaru ujistěte, že neporušujete licenční dohodu instalace softwaru, který chcete duplikovat.

Přehled procesu Sysprep

Tento oddíl popisuje proces vytvoření zdrojového počítače, který se použije pro duplikování disku.

1. Nainstalujte systém Windows 2000. – Systém Windows 2000 Professional nainstalujte na počítač, který má hardware podobný cílovým počítačům. Při tvorbě tohoto počítače jej nesmíte připojit k doméně a heslo místní správy musí zůstat prázdné.
2. Nakonfigurujte počítač. – Přihlaste se jako správce a pak nainstalujte a nastavte systém Windows 2000 Professional a přidružené aplikace. Sem mohou patřit výrobní aplikace, jako je sada Microsoft Office 2000, obchodní či výrobní aplikace a další aplikace nebo nastavení, která jsou součástí společné konfigurace všech klientů.
3. Zkontrolujte obraz. – Pomocí auditování podle svých kritérií ověřte, že konfigurace obrazu (bitové kopie) je správná. Odstraňte nadbytečné informace včetně zbytků protokolů auditování a událostí.
4. Připravte obraz na duplikaci. – Jakmile jste si jisti, že je počítač nakonfigurován přesně podle vašich požadavků, můžete spustit přípravu systému na duplikování. Toho dosáhnete spuštěním nástroje Sysprep s volitelným souborem Sysprep.inf, který je popsán dále v této kapitole. Po dokončení funkce nástroje Sysprep se počítač automaticky vypne nebo oznámí, že je možné jej bezpečně vypnout.
5. Zadejte duplikování. – V tomto okamžiku je pevný disk počítače nastaven tak, že při dalším startu počítače se spustí detekce Plug-and-Play, vytvoření nových identifikátorů zabezpečení (SID) a spuštění minimální verze průvodce instalací. Nyní jste připraveni systém duplikovat pomocí nějakého hardwarového nebo softwarového řešení. Při dalším spuštění systému Windows 2000 Professional z tohoto disku nebo z jiného disku vytvořeného duplikováním daného obrazu bude systém detekovat a vyhodnocovat zařízení Plug-and-Play, čímž se dokončí instalace a konfigurace na cílovém počítači.

Důležité Komponenty, které závisí na službě Active Directory, nelze duplikovat.

Soubory nástroje Sysprep

Chcete-li použít nástroj Sysprep, ručně spusťte soubor Sysprep.exe nebo pomocí oddílu [GuiRunOnce] souboru odpovědí instalačního programu zajistíte, aby se Sysprep.exe spustil automaticky. Chcete-li použít nástroj Sysprep, musí se ve složce Sysprep v kořenu systémové jednotky (%systemdrive%\Sysprep\) nacházet soubory Sysprep.exe a Setupcl.exe. Jestliže si přejete umístit tyto soubory na správné místo během automatizované instalace, musíte je přidat do svých distribučních složek do podsložky \$OEM\$\\$1\Sysprep\. Další informace o této podsložce najdete v oddílu „Vytvoření struktury distribuční složky“ dříve v této kapitole.

Tyto soubory připraví operační systém na duplikování a spustí minimální verzi průvodce instalací. Ve složce Sysprep můžete také použít volitelný soubor odpovědí Sysprep.inf. Soubor Sysprep.inf obsahuje výchozí parametry, jejichž pomocí můžete zajistit konzistentní reakce na případné výzvy. Tím se omezuje požadavek na zadání od uživatelů a následně i možné chyby uživatelů. Soubor Sysprep.inf můžete umístit také na disketu, která musí být po zobrazení obrazovky spuštění systému Windows vložena do disketové jednotky. Tím je zajištěna možnost dalších úprav nastavení na cílovém počítači. Disketová jednotka čte data v okamžiku, kdy se objeví obrazovka „Prosím čekejte“ minimální verze průvodce instalací. Jakmile průvodce úspěšně dokončí svou činnost, systém ještě naposledy restartuje, odstraní se složka Sysprep a celý její obsah a systém je připraven na přihlášení uživatele.

Následující oddíly definují soubory nástroje Sysprep.

Sysprep.exe

Program Sysprep.exe má tři volitelné parametry:

- *quiet* – spustí Sysprep bez zobrazování hlášení.
- *nosidgen* – spustí Sysprep bez obnovení čísel SID, která již na systému existují. To je užitečné v případě, že nemáte v úmyslu duplikovat počítač, na němž je nástroj Sysprep spuštěný.
- *reboot* – automaticky restartuje počítač poté, co jej Sysprep vypne. Není tedy nutné počítač znovu ručně zapínat.

Sysprep.inf

Soubor Sysprep.inf je soubor odpovědí, který se používá k automatizaci procesu minimální verze průvodce instalací. Používá stejnou syntaxi souborů .ini a názvy klíčů (podporovaných) jako soubor odpovědí instalačního programu. Soubor Sysprep.inf je zapotřebí umístit do složky %systemdrive%\Sysprep nebo na disketu. Použijete-li disketu, musíte ji použít po zobrazení obrazovky spouštění systému Windows. Disketa se přečte v okamžiku, kdy se objeví obrazovka „Prosím čekejte“ průvodce instalací. Uvědomte si, že pokud soubor Sysprep.inf během spuštění nástroje Sysprep nevyužijete, průvodce zobrazí všechna dialogová okna vypsaná v dále uvedeném oddílu „Minimální verze instalačního programu“.

Poznámka Jestliže jste vytvořili soubor Sysprep.inf na hlavním počítači a potřebujete jej měnit podle jednotlivých počítačů, můžete použít dříve popsanou metodu disket.

Následující kód je příklad souboru Sysprep.inf:

```
[Unattended]
;Vyzvat uživatele k přijetí licenčních podmínek (EULA).
OemSkipEula=No
;Použít výchozí nastavení Sysprep a znovu vytvořit stránkový soubor
;systému, aby se vyrovnaly možné rozdíly ve velikosti dostupné RAM.
KeepPageFile=0
;Zadat umístění dodatečných jazykových souborů, které mohou být
;zapotřebí v případě globální organizace.
InstallFilePath=%systemdrive%\Sysprep\i386

[GuiUnattended]
;Zadat neprázdné heslo správce.
;Zadané heslo bude použito, pouze pokud bylo na původním zdroji obrazu
;(hlavním počítači) zadáno neprázdné heslo. Jinak bude heslo zadané
;na hlavním počítači heslem použitým i na tomto počítači. Lze jej
;zaměnit přihlášením se jako místní správce a ruční změnou hesla.
AdminPassword=""
;Nastavit časovou zónu.
TimeZone=20
;Přeskočit uvítací obrazovku při spouštění systému.
OemSkipWelcome=1
;Nepřeskočit dialogové okno místních nastavení, aby mohl uživatel
;zadat, která místní nastavení se použijí.
OemSkipRegional=0

[UserData]
;Znovu zadat informace o uživateli pro systém.
FullName="Autorizovaný uživatel"
OrgName="Název organizace"
ComputerName=XYZ_Pocitac1

[Identification]
;Připojit počítač do domény ITDOMAIN
JoinDomain=ITDOMAIN

[Networking]
;Svázat výchozí protokoly a služby k síťové kartě (kartám) použité
;v daném počítači.
InstallDefaultComponents=Yes
```

Poznámka Heslo správce lze pomocí souboru Sysprep.inf změnit, pouze pokud je existující heslo správce prázdné. To platí také v případě, kdy chcete změnit heslo správce pomocí grafického rozhraní nástroje Sysprep.

Další informace o oddílech souboru odpovědí a příkazech souvisejících se souborem Sysprep.inf najdete v dokumentu „Microsoft Windows 2000 Guide to Unattended Setup“ (Unattend.doc) na CD operačního systému Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému

Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

Setupcl.exe

Soubor Setupcl.exe vykonává toto:

- Vytváří nový identifikátor zabezpečení počítače.
- Spouští minimální verzi instalačního programu.

Minimální verze instalačního programu

Minimální verze instalačního programu se rozběhne při prvním spuštění počítače z disku duplikovaného metodou Sysprep. Tento průvodce získá všechny informace potřebné k dalšímu nastavení cílového počítače. Nepoužíváte-li soubor Sysprep.inf nebo necháte-li některé jeho oddíly prázdné, minimální verze instalačního programu zobrazí ta okna, jejichž otázky nebyly zodpovězeny v souboru Sysprep.inf. Možnými obrazovkami jsou:

- Licenční dohoda pro koncového uživatele (EULA)
- Místní volby
- Název uživatele a společnosti
- Název počítače a heslo správce
- Nastavení sítě
- Nastavení TAPI (zobrazí se, pouze existuje-li na počítači modem nebo nové modemové zařízení)
- Licence serveru (pouze u serveru)
- Volba časové zóny
- Dokončení/restart

Chcete-li přeskočit tyto obrazovky, musíte zadat určité parametry v souboru Sysprep.inf. Tyto parametry jsou uvedeny v tabulce 25.6.

Poznámka Protože instalační program zjišťuje optimální nastavení grafických zařízení, nezobrazí se již při probíhání instalačního programu nebo jeho minimální verze obrazovka „Nastavení zobrazení“. Nastavení zobrazení lze zadat buď v oddílu [Display] souboru odpovědí použitým pro váš hlavní počítač nebo v souboru Sysprep.inf použitým pro cílový počítač. Jsou-li v souboru odpovědí určeném pro hlavní počítač zadána nastavení [Display], Sysprep tato nastavení zachová, pokud nebude Sysprep.inf obsahovat jiná nastavení nebo nebude grafická karta či monitor požadovat nastavení, která se odlišují od nastavení na hlavním počítači.

Tabulka 25.6 Parametry přeskočení obrazovek minimální verze průvodce v souboru Sysprep.inf

Parametr	Hodnota
Místní volby	oddíl [RegionalSettings] [GuiUnattended] OemSkipRegional=1
Název uživatele a společnosti	[UserData] FullName="Název uživatele" OrgName="Název organizace"
Název počítače a heslo správce	[UserData] ComputerName=W2B32054 [GuiUnattended] AdminPassword=""
Nastavení sítě	[Networking] InstallDefaultComponents=Yes
Nastavení TAPI	[TapiLocation] AreaCode=425
Licencování serveru (pouze server)	[LicenceFilePrintData] AutoMode = PerServer AutoUsers = 5
Výběr časové zóny	[GuiUnattended] TimeZone=<index požadované časové zóny>
Dokončení/restart	Nelze aplikovat

Ruční spuštění nástroje Sysprep

Po instalaci systému Windows 2000 Professional můžete připravit systém na přenos na jiné podobně konfigurované počítače pomocí nástroje Sysprep. Chcete-li Sysprep spustit ručně, musíte nejprve nainstalovat systém Windows 2000 Professional, nakonfigurovat jej a nainstalovat aplikace. Pak spusíte Sysprep bez přepínače *-reboot* příkazového řádku. Jakmile se systém vypne, duplikujte obraz jednotky na podobně nakonfigurované počítače.

Když uživatelé poprvé spustí své duplikované počítače, spustí se minimální verze instalace nástroje Sysprep, která umožní uživatelům nastavení jejich systémů. Pomocí souboru Sysprep.inf můžete také přednastavit některé nebo všechny konfigurační parametry nástroje Sysprep. Složka Sysprep (která obsahuje soubory Sysprep.exe a Setupcl.exe) se po dokončení minimální verze průvodce nástroje Sysprep automaticky odstraní.

▼ Chcete-li připravit instalaci systému Windows 2000 Professional na duplikování, postupujte takto:

1. Stiskněte tlačítko **Start**, zadejte příkaz **Spustit** (Run) a pak запиšte:

```
cmd
```

2. V příkazovém řádku se přepněte do kořenové složky jednotky C a pak zadejte:

```
md sysprep
```

3. Vložte do mechaniky CD systému Windows 2000 Professional. Otevřete si soubor Deploy.cab ve složce \Support\Tools.
4. Zkopírujte soubory Sysprep.exe a Setupcl.exe do složky Sysprep.
Používáte-li soubor Sysprep.inf, také jej zkopírujte do složky Sysprep. Uvědomte si, že pro zajištění správné funkce nástroje Sysprep se musí soubory Sysprep.exe, Setupcl.exe a Sysprep.inf nacházet ve stejné složce.
5. V příkazovém řádku se přepněte do složky Sysprep:

```
cd sysprep
```

6. Podle potřeby zadejte jeden z následujících příkazů:

```
Sysprep  
Sysprep -reboot  
Sysprep /<volitelný parametr>  
Sysprep /<volitelný parametr> -reboot  
Sysprep /<volitelný parametr 1>.../<volitelný parametr X>  
Sysprep /<volitelný parametr 1>.../<volitelný parametr X> -reboot
```

7. Jestliže nezadáte přepínač **-reboot** příkazového řádku, vykonáte následující:
Jakmile se objeví zpráva o tom, že máte vypnout počítač, zadejte příkaz **Vypnout** (Shut Down) nabídky **Start**. Nyní můžete použít nástroj kopírování disků jiného výrobce a vytvořit obraz instalace.
8. Jestliže jste zadali přepínač **-reboot** příkazového řádku pouze pro účely auditování, pak se počítač restartuje a spustí se minimální verze průvodce instalací. V takovém případě vykonáte následující:
 - Zkontrolujte, že minimální verze instalace zobrazuje požadované výzvy. V tomto okamžiku můžete také auditovat systém a další aplikace. Jakmile je auditování ukončeno, opakovaně spusíte Sysprep bez přepínače **-reboot** příkazového řádku.
 - Jakmile se objeví zpráva o tom, že máte vypnout počítač, zadejte příkaz **Vypnout** (Shut Down) nabídky **Start**. Nyní můžete použít nástroj kopírování disků jiného výrobce a vytvořit obraz instalace.

Poznámka Do složky Sysprep můžete také přidat soubor Cmdlines.txt, který instalační program následně zpracuje. Tento soubor spustí příkazy po dokončení instalace včetně těch požadovaných pro instalaci aplikací.

Automatické spuštění nástroje Sysprep po dokončení instalačního programu

Oddíl [GuiRunOnce] souboru odpovědí obsahuje příkazy vykonané po dokončení instalačního programu. Oddíl [GuiRunOnce] můžete použít k vytvoření instalace, která dokončí instalační program, automaticky se přihlásí k počítači, spustí nástroj Sysprep v režimu *-quiet* a nakonec počítač vypne. Aby k tomu všemu došlo, musíte zajistit následující:

1. Potřebné soubory nástroje Sysprep umístíte do distribuční složky \$OEM\$\\$1\Sysprep\, aby se zkopírovaly na správné místo na systémové jednotce.

2. Do oddílu [GuiRunOnce] souboru odpovědí zadejte následující poslední příkaz, který se spustí na počítači:

```
%systemdrive%\Sysprep\Sysprep.exe -quiet
```

Je-li zapotřebí více restartů, zadejte tento příkaz tak, aby byl spuštěn jako poslední při posledním použití oddílu [GuiRunOnce].

Rozšiřování diskových oddílů pomocí nástroje Sysprep

Grafický instalační program systému Windows 2000 a jeho minimální verzi lze použít k rozšíření oddílů NTFS prostřednictvím souborů odpovědí. Tento nový prvek má tyto funkce:

- Umožňuje vám vytvářet obrazy, které lze rozšířit na větší diskové oddíly a plně tak využít pevné disky, jež mají více prostoru než původní pevný disk na hlavním počítači.
- Umožňuje vytvářet obrazy na menších discích.

Abyste určili nejlepší možnosti integrace této funkce do svého prostředí, musíte projít následující kroky a na základě nástrojů používaných k vytváření obrazů operačního systému vybrat metodu, která bude ve vašem případě fungovat nejlépe.

Upozornění Jestliže vám vaše nástroje obrazů umožňují obraz upravovat, můžete odstranit soubory Pagefile.sys, Setupapi.log a Hyberfil.sys (jestliže existují), protože tyto soubory na cílovém počítači minimální verze instalace znovu vytvoří. Tyto soubory nesmíte odstranit na aktivním systému, protože to může znamenat chybnou funkci systému. Tyto soubory však lze v případě potřeby odstranit z obrazu.

▼ Chcete-li rozšířit oddíl pevného disku při použití nástroje vytváření obrazů od jiného výrobce nebo hardwarového zařízení vytváření obrazů, které podporuje systém NTFS používaný Windows 2000, postupujte takto:

1. Nakonfigurujte oddíl na pevném disku hlavního počítače tak, aby měl minimální velikost nutnou pro instalaci systému Windows 2000 a všech jeho komponent a aplikací, které chcete předběžně instalovat. Tím se omezí požadavky na celkovou velikost obrazu.
2. Do oddílu [Unattended] souboru odpovědí, který se používá k vytvoření hlavního obrazu, vložte příkaz FileSystem=ConvertNTFS. Nemusíte sem zadávat parametr ExtendOemPartition, protože chcete udržet co nejmenší možnou velikost obrazu.

Poznámka Příkaz ConvertNTFS v souboru Sysprep.inf nefunguje, protože se jedná výhradně o funkci textového režimu a nástroj Sysprep textovým režimem neprochází.

3. Do oddílu [Unattended] souboru Sysprep.inf vložte příkaz:

```
ExtendOemPartition = 1
```

(nebo jinou velikost v megabajtech, o kterou se má oddíl rozšířit)

4. Nainstalujte systém Windows 2000 na hlavní počítač. Nástroj Sysprep systém automaticky vypne.
5. Vytvořte obraz (bitovou kopii) jednotky.

6. Umístěte obraz na cílový počítač, kde má cílový počítač stejnou velikost systémového oddílu jako hlavní počítač.
7. Restartujte cílový počítač.
Spustí se minimální verzi instalačního programu a téměř okamžitě dojde k rozšíření oddílu.

▼ **Chcete-li rozšířit oddíl pevného disku při použití nástroje vytváření obrazů, který nepodporuje systém NTFS používaný systémem Windows 2000, postupujte takto:**

1. Nakonfigurujte oddíl na pevném disku hlavního počítače tak, aby měl minimální velikost nutnou pro instalaci systému Windows 2000 a všech jeho komponent a aplikací, které chcete předběžně instalovat. Tím se omezí požadavky na celkovou velikost obrazu.
2. Převedte systém souborů pomocí nástroje Convert.exe, který je součástí systému Windows 2000, na NTFS.
3. Do oddílu [GuiRunOnce] souboru odpovědí, který se používá k vytvoření hlavního obrazu, vložte jako poslední dvě položky následující příkazy:

```
[GuiRunOnce]
<Příkaz1> = „<příkazový řádek>“
<Příkaz2> = „<příkazová řádek>“
...
<Příkazn-1> = „Convert c:\ /fs:ntfs“
<Příkazn> = „%systemdrive%\sysprep\sysprep.exe -quiet“
```

kde:

- <příkazový řádek> zahrnuje všechny příkazy, které je zapotřebí spustit v zájmu instalace aplikací nebo konfigurace operačního systému před vytvořením jeho obrazu.
- <Příkazn-1> je předposlední příkaz, který se vykoná v oddílu [GuiRunOnce] souboru odpovědí. Tím se spustí program **convert**. Protože program Convert nemůže převést aktivní systém na NTFS v době, kdy běží operační systém, operační systém se nastaví tak, aby k tomu došlo při dalším restartu. Jelikož následující spouštěnou položkou je Sysprep, systém se v tomto procesu nepřevede na NTFS.
- <Příkazn> je poslední příkaz spuštěný na počítači. To musí být Sysprep.exe. Po svém spuštění připraví Sysprep počítač na vytváření obrazů a pak počítač vypne.

Poznámka Do souboru odpovědí nemůžete v tomto kroku zahrnout parametr ExtendOemPartition, protože oddíl, na kterém je obraz vytvořen, není NTFS. Také bude vhodné mít co nejmenší obraz.

4. Do oddílu [Unattended] souboru Sysprep.inf vložte příkaz:

```
ExtendOemPartition = 1
```

(nebo jinou velikost v megabajtech, o kterou se má oddíl rozšířit)

5. Nainstalujte systém Windows 2000 na hlavní počítač. Nástroj Sysprep systém automaticky vypne.

Důležité Počítač nerestartujte.

6. Vytvořte obraz jednotky.
7. Umístěte obraz na cílový počítač, kde má cílový počítač stejnou velikost systémového oddílu jako hlavní počítač.
8. Restartujte cílový počítač.

Program nejprve převede systémový oddíl cílového počítače na NTFS.

Počítač se pak automaticky restartuje.

Spustí se minimální verze instalačního programu a téměř okamžitě dojde k rozšíření oddílu.

Použití serveru Systems Management Server

K zajištění spravovaných inovací programu Windows 2000 Professional na více systémech, zejména jsou-li geograficky roztroušené, můžete použít server SMS. Uvědomte si, že SMS se používá pouze při instalaci na počítače obsahující již dříve instalovaný operační systém. Před inovací pomocí SMS je důležité vyhodnotit stávající síťovou infrastrukturu včetně šířky přenosového pásma, hardwaru a geografických omezení. Hlavní výhodnou inovace pomocí SMS je, že můžete udržovat centralizované řízení procesu inovace. Můžete například řídit, kdy k inovaci dojde (například během školení nebo po něm, po ověření hardwaru a po zálohování uživatelských dat), které počítače se budou inovovat a jak se budou aplikovat síťová omezení. Další informace o zavedení pomocí serveru SMS najdete v kapitole „Zavádění systému Windows 2000 pomocí serveru Systems Management Server“ v této knize.

Použití spustitelného kompaktního disku

Metodu instalace systému Windows 2000 Professional pomocí spustitelného CD lze použít na počítači, jehož systém základních vstupů a výstupů (BIOS) umožňuje spuštění počítače z CD. Tato metoda je velmi užitečná u počítačů ve vzdálených sídlech s pomalým připojením a bez místního oddělení IT. Metoda spustitelného CD používá Winnt32.exe, což umožňuje rychlou instalaci.

Poznámka Metodu spustitelného CD lze použít pouze pro čisté instalace. Chcete-li vykonat inovaci, musíte spustit Winnt32.exe z existujícího operačního systému.

Pro zajištění maximální flexibility nastavte následující pořadí spouštění v systému BIOS:

- Síťová karta
- CD
- Pevný disk
- Disketa

Chcete-li použít spustitelné CD, musí být splněna následující kritéria:

- Váš počítač musí podporovat spustitelná CD standardu El Torito bez emulace.
- Soubor odpovědí musí obsahovat oddíl [Data] s potřebnými klíči.
- Soubor odpovědí musí být pojmenován Winnt.sif a musí být umístěn na disketě.

Další informace o parametrech a syntaxi souboru odpovědí najdete v dokumentu „Microsoft Windows 2000 Guide to Unattended Setup“ (Unattend.doc) na CD operačního systému Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

▼ **Chcete-li nainstalovat systém Windows 2000 Professional pomocí spustitelného kompaktního disku, postupujte takto:**

1. Spustíte systém z CD Windows 2000 Professional.
2. Jakmile se objeví modrá obrazovka „Instalace systému Windows 2000“ v textovém režimu, vložte do disketové jednotky disketu obsahující soubor Winnt.sif.
3. Když počítač přečte z diskety potřebné informace, disketu z mechaniky odstraňte. Nyní se spustí instalace z CD, jak je zadáno v souboru Winnt.sif.

Poznámka Metoda spustitelného CD vyžaduje, aby byly všechny potřebné soubory na CD. Ve spojení s touto metodou nelze použít soubory Uniqueness Database Files (UDB).

Použití vzdálené instalace operačního systému

Vzdálená instalace operačního systému je volitelná součást systému Windows 2000 Server, která vychází z technologie Služeb vzdálené instalace (Remote Installation Services – RIS). Protože služba RIS používá technologii vzdáleného spouštění PXE a software serveru, můžete vzdáleně instalovat obraz (bitovou kopii) systému Windows 2000 Professional na podporované počítače a nemusíte při instalaci fyzicky navštěvovat jednotlivé počítače. Musíte však zajistit kompatibilitu hardwaru každého počítače a instalaci síťové karty podporující funkci spouštění. Pro každou konfiguraci specifickou nějaké skupině počítačů můžete vytvořit jiný obraz RIS. Během instalace se nabídnou seznam možností instalace, který lze omezit podle zásad nastavených pro danou skupinu uživatelů nebo počítačů. Udržovaných obrazů RIS může existovat až tolik, jako různých sad zásad skupiny. V takovém případě bude výhodné, když se budou touto metodou instalovat pouze možnosti instalace společné všem konfiguracím.

Další informace o funkci vzdálené instalace operačního systému najdete v kapitole „Aplikování správy změn a konfigurací“ v této knize a v kapitole „Vzdálená instalace OS“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.

Dopady zavedení serveru RIS na zatížení sítě

Protože se k instalaci obrazů operačního systému na klientské počítače používá server RIS, zatížení vytvářené tímto serverem se podobá provozu, který na vaší síti vytvářejí jiné servery fungující jako body instalace operačních systémů. Obecně je provoz serveru RIS předvídatelnější než provoz bodů instalace softwaru s obecným účelem, které nabízejí různé aplikační a pravidelné inovace. Provoz vytvářený serverem RIS je větší, když si obrazy nahrává mnoho uživatelů – například během nového zavedení obrazů operačních systémů nebo když se k síti přidá skupina nových počítačů. Po instalaci systému bude stále denní zatížení nižší.

Obecně platí, že byste server RIS měli umístit poblíž klientských počítačů, které bude obsluhovat. Výsledný provoz v síti tak bude pouze lokální a jeho vliv bude omezený.

Jestliže vaše prostředí vyžaduje některý z následujících procesů, umožněte jejich optimalizaci bez vlivu na další aplikace:

- Časté opakované instalace systémů, například ve školící místnosti.
- Pravidelná instalace většího počtu systémů, jako třeba při předběžné instalaci všech nových systémů před jejich odesláním uživatelům.

V případě školící místnosti zvažte segmentaci fyzické sítě a zajištění vyhrazeného serveru RIS pro každou učebnu nebo skupinu učeben, kterou dokáže hardware vašeho serveru RIS podporovat.

V případě předběžných instalací zvažte vytvoření instalačních laboratoří, kde lze pomocí vysokorychlostní sítě a výkonného hardwaru serveru RIS zpracovávat větší množství počítačů při zkrácení instalačního času.

Optimalizace výkonu

Protože vzdálená instalace operačního systému je převážně proces kopírování souborů, obecné faktory výkonu serveru RIS se podobají faktorům jiných serverů s výrazně zatěžovanými vstupy a výstupy (I/O), jako jsou webové servery a souborové a tiskové servery. Mezi tyto faktory patří propustnost disku serveru a šířka pásma sítě. Při optimalizaci výkonu serverů RIS vyhodnoťte tyto faktory a další omezení, která mohou existovat na síti mezi servery RIS a obsluhovanými klienty. Pokud je server RIS na svém připojení k síti přetížen, výsledkem je delší doba instalace klientských počítačů a vypršení relací TFTP během počáteční fáze kopírování souborů.

Protokol DHCP a Servery DHCP

Protože klienti podporující vzdálenou instalaci operačního systému (podporující PXE) používají k získání síťové adresy a nalezení serverů RIS mechanismus vyhledávání protokolu DHCP, vztah mezi RIS a DHCP ve vaší organizaci hraje při určování strategie umísťování serverů RIS klíčovou roli.

V jednoduchých prostředích je obvyklým řešením přidání serveru RIS ke každému používanému serveru DHCP. Při použití kombinace serverů DHCP/RIS systému Windows 2000 se omezuje počet počátečních síťových paketů odesílaných mezi klientem RIS a servery DHCP a RIS a také počáteční reakce serveru je rychlejší. Navíc kombinace serverů DHCP/RIS systému Windows 2000 vždy odpovídá klientovi společně. Jedná se vlastně o jednoduchou formu vyrovnávání zatížení, která využívá již vytvořené plánování seskupující klientské počítače se servery DHCP, a zároveň se také zjednodušuje řešení problémů a procedury správy.

Zatímco servery RIS musí být umístěny blízko klientských počítačů a mohou vytvářet velká zatížení sítě, a proto musí mít často ten nejvýkonnější hardware, pro servery DHCP platí přesný opak. Servery DHCP vytvářejí mnohem méně síťového provozu, obvykle nevyžadují nejvýkonnější serverový hardware a někdy jsou centralizovány a nenacházejí se blízko klientských počítačů. Proto můžete zjistit, že jednoduché přidání serveru RIS na existující server DHCP je nepraktické. V takových případech můžete přidat služby RIS na existující servery bodů instalace softwaru, protože pro ně platí podobné plánovací požadavky a potřeby umístění, jako pro servery RIS. Můžete také vytvořit servery RIS nezávisle na dalších podpůrných serverech.

Jestliže jsou servery RIS odděleny od serverů DHCP nebo používají-li se servery DHCP s jiným systémem než Windows 2000, nejdůležitějším problémem se stává řízení toho, který server RIS bude odpovídat na požadavky specifických klientů. Je tomu tak pro-

to, že proces vzdáleného spouštění PXE neposkytuje možnost určit, ze kterého serveru klient službu získá. Další informace o metodách řízení tohoto procesu najdete v oddílu „Řízení výběru serveru RIS a vyrovňování zatížení“ dále v této kapitole.

Bez ohledu na vaše konkrétní řešení zkombinování serverů DHCP a RIS musí být každý server RIS autorizován ve službě Active Directory – to zabráňuje obsluhu klientů neautorizovanými servery. K procesu autorizace serverů RIS i serverů DHCP systému Windows 2000 dochází v modulu snap-in DHCP konzoly Microsoft Management Console (MMC). Tento proces nemá přímý vztah ani ke zkombinování či oddělení serverů RIS a DHCP, ani k používání služby DHCP systému Windows 2000. Modul snap-in DHCP systému Windows 2000 se prostě opakovaně používá jako mechanismus ověření a lze jej spustit i bez instalace služby DHCP na některém z počítačů se systémem Windows 2000, na kterém je instalovaný balíček nástrojů pro správce (Administrator Tools).

Upozornění Nepokoušejte se instalovat službu DHCP na server RIS systému Windows 2000 jenom proto, abyste získali zmíněný modul snap-in. Aby bylo možné obsluhovat klienty RIS, každý zkombinovaný server DHCP a RIS systému Windows 2000 musí mít plně funkční službu DHCP (včetně definovaných a aktivních rozsahů). Služba DHCP na kombinovaném serveru systému Windows 2000 totiž ví, že je také instalován server RIS. Jestliže klient ve svém vysílání vyhledávání DHCP indikuje, že požaduje jak DHCP tak i služby vzdáleného spouštění, služba DHCP vystaví jedinou odpověď obsahující specifické podrobnosti o protokolu DHCP a vzdáleném spouštění na daném serveru. Jestliže služba DHCP systému Windows 2000 na serveru neodpovídá klientům řádně, daný server nevytvoří odpověď na vzdálené spuštění.

Řízení výběru serveru RIS a vyrovňování zatížení

Standardně platí, že když klient PXE odvysílá svůj požadavek na službu, odpoví mu všechny servery, které tento požadavek obdrží. Prvním reagujícím serverem je ten, který službu poskytuje; přednost před odpověďmi ze samostatných serverů se dává odpovědím z kombinovaných serverů DHCP/RIS. Tím je sice zaručeno základní vyrovňování zatížení v případě dostupnosti více serverů klientovi, aby však klienti nemohli používat nesprávné servery, je často nejlepší určit, které servery mohou odpovídat specifickým klientům. Příkladem je server, který je z hlediska klienta místní, ale který je v okamžiku požadavku na službu od klienta plně vytížený nebo odstavený.

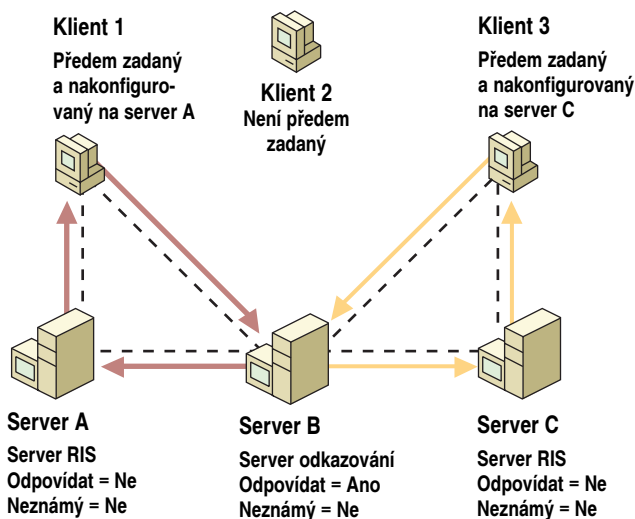
První možností řízení výběru serveru je fyzicky řídit směřování v síti, aby se vysílání vyhledávání DHCP předala pouze v případech, kdy je to zapotřebí. To fyzicky umožní odpovídat pouze těm serverům DHCP/RIS, které mají povoleno přijmout požadavky na službu od klientů. Jestliže jsou vaše servery DHCP/RIS v podobných místech na síti vzhledem ke klientům, může toto řešení postačovat.

Abyste mohli použít také jiné scénáře, služba vzdálené instalace operačního systému poskytuje další funkce řízení výběru serveru. Tyto funkce zahrnují konfigurování účtů klientských počítačů ve službě Active Directory tak, aby používaly určitý server RIS. Tento proces se označuje za „předběžné nastavení“. Předběžné nastavení lze vykonat na existujících účtech počítačů i při vytváření nových účtů počítačů, ještě než se systém připojí k doméně. Když server RIS odpoví na požadavek na službu od klienta, server prověří ve službě Active Directory (v celé doménové struktuře) existenci účtu počítače s globálně jednoznačným identifikátorem (GUID) odpovídajícím identifikátoru GUID, který je součástí požadavku na službu. Je-li nalezen odpovídající účet počítače, zjistí se, zda nebyl nakonfigurován na použití specifického serveru RIS. Je-li tomu tak, server RIS

zadaný v účtu počítače bude vždy obsažen v odpovědi klientovi, i když se jedná o jiný server, než který poskytuje klientovi prvotní odpověď. Tato technika se označuje za *odkazování serverů* a představuje jednoduchý způsob určení, jaké servery RIS budou nakonec specifickým klientským počítačem poskytovat služby instalace operačního systému. Přitom nezáleží na tom, který konkrétní server RIS odpověděl na první požadavek na službu od klienta.

Chcete-li dosáhnout další flexibility a zabezpečení, můžete zkombinovat techniky předběžného nastavení a odkazování serverů s nastaveními serveru RIS, která ovládají způsob reakce serverů na klienty. Každý server RIS má dvě nastavení: „Odpovědět klientským počítačům požadujícím službu“ (Respond to client computers requesting service) a „Neodpovídat neznámým klientským počítačům“ (Do not respond to unknown client computers). Když zavedete předběžné nastavení na všech účtech počítačů a selektivně budete řídit, které servery RIS jsou nakonfigurovány na odpovídání klientům, můžete vytvořit servery vyhrazené pro odpovídání na požadavky na služby od klientů a poskytnutí příslušných odkazů a servery zajišťující vlastní služby vzdálené instalace OS klientům.

Obrázek 25.3 ukazuje příklad vztahu klientských počítačů k serverům RIS.



Vysvětlení konfigurace serverů:

Odpovídat = Odpovídat klientským počítačům

Neznámý = Neodpovídat neznámým klientským počítačům

Obrázek 25.3 Příklad vztahu klientských počítačů k serverům RIS

Na obrázku 25.3 bude klientským počítačům požadujícím službu odpovídat pouze počítač B. Protože klientské počítače 1 a 3 byly předem nastaveny a nakonfigurovány na využívání služeb určitého serveru RIS, obdrží odpověď odkazující je na příslušný server (A nebo C). Je-li to zapotřebí, je možné vytvořit více odkazujících serverů, jako je server B. Všechny takové servery budou k určení správného odkazu používat předem nastavené účty počítačů ve službě Active Directory. Servery A a C nikdy neodpoví na

počáteční požadavek na službu od klienta. Přes odkazování však budou tyto servery zajišťovat vlastní služby instalace operačního systému pro klienty.

Pak můžete určit, zda musí být konfigurační volba „Neodpovídat neznámým klientským počítačům“ zadána na odkazovacích serverech, jako je server B. Výběr této možnosti zaručí, že:

- server B bude odesílat odpovědi pouze předem nastaveným klientským počítačům;
- pokud jsou nějací klienti nakonfigurováni tak, aby přijímali službu speciálně z tohoto serveru, server B se vlastně stane vyhrazeným serverem odkazování nebo bude také poskytovat vlastní služby instalace operačního systému.

Není-li vybrána volba „Neodpovídat neznámým klientským počítačům“, server B bude reagovat i na požadavky na služby od předem nenastavených klientů (v našem případě klientského počítače 2) a bude se nabízet jako server vzdáleného spouštění.

Ať už používáte servery odkazování nebo ne, výběr položky „Neodpovídat neznámým klientským počítačům“ zajišťuje prostředek zabezpečení zabráňující klientským počítačům, které nebyly předem nastaveny, ve vykonání instalace operačního systému ze serverů RIS. Navíc výrobci nabízející řešení vycházející ze stejného protokolu vzdáleného spouštění jako služba vzdálené instalace operačního systému neposkytují vždy možnosti řízení toho, na které klientské požadavky služeb se bude odpovídat. Pomocí předběžného nastavení a omezením reakcí serverů RIS pouze na známé klientské počítače umožníte implementování funkce vzdálené instalace operačního systému bez narušení sítě, která obsahuje další produkty vzdáleného spouštění.

Práce se směrovači

Protože klientské požadavky na služby vycházejí z procesu vyhledávání protokolu DHCP, konfigurace sítě pro podporu vzdálené instalace operačního systému přes směrovače má stejné požadavky, jako podpora DHCP přes směrovače.

Směrovače nakonfigurované na předávání vysílání DHCP budou také automaticky předávat dále klientské požadavky na služby. Kromě předávání na servery DHCP však musíte zajistit také předání požadavků příslušným serverům RIS. Podle používaných modelů směrovačů může být podporována konfigurace specifických směrovačů předávání vysílání DHCP buď na podsít (neboli rozhraní směrovače) nebo specifickému hostiteli. Používáte-li službu DHCP systému Windows 2000, ale přitom máte servery RIS na samostatných počítačích, nebo jestliže používáte službu DHCP jiného systému než Windows 2000, musíte zajistit, aby směrovače předávaly vysílání DHCP jak serverům DHCP tak i serverům RIS. Jinak klient neobdrží odpověď na požadavek vzdáleného spouštění.

Protože instalace operačního systému představuje značný síťový provoz, pečlivě zvažte umístění serverů RIS a použití předběžného nastavení a odkazovacích serverů. Musíte použít konfiguraci odpovídající vašemu stávajícímu návrhu sítě, která zároveň zajistí minimalizaci vlivu klientských instalací.

Příklady konfigurace instalace

Následující příklady obsahují procedury instalace systému Windows 2000 Professional na počítačích s již existující klientskou konfigurací i bez ní.

Existující klientské počítače

Příklady v tomto oddílu jsou pro počítače s následujícími již existujícími klientskými konfiguracemi:

- Počítače se systémem Windows NT Workstation 4.0 s klientskými aplikacemi kompatibilními s programem Windows 2000 Professional.
- Počítače se systémem Microsoft Windows NT Workstation verze 3.5 či dřívější a klientské počítače s operačními systémy nepocházejícími od společnosti Microsoft.

Příklad 1: Windows NT Workstation 4.0

s klientskými aplikacemi kompatibilními se systémem Windows 2000

Vykonejte inovaci. Mezi klientské operační systémy, které lze inovovat, patří Windows 95, Windows 98, Windows NT Workstation 4.0 a Windows NT Workstation 3.51.

Další informace o aplikacích kompatibilních se systémem Windows 2000 Professional najdete v odkazu Directory of Windows 2000 Applications stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

▼ Chcete-li instalovat systém Windows 2000 Professional na počítače s kompatibilním hardwarem, postupujte takto:

1. Zálohujte uživatelská nastavení.
2. Inovujte systém jednou z následujících metod:
 - Iniciujte nevyžádanou (plně automatickou) instalaci jednou z následujících akcí:
 - Použijte software správy systémů, jako je například Microsoft Systems Management Server.
 - Vykonejte síťovou instalaci.
 - Vykonejte vzdálené spuštění. To vyžaduje nakonfigurovaný server vzdáleného spouštění a instalovanou síťovou kartu podporující spouštění.
 - Iniciujte místní instalaci spuštěním souboru Winnt32.exe z příkazového řádku s potřebnými parametry a dále:
 - Vykonejte ruční instalaci (bez souboru odpovědí) a zodpovězte všechny výzvy.
 - Vykonejte automatickou nebo poloautomatickou instalaci se souborem odpovědí. Při plně automatické instalaci poskytne soubor odpovědí odpovědi na všechny otázky. Poloautomatická instalace vám umožní příjem určitých vámi vybraných zadání od uživatelů.

▼ Chcete-li instalovat systém Windows 2000 Professional na počítač s nekompatibilním hardwarem, u kterého není zapotřebí vyměnit pevný disk, postupujte takto:

1. Vyměňte potřebný hardware s výjimkou pevného disku.
2. Proveďte, že všechny nový hardware řádně funguje.
3. Zálohujte uživatelská nastavení.
4. Inovujte systém jednou z následujících metod:
 - Iniciujte nevyžádanou (plně automatickou) instalaci jednou z následujících akcí:
 - Použijte software správy systémů, jako je například Microsoft Systems Management Server.
 - Vykonejte síťovou instalaci.

- Vykonejte vzdálené spuštění. To vyžaduje nakonfigurovaný server vzdáleného spouštění a instalovanou síťovou kartu podporující spouštění.
- Iniciujte místní instalaci spuštěním souboru Winnt32.exe z příkazového řádku s potřebnými parametry a dále:
 - Vykonejte ruční instalaci (bez souboru odpovědí) a zodpovězte všechny výzvy.
 - Vykonejte automatickou nebo poloautomatickou instalaci.

▼ **Chcete-li instalovat systém Windows 2000 Professional na počítač s nekompatibilním hardwarem, u kterého je zapotřebí vyměnit pevný disk, postupujte takto:**

1. Inovujte alespoň jednu z následujících položek:
 - Paměť RAM
 - Procesor
2. Provéřte, že všechny nový hardware řádně funguje.
3. Zálohujte uživatelská nastavení.

Poznámka I když je možné zálohovat před inovací počítače celý obsah pevného disku na nový pevný disk, v případě klientských počítačů to obvykle není nutné.

4. Vyměňte pevný disk. Zkopírujte na něj zálohovaný obraz.
5. Jednou z následujících metod spusťte soubor Winnt.exe z příkazového řádku s požadovanými parametry:
 - Vykonejte ruční instalaci (bez souboru odpovědí) a zodpovězte všechny výzvy.
 - Vykonejte automatickou nebo poloautomatickou instalaci. Použijte jednu z následujících metod:
 - Instalace ze spustitelného disku CD-ROM.
 - Syspart. To je užitečné při instalaci nových pevných disků na počítače.
 - Sysprep. Tento nástroj použijte při instalaci na identické počítače (ovladače vrstev HAL a zařízení hromadného ukládání dat musí být stejné).
 - Vzdálené spuštění. Tato metoda vyžaduje nakonfigurovaný server RIS a instalovanou síťovou kartu podporující vzdálené spouštění.
6. Nainstalujte aplikace kompatibilní se systémem Windows 2000 Professional.
7. Podle potřeby ověřte funkce systému.
8. Importujte uživatelská nastavení (například Regedit/Regedt32, přihlašovací skripty, zásady a cestovní profily).

Příklad 2: Počítače se systémem Windows NT Workstation 3.5 či dřívějším a klientské počítače s operačními systémy nepocházejícími od společnosti Microsoft

Mezi klientské operační systémy, které nelze přímo inovovat, patří MS-DOS, Windows 3.x, Windows NT Workstation 3.5 nebo dřívější a OS/2.

Chcete-li se připravit na čistou instalaci, obstarajte si klientský počítač sestavený vaším partnerem OEM nebo poskytovatelem řešení. Chcete-li vykonat čistou instalaci na novém počítači nebo instalovat operační systém na existující počítač, postupujte podle dále uvedených kroků.

Poznámka Další informace o aplikacích kompatibilních se systémem Windows 2000 Professional najdete v odkazu Directory of Windows 2000 Applications stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

▼ **Chcete-li instalovat systém Windows 2000 Professional na klientský operační systém, který nelze inovovat, postupujte takto:**

1. Zálohujte uživatelská nastavení.

Upozornění Jestliže nainstalujete systém Windows 2000 Professional na existující počítač s operačním systémem, který nelze přímo inovovat na Windows 2000, všechna uživatelská nastavení budou ztracena.

2. Jednou z následujících metod spusťte soubor Winnt.exe z příkazového řádku s požadovanými parametry:
 - Vykonejte ruční instalaci (bez souboru odpovědí) a zodpovězte všechny výzvy.
 - Vykonejte automatickou nebo poloautomatickou instalaci. Použijte jednu z následujících metod:
 - Instalace ze spustitelného disku CD-ROM.
 - Syspart. To je užitečné při instalaci nových pevných disků na počítače.
 - Sysprep. Tento nástroj použijte při instalaci na identické počítače (ovladače vrstev HAL a zařízení hromadného ukládání dat musí být stejné).
 - Vzdálené spuštění. Tato metoda vyžaduje nakonfigurovaný server RIS a instalovanou síťovou kartu podporující vzdálené spuštění.
3. Nainstalujte aplikace kompatibilní se systémem Windows 2000 Professional.
4. Podle potřeby ověřte funkce systému.
5. Importujte uživatelská nastavení (například Regedit/Regedt32, přihlašovací skripty, zásady a cestovní profily).

Nové klientské počítače

Klientské počítače bez jakéhokoli operačního systému dřívější verze než Windows 2000 vyžadují čistou instalaci systému Windows 2000 Professional.

Na instalaci se připravte získáním klientského počítače od partnera OEM nebo poskytovatele řešení.

▼ **Chcete-li instalovat systém Windows 2000 Professional na počítač, na kterém není instalován žádný dřívější operační systém, postupujte takto:**

- Vykonejte ruční instalaci (bez souboru odpovědí) a zodpovězte všechny výzvy.
- Vykonejte automatickou nebo poloautomatickou instalaci. Použijte jednu z těchto metod:
 - Metodu spustitelného CD.
 - Metodu Syspart. To je užitečné při instalaci nových pevných disků do počítačů.
 - Metodu Sysprep. Používá se při instalaci na identické počítače (ovladače HAL a zařízení hromadného ukládání dat musí být shodné).

- Metodu spouštěcí diskety a spuštění instalačního programu se souborem odpovědí.
- Metodu vzdáleného spuštění. Tato metoda vyžaduje nakonfigurovaný server RIS a instalovanou síťovou kartu podporující vzdálené spuštění.

Seznam úkolů plánování instalace

Tabulka 25.7 představuje souhrn hlavních úkolů souvisejících s instalací systému Windows 2000 Professional a požadovaných aplikací.

Tabulka 25.7 Přehled úkolů instalace

Úkol	Umístění v kapitole
Vyřešte kritické problémy plánování.	Řešení kritických problémů
Vytvořte distribuční složku.	Příprava instalace
Seznamte se se souborem odpovědí.	Přehled souboru odpovědí
Seznamte se s příkazy instalačního programu systému Windows 2000.	Přehled příkazů instalačního programu systému Windows 2000
Na základě kritického plánování zvolte metodu instalace aplikací.	Automatizování instalace klientských aplikací
Na základě kritického plánování zvolte metodu instalace operačního systému.	Automatizování instalace systému Windows 2000 Professional

ČÁST VII

Přílohy



Použití dalších nástrojů a podpůrných informací systému Microsoft Windows 2000 vám pomůže dosáhnout úspěšného zavedení. Přílohy představují dalších nástroje, jako jsou plánovací listy, příkazy instalačního programu a informace pro osoby s postižením, které zlepší vaše možnosti zavádění systému Windows 2000.

V této části

Ukázkové listy plánování 791

Příkazy instalačního programu 835

Příklady souborů odpovědí pro bezobslužnou instalaci 841

Nástroje zavádění 859

Možnosti usnadnění pro postižené osoby 869

PŘÍLOHA A

Ukázkové listy plánování

Při zavádění systému Microsoft Windows 2000 musíte naplánovat a zkoordinovat několik projektů zavádění. V této příloze najdete plánovací listy, které můžete použít k zavedení systému Windows 2000 způsobem, jenž bude pro vaši organizaci z hlediska nákladů nejefektivnější a nejvýkonnější.

Použijete-li plánovací listy zavádění, odhalíte zvláštnosti požadavků IT vaší organizace a také se seznámíte s funkcemi systému Windows 2000, které vám dané požadavky pomohou naplnit. Ještě před vyplněním uvedených listů byste si měli přečíst kapitolu nebo kapitoly k listům přiřazené. Tyto kapitoly představují nové koncepty a poskytují základní informace, jež vám umožní listy plánování dokonale využít.

V této příloze

Použití této přílohy 791

Úvod do plánování zavádění systému Windows 2000 793

Vytváření testovací laboratoře systému Windows 2000 802

Příprava infrastruktury sítě na systém Windows 2000 804

Určení strategií migrace domén 805

Plánování distribuovaného zabezpečení 806

Automatizování instalace a inovace serveru 807

Inovace a instalace členských serverů 809

Zajištění dostupnosti aplikací a služeb 815

Synchronizování služby Active Directory
s adresářovou službou programu Exchange Server 820

Testování kompatibility aplikací se systémem Windows 2000 824

Definování standardů správy a konfigurace klientů 826

Aplikování správy změn a konfigurací 831

Automatizování instalace a inovace klientů 833

Použití této přílohy

Pracovní listy v této příloze jsou uspořádány podle odpovídajícího názvu kapitoly; pracovní list však nemá každá kapitola a některé kapitoly mají více pracovních listů. Ta-

bulka A.1 uvádí kapitoly, k nimž patří nějaké pracovní listy, a ukazuje pořadí pracovních listů uvedených v této příloze.

Tabulka A.1 Pracovní listy v této příloze

Název kapitoly a pracovního listu	Číslo kapitoly
Úvod do plánování zavádění systému Windows 2000	Kapitola 1
Zavedení služeb infrastruktury správy	
Řešení správy počítačů	
Funkce zabezpečení	
Publikování a sdílení informací	
Služby pro aplikace COM	
Škálovatelnost a dostupnost	
Práce v síti a komunikace	
Správa úložišť	
Vytváření testovací laboratoře systému Windows 2000	Kapitola 4
Dokumentování rozsahu a cílů jednotlivých testů	
Sledování výsledků testů	
Příprava infrastruktury sítě na systém Windows 2000	Kapitola 6
Určení strategií migrace domén	Kapitola 10
Dokumentování hlavních cílů migrace	
Zaznamenání dokončení úkolů migrace domén	
Plánování distribuovaného zabezpečení	Kapitola 11
Určení možných rizik zabezpečení	
Automatizování instalace a inovace serveru	Kapitola 13
Určení času a místa použití metody automatizované instalace	
Zaznamenání dokončení úkolů instalace	
Inovace a instalace členských serverů	Kapitola 15
Vytvoření pracovního listu plánování členských serverů	
Vytvoření plánu zálohování dat serveru a zotavení po havárii	
Určení nových hardwarových požadavků	
Zaznamenání specifikací serverů	
Naplánování inovace nebo čisté instalace	
Zajištění dostupnosti aplikací a služeb	Kapitola 18
Určení potřeb vysoké dostupnosti	
Plánování vyrovnávání zatížení sítě	
Synchronizování služby Active Directory s adresářovou službou programu Exchange Server	Kapitola 20
Vytvoření dohod o spojení	
Určení připojovaných adresářových objektů	
Vytvoření seznamu nepřipojovaných atributů	
Vytvoření časového plánu synchronizace adresářů	
Zaznamenání kontaktů pro synchronizaci adresářů	
Testování kompatibility aplikací se systémem Windows 2000	Kapitola 21

Určení priorit aplikací	
Plánování a sledování strategie testování	
Definování standardů správy a konfigurace klientů	Kapitola 23
Určení počítačových požadavků uživatelů	
Definování problémů podpory klientů	
Přřazení úkolů správy a podpory klientů	
Definování požadavků zásad skupiny	
Aplikování správy změn a konfigurací	Kapitola 24
Zaznamenání aplikací a možností jejich správy	
Definování strategie správy konfigurací uživatelů	
Automatizování instalace a inovace klientů	Kapitola 25
Zaznamenání metod automatizované instalace	
Zaznamenání úkolů instalace klientů	

Důležité Tyto listy najdete také v souboru DPGDocs.doc na disku CD, který je součástí sady *Microsoft Windows 2000 Server Resource Kit*. Toto CD obsahuje verzi uvedených pracovních listů, kterou si můžete upravit, vytisknout a používat ve své organizaci.

Úvod do plánování zavádění systému Windows 2000

Kapitola „Úvod do plánování zavádění systému Windows 2000“ obsahuje úvod do funkcí a výhod operačního systému Windows 2000 na vysoké úrovni. Následující plánovací listy uvádějí klíčové funkce systémů Microsoft Windows 2000 Server a Microsoft Windows 2000 Professional. Při čtení kapitol v této knize vám uvedené plánovací listy pomohou identifikovat klíčové funkce systému Windows 2000 a jejich možností naplnění obchodních či výrobních potřeb vaší organizace. Při seznamování se s těmito funkcemi berte v úvahu jak krátkodobé tak i dlouhodobé cíle vaší organizace.

Tabulky jsou vytvořeny tak, že si do nich můžete poznamenat své vlastní komentáře o možných rolích daných funkcí ve vaší organizaci. Tyto pracovní listy použijte k vytvoření upraveného souhrnu funkcí systému Windows 2000, které vaše organizace požaduje.

Poznámka Následující tabulky uvádějí především základní výhody systémů Windows 2000 Server a Windows 2000 Professional a nepředstavují úplný popis všech funkcí. Další informace o určité funkci najdete v souborech nápovědy produktu nebo v příslušné knize a kapitole sady *Microsoft Windows 2000 Server Resource Kit*.

Služby infrastruktury správy

Služby infrastruktury správy systému Windows 2000 Server dodávají oddělením IT nástroje umožňující poskytování nejvyšších dostupných úrovní služeb a omezení nákladů na vlastnictví. Tabulka A.2 popisuje služby infrastruktury správy systému Windows 2000 Server a jejich přínos.

Tabulka A.2 Služby infrastruktury správy

Funkce	Role této funkce ve vaší organizaci
Adresářové služby	
Služba Microsoft Active Directory ukládá informace o všech objektech v síti, což činí tyto objekty snadno vyhledatelnými. Poskytuje flexibilní adresářovou hierarchii, podrobné delegování zabezpečení, výkonné delegování oprávnění, integrované služby DNS, programovací rozhraní na vysoké úrovni a rozšiřitelné úložiště objektů.	
Služby správy	
Nástroj Microsoft Management Console (MMC) poskytuje správcům systému společnou konzolu pro sledování síťových funkcí a používání nástrojů správy. MMC je plně upravitelná podle všech úkolů vykonávaných jednotlivými členy oddělení podpory a správy IT.	
Zásady skupiny	
Zásady skupiny (Group Policy) umožňují správci definovat a řídit stav počítačů a uživatelů. Zásady skupiny lze zadat na libovolné úrovni adresářové služby, včetně síťových sídel, domén a organizačních jednotek. Zásady skupiny lze také filtrovat na základě členství ve skupinách se zabezpečením.	
Instrumentační služby	
Pomocí služby Windows Management Instrumentation (WMI) mohou správci vytvářet vztahy mezi daty a událostmi z více zdrojů v místě nebo v celé organizaci.	
Skriptové služby	
Nástroj Windows Script Host (WSH) podporuje přímé vykonávání skriptů jazyků Microsoft Visual Basic Script, Java a dalších z uživatelského rozhraní nebo z příkazového řádku.	

Další informace o návrhu a vytváření adresářových služeb a zásad skupiny systému Windows 2000 najdete v kapitolách „Návrh struktury služby Active Directory“, „Plánování distribuovaného zabezpečení“, „Definování standardů správy a konfigurace klientů“ a „Aplikování správy změn a konfigurací“ v této knize.

Řešení správy počítačů

Řešení správy počítačů jsou funkce umožňující vám snížit celkové náklady na vlastnictví ve vaší organizaci tím, že usnadňují instalaci, konfiguraci, správu a použití klientských počítačů. Tabulka A.3 uvádí funkce správy počítačů systémů Windows 2000 Server a Windows 2000 Professional, které zvyšují produktivitu uživatelů.

Tabulka A.3 Řešení správy počítačů

Funkce	Role této služby ve vaší organizaci
Funkce IntelliMirror Microsoft IntelliMirror je skupina funkcí, které lze použít k tomu, aby data, aplikace a upravená nastavení operačního systému následovaly uživatele při přesunu na jiný počítač v organizaci.	
Služba Windows Installer Služba Windows Installer řídí instalaci, úpravu, opravu a odebrání softwaru. Poskytuje model pro zabalení instalačních informací a rozhraní API pro aplikace, které se službou Windows Installer spolupracují.	
Vzdálená instalace Technologie vzdáleného spuštění založená na službě DHCP instaluje operační systém na pevný disk klienta ze vzdáleného zdroje. Síť lze inicializovat buď prostředím PXE nebo síťovou kartou podporující standard PXE, specifickým funkčním tlačítkem nebo disketou vzdáleného spouštění u klientů bez podpory PXE.	
Cestovní uživatelské profily Cestovní uživatelské profily kopírují hodnoty registru a informace dokumentů na nějaké místo na síti, aby byla nastavení uživateli dostupná na všech místech, kam se přihlásí.	
Správce součástí systému instalační program systému Windows 2000 Server vám umožňuje pomocí instalačního modulu zabalit a nainstalovat doplňkové komponenty během nastavování systému nebo po něm.	
Duplikování disku Stačí vám nastavit jen jedinou instalaci systému Windows 2000 Server nebo Windows 2000 Professional a tu pak zkopírovat na podobné počítače.	
Poznámka Pro doplnění technologií systému Windows 2000 správy kancelářských počítačů můžete použít server Microsoft Systems Management Server (SMS).	

Další informace o zavádění řešení správy systému Windows 2000 Server a Windows 2000 Professional najdete v kapitolách „Definování standardů správy a konfigurace klientů“ a „Aplikování správy změn a konfigurací“ v této knize.

Funkce zabezpečení

Zabezpečení na úrovni podniku musí být flexibilní a robustní, aby správci mohli nakonfigurovat pravidla možné zodpovědnosti za zabezpečení, aniž by přitom docházelo ke zbytečnému bránění volnému toku potřebných informací. Tabulka A.4 uvádí funkce zabezpečení systému Windows 2000.

Tabulka A.4 Funkce zabezpečení

Funkce	Role této funkce ve vaší organizaci
Šablony zabezpečení	
Umožňují správcům nastavovat různá globální a místní nastavení zabezpečení včetně citlivých (z hlediska zabezpečení) hodnot registru, řízení přístupu k souborům a k registru a zabezpečení systémových služeb.	
Ověřování Kerberos	
Hlavní protokol zabezpečení pro přístup v rámci domény systému Windows 2000 nebo mezi doménami. Poskytuje vzájemné ověřování klientů a serverů a podporuje delegování a autorizování pomocí mechanismů proxy.	
Infrastruktura veřejných klíčů (PKI)	
Integrovanou strukturu PKI můžete používat pro zajištění vysokého zabezpečení ve více internetových a podnikových službách systému Windows 2000 včetně extranetových komunikací.	
Infrastruktura karet Smart Card	
Systém Windows 2000 obsahuje standardní model připojení čteček karet Smart Card k počítačům a rozhraní API nezávislá na zařízení, která umějí s kartami Smart Card pracovat.	
Správa zabezpečeného protokolu IP (Internet Protocol security – IPSec)	
Protokol IPSec podporuje ověřování na úrovni sítě, integritu dat a šifrování, čímž zabezpečuje intranetové, extranetové a internetové webové komunikace.	
Šifrování systému souborů NTFS	
Systém NTFS s využívání veřejného klíče lze povolit na úrovni jednotlivých souborů nebo adresářů.	

Další informace o zavádění služeb zabezpečení systému Windows 2000 najdete v kapitolách „Plánování distribuovaného zabezpečení“ a „Určení strategií zabezpečení sítě systému Windows 2000“ v této knize.

Publikování a sdílení informací

Technologie publikování a sdílení informací v systému Windows 2000 usnadňují sdílení informací přes Internet, váš intranet nebo extranet. Tabulka A.5 shrnuje funkce publikování a sdílení informací.

Tabulka A.5 Publikování a sdílení informací

Funkce	Role této funkce ve vaší organizaci
Integrované webové služby Webové služby integrované do systému Windows 2000 Server vám umožňují používat různé webové publikační protokoly.	
Služba Indexing Service Integrovaná indexová služba umožňuje uživatelům vykonávat fultextové hledání v souborech různých formátů a jazyků.	
Vyměnitelná úložiště Umožňuje správcům spravovat zařízení a funkce vyměnitelných úložišť. Správci mohou vytvářet fondy médií, které vlastní a používá nějaká konkrétní aplikace.	
Tisk Systém Windows 2000 zpřístupňuje všechny sdílené tiskárny v doméně službě Active Directory.	

Další informace o zavádění služeb publikování a sdílení informací systému Windows 2000 najdete v kapitole „Inovace a instalace členských serverů“ v této knize a v knize *Microsoft Internet Information Services 5.0 Resource Kit*.

Podpora aplikací COM

Jako vývojová platforma nabízí systém Windows 2000 podporu modelu Component Object Model (COM) a Distributed COM (DCOM), který rozšiřuje schopnosti vývojových týmů výkonně vytvářet škálovatelnější aplikace se součástmi. Tabulka A.6 uvádí hlavní funkce podpory aplikací COM.

Tabulka A.6 Zavedení podpory aplikací COM

Funkce	Role této funkce ve vaší organizaci
Řazení komponent do fronty	
Vývojáři a správci mohou vybrat vhodný komunikační protokol (DCOM nebo asynchronní) používaný při zavádění.	
Publikování a odebrání	
Funkce COM Events poskytuje všem aplikacím systému Windows 2000 Server jednotný mechanismus publikování a odebrání.	
Transakční služby	
Poskytují aktualizace informací voláním aplikací na mainframovém počítači nebo odesláním zprávy do fronty zpráv a jejím přijetím z fronty zpráv.	
Služby řazení zpráv	
V podnikovém prostředí zajišťuje úplné dokončení transakce nebo její bezpečné vrácení do předchozího stavu.	
Služby webových aplikací	
Vývojáři mohou k vytvoření webového rozhraní svých existujících serverových aplikací použít technologii Active Server Pages.	

Další informace o zavádění služeb Component Application Services a rozhraní Microsoft Security Support Provider Interface systému Windows 2000 najdete v kapitole „Určení strategií zabezpečení sítě systému Windows 2000“ v této knize. Další informace pro vývojáře najdete v odkazu MSDN Platform SDK stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Poznámka Tyto funkce a jejich potenciální význam pro vaši společnost byste měli prodiskutovat se členy týmu vývoje aplikací. Jejich znalosti vám pomohou určit možnou hodnotu těchto technologií ve vaší organizaci.

Škálovatelnost a dostupnost

Kdysi byly rychlejší procesory a síťové karty tradičními zárukami vysokého výkonu sítě. V budoucnosti budou stejně důležitými charakteristikami síťové architektury výkonnější možnosti čtení a zápisu, zvýšený výkon vstupů a výstupů a rychlejší přístup k disku. Prostředí vyžadující použití velmi důležitých (mission-critical) počítačů mohou nyní využívat tyto rozšířené možnosti systému Windows 2000. Tabulka A.7 uvádí funkce systému Windows 2000, které vám pomohou zlepšit škálovatelnost a dostupnost sítě.

Tabulka A.7 Škálovatelnost a dostupnost

Funkce	Role této funkce ve vaší organizaci
Architektura paměti	
Systém Windows 2000 Advanced Server umožňuje procesorům přístup k až 32 gigabajtům (GB) paměti.	
Zlepšená škálovatelnost symetrického multiprocessingu (SMP)	
Systém Windows 2000 Advanced Server byl optimalizován pro osmiprocessorové servery SMP.	
Klastrová služba	
Umožňuje dvou nebo více serverům fungovat společně jako jediný systém.	
Podpora inteligentních vstupů a výstupů (I2O)	
Technologie I2O zbavuje hostitele úkolů I/O náročných na přerušení, protože se zatížení odstraňuje z hlavních procesorů.	
Terminálové služby	
Pomocí emulace terminálu umožňují terminálové služby běžet jedné sadě aplikací na různých typech klientského hardwaru včetně tenkých klientů, starších počítačů a klientů neobsahujících systém Windows. Tyto služby lze také používat ke vzdálené správě.	
Vyrovňování zatížení sítě	
Kombinuje až 32 serverů se spuštěným systémem Windows 2000 Advanced Server do jediného klastru s vyrovňováním zatížení. Nejčastěji se používá k distribuci příchozích webových požadavků do klastru aplikací internetového serveru.	
Funkce IntelliMirror	
Funkce IntelliMirror umožňuje uživatelům, aby je jejich data, aplikace a nastavení následovaly při jejich připojení k síti.	

Další informace o zavádění klastrové služby systému Windows 2000 najdete v kapitole „Zajištění dostupnosti aplikací a služeb“ v této knize.

Další informace o terminálových službách najdete v kapitole „Zavádění terminálových služeb“ v této knize.

Práce v síti a komunikace

Chcete-li zlepšit možnosti práce v síti, zamyslete se nad použitím technologií systému Windows 2000 uvedených v tabulce A.8, které rozšíří vaše možnosti řízení, zajistí zabezpečený vzdálený přístup k síti a nativní podporu nové generace komunikačních řešení.

Tabulka A.8 Práce v síti a komunikace

Funkce	Role této funkce ve vaší organizaci
Protokol dynamické aktualizace DNS	
Eliminuje nutnost ručně upravovat a replikovat databázi DNS.	
Služba Quality of Service (QoS)	
Protokoly a služby QoS poskytují zaručený expresní systém dodávek mezi dvěma body provozem IP.	
Protokol Resource Reservation Protocol (RSVP)	
Signalizační protokol, který umožňuje odesílateli a příjemci vytvořit rezervovanou cestu přenosu dat s určenou kvalitou služeb.	
Režim asynchronního přenosu (Asynchronous Transfer Mode – ATM)	
Síť ATM může simultánně přepravovat velké množství různého síťového provozu včetně hlasu, dat obrázků a videa.	
Služby multimediálních proudů	
Serverové součásti a nástroje pro přenos multimediálních souborů přes síť.	
Technologie Fibre Channel	
Technologie Fibre Channel poskytuje přenosy dat rychlostí jednoho gigabitu za sekundu tím, že se mapují obvyklé přenosové protokoly a síťové a vysokorychlostní vstupy a výstupy se slučují do jediné kolekce.	
Telefonování přes IP	
Telefonické rozhraní API 3.0 (TAPI) unifikuje tradiční a IP telefonování.	

Další informace o práci v síti a komunikačních funkcích systému Windows 2000 najdete v kapitole „Příprava infrastruktury sítě na systém Windows 2000“ a „Určení strategií konektivity sítě“ v této knize.

Správa úložišť

Systém Windows 2000 Server poskytuje služby úložišť určené jak ke zlepšení spolehlivosti tak i přístupu uživatelů. Tabulka A.9 uvádí tyto služby.

Tabulka A.9 Správa úložišť

Funkce	Role této funkce ve vaší organizaci
Vzdálené úložiště	
Sleduje množství prostoru dostupného na místním pevném disku. Když volný prostor na primárním pevném disku klesne pod úroveň nezbytnou pro spolehlivé fungování, služba Vzdálené úložiště (Remote Storage) odstraní místní data, která byla zkopírována na vzdálené úložiště.	
Vyměnitelné úložiště	
Umožňuje správcům spravovat zařízení a funkce vyměnitelných úložišť. Správci mohou vytvářet fondy médií, které vlastní a používá nějaká konkrétní aplikace.	
Vylepšení systému souborů NTFS	
Podporuje vylepšení výkonu, jako je šifrování souborů, schopnost přidat diskový prostor ke svazku NTFS bez restartování, distribuované sledování odkazů a kvóty svazků pro jednotlivé uživatele, které jsou určeny ke sledování a omezování použití diskového prostoru.	
Diskové kvóty	
Pomáhají správcům plánovat a implementovat používání disků.	
Zálohování	
Pomocí programu Zálohování (Backup) si mohou uživatelé zálohovat data na různá ukládací média včetně pevných disků a magnetických a optických médií.	
Podpora distribuovaného systému souborů (DFS)	
Umožňuje správcům vytvořit jediné adresářový strom obsahující více souborových serverů a míst sdílení souborů a umožňují spolupráci (interoperabilitu) mezi klienty systému Windows 2000 a libovolným souborovým serverem s odpovídajícím protokolem.	

Další informace o zavádění technologií správy úložišť systému Windows 2000 Server najdete v kapitole „Určení strategií správy úložišť systému Windows 2000“ v této knize.

Vytváření testovací laboratoře systému Windows 2000

Kapitola „Vytvoření testovací laboratoře systému Windows 2000“ v této knize zdůrazňuje důležitost zevrubného testování systému Windows 2000 na základě reálných scénářů. Poskytuje také mnoho pokynů, které můžete využít při vytváření laboratoře vaší organizace a vykonání zevrubného programu testování.

Abyste mohli začít, potřebujete:

- Vytvořit testovací plán popisující váš rozsah, cíle a metodologii.
- Navrhnout testovací případy popisující testovací scénáře a problémy, kterými se musíte zabývat.
- Vykonat testy a vyhodnotit výsledky.
- Dokumentovat výsledky testů.
- Problémy předat k řešení příslušným osobám.

Podle možností vaší laboratoře musíte simulovat skutečné pracovní prostředí. Mezi základní komponenty, které musí být součástí plánu testování, patří ty následující:

- Současný návrh sítě (logický a fyzický).
- Předkládaný návrh systému Windows 2000.
- Seznam funkcí, které je zapotřebí vyhodnotit a prozkoumat.
- Inventář existujícího hardwaru (serverů, klientských počítačů a přenosných počítačů).
- Seznam hardwaru navrhovaného pro systém Windows 2000.

Tento seznam se může během testování vyvíjet, laboratoři však musíte dodat jeho počáteční verzi.

- Seznam nástrojů správy (systému Windows 2000, jiných společností a vytvořených ve vaší organizaci).
- Seznam inovací, jako jsou servisní balíčky, ovladače a systém BIOS, které je zapotřebí instalovat v rámci přípravy na systém Windows 2000.

Do popisu laboratoře zahrňte také následující typy informací:

- Struktura domény včetně:
 - doménové struktury a hierarchie;
 - objektů zásad skupiny (nastavení a místo jejich aplikování);
 - smyslu každé domény;
 - metody zaplnění daty uživatelských účtů;
 - vztahů důvěryhodnosti (přenosné a explicitní).
- Řadiče domén včetně:
 - primárních řadičů domén (PDC) a záložních řadičů domén (BDC), jestliže migrujete ze systému Microsoft Windows NT verze 4.0;
 - serverů, které povýšíte na řadiče domén, jestliže migrujete z jiného operačního systému.

- Členské servery včetně služeb, které na nich poběží.
- Klientské počítače včetně:
 - výrobce a modelu počítače;
 - množství paměti;
 - typu a rychlosti procesoru;
 - kapacity pevného disku;
 - grafických karet (typ, rozlišení a barevná hloubka).
- Použití návrhu laboratoře ke specifickým testům včetně:
 - testování kombinovaného a nativního režimu;
 - testování telefonického a jiného vzdáleného připojení;
 - testování interoperability (UNIX, mainframové počítače a další systémy);
 - testování replikace a sídla adresářové služby Active Directory;
 - testování propojení WAN.

S dokumentováním rozsahu a cílů jednotlivých testů vám pomůže tabulka A.10. Pro každý test vyplňte samostatný list.

Tabulka A.10 Dokumentování rozsahu a cílů jednotlivých testů

Identifikátor testu:		Datum testu:	
		Rozsah a cíle testu:	
Účel testu			
Speciální hardwarové požadavky			
Speciální softwarové požadavky			
Speciální konfigurační požadavky			
Použitá procedura testování			
Očekávané výsledky nebo kritéria úspěchu			

Tabulka A.11 ilustruje typ listu sledování, který lze používat k monitorování postupu vašich testů a zajištění všech následných problémů.

Tabulka A.11 Sledování výsledků testů

Identifikátor testu	Datum testu	Výsledek	Další činnosti

Příprava infrastruktury sítě na systém Windows 2000

Kapitola „Příprava infrastruktury sítě na systém Windows 2000“ v této knize poskytuje doporučení pro zdokumentování vaší současné infrastruktury sítě. Také vám pomůže určit oblasti infrastruktury sítě, jako jsou servery, směrovače a síťové služby, které může být zapotřebí před zavedením systému Windows 2000 inovovat nebo upravit.

Oblastmi vašeho současného prostředí sítě, které musíte zdokumentovat a připravit na zavedení systému Windows 2000, jsou:

- Hardware a software
- Infrastruktura sítě
- Souborové, tiskové a webové servery
- Obchodní aplikace
- Architektura adresářových služeb
- Zabezpečení

Měli byste dokonale zdokumentovat následující hardwarové položky:

- Směrovače
- Tiskárny
- Modemy
- Další hardware, jako je redundantní pole nezávislých disků (RAID) a hardware serveru služby Směrování a vzdálený přístup (Routing and Remote Access Service – RRAS)
- Nastavení systému BIOS
- Verze ovladačů a další informace o softwaru a firmwaru.

Váš inventář softwaru musí zahrnovat:

- Všechny aplikace na všech počítačích.
- Čísla verzí (nebo datum a čas) dynamicky připojitelných knihoven přiřazených těmto aplikacím.
- Servisní balíčky aplikované na operační systém či aplikace.

Také zdokumentujte síťové konfigurace serverů a klientských počítačů. Mezi tyto informace, které najdete v ovládacím panelu Síťová a telefonická připojení, patří:

- Identifikace
- Služby
- Protokoly
- Adaptéry
- Vazby
- Adresy protokolu IP

Musíte zdokumentovat:

- Logickou organizaci vaší sítě
- Metody překladu názvů a adres
- Konfiguraci používaných služeb
- Umístění síťových sídel
- Dostupnou šířku pásma mezi sídly

Řadu z uvedených informací potřebujete také k vytvoření fyzických a logických diagramů sítě, jejichž verze před zavedením systému Windows 2000 a po něm můžete projednat s dalšími lidmi. Další informace o důležitých technických problémech, které je zapotřebí zdokumentovat, najdete v kapitole „Příprava infrastruktury sítě na systém Windows 2000“ v této knize.

Určení strategií migrace domén

Abyste mohli naplánovat migraci vaší struktury domén ze systému Windows NT na systém Windows 2000, musíte nejprve stanovit cíle migrace. Tyto cíle mohou aktivně pojednávat o problémech se zaváděním, jako je možné narušení výrobních či obchodních systémů, výkon systému a možnosti zvýšení střední doby mezi poruchami. Cíle vaší migrace také ovlivňují testovací plány a kritéria přijatelnosti.

Přečtěte si kapitolu „Určení strategií migrace domén“ a pak s pomocí následujících pracovních listů začněte plánovat strategie migrace. K dokumentování cílů migrace specifických pro vaši organizaci použijte tabulku A.12. Tato tabulka uvádí některé ukázkové cíle, abyste měli s čím začít.

Tabulka A.12 Dokumentování cílů migrace

Cíl	Pokyny pro dosažení cíle
Minimalizovat narušení produkčního prostředí.	■ Během migrace a po ní udržet přístup uživatelů k datům, prostředkům a aplikacím.
Udržet výkon systému.	■ Během migrace a po ní udržet známé prostředí pro uživatele.
	■ Během migrace a po ní udržet přístup uživatelů k datům, prostředkům a aplikacím.
Zvýšit střední dobu mezi poruchami.	■ Během migrace a po ní udržet známé prostředí pro uživatele.
	■ Během migrace a po ní udržet přístup uživatelů k datům, prostředkům a aplikacím.

Minimalizovat nároky na správu.	<ul style="list-style-type: none"> ■ Během migrace a po ní udržet známé prostředí pro uživatele. ■ Zajistit bezproblémovou migraci účtů uživatelů. Je-li to možné, uživatelům musí zůstat jejich hesla. ■ Minimalizovat počet návštěv správce u klientského počítače. ■ Minimalizovat počet nových oprávnění k prostředkům.
Maximalizovat úspěšnost zavádění.	■ Nejprve zavést klíčové funkce.
Udržet zabezpečení systému.	<ul style="list-style-type: none"> ■ Zavádět tak, aby byl vždy zajištěn zabezpečený systém. ■ Vytvořit zásady zabezpečeného zavádění.

K zaznamenání data dokončení jednotlivých úkolů použijte tabulku A.13.

Tabulka A.13 Záznam dokončení úkolů migrace domén

Úkol	Datum dokončení
Určení způsobu migrace.	
Určení podporovaných cest inovace.	
Prozkoumání existující struktury domén.	
Vývoj plánu zotavení.	
Určení strategie inovace řadičů domény.	
Určení pořadí inovace domén.	
Určení okamžiku přechodu na nativní režim.	
Určení důvodů pro změnu uspořádání domén.	
Určení okamžiku změny uspořádání domén.	
Přesun uživatelů a skupin.	
Přesun počítačů.	
Přesun členských serverů.	
Vytvoření vztahů důvěryhodnosti.	
Klonování komitentů zabezpečení.	
Přechod na nativní režim.	

Plánování distribuovaného zabezpečení

Chcete-li implementovat celkové zásady zabezpečení, musíte zkoordinovat mnoho funkcí zabezpečení sítě. Ke zdokumentování všech aspektů zabezpečení platících pro vaši organizaci použijte tabulku A.14. Příklady rizik zabezpečení najdete v kapitole „Plánování distribuovaného zabezpečení“. Uvedte spíše specifická (a nikoli obecná) bezpečnostní rizika vaší společnosti. Do položky Strategie omezení uvedte podrobnosti ze

všech kapitol v této knize, které souvisejí se zabezpečením. Sem patří kapitoly „Plánování infrastruktury veřejných klíčů“ a „Určení strategií zabezpečení sítě systému Windows 2000“.

Tabulka A.14 Určení potenciálních rizik zabezpečení

Potenciální riziko zabezpečení	Popis	Strategie omezení (včetně zásad, funkcí systému Windows 2000 a dalších technologických řešení)

Automatizování instalace a inovace serveru

Před zautomatizováním instalace systému Windows 2000 Server se musíte rozhodnout, zda budete inovovat ze systému Windows NT, nebo zda vykonáte čistou instalaci. Kapitola „Automatizování instalace a inovace serveru“ vám pomůže rozhodnout, jaký typ instalace je zapotřebí zadat. Následující otázky vám s tímto rozhodnutím také pomohou.

1. Používá vaše organizace v současné době spravovanou instalaci systému Windows NT? Ano ☐ Ne ☐
2. Plánujete používat již existující hardware a softwarové aplikace? Ano ☐ Ne ☐
Jestliže jste na otázky 1 a 2 odpověděli kladně, pak bude asi vhodnější vykonat inovaci.
3. Plánujete instalovat systém Windows 2000 na nový hardware? Ano ☐ Ne ☐
4. Plánujete instalovat nové aplikace napsané pro prostředí systému Windows 2000? Ano ☐ Ne ☐
Jestliže jste odpověděli kladně na otázky 3 a 4, asi pro vás bude lepší čistá instalace.

Použité metody automatizované instalace a oblasti jejich použití ve vaší organizaci určete pomocí tabulky A.15.

Tabulka A.15 Určení času a místa použití metod automatizované instalace

Metoda	Kdy ji použít	Použít tuto metodu?	Kdy a kde?
Syspart	Pro čisté instalace na počítače s různým hardwarem.		
Sysprep	Když mají hlavní počítač a cílové počítače stejný hardware, kam patří vrstva abstrakce hardwaru (HAL) a zařízení hromadného ukládání dat.		
Systems Management Server (SMS)	K vykonání spravovaných inovací systému Windows 2000 Server na více systémech zejména geograficky rozptýlených.		
Spustitelné CD	Na počítači, kterému jeho systém BIOS umožňuje spouštění z disku CD.		

Tabulku A.16 použijte jako seznam úkolů, které musíte dokončit, a data jejich dokončení.

Tabulka A.16 Záznam dokončení úkolů instalace

Úkol	Datum dokončení
Vyřešení kritických problémů plánování.	
Vytvoření distribuční složky.	
Seznámení se se souborem odpovědí.	
Seznámení se s příkazy instalačního programu systému Windows 2000.	
Volba metody instalace aplikace na základě kritického plánování.	
Volba metody instalace operačního systému na základě kritického plánování.	

Inovace a instalace členských serverů

Následující pracovní list vám společně s kapitolou „Inovace a instalace členských serverů“ pomůže určit nákladově nejvýhodnější a nejvýkonnější metodu inovace a instalace členských serverů systému Windows 2000 ve vaší organizaci. Plánování inovace nebo čisté instalace systému Windows 2000 Server začněte definováním specifikací jednotlivých členských serverů.

Abyste mohli začít s inovací nebo čistou instalací, musíte mít k dispozici aktuální diagram existující sítě. Nemáte-li aktuální síťový diagram, nejprve jej vytvořte a pak začněte vytvářet plány pro novou instalaci nebo inovaci členských serverů.

Dále zjistěte, zda se vaše organizace rozhodla instalovat a provozovat adresářovou službu Active Directory systému Windows 2000. Službu Active Directory potřebují určité pokročilé služby operačního systému.

Pak určete, kolik serverů jednotlivých typů máte v organizaci:

- Souborové servery:

- Tiskové servery:

- Aplikační servery:

- Webové servery:

- Faxové servery:

- Proxy-servery:

- Servery služby Směrování a vzdálený přístup:

- Databázové servery:

Nyní pro jednotlivé servery v existujícím prostředí vyplňte pracovní list plánování členských serverů. Tento pracovní list vám pomůže definovat individuální inovační cesty jednotlivých serverů v organizaci. Po určení priorit serverů můžete vytvořit časový plán čisté instalace a inovace.

Pracovní list plánování členských serverů

Pomocí následujících volitelných charakteristik popište každý server ve vašem existujícím prostředí.

Typ serveru:

Souborový server ☐ Tiskový server ☐ Webový server ☐ Proxy-server ☐ Faxový server ☐ Server služby Směrování a vzdálený přístup ☐ Databázový server ☐ Aplikační server ☐ Určete instalované aplikace:

Název členského serveru: _____

Jaké množství dat je uloženo na serveru? _____

Jaké množství dat se přenáší na server a z něj? _____

Aktuální počet uživatelů: _____

Aktuální hodiny provozu: _____

Specifikace serveru:

Je tento počítačový systém uveden v seznamu Windows Hardware Compatibility List (HCL) společnosti Microsoft? Ano ☐ Ne ☐

Sériové číslo: _____

Nějaké změny hardwaru? Ano ☐ Ne ☐

Pokud ano, uveďte specifikata: _____

Výrobce počítačového systému: _____

Model počítačového systému: _____

Verze počítačového systému: _____

Množství instalované fyzické paměti: _____

Typ instalovaných síťových adaptérů:

Ethernet ☐ Token Ring ☐ FDDI ☐ ATM ☐

Jiný _____

Jsou síťové adaptéry uvedeny v seznamu HCL? Ano ☐ Ne ☐

Typ instalované jednotky CD-ROM: _____

Uvedte všechna zařízení standardu Plug-and-Play:

_____	_____
_____	_____

Typ externích disků připojených k počítači: _____

Oddíly pevného disku a dostupný volný prostor: _____

Používáte pole redundantních nezávislých disků (RAID)? Jestliže ano, zadejte: Softwarové pole RAID ☐ Hardwarové pole RAID ☐

Jaké úrovně pole RAID používáte? _____

Jaké z následujících typů softwaru jsou instalovány na serveru?

Síťové služby jiných společností ☐ Antivirové programy ☐ Jiný klientský software ☐

Informace o známých problémech s určitými aplikacemi najdete v souboru relnotes.htm na disku CD operačního systému Windows 2000 Server.

Před inovací nebo čistou instalací odinstalujte všechny aplikace zmíněné v uvedeném souboru.

Plán zálohování dat serveru a zotavení po havárii

Před inovací zálohujte tyto položky:

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

Maximální tolerovaná doba výpadku: _____

Měřitelné náklady na výpadek: _____

Určení nových hardwarových požadavků

Počet inovovaných členských serverů: _____

Počet členských serverů nahrazených novým hardwarem před inovací nebo čistou instalací: _____

Počet síťových karet potřebných pro inovaci: _____

Typ síťových karet:

Ethernet ☐ Token Ring ☐ FDDI ☐ ATM

Jiný _____

Plánovaný objem dat: _____

Plánovaný počet uživatelů: _____

Plánované hodiny provozu: _____

Zaznamenání specifikací serverů

Tiskové servery

Jedná-li se o tiskový server, určete tyto položky:

- Počet uživatelů, kteří budou tisknout, a jimi vytvářené zatížení:

- Typy potřeb tisku (například pro tisk barevných prospektů uživateli z oddělení prodeje budete potřebovat barevnou tiskárnu):

- Umístění tiskáren. Uživatelé by měli mít možnost jednoduše si vyzvednout své vytištěné dokumenty. Tiskárny přiřadte k jednotlivým tiskovým serverům s pomocí tabulky A.17.

Tabulka A.17 Přířazení tiskových serverů, tiskáren a jejich umístění

Tiskový server	Název tiskárny	Umístění

Nainstalovali jste všechny požadované ovladače tisku? Ano ☐ Ne ☐

(Ovladače tiskárny najdete na CD operačního systému Windows 2000 Server nebo si je obstaráte od výrobce tiskárny.)

Pracuje na některých klientech na síti operační systém jiného výrobce?

Macintosh ☐ NetWare ☐ UNIX ☐ Jiný ☐ _____

Na tiskové servery musíte nainstalovat další služby a na klienty s operačními systémy jiných výrobců musíte nainstalovat příslušné ovladače tiskáren. Potřebné ovladače získáte u výrobce tiskárny.

Souborové servery

Plánujete provozovat doménový systém DFS? Ano ☐ Ne ☐

Poznámka Systém DFS provozovaný na doméně vyžaduje spuštěnou službu Active Directory.

Uspořádejte servery do skupin a určete, která místa sdílení souborů budou jednotlivé servery používat:

Skupina _____ obsahuje tyto servery:

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

Aplikační servery

Jaké služby bude tento aplikační server hostit?

Služby Component Services ☐ Služby Terminal Services ☐ Databáze ☐ Elektronická pošta ☐

Vyžadujete-li služby Component Services, vyberte jednu z následujících možností:

Vyrovňování zatížení aplikací: Ano ☐ Ne ☐

Transakční služby: Ano ☐ Ne ☐

Správa aplikací: Ano ☐ Ne ☐

Služby Message Queuing: Ano ☐ Ne ☐

Jiné: _____

Webové servery

Jakou novou nebo dodatečnou součást musíte na tento server instalovat?

Naplánování inovace nebo čisté instalace

Proces pilotního testování je iterační. Zavedete omezený počet počítačů v řízeném prostředí, vyhodnotíte výsledky, vyřešíte vzniklé problémy a zavedete nový pilotní program – to vše dokud nedosáhnete rozsahu a kvality indikujících připravenost na plné zavedení.

Určení priorit zavedení každého členského serveru

Vytvořte svůj vlastní systém určení priorit inovace nebo instalace, který vám umožní seskupit servery pro zavádění ve fázích. Každému pilotnímu programu přiřadte číslo skupiny nebo název, abyste mohli později identifikovat prioritu inovace nebo instalace serveru.

Číslo skupiny nebo název pilotního programu je: _____

Zamýšlíte inovovat tento konkrétní server nebo vykonat čistou instalaci? Vyberte jednu z těchto možností:

Pilotní fáze 1 ☐ Pilotní fáze 2 ☐ Výroba ☐

Další informace o:

- vytvoření testovací laboratoře najdete v kapitole „Vytvoření testovací laboratoře systému Windows 2000“ v této knize;
- vytvoření plánu pilotního testování najdete v kapitole „Vykonání pilotního programu systému Windows 2000“ v této knize.

Zajištění dostupnosti aplikací a služeb

Chcete-li vytvořit plán zajištění vysoké dostupnosti aplikací a služeb, vyplňte jeden pracovní list plánování zavedení clusteringu pro každou důležitou aplikaci nebo službu, jejíž vysokou dostupnost chcete ve své organizaci zajistit.

Ještě než začnete vyplňovat uvedený pracovní list, přečtěte si kapitolu „Zajištění dostupnosti aplikací a služeb“. Tato kapitola vás uvede do nových konceptů a poskytne vám pokyny potřebné k dokonalému využití pracovního listu plánování.

Určení potřeb vysoké dostupnosti

Vaše prostředí může zahrnovat jeden nebo více následujících typů aplikací a služeb:

- Databáze (Microsoft SQL Server nebo jiná databázová aplikace)
- Nástroj pro práci ve skupině (Microsoft Exchange Server nebo jiná aplikace práce ve skupině)
- Webová služba (Microsoft Internet Information Services nebo jiná webová služba)
- Služba Windows Internet Name Service (WINS)
- Protokol Dynamic Host Configuration Protocol (DHCP)
- Interně vyvinuté obchodní či výrobní aplikace
- Aplikace od jiných společností
- Místa sdílení souborů a tiskáren

V následujících pododdílech definujte specifikace jednotlivých důležitých aplikací nebo služeb, které chcete používat ve spojení se systémem Windows 2000 Server.

Specifikace aplikace a služby

Název aplikace nebo služby: _____

Požadavky vysoké dostupnosti této aplikace nebo služby

Jaký síťový protokol daná aplikace nebo služba vyžaduje?

TCP/IP ☐ IPX/SPX ☐

Poznámka Společnost Microsoft nedodává řešení vysoké dostupnosti podporující protokoly IPX/SPX.

Vyžaduje vaše řešení clusteringu některou z následujících položek?

- Zajištění zálohování dat ☐
- Ochrana přístupu k datům ☐
- Ochrana samotných dat ☐
- Ochrana před výpadky napájení ☐
- Ochrana před výpadky sítě ☐
- Správa objektů a konfigurace klastru ☐
- Koordinace s dalšími instancemi služby Cluster Service v klastru ☐
- Vykonání operací překlopení ☐
- Zpracování upozornění na událost ☐
- Umožnění komunikace mezi dalšími softwarovými součástmi ☐

Problémy kompatibility softwaru:

Máte knihovnu prostředků DLL? Ano ☐ Ne ☐

Je možné použít generickou knihovnu prostředků DLL? Ano ☐ Ne ☐

Podporuje dostupná knihovna prostředků DLL:

Dvouuzlové klastry ☐ N-uzlové klastry ☐

Podporuje instalace aplikace:

Dvouuzlové klastry ☐ N-uzlové klastry ☐

Funguje aplikace v systému Windows 2000 správně? Ano ☐ Ne ☐

Je aplikace nestavová nebo udržuje stav klientské strany?

Speciální hardwarové požadavky:

Je systém na seznamu Hardware Compatibility List (HCL)? Ano ☐ Ne ☐

Podporuje systém rozsáhlou paměť? Ano ☐ Ne ☐

Instalujete program Microsoft Windows 2000 Advanced Server na nějaký počítač s architekturou Intel PAE, který má více než 4 GB paměti s náhodným přístupem (RAM)? Ano ☐ Ne ☐

Jestliže ano, musíte:

- Prověřit seznam HCL a ujistit se, že je zajištěna podpora vysoké paměti daného systému a komponent.
- Zařídit kompatibilitu systému a komponent.
- Systém kompletně zálohovat.
- Upravit soubor boot.ini tak, aby obsahoval přepínač PAE.
- Systém otestovat a ujistit se o jeho řádné funkci.

Bude systém používat:

SCSI (dvouuzlový) ☐ Přepínač SCSI (n-uzlový) ☐ Fiber Channel (n-uzlový) ☐

Jaké síťové adaptéry máte ve svém prostředí?

Ethernet ☐ Token Ring ☐ FDDI ☐ ATM ☐

Jiné _____

Jsou tyto síťové adaptéry na seznamu? Ano ☐ Ne ☐

Množství dat: _____

Počet uživatelů: _____

Hodin provozu: _____

Očekávané změny požadavků na velikost a výkon dané aplikace nebo služby

Špičky v určitých časech nebo jiné plánované špičky: _____

Očekávaný nárůst počtu uživatelů: _____

Očekávaný nárůst objemu dat: _____

Plány zálohování dat a zotavení po havárii dané aplikace nebo služby

Maximální tolerovaný výpadek: _____

Vliv výpadků (zaškrtněte platné položky):

Ztráta prodeje ☐

Ztráta produktivity ☐

Snížení spokojenosti zákazníků ☐

Nesplnění smluvní povinnosti nebo právní závazky ☐

Ztráta konkurenceschopnosti ☐

Zvýšené náklady způsobené časem na odstranění poruchy ☐

Jiné: _____

Měřitelné náklady na výpadek (definujte náklady na aplikace a na služby při výpadku přesahujícím zadané tolerovatelné maximum):

Havárie síťového sídla

Je zapotřebí zajistit fungování mimo sídlo? Ano ☐ Ne ☐

Určete jediné body selhání (chyby):

Síťový rozbočovač ☐

Síťový směrovač ☐

Výpadek napájení ☐

Disk serveru ☐

Další hardware serveru, jako je procesor a paměť ☐

Software serveru /

Připojení WAN jako jsou směrovače a vyhrazené linky ☐

Telefonické připojení ☐

Jiný: _____

Jestliže dojde k selhání aplikace nebo služby, jaký je plán zajištění dostupnosti:

Jestliže dojde k selhání služby nebo dojde k výpadku, máte:

Pole RAID:

Level 0 (prokládání) ☐

Level 1 (zrcadlení) ☐

Level 5 (prokládání s paritou) ☐

Náhradní řadiče SCSI nebo Fibre Channel Ano ☐ Ne ☐

Náhradní disky Ano ☐ Ne ☐

Ochranu pomocí zařízení UPS pro jednotlivé uživatele Ano ☐ Ne ☐

Ochranu pomocí zařízení UPS pro síť (včetně rozbočovačů, mostů, směrovačů atd.)
Ano ☐ Ne ☐

K vytvoření strategie zálohování a obnovení klastru použijte následující seznam:

Připojte (mapujte) klíče registru k jednotlivým prostředkům. ☐

Vytvořte katalog pro dokumentování jednotlivých zálohování. ☐

Najděte bezpečné místo, kam můžete zálohy ukládat. ☐

Pomocí programu Zálohování (Backup) vytvořte disketu nouzového opravení. ☐

Plánování vyrovnávání zatížení sítě

Pracuje aplikace nebo služba na všech hostitelích v klastru nebo má každý hostitel svou vlastní aplikaci nebo službu?

Aplikace nebo služba běží na jednom hostiteli ☐

Všichni hostitelé sdílejí jednu aplikaci nebo službu ☐

Používá vaše aplikace port TCP nebo UDP? Port TCP ☐ Port UDP ☐

Počet hostitelů v klastru (1–32): _____

Poznámka Vždy musíte zajistit dostatek náhradní kapacity, aby ostatní servery dokázaly zvládnout zvýšené zatížení způsobené výpadkem jednoho ze serverů.

Používáte-li směrovač, v jakém režimu bude pracovat? Jednosměrové vysílání ☐ Vícesměrové vysílání ☐

Specifické volby vyrovnávání zatížení sítě

Implementovali jste nad protokolem TCP/IP následující technologie?

Model Distributed Component Object Model (DCOM) ☐

Pojmenované kanály ☐

Vzdálené volání procedury ☐

Výběr role serveru

Mají uzle ve vašem klastru být:

Členskými servery ☐ Řadiči domény ☐ Globálními katalogy ☐

Poznámka Vyberete-li řadiče domény, musíte mít hardware potřebný k jejich podpoře. Další informace najdete v kapitole „Zajištění dostupnosti aplikací a služeb“ v této knize.

Volba modelu klastru

Implementujete:

Klastr s jediným uzlem (překlopení není dostupné) ☐

Klastr s vyhrazeným sekundárním uzlem ☐

Konfiguraci vysoké dostupnosti (dostupnost prostředků pomocí virtuálních serverů):

Clustering jednoho typu aplikace ☐

Clustering více aplikací ☐

Složitá hybridní konfigurace ☐

Plánování skupin prostředků

Jaký typ prostředku tento klastr vyžaduje?

Adresu IP ☐

Síťový název ☐

Fyzický disk ☐

Generickou nebo zákaznickou aplikaci či službu ☐

Zadejte: _____

Uvedte všechny serverové aplikace v jednotlivých skupinách prostředků:

Kolik virtuálních serverů bude ve vašem prostředí pracovat? _____

Jaký další software budete provozovat nezávisle na těchto skupinách?

Který hardware, připojení a software operačního systému může tento klastr serverů chránit ve vašem síťovém prostředí? Uvedte všechny prostředky, které nejsou aplikacemi.

Uvedte všechny závislosti pro jednotlivé prostředky (včetně všech prostředků podporujících základní prostředky):

Jaké zásady překlopení budou jednotlivé prostředky vyžadovat?

Při vytváření skupin si usnadněte správu prostředků. Například:

- zkombinujte prostředky sdílení souborů a prostředky řazení tiskových úloh do jedné skupiny;
- umístěte aplikace závislé na určitém prostředku do jedné skupiny.

Synchronizování služby Active Directory s adresářovou službou programu Exchange Server

Kapitola „Synchronizování služby Active Directory s adresářovou službou programu Exchange Server“ uvádí koncepty a procesy synchronizace adresářů, které vám pomohou určit z hlediska nákladů nejvýhodnější a nejvýkonnější metodu integrování adresářových služeb Active Directory a Microsoft Exchange Server verze 5.5.

Chcete-li vytvořit plán dohody o spojení, vyplňte pracovní list plánování pro každou dohodu o spojení, kterou vaše organizace potřebuje. Po zdokumentování dohod o spojení v pracovních listech můžete začít s jejich konfigurací v systému Windows 2000. (Viz hned následující oddíl „Vytvoření dohod o spojení“.)

Vytvoření dohod o spojení

Referenční číslo nebo název dohody o spojení: _____

Správce zodpovědný za tuto dohodu o spojení: _____

Adresářová služba, ze které budete objekty spravovat:

Active Directory systému Windows 2000 ☐ Adresářová služba programu Exchange Server 5.5 ☐

Směr: Jednosměrná ☐ Obousměrná ☐

Určení zdrojového a cílového serveru dohody o spojení

Jednosměrná dohoda o spojení:

Je-li *zdrojovým* serverem server Exchange 5.5:

Předmostí ☐ Jiný ☐ _____

Název zdrojového serveru: _____

Je-li *cílovým* serverem server Windows 2000:

Globální katalog ☐ Řadič domény ☐ Předmostí ☐

Název cílového serveru: _____

Dvousměrná dohoda o spojení:

Je-li prvním *zdrojovým* serverem server Exchange 5.5:

Předmostí ☐ Jiný ☐ _____

Název zdrojového serveru: _____

Je-li prvním *cílovým* serverem server Windows 2000:

Globální katalog ☐ Řadič domény ☐ Předmostí ☐

Název cílového serveru: _____

Je-li druhým *zdrojovým* serverem server Windows 2000:

Globální katalog ☐ Řadič domény ☐ Předmostí ☐

Název zdrojového serveru: _____

Je-li druhým *cílovým* serverem server Exchange 5.5:

Název cílového serveru: _____

Připojované (mapované) objekty určete pomocí tabulky A.18.

Tabulka A.18 Určení připojovaných adresářových objektů

Adresář programu Exchange Server 5.5	Služba Active Directory

Atributy, které nebudete připojovat (mapovat), uveďte do tabulky A.19.

Tabulka A.19 Seznam nepřipojovaných atributů

Adresář programu Exchange Server 5.5	Služba Active Directory

Určete synchronizační požadavky elektronické pošty jiných výrobců: _____

Vytvoření časového plánu synchronizace adresářů

Chcete-li vytvořit časový plán synchronizace ve vaší organizaci, seznamte se s ukázkovým plánem synchronizace adresářů uvedeným v kapitole „Synchronizování služby Active Directory s adresářovou službou programu Exchange Server“ v této knize. K vytvoření svého časového plánu synchronizace adresářů použijte tabulku A.20.

Tabulka A.20 Matice synchronizace adresářů

Hodina	Po	Út	St	Čt	Pá	So	Ne
0-1							
1-2							
2-3							
3-4							
4-5							
5-6							
6-7							
7-8							
8-9							
9-10							
10-11							
11-12							
12-13							
13-14							
14-15							
15-16							
16-17							
17-18							
18-19							
19-20							
20-21							
21-22							
22-23							
23-24							

Záznam kontaktů synchronizování adresářů

Skupina správců schéma

Hlavní kontaktní jméno a telefonní číslo: _____

Sekundární kontaktní jméno a telefonní číslo: _____

Čas potřebný pro možné změny schéma: _____

Správce domény systému Windows 2000

Organizace zodpovědná za domény systému Windows 2000: _____

Hlavní kontaktní jméno a telefonní číslo: _____

Sekundární kontaktní jméno a telefonní číslo: _____

Správce sídla programu Exchange Server 5.5

Organizace zodpovědná za sídla Exchange: _____

Hlavní kontaktní jméno a telefonní číslo: _____

Sekundární kontaktní jméno a telefonní číslo: _____

Ospravedlnění této dohody o spojení: _____

Testování kompatibility aplikací se systémem Windows 2000

Mnoho velkých organizací má stovky nebo dokonce tisíce aplikací. Je-li to také váš případ, může být vytvoření seznamu aplikací časově velmi náročné.

Měli byste získat následující informace o jednotlivých aplikacích:

- Název a verze aplikace
- Název výrobce

- Aktuální stav (například ve výrobním prostředí, ve vývoji nebo již nepoužívaná)
- Počet uživatelů a jejich výrobní či obchodní jednotky
- Priorita neboli důležitost pro vaši organizaci
- Aktuální operační systémy, kde se aplikace používá
Uveďte, zda jde o klientskou nebo serverovou aplikaci a které součásti se nacházejí na serveru a na klientovi.
- Pro webové aplikace adresy webových sídel (URL)
- Požadavky na instalaci (například nastavení zabezpečení a instalační adresáře).
- Nástroj nebo technologie vývoje (pro aplikace vyvinuté interně)
- Kontaktní jména a telefonní čísla (interní a prodejci)

Najdete-li více kontaktů na jednoho výrobce, pokuste se je zkonsolidovat.

Je-li jedním z vašich cílů konsolidace aplikací nebo lepší naplánování testovacích činností, můžete určit priority aplikací pomocí tabulky A.21.

Tabulka A.21 Určení priorit aplikací

Aplikace	Důležitost aplikace pro vaši organizaci	Počet uživatelů	Jedná se o nejnovější verzi?	Používají se nebo jsou zapotřebí lokalizované verze?
			Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>
			Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>
			Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>
			Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>
			Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>
			Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>
			Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>

Tabulka A.22 obsahuje některé testy, které můžete použít při plánování strategie testování. V případě jiných potřeb vaší organizace tento seznam rozšířte o další problémy. Chcete-li sledovat výsledky testování, zaznamenejte si do tabulky, zda byl test úspěšný, neúspěšný, probíhá nebo je jeho stav neznámý. Můžete si také poznamenat jméno osoby zodpovědné za testování dané aplikace a datum skutečného nebo očekávaného dokončení testování.

Tabulka A.22 Plánování a sledování strategie testování

Test	Odpovědná osoba	Plánované datum testu	Výsledek testu	Datum dokončení
Čistá instalace				
Instalace inovací				
Odebrání instalace				
Možnosti instalace				
Základní funkce a obecné úkoly a postupy				
Práce s více otevřenými aplikacemi				
Práce s doplňkovým hardwarem, jako jsou skenery				
Tisk				
Přístup k datům na serveru a práce s nimi				

Definování standardů správy a konfigurace klientů

Kapitola „Definování standardů správy a konfigurace klientů“ v této knize popisuje klíčové kroky plánování, které musíte vykonat v zájmu naplnění a správy potřeb uživatelů ve vaší organizaci. Abyste toho dosáhli, nejprve musíte pochopit zvláštní požadavky uživatelů a problémy, kterými se musí váš tým podpory klientů zabývat při uspokojování potřeb uživatelů.

Tabulka A.23 vám pomůže určit požadavky na počítače kladené různými typy uživatelů v rámci vaší organizace. Použijte ji k seskupení uživatelů podle typu práce, kterou vykonávají (cestující, stacionární profesionál, s konkrétními úkoly atd.) a kam do organizace patří (umístění a pracovní skupina), abyste mohli vytvořit společné standardy pro aplikace, konfigurace a autonomii. Ukázkovou tabulku podobné té následující a informace, které vám pomohou s jejím vyplněním, najdete v kapitole „Definování standardů správy a konfigurace klientů“ v této knize.

Tabulka A.23 Určení požadavků na počítače kladených vašimi uživateli

	Název práce 1	Název práce 2	Název práce 3
Kategorie			
Pracovní skupina			
Umístění			
Požadavky na aplikace			
Požadavky na operační systém			
Požadavky na hardware počítače			
Požadavky na podporu			
Povolená nebo požadovaná autonomie			

Tabulka A.24 vám pomůže definovat hlavní problémy technické podpory uživatelů a určit někoho k jejich vyřešení. Později v plánovacím procesu můžete tuto tabulku použít ke sledování postupu v řešení těchto problémů podpory klientů.

Tabulka A.24 Definování problémů technické podpory klientů

Problém nebo otázka podpory	Závažnost/Četnost	Vlastník	Řešení

Chcete-li změnit přiřazení úkolů podpory klientů, použijte tabulku A.25 k určení míst, kde se v současné době ve vaší organizaci tyto úkoly vykonávají a kde by měly být vykonávány.

Tabulka A.25 Přirazení úkolů správy klientů a podpory

Úkol podpory klientů	Současný vlastník	Navrhovaný vlastní

Definování požadavků zásad skupiny

Chcete-li implementovat standardy správy klientů, musíte vytvořit objekty zásad skupiny obsahující nastavení v mnoha různých oblastech: zabezpečení, aplikace, počítačové systémy, uživatelské prostředí a podle konkrétních aplikací. Většina těchto možností je vysvětlena v kapitole „Definování standardů správy a konfigurace klientů“. O problémech se zabezpečením pojednává kapitola „Plánování distribuovaného zabezpečení“. (Může být také zapotřebí vytvořit další nastavení, jestliže plánujete implementovat schopnosti popsané v kapitole „Aplikování správy změn a konfigurací“.)

Chcete-li definovat požadavky zásad skupiny ve vaší organizaci, nejprve určete typy nastavení požadovaných zásad. Obvykle půjde o následující oblasti:

Nastavení zabezpečení: _____

Zavádění balíčky aplikací: _____

Nastavení počítačového systému: _____

Nastavení uživatelského prostředí: _____

Nastavení jednotlivých aplikací: _____

Dále použijte tabulku podobnou té uvedené dále k určení typu objektu v adresáři (uživatel, počítač atd.), kde budete tato nastavení aplikovat:

- Doména (zásady hesel a účtů)
- Klientské počítače
- Uživatelé
- Řadiče domény
- Servery (aplikační, souborové a tiskové)

V této fázi by měl být vytvořený dokument prvním návrhem struktury zásad skupiny. Je pravděpodobné, že bude mnoho nastavení vašich zásad skupiny společných všem klientským počítačům, uživatelům, serverům atd. ve vaší organizaci. Takové univerzální nastavení zásad skupiny můžete zkombinovat do jediného objektu zásad skupiny (Group Policy) pro klienty, uživatele, servery atd.

Tabulka A.26 Definování požadavků zásad skupiny systému Windows 2000

	Doména	Klientské počítače	Uživatelé	Řadiče domény	Servery
Zabezpečení	Heslo; Účet; Zásady Kerberos; Seznam důvěry- hodnosti PK	Práva uživatelů; Seznamy ACL souborů a registru; Auditování a protokol událostí; Místní nastavení	Zásady EFS	Práva uživa- telů; Seznamy ACL souborů a registru; Auditování a protokol událostí; Místní nastavení	Práva uživatelů; Seznamy ACL souborů a re- gistru; Auditování a protokol událostí; Místní nastavení
Zavádění aplikací		Nutné základní aplikace	Publikované volitelné aplikace a součásti	Nástroje pro správu	Nástroje pro správu
Nastavení počítače (hardwaru)		Spouštěcí skripty; Přihlašování; Diskové kvóty; Soubory offline		Diskové kvóty	Přesun tiskáren
Uživatelská nastavení			Přihlašovací skripty; Nastavení aplikace Internet Explorer; Vzdálený přístup; Přesměrování složek; Zamknutí počítače; Síť; Systém	Zákaz stan- dardních nastavení počítače uživatele	Zákaz stan- dardních nastavení počítače uživatele
Nastavení aplikací			Office 2000; Interní aplikace		

Některá nastavení zásad skupiny nebudou platit pro všechny objekty určitého typu. Můžete pak vytvořit dodatečné objekty zásad skupiny nebo použít některou ze speciálních možností implementování zásad skupiny popsanych v kapitole „Definování standardů správy a konfigurace klientů“. Můžete například potřebovat zvláštní objekt zásad skupiny k zajištění správné konfigurace počítačů uživatelů, kteří přistupují k síti ze vzdálených počítačů. Podobně v případě uživatelů s odpovědností správce asi nebude-

te chtít, aby se jejich aplikace instalovaly po přihlášení k nějaké serverové konzole. Tomu můžete zabránit nastavením duplicitních zásad u systémů, které chcete chránit, čímž dodáte jiná nebo přepíšete standardní nastavení uživatele.

Kapitola „Definování standardů správy a konfigurace klientů“ v této knize vám vysvětlí mnoho z možností zásad skupiny, které můžete použít k úpravě a efektivní správě zásad skupiny. Tabulka A.27 ukazuje, jak můžete zdokumentovat rozsah a výjimky nastavení zásad skupiny.

Tabulka A.27 Definování rozsahu a výjimek zásad skupiny

Nastavení zásad skupiny	Rozsah	Výjimky
Doména (zabezpečení)		
Pracovní stanice (zabezpečení, aplikace a systém)		
Uživatel (zabezpečení, aplikace a systém)		
Řadič domény (zabezpečení, aplikace a systém)		
Server (zabezpečení, aplikace a systém)		

Aplikování správy změn a konfigurací

V kapitole „Definování standardů správy a konfigurace klientů“ v této knize jste měli za úkol definovat konfigurace počítačů a požadavky na aplikace pro různé typy uživatelů. Vykonáním kroků plánování uvedených v kapitole „Aplikování správy změn a konfigurací“ můžete implementovat své nové standardy správy a konfigurací pomocí funkcí IntelliMirror a vzdálené instalace systému Windows 2000.

Aplikace zaváděné pomocí funkcí instalace a údržby softwaru systému Windows 2000 lze publikovat, přiřazovat uživatelům nebo přiřazovat počítačům. Abyste porozuměli důsledkům jednotlivých možností a abyste je dokázali v aplikacích své organizace používat, přečtěte si kapitolu „Aplikování správy změn a konfigurací“ v této knize.

Pomocí tabulky A.28 si poznamenejte aplikace používané ve vaší organizaci a způsob jejich zavádění.

Tabulka A.28 Záznam aplikací a možností jejich správy

Aplikace	Přiřazena uživateli	Přiřazena počítači	Publikována
	Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>
	Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>
	Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>
	Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>
	Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>
	Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>
	Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>	Ano <input type="checkbox"/> Ne <input type="checkbox"/>

Pomocí tabulky A.29 definujte, které funkce správy změn a konfigurací jsou vhodné pro jednotlivé typy uživatelů ve vaší organizaci. Do levého sloupce zadejte typy uživatelů definované v tabulce A.23. Příklad takové dokončené tabulky najdete v kapitole „Aplikování správy změn a konfigurací“ v této knize.

Tabulka A.29 Definování strategií správy konfigurace uživatelů

Typ uživatele	Správa uživatelských dat	Správa uživatelských nastavení	Instalace a údržba softwaru	Vzdálená instalace OS

Automatizování instalace a inovace klientů

Před zautomatizováním instalace systému Windows 2000 Professional se musíte rozhodnout, zda budete inovovat z některého z dřívějších systémů, nebo zda vykonáte čistou instalaci. Následující otázky vám pomohou určit, jestli máte vykonat inovaci nebo čistou instalaci.

1. Používá vaše organizace v současné době spravovanou instalaci systému Windows NT? Ano ☐ Ne ☐
2. Plánujete používat již existující hardware a softwarové aplikace? Ano ☐ Ne ☐

Jestliže jste na otázky 1 a 2 odpověděli kladně, pak bude asi vhodnější vykonat inovaci.

3. Plánujete instalovat systém Windows 2000 na nový hardware? Ano ☐ Ne ☐
4. Plánujete instalovat nové aplikace napsané pro prostředí systému Windows 2000? Ano ☐ Ne ☐

Jestliže jste odpověděli kladně na otázky 3 a 4, asi pro vás bude lepší čistá instalace.

Použité metody automatizované instalace a oblasti jejich použití ve vaší organizaci určete pomocí tabulky A.30.

Tabulka A.30 Určení času a místa použití metod automatizované instalace

Metoda	Kdy ji použít	Použít tuto metodu?	Kdy a kde?
Syspart	Pro čisté instalace na počítače s různým hardwarem.		
Sysprep	Když mají hlavní počítač a cílové počítače stejný hardware, kam patří vrstva abstrakce hardwaru (HAL) a zařízení hromadného ukládání dat.		
Systems Management Server (SMS)	K vykonání spravovaných inovací systému Windows 2000 Professional na více systémech zejména geograficky rozptýlených.		
Spustitelné CD	Na počítači, kterému jeho systém BIOS umožňuje spouštění z disku CD.		
Vzdálená instalace OS	Pro vzdálenou instalaci obrazu (bitové kopie) systému Windows 2000 Professional na podporované počítače, čímž se eliminuje nutnost fyzicky při inovacích navštěvovat jednotlivé počítače.		

Tabulku A.31 použijte k zaznamenání data dokončení jednotlivých úkolů instalace klientů.

Tabulka A.31 Záznam úkolů instalace klientů

Úkol	Datum dokončení
Vyřešení kritických problémů plánování.	
Vytvoření distribuční složky.	
Seznámení se se souborem odpovědí.	
Seznámení se s příkazy instalačního programu systému Windows 2000.	
Volba metody instalace aplikace na základě kritického plánování.	
Volba metody instalace operačního systému na základě kritického plánování.	

PŘÍLOHA B

Příkazy instalačního programu

Systém Microsoft Windows 2000 se instaluje pomocí instalačního programu představovaného souborem Winnt.exe nebo Winnt32.exe. Tato příloha obsahuje informace o syntaxi a parametrech těchto programových souborů.

V této příloze

Instalace systému Windows 2000 pomocí příkazů instalačního programu 835

Související informace v sadě Resource Kit

- Další informace o automatizaci instalace systému Windows 2000 najdete v kapitole „Automatizování instalace a inovace serveru“ v této knize.
- Další informace o souborech odpovědí najdete v příloze C „Příklady souborů odpovědí pro bezobslužnou instalaci“ v této knize.

Instalace systému Windows 2000 pomocí příkazů instalačního programu

Chcete-li nainstalovat systém Windows 2000, použijte příslušný příkaz spuštění instalačního programu systému Windows 2000:

Winnt32.exe Pro čistou instalaci nebo inovaci na počítači se systémem Microsoft Windows NT verze 4.0, Microsoft Windows 95 nebo Microsoft Windows 98.

Winnt.exe Pro čistou instalaci na počítač se systémem Microsoft MS-DOS nebo Microsoft Windows 3.x (tyto systémy nelze inovovat).

Možnosti obou příkazů se liší. Popis jednotlivých příkazů najdete v následujících oddílech.

Upozornění Před inovací na operační systém Windows 2000 nezapomeňte restartovat počítač, pokud jste právě dokončili instalaci nějakých aplikací.

Syntaxe příkazu Winnt32

winnt32

[/checkupgradeonly]

[/cmd:*příkazový_řádek*]

[/cmdcons]

[/copydir:*název_složky*]

[/copysource:*název_složky*]

[/debug[*úroveň*][:*název_souboru*]]

[/m:*název_složky*]

[/makelocalsource]

[/noreboot]

[/s:*zdrojová_cesta*]

[/syspart:*písmeno_jednotky*]

[/tempdrive:*písmeno_jednotky*]

[/udf:*ID[,soubor_UDF]*]

[/unattend[*číslo*][:*soubor_odpovědí*]]

/checkupgradeonly

Prověří, zda počítač obsahuje systém kompatibilní s inovací na systém Windows 2000. Jedná se pouze o ověření a nedochází k instalaci systému Windows 2000.

/cmd:*příkazový_řádek*

Určuje příkaz vykonaný po dokončení části instalačního programu s grafickým uživatelských rozhraním (GUI). K vykonání příkazu dojde před úplným dokončením instalačního programu a po restartu počítače a sběru všech potřebných konfiguračních informací. Tato volba může například spustit soubor Cmdlines.txt, který obvykle zadává aplikace instalované ihned po dokončení instalačního programu.

/cmdcons

Přidá do obrazovky umožňující výběr operačního systému možnost konzoly pro zotavení k opravě neúspěšné instalace.

/copydir:*název_složky*

Ve složce obsahující soubory systému Windows 2000 vytvoří další složku. Obsahuje-li například zdrojová složka složku s názvem Soukromé_ovladače se specifickými úpravami, je možné zadáním parametru **/copydir:Soukromé_ovladače** tuto složku při instalaci zkopírovat do složky obsahující systém Windows 2000. Parametr **/copydir** lze použít k vytvoření libovolného počtu složek.

/copysource:*název_složky*

Ve složce, kam budou nainstalovány soubory systému Windows 2000, dočasně vytvoří další složku. Obsahuje-li například zdrojová složka složku s názvem Soukromé_ovladače se specifickými úpravami, je možné zadáním parametru **/copysource:Soukromé_ovladače** tuto složku zkopírovat do složky obsahující systém Windows 2000 a použít v ní obsažené soubory při instalaci. Na rozdíl od složek vytvořených parametrem **/copydir** jsou složky vytvořené parametrem **/copysource** po dokončení instalace odstraněny.

/debug[*úroveň*][:*název_souboru*]

Vytvoří protokol pro ladění na určené úrovni. Soubor protokolu pro ladění má výchozí umístění `%windir%\Winnt32.log` a jeho úroveň ladění je nastavená na hodnotu 2.

Úrovně ladění jsou následující: 0 = vážné chyby, 1 = chyby, 2 = varování, 3 = informace a 4 = podrobné informace o ladění. Každá úroveň zahrnuje úrovně nižší.

/m:název_složky

Určuje, že při instalaci budou zkopírovány nahrazující soubory z alternativního umístění. Na základě tohoto parametru prohledá instalační program nejdříve alternativní umístění, a pokud jsou soubory nalezeny, použije je místo souborů ve výchozím umístění.

/makelocalsource

Na základě tohoto parametru instalační program zkopíruje všechny zdrojové soubory instalace na místní pevný disk. Parametr **/makelocalsource** slouží při instalaci z disku CD-ROM k vytvoření zdroje instalačních souborů v případě, že disk CD-ROM nebude později v průběhu instalace k dispozici.

/noreboot

Na základě tohoto parametru instalační program nerestartuje počítač po dokončení fáze kopírování souborů, která je součástí příkazu Winnt32, aby bylo možné provést jiný příkaz.

/s:zdrojová cesta

Určuje zdrojové umístění souborů systému Windows 2000. Výchozí je aktuální složka. Chcete-li kopírovat současně soubory z více serverů, zadejte až osm zdrojů, například:

```
Winnt32 /s:server1 ... /s:server8
```

Systém Windows 2000 může využít až osmi přepínačů **/s** ukazujících na další distribuční servery jako na zdroje instalačních souborů pro cílový počítač. Tato funkce pomáhá zrychlit část kopírování instalačního programu na cílový počítač a pro distribuční servery, ze kterých lze instalační program spustit, představuje další možnost vyrovnávání zatížení. Například:

```
Cesta k distribuční složce 1\winnt32 [/unattend] [:cesta\odpoved.txt]  
[/s:cesta k distribuční složce 2] [/s:cesta k distribuční složce 3]  
[/s:cesta k distribuční složce 4]
```

/syspart:písmeno_jednotky

Určuje možnost kopírování spouštěcích souborů instalačního programu na pevný disk, označení disku jako aktivního a poté jeho nainstalování do jiného počítače. Když spustíte tento počítač, automaticky se spustí další fáze instalace. Při použití tohoto přepínače musíte vždy pamatovat na tyto body:

- Přepínač **/syspart** je vždy nutné použít společně s parametrem **/tempdrive**.
- Parametry **/syspart** i **/tempdrive** musí ukazovat na stejné místo sekundárního pevného disku.
- Systém Windows 2000 musíte instalovat na primární oddíl daného sekundárního pevného disku.
- Přepínač **/syspart** lze použít pouze na počítači se spuštěným systémem Windows NT 3.51, Windows NT 4.0 nebo Windows 2000. Tento přepínač nelze použít na počítači s operačním systémem Windows 85 nebo Windows 98.

/tempdrive:písmeno_jednotky

Na základě tohoto parametru bude instalační program umísťovat dočasné soubory do určeného oddílu a nainstaluje do něj systém Windows 2000. Při použití tohoto přepínače musíte vždy pamatovat na tyto body:

- Přepínač **/tempdrive** je vždy nutné použít společně s parametrem **/syspart**.
- Parametry **/tempdrive** i **/syspart** musí ukazovat na stejné místo sekundárního pevného disku.
- Systém Windows 2000 musíte instalovat na primární oddíl daného sekundárního pevného disku.

/udf:ID[,soubor_UDB]

Označuje identifikátor (ID), který při instalaci určuje, jak bude na základě souboru UDB (Uniqueness Database) upraven soubor odpovědí (viz parametr **/unattend** uvedený dále). Soubor .udf přepisuje hodnoty v souboru odpovědí a identifikátor určuje, které hodnoty v souboru UDB budou použity. Například parametr **/udf:uživatel_RAS,Naše_firma.udb** přepíše nastavení určené identifikátorem uživatel_RAS v souboru Naše_firma.udb. Pokud není zadán žádný soubor .udb, instalační program vyzve uživatele k vložení disku se souborem \$Unique\$.udb.

/unattend

Inovuje předchozí verzi systému Windows v bezobslužném režimu instalace. Zásah uživatele během instalace není vyžadován, protože všechna uživatelská nastavení se převzou z předchozí instalace.

Důležité Použitím přepínače **/unattend** k automatizaci instalace potvrzujete, že jste přečetli a přijali Licenční smlouvu společnosti Microsoft pro systém Windows 2000. Pokud bude systém Windows 2000 používán v jiné organizaci než vaší, je před použitím tohoto přepínače k instalaci systému nutné potvrdit, že koncový uživatel (fyzická nebo právnická osoba) obdržel, přečetl a přijal podmínky Licenční smlouvy společnosti Microsoft pro systém Windows 2000. Je možné, že výrobci OEM tento klíč na počítačích prodávaných koncovým uživatelům neuvedou.

/unattend[číslo]:[soubor_odpovědí]

Provede instalaci systému Windows 2000 v bezobslužném režimu nevyžadujícím zadání uživatele. Potřebné informace instalační program získá z předem připraveného souboru odpovědí. Další informace o souboru odpovědí najdete v příloze C „Příklady souborů odpovědí pro bezobslužnou instalaci“ v této knize.

Parametr *číslo* použijte pouze při inovování systému Windows NT 4.0. Tato hodnota udává v sekundách zpoždění mezi dokončením kopírování souborů instalačním programem a začátkem instalace systému.

Winnt

Winnt

/e:příkaz

/r:složka

/rx:složka

/s:zdrojová_cesta

/t:dočasná_jednotka

/u:soubor_odpovědí

/udf:ID [,soubor_UDB]

/a

/e:příkaz

Určuje příkaz, který má být proveden na závěr instalace v režimu grafického uživatelského rozhraní (GUI). Tato volba může například spustit soubor Cmdlines.txt, který obvykle zadává aplikace instalované ihned po dokončení instalačního programu.

/r:složka

Ve složce obsahující soubory systému Windows 2000 vytvoří další složku. Obsahuje-li například zdrojová složka složku s názvem Soukromé_ovladače se specifickými úpravami, je možné zadáním parametru **/r:Soukromé_ovladače** tuto složku při instalaci zkopírovat do složky obsahující systém Windows 2000. Parametr **/r** lze použít k vytvoření libovolného počtu složek.

/rx:složka

Ve složce, kam budou nainstalovány soubory systému Windows 2000, dočasně vytvoří další složku. Obsahuje-li například zdrojová složka složku s názvem Soukromé_ovladače se specifickými úpravami, je možné zadáním parametru **/rx:Soukromé_ovladače** tuto složku zkopírovat do složky obsahující systém Windows 2000 a použít v ní obsažené soubory při instalaci. Na rozdíl od složek vytvořených parametrem **/r** jsou složky vytvořené parametrem **/rx** po dokončení instalace odstraněny.

/s:zdrojová_cesta

Určuje zdrojové umístění souborů systému Windows 2000. Umístění musí být určeno zadáním úplné cesty, například *Písmeno_jednotky:\cesta* nebo *\\server\místo_sdílení\cesta*.

/t:dočasná_jednotka

Na základě tohoto parametru umístí instalační program dočasné soubory do určené jednotky a nainstaluje do ní systém Windows 2000. Neurčíte-li umístění, instalační program se pokusí najít jednotku automaticky.

/u:soubor_odpovědí

Provede instalaci systému Windows 2000 v bezobslužném režimu nevyžadujícím zadání uživatele. Potřebné informace instalační program získá z předem připraveného souboru odpovědí. Další informace o souboru odpovědí najdete v příloze C „Příklady souborů odpovědí pro bezobslužnou instalaci“ v této knize.

/udf:ID [,soubor_UDB]

Označuje identifikátor (ID), který při instalaci určuje, jak bude na základě souboru UDB (Uniqueness Database) upraven soubor odpovědí (viz parametr **/u**). Soubor .udf přepisuje hodnoty v souboru odpovědí a identifikátor určuje, které hodnoty v souboru UDB budou použity. Například parametr **/udf:uživatel_RAS,Naše_firma.udb** přepíše

nastavení určené identifikátorem uživatel_RAS v souboru Naše_firma.udb. Pokud není zadán žádný soubor .udb, instalační program vyzve uživatele k vložení disku se souborem \$Unique\$.udb.

/A

Zapne možnosti usnadnění.

PŘÍLOHA C

Příklady souborů odpovědí pro bezobslužnou instalaci

Bezobslužná instalace systému Microsoft Windows 2000 využívá textový soubor ve formátu ASCII, jenž se označuje za soubor odpovědí a dodává instalačnímu programu údaje, které by jinak bylo nutné zadávat interaktivně Průvodci instalací. Soubor odpovědí se zadá na příkazovém řádku spuštění programu Winnt.exe nebo Winnt32.exe pomocí volby bezobslužné instalace. (Další informace o použití jednotlivých příkazových řádků najdete v příloze B „Příkazy instalačního programu“ v této knize.)

Tato příloha obsahuje ukázkové soubory odpovědí vhodné pro obvyklé instalační konfigurace. Můžete si upravit výchozí soubor odpovědí (Unattend.txt), který je součástí systému Windows 2000, nebo můžete na základě ukázek uvedených v této kapitole vytvořit nový soubor.

V této příloze

Formát souboru odpovědí 841

Klíče a hodnoty souboru odpovědí 842

Ukázkové soubory odpovědí 842

Související informace v sadě Resource Kit

- Další informace o příkazech instalačního programu najdete v příloze B „Příkazy instalačního programu“ v této knize.

Formát souboru odpovědí

Soubor odpovědí se skládá ze záhlaví oddílů, klíčů a hodnot jednotlivých klíčů. Většina záhlaví oddílů je předdefinovaná, některé však může být zapotřebí definovat ručně. V souboru odpovědí není nutné zadávat všechny možné klíče, pokud je instalace nevyžaduje. Neplatné hodnoty klíčů způsobují chyby, které mohou zapříčinit nesprávnou funkci systému po instalaci. Soubor má následující formát:

[název_oddílu]

Oddíly obsahují klíče a jejich odpovídající hodnoty. Klíč a hodnota jsou vždy odděleny mezerou, rovnítkem a další mezerou. Příkladem je:

klíč = hodnota

Hodnoty obsahující mezery musí být uzavřeny v uvozovkách. Příkladem je:

klíč = „hodnota s mezerami“

Některé oddíly nemají žádné klíče a obsahují jen seznam hodnot. Příkladem je:

```
[OEMBootFiles]
Txtsetup.oem
```

Řádky komentáře začínají středníkem.

; Toto je příklad řádku komentáře.

Klíče a hodnoty souboru odpovědí

Každý klíč v souboru odpovědí musí mít přiřazenu hodnotu. Některé klíče jsou však volitelné a jiné mají výchozí hodnoty, které se použijí v případech, kdy není klíč zadán.

Hodnoty klíčů jsou řetězce textu, není-li tedy zadáno číslo. Jestliže je zadáno číslo, jeho hodnota je desítková, není-li uvedeno jinak.

Poznámka Klíče nerozlišují velikost písmen a lze je zapisovat malými i velkými znaky.

Další informace o klíčích a hodnotách souboru odpovědí najdete v dokumentu „Microsoft Windows 2000 Guide to Unattended Setup“ (Unattend.doc) na CD operačního systému Microsoft Windows 2000. Soubor Unattend.doc je součástí souboru Deploy.cab ve složce \Support\Tools. V systému Windows 98 nebo Windows 2000 použijte k získání uvedeného dokumentu Průzkumníka. V systému Windows 95 a dřívějším a v systému MS-DOS použijte k získání tohoto souboru příkaz **Extract**.

Ukázkové soubory odpovědí

Ukázkové soubory odpovědí uvedené v tomto oddílu jsou příklady obvyklejších instalačních konfigurací klíčů, které se často používají. Tyto soubory považujte pouze za příklady a upravte je podle potřeb vaší organizace.

Poznámka V následujících souborech odpovědí označuje kurzíva informace, které musí zadat uživatel. Aby bylo snazší vyhledat jednotlivé oddíly, jsou jejich záhlaví vyznačena tučným písmem. Tyto formátovací konvence však nemusíte ve svém souboru odpovědí používat.

Příklad 1 – Výchozí soubor Unattend.txt

Následující soubor odpovědí je výchozím souborem Unattend.txt uvedeným na disku CD systému Windows 2000.

```
; Microsoft Windows 2000 Professional, Server, Advanced Server a Datacenter
; (c) 1994 - 1999 Microsoft Corporation. Všechna práva vyhrazena.
;
; Ukázkový soubor odpovědí bezobslužné instalace
;
; Tento soubor obsahuje informace o možnostech automatizace instalace
; nebo inovace systému Windows 2000 Professional a Windows 2000 Server tak,
```

```
; aby instalační program nevyžadovat zásah uživatele.  
;
```

[Unattended]

```
Unattendmode = FullUnattended  
OemPreinstall = NO  
TargetPath = WINNT  
Filesystem = LeaveAlone
```

[UserData]

```
FullName = „Jméno uživatele“  
OrgName = „Název společnosti“  
; Doporučujeme vám vyhnout se mezerám v hodnotě ComputerName.  
ComputerName = „Nazev_pocitace“  
; Chcete-li zajistit plně bezobslužnou instalaci, musíte zadat hodnotu  
; klíče ProductID.  
ProductID = „ID vašeho produktu“
```

[GuiUnattended]

```
; Nastaví časové pásmo. Například chcete-li nastavit středoevropský čas,  
; použijete hodnotu „095“. Musíte vždy použít hodnotu představující vaši časovou  
; zónu. Tuto hodnotu najdete v souboru Unattend.doc na CD systému Windows 2000.  
TimeZone = „Vaše časová zóna“  
; Doporučujeme vám změnit heslo správce před umístěním počítače na cílové místo.  
AdminPassword = AdminPassword  
; Zapne funkci automatického přihlášení (AutoLogon) a umožní jedno přihlášení.  
AutoLogon = Yes  
AutoLogonCount = 1
```

[LicenseFilePrintData]

```
; Tento oddíl je rezervován pro instalace serverů.  
AutoMode = „PerServer“  
AutoUsers = „5“
```

[GuiRunOnce]

```
; Zde je možno uvést programy, které se mají spustit při prvním  
; přihlášení uživatele k počítači.
```

[Display]

```
BitsPerPel = 8  
XResolution = 800  
YResolution = 600  
VRefresh = 70
```

[Networking]

```
; Při zadání hodnoty YES klíče InstallDefaultComponents nainstaluje  
; instalační program výchozí síťové součásti. Tyto součásti jsou:  
; TCP/IP, sdílení souborů a tisku a služba Client for Microsoft Networks.  
InstallDefaultComponents = YES
```

[Identification]

```
; Určuje pracovní skupinu. V této hodnotě byste se měli vyhnout mezerám.  
JoinWorkgroup = „Skupina“
```

Příklad 2 – Bezobslužná instalace systému Windows 2000 Professional z disku CD-ROM

Následující soubor odpovědí instaluje systém Microsoft Windows 2000 Professional z disku CD-ROM. Aby tento soubor odpovědí správně fungoval, musíte jej pojmenovat Winnt.sif a umístit na disketu.

```
; Microsoft Windows 2000 Professional
; (c) 1994 - 1999 Microsoft Corporation. Všechna práva vyhrazena.
;
; Ukázkový soubor odpovědí bezobslužné instalace
;
; Tento soubor obsahuje informace o možnostech automatizace instalace
; nebo inovace systému Windows 2000 Professional tak,
; aby instalační program nevyžadovat zásah uživatele.
;
```

[Data]

```
; Tento oddíl je zapotřebí při vykonávání bezobslužné instalace spuštěním
; instalačního programu přímo z instalačního CD systému Windows 2000.
  Unattendedinstall = Yes
; Spouštíte-li bezobslužnou instalaci z disku CD-ROM, musíte nastavit klíč
; Msdosinitiated na hodnotu 0.
  Msdosinitiated = „0“
; AutoPartition umožní bezobslužné instalaci systému Windows 2000 vybrat si
; oddíl, na který se systém nainstaluje.
  AutoPartition = 1
```

[Unattended]

```
  UnattendMode = FullUnattended
; Klíč OemPreinstall říká bezobslužné instalaci, že k instalaci dochází
; z distribučních míst, je-li hodnota nastavena na Yes.
  OemPreinstall = Yes
  TargetPath = Winpro
  FileSystem = LeaveAlone
; Je-li hodnota klíče OemSkipEula nastavena na Yes, informuje bezobslužnou
; instalaci, že uživatel nebude vyzván k přijetí s dohodou EULA. Hodnota Yes
; představuje souhlas s touto dohodou a musí být použita v souvislosti
; s podmínkami licenční dohody.
  OemSkipEula = Yes
```

[GuiUnattended]

```
; Nastaví časové pásmo. Například chcete-li nastavit středoevropský čas, použijete
; hodnotu „095“. Musíte vždy použít hodnotu představující vaši časovou zónu. Tuto
; hodnotu najdete v souboru Unattend.doc na CD systému Windows 2000.
  TimeZone = „Vaše časová zóna“
; Doporučujeme vám změnit heslo správce před umístěním počítače na cílové místo.
  AdminPassword = AdminPassword
; Zapne funkci automatického přihlášení (AutoLogon) a umožní jedno přihlášení.
  AutoLogon = Yes
  AutoLogonCount = 1
; Klíč OemSkipWelcome určuje, zda se má přeskočit uvítací stránka ve fázi průvodce
```

```
; instalačního programu. Hodnota 1 způsobí přeskočení této stránky.
    OemSkipWelcome = 1
; Klíč OemSkipRegional umožňuje bezobslužné instalaci přeskočit místní nastavení,
; když je cílové umístění počítače neznámé.
    OemSkipRegional = 1

[UserData]
    FullName = „Jméno uživatele“
    OrgName = „Název společnosti“
; Doporučujeme vám vyhnout se mezerám v hodnotě ComputerName.
    ComputerName = „Název_pocitace“
; Chcete-li zajistit plně bezobslužnou instalaci, musíte zadat hodnotu
; klíče ProductID.
    ProductID = „ID vašeho produktu“

[Display]
    BitsPerPel = 8
    XResolution = 800
    YResolution = 600
    VRefresh = 60

[Networking]
; Při zadání hodnoty YES klíče InstallDefaultComponents nainstaluje
; instalační program výchozí síťové součásti. Tyto součásti jsou:
; TCP/IP, sdílení souborů a tisku a služba Client for Microsoft Networks.
    InstallDefaultComponents = YES
```

Příklad 3 – Instalace a konfigurace systému Windows 2000 a konfigurace aplikace Microsoft Internet Explorer nastaveními proxy

Následující soubor odpovědí instaluje a konfiguruje aplikaci Microsoft Internet Explorer a konfiguruje nastavení proxy.

```
; Microsoft Windows 2000 Professional, Server, Advanced Server
; (c) 1994 - 1999 Microsoft Corporation. Všechna práva vyhrazena.
;
; Ukázkový soubor odpovědí bezobslužné instalace
;
; Tento soubor obsahuje informace o možnostech automatizace instalace
; nebo inovace systému Windows 2000 Professional a Windows 2000 Server tak,
; aby instalační program nevyžadoval zásah uživatele.
;

[Unattended]
    UnattendMode = FullUnattended
    TargetPath = Windows
    FileSystem = LeaveAlone
    OemPreinstall = Yes
    OemSkipEula = Yes
```

[GuiUnattended]

```

; Nastaví časové pásmo. Například chcete-li nastavit středoevropský čas, použijete
; hodnotu „095“. Musíte vždy použít hodnotu představující vaši časovou zónu. Tuto
; hodnotu najdete v souboru Unattend.doc na CD systému Windows 2000.
    TimeZone = „Vaše časová zóna“
; Doporučujeme vám změnit heslo správce před umístěním počítače na cílové místo.
    AdminPassword = AdminPassword
; Zapne funkci automatického přihlášení (AutoLogon) a umožní jedno přihlášení.
    AutoLogon = Yes
    AutoLogonCount = 1
; Klíč OemSkipRegional umožňuje bezobslužné instalaci přeskočit místní nastavení,
; když je cílové umístění počítače neznámé.
    OemSkipRegional = 1

```

[UserData]

```

    FullName = „Jméno uživatele“
    OrgName = „Název společnosti“
; Doporučujeme vám vyhnout se mezerám v hodnotě ComputerName.
    ComputerName = „Nazev_pocitace“
; Chcete-li zajistit plně bezobslužnou instalaci, musíte zadat hodnotu
; klíče ProductID.
    ProductID = „ID vašeho produktu“

```

[LicenseFilePrintData]

```

; Tento oddíl je rezervován pro instalace serverů.
    AutoMode = „PerServer“
    AutoUsers = „50“

```

[Display]

```

    BitsPerPel = 8
    XResolution = 800
    YResolution = 600
    VRefresh = 60

```

[Components]

```

; Tento oddíl obsahuje klíče pro instalaci součástí systému
; Windows 2000. Hodnota On součást instaluje a hodnota
; Off zabrání v instalaci součástí.
    iis_common = On
    iis_inetmgr = Off
    iis_www = Off
    iis_ftp = Off
    iis_htmla = Off
    iis_doc = Off
    iis_pwmgr = Off
    iis_smtp = On
    iis_smtp_docs = Off
    Mts_core = On
; Klíč Fp instaluje serverová rozšíření programu Front Page.
    Fp = On
    Msmq = Off
; Nastavíte-li klíč TSEnable na hodnotu On, nainstaluje se na systém

```

```
; Windows 2000 server služba Terminal Services.  
    TSEnable = On  
; Nastavíte-li klíč TSclients na hodnotu On, nainstalují se soubory potřebné  
; k vytvoření disket klientů terminálových služeb. Nastavíte-li tento  
; klíč na hodnotu On, musíte na hodnotu On nastavit také klíč TSEnable.  
    TSclients = On  
; Klíče TSprinterDrivers a TSKeyboardDrivers jsou volitelné. Při povolení  
; požadují další diskový prostor.  
    TSprinterDrivers = Off  
    TSKeyboardDrivers = Off  
    Netoc = On  
    Reminst = On  
    Certsrv = Off  
    Rstorage = Off  
    Indexsrv_system = On  
    Certsrv_client = Off  
    Certsrv_server = Off  
    Certsrv_doc = Off  
    Accessopt = On  
    Calc = On  
    Cdplayer = On  
    Charmap = On  
    Chat = Off  
    Clipbook = On  
    Deskpaper = On  
    Dialer = On  
    Freecell = Off  
    Hypertrm = On  
    Media_blindnoisy = On  
    Media_blindquiet = On  
    Media_clips = On  
    Media_jungle = On  
    Media_musica = On  
    Media_robotz = On  
    Media_utopia = On  
    Minesweeper = Off  
    Mousepoint = Off  
    Mplay = On  
    Mwordpad = On  
    Objectpkg = On  
    Paint = On  
    Pinball = Off  
    Rec = On  
    Solitaire = Off  
    Templates = On  
    Vol = On
```

[TapiLocation]

```
    CountryCode = „1“  
    Dialing = Pulse  
; Indikuje kód oblasti vašeho telefonu. Tato hodnota by měla být  
; číslem se třemi číslicemi.
```



```
AreaCode = „Kód telefonní oblasti“
LongDistanceAccess = 9
```

[Networking]

```
; Při zadání hodnoty YES klíče InstallDefaultComponents nainstaluje
; instalační program výchozí síťové součásti. Tyto součásti jsou:
; TCP/IP, sdílení souborů a tisku a služba Client for Microsoft Networks.
InstallDefaultComponents = YES
```

[Identification]

```
JoinDomain = SíťSpolečnosti
DomainAdmin = SprávceDomény
DomainAdminPassword = HesloSprávceDomény
```

[NetOptionalComponents]

```
; Tento oddíl obsahuje seznam instalovaných volitelných síťových součástí.
Wins = Off
Dns = Off
Dhcpserver = Off
ils = Off
Snmp = Off
Lpdsvc = Off
Simptcp = Off
Netmontools = On
Dsmigrat = Off
```

[Branding]

```
; Tento oddíl vybavuje aplikaci Microsoft Internet Explorer zvláštními
; vlastnostmi ze souboru odpovědí bezobslužné instalace.
BrandIEUsingUnattended = Yes
```

[URL]

```
; Tento oddíl obsahuje vlastní nastavení adres URL pro aplikaci Microsoft
; Internet Explorer. Nejsou-li tato nastavení uvedena, použijí se výchozí
; nastavení.
; Určuje adresu URL výchozí domovské stránky prohlížeče.
; Můžete použít například: Home_Page = www.microsoft.com.
Home_Page = AdresaURLDomovskéStránky
; Určuje adresu URL výchozí stránky hledání. For Můžete použít
; například: Search Page = www.msn.com
Search_Page = AdresaURLStránkyHledání
; Určuje název zástupce ve složce odkazů oblíbených položek. Můžete použít
; například: Quick_Link_1_Name = „Technická podpora společnosti Microsoft“
Quick_Link_1_Name = „Název rychlého odkazu“
; Určuje adresu URL zástupce ve složce odkazů oblíbených položek. Můžete
; použít například: Quick_Link_1 = http://support.microsoft.com/.
Quick_Link_1 = AdresaURLRychléhoOdkazu
```

[Proxy]

```
; Tento oddíl obsahuje vaše vlastní nastavení proxy pro aplikaci Microsoft
; Internet Explorer. Nejsou-li tato nastavení uvedena, použijí se výchozí
; nastavení. Neplatí-li ve vaší konfiguraci zadání proxysrv:80, uveďte zde
```

```
; své vlastní parametry proxy-serveru a čísla portu.
HTTP_Proxy_Server = proxysrv:80
Use_Same_Proxy = 1
Proxy_Enable = 1
Proxy_Override = <local>
```

Příklad 4 – Instalace a konfigurace systému Windows 2000 Server se dvěma síťovými adaptéry

Následující soubor odpovědí instaluje systém Microsoft Windows 2000 Server se dvěma síťovými adaptéry. Jeden adaptér používá protokol Dynamic Host Configuration Protocol (DHCP) a druhý používá statické informace.

```
; Microsoft Windows 2000 Server, Advanced Server
; (c) 1994 - 1999 Microsoft Corporation. Všechna práva vyhrazena.
;
; Ukázkový soubor odpovědí bezobslužné instalace
;
; Tento soubor obsahuje informace o možnostech automatizace instalace
; nebo inovace systému Windows 2000 Server a Windows 2000 Advanced Server tak,
; aby instalační program nevyžadoval zásah uživatele.
;
```

[Unattended]

```
UnattendMode = FullUnattended
TargetPath = Winnt
Filesystem = ConvertNTFS
```

[GuiUnattended]

```
; Nastaví časové pásmo. Například chcete-li nastavit středoevropský čas, použijete
; hodnotu „095“. Musíte vždy použít hodnotu představující vaši časovou zónu. Tuto
; hodnotu najdete v souboru Unattend.doc na CD systému Windows 2000.
TimeZone = „Vaše časová zóna“
; Doporučujeme vám změnit heslo správce před umístěním počítače na cílové místo.
AdminPassword = AdminPassword
; Zapne funkci automatického přihlášení (AutoLogon) a umožní jedno přihlášení.
AutoLogon = Yes
AutoLogonCount = 1
```

[LicenseFilePrintData]

```
; Tento oddíl je rezervován pro instalace serverů.
AutoMode = „PerServer“
AutoUsers = „50“
```

[UserData]

```
FullName = „Jméno uživatele“
OrgName = „Název společnosti“
; Doporučujeme vám vyhnout se mezerám v hodnotě ComputerName.
ComputerName = „Název_pocitace“
; Chcete-li zajistit plně bezobslužnou instalaci, musíte zadat hodnotu
; klíče ProductID.
ProductID = „ID vašeho produktu“
```

[Display]

```

BitsPerPel = 8
XResolution = 800
YResolution = 600
VRefresh = 70

```

[Networking]

```

; Při zadání hodnoty YES klíče InstallDefaultComponents nainstaluje
; instalační program výchozí síťové součásti. Tyto součásti jsou:
; TCP/IP, sdílení souborů a tisku a služba Client for Microsoft Networks.
InstallDefaultComponents = YES

```

[Identification]

```

JoinDomain = SíťSpolečnosti
DomainAdmin = SprávceDomény
DomainAdminPassword = HesloSprávceDomény

```

[NetAdapters]

```

; V tomto příkladu existují dva adaptéry, Adapter01 a Adapter02.
; Uvědomte si, že adaptér zadaný zde jako 01 nemusí být vždy
; připojením 1 k místní síti v uživatelském rozhraní.
Adapter01 = Params.Adapter01
Adapter02 = Params.Adapter02

```

[Params.Adapter01]

```

; Určuje, který adaptér má číslo jedna. Klíč InfID musí odpovídat platné
; hodnotě PNP ID v systému. Platná hodnota PNP ID může vypadat například
; takto: InfID = „pci\ven_0e11&dev_ae32“
InfID = „PNP_ID_adaptéru_01“

```

[Params.Adapter02]

```

; Určuje, který adaptér má číslo dvě. Klíč InfID musí odpovídat platné
; hodnotě PNP ID v systému. Platná hodnota PNP ID může vypadat například
; takto InfID = „pci\ven_8086&dev_1229&subsys_00018086“
InfID = „PNP_ID_adaptéru_02“

```

[NetClients]

```

; Instaluje službu Client for Microsoft Networks.
MS_MSCClient = params.MS_MSCClient

```

[Params.MS_MSCClient]**[NetProtocols]**

```

; Instaluje pouze protokol TCP/IP.
MS_TCPIP = params.MS_TCPIP

```

[params.MS_TCPIP]

```

; Tento oddíl konfiguruje vlastnosti TCP/IP.
AdapterSections = Params.MS_TCPIP.Adapter01,params.MS_TCPIP.Adapter02

```

[Params.MS_TCPIP.Adapter01]

```

; Adapter01 používá informace serveru DHCP.

```

```
SpecificTo = Adapter01
DHCP = Yes
Wins = Yes

[Params.MS_TCPIP.Adapter02]
: Adapter02 používá statickou konfiguraci TCP/IP.
SpecificTo = Adapter02
IPAddress = 1.1.1.1
SubnetMask = 255.255.248.0
DefaultGateway = 2.2.2.2
DHCP = No
Wins = No

[NetServices]
: Instaluje souborové a tiskové služby.
MS_Server = Params.MS_Server

[Params.MS_Server]
```

Příklad 5 – Instalace systému Windows 2000 Advanced Server s vyrovnáváním zatížení sítě

Následující soubor odpovědí instaluje systém Microsoft Windows 2000 Advanced Server s vyrovnáváním zatížení sítě.

```
; Microsoft Windows 2000 Advanced Server
; (c) 1994 - 1999 Microsoft Corporation. Všechna práva vyhrazena.
;
; Ukázkový soubor odpovědí bezobslužné instalace
;
; Tento soubor obsahuje informace o možnostech automatizace instalace
; nebo inovace systému Windows 2000 Advanced Server tak,
; aby instalační program nevyžadoval zásah uživatele.
;

[Unattended]
UnattendMode = FullUnattended
TargetPath = Windows
FileSystem = ConvertNTFS

[GuiUnattended]
; Nastaví časové pásmo. Například chcete-li nastavit středoevropský čas, použijete
; hodnotu „095“. Musíte vždy použít hodnotu představující vaši časovou zónu. Tuto
; hodnotu najdete v souboru Unattend.doc na CD systému Windows 2000.
TimeZone = „Vaše časová zóna“
; Doporučujeme vám změnit heslo správce před umístěním počítače na cílové místo.
AdminPassword = AdminPassword
; Zapne funkci automatického přihlášení (AutoLogon) a umožní jedno přihlášení.
AutoLogon = Yes
AutoLogonCount = 1
AdvServerType = Servernt
```

[LicenseFilePrintData]

; Tento oddíl je rezervován pro instalace serverů.

AutoMode = „PerServer“

AutoUsers = „50“

[UserData]

FullName = „*Jméno uživatele*“

OrgName = „*Název společnosti*“

; Doporučujeme vám vyhnout se mezerám v hodnotě ComputerName.

ComputerName = „*Nazev_pocitace*“

; Chcete-li zajistit plně bezobslužnou instalaci, musíte zadat hodnotu

; klíče ProductID.

ProductID = „*ID vašeho produktu*“

[Display]

BitsPerPel = 8

XResolution = 800

YResolution = 600

VRefresh = 70

[Networking]

; Při zadání hodnoty YES klíče InstallDefaultComponents nainstaluje

; instalační program výchozí síťové součásti. Tyto součásti jsou:

; TCP/IP, sdílení souborů a tisku a služba Client for Microsoft Networks.

InstallDefaultComponents = YES

[Identification]

JoinDomain = *SíťSpolečnosti*

DomainAdmin = *SprávceDomény*

DomainAdminPassword = *HesloSprávceDomény*

[NetAdapters]

; V tomto příkladu existují dva adaptéry, Adapter01 a Adapter02.

; Uvědomte si, že adaptér zadaný zde jako 01 nemusí být vždy

; připojením 1 k místní síti v uživatelském rozhraní.

Adapter01 = Params.Adapter01

Adapter02 = Params.Adapter02

[NetBindings]

Enable = MS_WLBS, Adapter01

Enable = MS_TCPIP, Adapter02

[Params.Adapter01]

; Určuje, který adaptér má číslo jedna.

PseudoAdapter = No

PreUpgradeInstance = *E100B1*

; Klíč InfID musí odpovídat platné hodnotě PNP ID v systému.

; Platná hodnota PNP ID může vypadat například takto:

; InfID = „pci\ven_0e11&dev_ae32“

InfID = „*PNP_ID_adaptéru_01*“

BusType = PCI

```
; Klíč ConnectionName určuje název síťového připojení přiřazeného  
; k instalovanému síťovému adaptéru.  
ConnectionName = „Připojení1“
```

[Params.Adapter02]

```
; Určuje, který adaptér má číslo dvě.  
PseudoAdapter = No  
PreUpgradeInstance = E190x2  
; Klíč InfID musí odpovídat platné hodnotě PNP ID v systému.  
; Platná hodnota PNP ID může vypadat například takto:  
; InfID = PCI\VEN_10b7&DEV_9050  
InfID = „PNP_ID_adaptéru_02“  
BusType = PCI  
; Klíč ConnectionName určuje název síťového připojení přiřazeného  
; k instalovanému síťovému adaptéru.  
ConnectionName = „Připojení2“
```

[NetProtocols]

```
MS_TCPIP = Params.MS_TCPIP  
MS_NetMon = Params.MS_NetMon
```

[Params.MS_TCPIP]

```
AdapterSections = params.MS_TCPIP.Adapter01,params.MS_TCPIP.Adapter02
```

[Params.MS_TCPIP.Adapter01]

```
SpecificTo = Adapter01  
DNSServerSearchOrder = 192.31.56.150  
Wins = Yes  
WinsServerList = 192.31.56.150  
NetBIOSOptions = 0  
DHCP = No  
IPAddress = 192.31.56.90,192.31.56.91  
SubnetMask = 255.255.255.0,255.255.255.0  
DefaultGateway = 192.31.56.150
```

[Params.MS_TCPIP.Adapter02]

```
SpecificTo = Adapter02  
DNSServerSearchOrder = 192.31.56.150  
Wins = Yes  
WinsServerList = 192.31.56.150  
NetBIOSOptions = 0  
DHCP = No  
IPAddress = 192.31.56.92  
SubnetMask = 255.255.255.0  
DefaultGateway = 192.31.56.150
```

[Params.MS_NetMon]

[Params.MS_WLBS]

```
; Tento oddíl obsahuje klíče specifické nastavení vlastností  
; vyrovnávání zatížení sítě.  
HostPriority = 1
```

```

ClusterModeOnStart = 0
ClusterIPAddress = 192.31.56.91
ClusterNetworkMask = 255.255.255.0
DedicatedIPAddress = 192.31.56.90
DedicatedNetworkMask = 255.255.255.0
ClusterName = cluster.domena.cz
MulticastSupportEnable = 0
MaskSourceMAC = 1
RemoteControlCode = 0x00000000
RemoteControlUDPPort = 2504
RemoteControlEnabled = 1
Ports = 80,80,Both,Multiple,None,Equal,443,443,Both,Multiple,Single,Equal
AliveMsgPeriod = 2000
AliveMsgTolerance = 10
NumActions = 50
NumPackets = 100
NumAliveMsgs = 10
DescriptorsPerAlloc = 512
MaxDescriptorAllocs = 512
ConnectionCleanupDelay = 300000
NBTSupportEnable = 1

[NetClients]
MS_MSCClient = Params.MS_Client

[Params.MS_Client]

[NetServices]
MS_Server = Params.MS_Server
MS_WLBS = Params.MS_WLBS

[Params.MS_Server]
Optimizations = Balance

[NetOptionalComponents]
Netmontools = 1

```

Příklad 6 – Instalace systému Windows 2000 Advanced Server se službou Windows Clustering

Následující soubor odpovědí instaluje systém Windows 2000 Advanced Server se službou Windows Clustering.

```

; Microsoft Windows 2000 Advanced Server.
; (c) 1994 - 1999 Microsoft Corporation. Všechna práva vyhrazena.
;
; Ukázkový soubor odpovědí bezobslužné instalace
;
; Tento soubor obsahuje informace o možnostech automatizace instalace
; nebo inovace systému Windows 2000 Advanced Server tak,
; aby instalační program nevyžadoval zásah uživatele.
;

```

[Unattended]

```
UnattendMode = FullUnattended
TargetPath = Advsrv
FileSystem = ConvertNTFS
OemPreinstall = Yes
OemSkipEula = Yes
```

[GuiUnattended]

: Nastaví časové pásmo. Například chcete-li nastavit středoevropský čas, použijete
: hodnotu „095“. Musíte vždy použít hodnotu představující vaši časovou zónu. Tuto
: hodnotu najdete v souboru Unattend.doc na CD systému Windows 2000.

```
TimeZone = „Vaše časová zóna“
```

: Doporučujeme vám změnit heslo správce před umístěním počítače na cílové místo.

```
AdminPassword = AdminPassword
```

: Zapne funkci automatického přihlášení (AutoLogon) a umožní jedno přihlášení.

```
AutoLogon = Yes
```

```
AutoLogonCount = 1
```

```
AdvServerType = Servernt
```

: Klíč OemSkipWelcome určuje, zda se má přeskočit uvítací stránka ve fázi průvodce
: instalačního programu. Hodnota 1 způsobí přeskočení této stránky.

```
OemSkipWelcome = 1
```

: Klíč OemSkipRegional umožňuje bezobslužné instalaci přeskočit místní nastavení,
: když je cílové umístění počítače neznámé.

```
OemSkipRegional = 1
```

[LicenseFilePrintData]

: Tento oddíl je rezervován pro instalace serverů.

```
AutoMode = „PerServer“
```

```
AutoUsers = „50“
```

[UserData]

```
FullName = „Jméno uživatele“
```

```
OrgName = „Název společnosti“
```

: Doporučujeme vám vyhnout se mezerám v hodnotě ComputerName.

```
ComputerName = „Název_pocitace“
```

: Chcete-li zajistit plně bezobslužnou instalaci, musíte zadat hodnotu

: klíče ProductID.

```
ProductID = „ID vašeho produktu“
```

[Display]

```
BitsPerPel = 8
```

```
XResolution = 800
```

```
YResolution = 600
```

```
VRefresh = 70
```

[Networking]

: Při zadání hodnoty YES klíče InstallDefaultComponents nainstaluje

: instalační program výchozí síťové součásti. Tyto součásti jsou:

: TCP/IP, sdílení souborů a tisku a služba Client for Microsoft Networks.

```
InstallDefaultComponents = YES
```


[Identification]

```
JoinDomain = SíťSpolečnosti
DomainAdmin = SprávceDomény
DomainAdminPassword = HesloSprávceDomény
```

[NetAdapters]

```
; V tomto příkladu existují tři adaptéry, Adapter01, Adapter02 a Adapter03.
; Uvědomte si, že adaptér zadaný zde jako 01 nemusí být vždy připojením 1
; k místní síti v uživatelském rozhraní. Síťové adaptéry v tomto příkladu
; nejsou totožné
Adapter01 = Params.Adapter01
Adapter02 = Params.Adapter02
Adapter03 = Params.Adapter03
```

[Params.Adapter01]

```
; Určuje, který adaptér má číslo jedna. Klíč NetCardAddress musí
; odpovídat platné adrese adaptéru v systému. Platná adresa může
; vypadat například takto: NetCardAddress = 0x00C04F778A5A
NetCardAddress = AdresaSíťovéKarty
; Klíč ConnectionName určuje název síťového připojení přiřazeného
; k instalovanému síťovému adaptéru.
ConnectionName = SíťSpolečnosti
```

[Params.Adapter02]

```
; Určuje, který adaptér má číslo dvě. Klíč NetCardAddress musí
; odpovídat platné adrese adaptéru v systému. Platná adresa může
; vypadat například takto: NetCardAddress = 0x00C04F778A5A
NetCardAddress = AdresaSíťovéKarty
; Klíč ConnectionName určuje název síťového připojení přiřazeného
; k instalovanému síťovému adaptéru.
ConnectionName = SíťPodejce
```

[Params.Adapter03]

```
; Určuje, který adaptér má číslo tři. Klíč NetCardAddress musí
; odpovídat platné adrese adaptéru v systému. Platná adresa může
; vypadat například takto: NetCardAddress = 0x00C04F778A5A
NetCardAddress = AdresaSíťovéKarty
; Klíč ConnectionName určuje název síťového připojení přiřazeného
; k instalovanému síťovému adaptéru.
ConnectionName = PrivátníSíť
```

[NetClients]

```
; Instaluje službu Client for Microsoft Networks.
MS_MSClient = Params.MS_MSClient
```

[Params.MS_MSClient]

[NetProtocols]

```
; Instaluje pouze protokol TCP/IP.
MS_TCPIP = Params.MS_TCPIP
```

```
[Params.MS_TCPIP]
; Tento oddíl konfiguruje vlastnosti TCP/IP.
AdapterSections = Params.MS_TCPIP.Adapter01,params.MS_TCPIP.Adapter02,params.MS_TCPIP.Adapter03

[Params.MS_TCPIP.Adapter01]
; SíťSpolečnosti na adaptéru Adapter01 používá informace serveru DHCP.
SpecificTo = Adapter01
DHCP = Yes
DNSServerSearchOrder = 172.31.240.226, 172.31.240.225
DNSSuffixSearchOrder = SíťSpolečnosti, dns.domena.cz
DNSDomain = CorpNet

[Params.MS_TCPIP.Adapter02]
; SíťProdejce na adaptéru Adapter02 používá místní informace DHCP.
SpecificTo = Adapter02
DHCP = Yes

[Params.MS_TCPIP.Adapter03]
; PrivátníSíť na adaptéru Adapter03 používá statické informace.
SpecificTo = Adapter03
DHCP = No
WINS = No
IPAddress = 10.2.0.41
SubnetMask = 255.255.0.0
DefaultGateway = 2.2.2.2
DNSServerSearchOrder = 10.2.0.253, 10.2.0.254

[NetServices]
; Instaluje souborové a tiskové služby.
MS_Server = Params.MS_Server

[Params.MS_Server]

[Components]
; Při zadané hodnotě On instaluje službu Windows Clustering a součásti
; správy systému Advanced Server.
Cluster = On

[Cluster]
Name = ClusterSpolečnosti
Action = Form
Account = SprávceSpolečnosti
Domain = SíťSpolečnosti
IPAddr = 172.31.240.227
Subnet = 255.255.248.0
Network = SíťSpolečnosti, ALL
Network = SíťProdejce, ALL

[GuiRunOnce]
; Spuštění souboru Cluscfg.exe můžete automatizovat vložení příkazu
; Cluscfg.exe do oddílu [GuiRunOnce] souboru odpovědí bezobslužné instalace.
```

```
; Tím se vykoná program Cluscfg.exe a nakonfiguruje se podpora clusteringu  
; při prvním spuštění po dokončení grafické části instalačního programu.  
; Do uvozovek musíte uvést úplnou cestu k programu.  
    „%Windir%\Cluster\Cluscfg.exe -unattend“
```

```
[NetOptionalComponents]
```

```
    NETMONTTOOLS = 1
```

PŘÍLOHA D

Nástroje zavádění

V celé knize se nacházejí odkazy na nástroje, které vám mohou pomoci se zaváděním systému Microsoft Windows 2000. Tabulka D.1 shrnuje tyto nástroje a umožňuje vám tak rychle zjistit jejich názvy a přečíst si krátký popis jejich funkce.

Kde najít další informace o těchto nástrojích

Další informace o nástrojích uvedených v této příloze najdete na následujících místech:

- Další informace o nástrojích, které jsou součástí operačního systému Windows 2000, najdete v nápovědě systému Windows 2000.
- Další informace o instalaci a používání podpůrných nástrojů a nápovědy podpůrných nástrojů systému Windows 2000 najdete v dokumentu Sreadme.doc v adresáři \Support\Tools na disku CD operačního systému Windows 2000.
- Další informace o nástrojích, které jsou součástí plné sady *Microsoft Windows 2000 Server Resource Kit*, najdete v odkazu ResourceLink stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Poznámka Hvězdička (*) u názvu nástroje označuje, že daný nástroj je součástí CD operačního systému Windows 2000. Ne všechny tyto nástroje se při standardní instalaci systému instalují; některé se instalují jako součást podpůrných nástrojů systému Windows 2000.

Tabulka D.1 Nástroje zavedení

Název nástroje	Název souboru	Umístění v této knize	Popis
* Modul snap-in Active Directory Connector (ADC) konzoly	Adcdadmin.msc	Kapitola 20, „Synchronizování služby Active Directory s adresářovou službou programu Exchange Server“	Tento modul snap-in konzole Microsoft Management Console (MMC) vám umožňuje synchronizovat a spravovat komunikaci mezi službou Microsoft Active Directory a adresářovou službou programu Microsoft Exchange Server verze 5.5.
* Modul snap-in Uživatelé a počítače služby Active Directory (Active Directory Users and Computers) konzoly MMC	Dsa.msc	Kapitola 9, „Návrh struktury služby Active Directory“ Kapitola 11, „Plánování distribuovaného zabezpečení“ Kapitola 20, „Synchronizování služby Active Directory s adresářovou službou programu Exchange Server“ Kapitola 24, „Aplikování správy změn a konfigurací“	Tento modul snap-in konzoly MMC je grafický nástroj správy adresáře, který vám umožňuje přidávat, upravovat, odstraňovat a organizovat účty uživatelů, účty počítačů, distribuční skupiny a skupiny se zabezpečením a publikované prostředky systému Windows 2000 v adresáři vaší organizace. Tento nástroj se instaluje na počítače nakonfigurované jako řadiče domény.
ApiMon	Apimon.exe	Kapitola 21, „Testování kompatibility aplikací se systémem Windows 2000“	Nástroj sledování aplikací, který počítá a časuje volání rozhraní programování aplikací (API). Tento nástroj lze používat k určení počtu volání API a jejich časech nebo ke sledování volání API v pořadí, v jakém k nim dochází. Tento nástroj najdete v nápovědě nástrojů sady <i>Microsoft Windows 2000 Resource Kit</i> .
* ClonePrincipal	Clonepr.dll Clone-gg.vbs Clone-ggu.vbs Clone-lg.vbs Clone-pr.vbs Sidhist.vbs ADsSecurity.dll ADsError.dll	Kapitola 9, „Návrh struktury služby Active Directory“ Kapitola 10, „Určení strategií migrace domén“	Nástroj používaný pro migraci domén. Tento nástroj použijte ke klonování uživatele nebo skupiny ze zdrojové domény systému Microsoft Windows NT verze 4.0 nebo ze zdrojové domény systému Windows 2000 do domény systému Windows 2000 pracující v nativním režimu, aniž byste museli odstranit zdrojový účet. Původní identifikátor zabezpečení účtu (SID) je přidán do historie nového účtu, aby byl zachován přístup k prostředkům.

* Clustcfg	Clustcfg.exe	Kapitola 18, „Zajištění dostupnosti aplikací a služeb“	Základní konfigurační nástroj podpory klastrů v systému Windows.
* Správce připojení (Connection Manager)	Balíček nástrojů	Kapitola 7, „Určení strategií konektivity sítí“	Grafický nástroj, který vám umožňuje vytvářet své vlastní balíčky připojení zjednodušující konfiguraci klientů.
* Dependency Walker	Depends.exe	Kapitola 21, „Testování kompatibility aplikací se systémem Windows 2000“	Nástroj skenující všechny závislé moduly požadované nějakou aplikací. Tento nástroj detekuje takové problémy, jako jsou chybějící nebo nesprávné soubory. Nástroj Dependency Walker použijte k ladění aplikací napsaných pro systém Windows 2000 nebo pro něj upravených.
* Správce disku (Disk Administrator)	Windisk.exe	Kapitola 15, „Inovace a instalace členských serverů“	Grafický nástroj správy disku poskytovaný systémem Microsoft Windows NT. Tento nástroj vám umožňuje zálohovat a obnovovat informace o konfiguraci disku.
* Modul snap-in Defragmentace disku (Disk Defragmenter) konzoly MMC	Compmgmt.mmc	Kapitola 19, „Určení strategií správy úložišť systému Windows 2000“	Tento modul snap-in konzoly MMC vám umožňuje vyhledat fragmentované soubory a složky a změnit uspořádání klastrů na diskovém svazku. Klastry lze uspořádat tak, aby byly soubory, adresáře a volný prostor fyzicky souvislejší.
* Modul snap-in Správa disku (Disk Management) konzoly MMC	Compmgmt.mmc	Kapitola 19, „Určení strategií správy úložišť systému Windows 2000“	Tento modul snap-in konzoly MMC je grafický nástroj správy disků a svazků. Podporuje oddíly, logické jednotky, nové dynamické svazky a vzdálenou správu disků.
* Modul snap-in Zásady skupiny (Group Policy) konzoly MMC	Gpedit.msc	Kapitola 11, „Plánování distribuovaného zabezpečení“ Kapitola 12, „Plánování infrastruktury veřejných klíčů“ Kapitola 23, „Definování standardů správy a konfigurace klientů“ Kapitola 24, „Aplikování správy změn a konfigurací“	Tento modul snap-in konzoly MMC je grafický nástroj správy zásad skupiny, který umožňuje správci systému vytvářet specifické konfigurace počítačů pro určitou skupinu uživatelů. Nastavení zásad skupiny definují různé součásti kancelářských počítačů uživatelů, jako jsou například programy dostupné uživatelům, programy zobrazované na pracovní ploše uživatelů a možnosti nabídky Start.

Internet Explorer Administration Kit (IEAK)	Balíček nástrojů	Kapitola 23, „Definování standardů správy a konfigurace klientů“	Sada nástrojů umožňující vám upravit konfiguraci a nastavení aplikace Microsoft Internet Explorer. Poznámka: Sada IEAK není součástí systému Windows 2000. Další informace o sadě IEAK najdete v oddílu „Další zdroje“ dále v této kapitole.
* Ipconfig	Ipconfig.exe	Kapitola 6, „Příprava infrastruktury sítě na systém Windows 2000“ Kapitola 15, „Inovace a instalace členských serverů“	Textový nástroj konfigurace a diagnostiky protokolu TCP/IP. Tento nástroj použijte k ověření konfiguračních parametrů protokolu TCP/IP na nově inovovaných systémech Windows 2000. Můžete tak například ověřit adresu IP, masku podsítě a výchozí bránu.
* Modul snap-in Internet Information Services konzoly MMC	iis.msc	Kapitola 15, „Inovace a instalace členských serverů“	Modul snap-in Internet Information Services (IIS) konzoly MMC je mocný nástroj správy sídla zajišťující přístup ke všem nastavením vašeho serveru. Modul snap-in IIS používáte ke správě komplexního sídla na vašem podnikovém intranetu a k publikování informací na Internet.
* LDAP Data Interchange Format	Ldifde.exe	Kapitola 9, „Návrh struktury služby Active Directory“	Nástroj příkazového řádku, který vykonává hromadný import a export dat služby Active Directory.
* Licenční server (License Server)	Licmgr.exe	Kapitola 16, „Zavádění terminálových služeb“	Nástroj ukládající, sledující a ověřující licence klientského přístupu služby Terminal Services systému Windows 2000.
* Microsoft Management Console (MMC)	Mmc.exe	Kapitola 1, „Úvod do plánování zavádění systému Windows 2000“ Kapitola 9, „Návrh struktury služby Active Directory“ Kapitola 10, „Určení strategií migrace domén“ Kapitola 11, „Plánování distribuovaného zabezpečení“ Kapitola 12, „Plánování infrastruktury veřejných klíčů“ Kapitola 15, „Inovace	Grafický rámec, který hostí nástroje pro správu. Pomocí modulů snap-in konzoly MMC můžete spravovat síť, počítače, uživatele, služby a další součásti systému.

		a instalace členských serverů“ Kapitola 16, „Zavádění terminálových služeb“ Kapitola 19, „Určení strategií správy úložišť systému Windows 2000“ Kapitola 20, „Synchronizování služby Active Directory s adresářovou službou programu Exchange Server“ Kapitola 23, „Definování standardů správy a konfigurace klientů“ Kapitola 24, „Aplikování správy změn a konfigurací“	
* Sledování sítě (Network Monitor)	Netmon.exe	Kapitola 8, „Analýza infrastruktury sítě pomocí serveru Systems Management Server“	Grafický nástroj zachytávání a analyzování dat o síti. Tento nástroj vám umožňuje sledovat vzory síťového provozu a diagnostikovat problémy práce v místní síti (LAN).
Muisetup	Muisetup.exe	Kapitola 23, „Definování standardů správy a konfigurace klientů“	Nástroj používaný ke konfiguraci vícejazyčné verze systému Windows 2000. Pomocí programu Muisetup.exe můžete měnit výchozí uživatelské rozhraní (UI) nebo přidávat a odstraňovat jazyky UI.
* Netdom	Netdom.exe	Kapitola 10, „Určení strategií migrace domén“	Nástroj správy domény, který vám dovoluje spravovat doménu systému Windows 2000 a vztahy důvěryhodnosti z příkazového řádku. Tímto nástrojem lze také řídit členství počítače v doméně.
* Ping	Ping.exe	Kapitola 15, „Inovace a instalace členských serverů“	Znakový nástroj konfigurace a diagnostiky protokolu TCP/IP. Tento nástroj je vhodný k ověření konfigurace TCP/IP a k určení problémů připojení.
* Služby vzdálené instalace (Remote Installation Services – RIS)	Balíček nástrojů včetně RISetup.exe RIPrep.exe RBFg.exe OSChooser.exe	Kapitola 24, „Aplikování správy změn a konfigurací“	Balíček nástrojů, které vám umožňují vytvářet vlastní obrazy (bitové kopie) systému Windows 2000 Professional, umisťovat tyto obrazy na servery služby RIS a používat zásady skupiny k jejich automatické instalaci na klientské počítače.

Registry Backup	Regback.exe	Kapitola 15, „Inovace a instalace členských serverů“	Tento nástroj se nachází na doprovodném disku CD sady <i>Microsoft Windows NT Server Resource Kit</i> a sady <i>Microsoft Windows 2000 Server Resource Kit</i> . Tento nástroj zálohuje registr do souborů bez použití pásků, takže v případě problémů s konfigurací můžete obnovit původní nastavení registru. Stejně jako je tomu i u ostatních důležitých dat, musíte registr zálohovat často, zejména před instalací a testováním aplikací, o jejichž stabilitě nic nevíte. Registr lze obnovit pomocí programu Regrest.exe, které také najdete na discích CD zmíněných v předchozím odstavci.
* Modul snap-in Směrování a vzdálený přístup (Routing and Remote Access) konzoly MMC	Rasmgmt.mmc	Kapitola 7, „Určení strategií konektivity sítě“	Tento modul snap-in konzoly MMC je grafický nástroj pro správu a konfiguraci služby Směrování a vzdálený přístup (Routing and Remote Access) v systému Windows 2000.
* Správce instalace (Setup Manager)	Setupmgr.exe	Kapitola 13, „Automatizování instalace a inovace serveru“ Kapitola 18, „Zajištění dostupnosti aplikací a služeb“ Kapitola 25, „Automatizování instalace a inovace klientů“	Nástroj ve formě průvodce, který vám pomáhá vytvořit skripty bezobslužné instalace. Správce instalace také vytváří sdílené distribuční místo na síti, které je zapotřebí pro bezobslužné zavádění a zavádění pomocí nástroje Sysprep.
* Setupcl	Setupcl.exe	Kapitola 13, „Automatizování instalace a inovace serveru“ Kapitola 25, „Automatizování instalace a inovace klientů“	Tento nástroj příkazového řádku spolupracuje s nástrojem Sysprep při přípravě pevného disku na hlavním (zdrojovém) počítači, aby mohl nějaký nástroj kopírování disků přenést obraz (bitovou kopii) pevného disku na jiné počítače. Tento nástroj regeneruje nové identifikátory zabezpečení (SID).
SMS Installer	Sada nástrojů	Kapitola 14, „Zavádění systému Windows 2000 pomocí serveru Systems Management Server“	Nástroj serveru Microsoft Systems Management Server (SMS), který připravuje aplikace na distribuci softwaru. Nástroj SMS Installer může vytvářet skripty obslužné i bezobslužné instalace, které můžete plně upravovat.

SMS Query Extract	SMSExtract.mdb pro Microsoft Access SMSExtract.xls pro Microsoft Excel	Kapitola 8, „Analýza infrastruktury sítě po- mocí serveru Systems Management Server“	Nástroj extrakce dat pro server, který vám umožňuje používat dotazy SMS v aplikacích Microsoft Access a Microsoft Excel.
* Sysprep	Sysprep.exe	Kapitola 2, „Vytvoření cesty postupného zavádění“ Kapitola 13, „Automa- tizování instalace a inovace serveru“ Kapitola 18, „Zajištění dostupnosti aplikací a služeb“ Kapitola 23, „Definování standardů správy a konfigurace klientů“ Kapitola 24, „Aplikování správy změn a konfigurací“ Kapitola 25, „Automati- zování instalace a inovace klientů“	Instalační nástroj umožňující duplikování disků. Nástroj Sysprep vám umožňuje nainstalovat systém s aplikacemi pro Windows 2000 a pak jej duplikovat na další systémy.
* Vytváření klientů služby Terminal Services (Terminal Services Client Creator)	Tsclient.exe	Kapitola 16, „Zavádění terminálových služeb“	Grafický nástroj vytvářející diskety pro klientský software terminálových služeb na těchto operačních systémech: Micro- soft Windows for Workgroups, Microsoft Windows 95, Micro- soft Windows 98 a Microsoft Windows NT Server.
* Modul snap-in Konfi- gurace služby Terminal Services (Terminal Services Configuration) konzoly MMC	Tscc.msc	Kapitola 16, „Zavádění terminálových služeb“	Tento modul snap-in konzoly MMC vám umožňuje spravovat konfiguraci terminálových služeb. Změny zadané tímto nástrojem jsou globální, pokud nezvolíte dědění informací stej- ných voleb v konfiguraci uživa- telů.
* Správce služby Ter- minal Services (Terminal Services Manager)	Tsadmin.exe	Kapitola 16, „Zavádění terminálových služeb“	Grafický nástroj umožňující vám spravovat všechny servery se systémem Windows 2000, na nichž běží terminálové služby. Pomocí tohoto nástroje si mo- hou správci zobrazovat aktuální uživatelé, servery a procesory. Navíc můžete odesílat zprávy určitým uživatelům a používat funkci vzdáleného řízení a ter- minálové procesy.
* Správce nástrojů (Utility Manager)	Utilman.exe	Příloha E, „Možnosti usnadnění pro posti-	Tento nástroj umožňuje správci určit, které počítače automa-

		žené osoby“	ticky otevřou nástroje usnadnění po spuštění systému Windows 2000.
Windows DNA Performance Kit	balíček nástrojů	Kapitola 18, „Zajištění dostupnosti aplikací a služeb“	Tato sada nástrojů vám dovolu- je testovat a ladit výkon vašich aplikací. Sada obsahuje infor- mace o výkonu služeb Compo- nent Services a IIS i nástroje si- mulující vliv přístupu mnoha uživatelů k vaší aplikaci IIS ne- bo Component Services. Další informace o této sadě nástrojů najdete v oddílu „Další zdroje“ dále v této kapitole.
* Windows Installer	Zabudovaná služba	Kapitola 1, „Úvod do plánování zavedení systému Windows 2000“ Kapitola 24, „Aplikování správy změn a kon- figurací“ Kapitola 25, „Automati- zování instalace a inovace klientů“ Příloha A, „Ukázkové listy plánování“	Výkonná nová instalační služba v systému Windows 2000, která standardizuje způsob instalace aplikací na více počítačů. Služba Windows Installer používá k instalaci aplikací soubory balíčku s příponou .msi.
* Windows Manage- ment Instrumentation (WMI)	Zabudované rozhraní	Kapitola 1, „Úvod do plánování zavedení systému“ Příloha A, „Ukázkové listy plánování“	Infrastruktura správy v systému Windows 2000, která podporuje sledování a řízení systémových prostředků pomocí obecné sady rozhraní a která poskytuje logicky uspořádaný, konzistent- ní model fungování, configura- ce a stavu systému Windows. Pomocí rozhraní Windows Ma- nagement Instrumentation (WMI) mohou správci zjišťovat vztahy mezi daty a událostmi na více místních zdrojích nebo zdrojích v celé organizaci. WMI vám umožňuje vytvářet vlastní aplikace a moduly snap-in tím, že vám zpřístupňuje objekty sy- stému Windows 2000.
* Windows Script Host (WSH)	Cscript.exe Wscript.exe	Kapitola 1, „Úvod do plánování zavedení systému“ Příloha A, „Ukázkové listy plánování“	Nástroj podporující přímé vykonávání skriptů jazyka Microsoft Visual Basic Script, Java a dalších z uživatelského rozhraní nebo příkazového řád- ku.
* WinInstall LE	Sada nástrojů	Kapitola 24, „Aplikování správy změn a konfigu- rací“	Grafický nástroj opakovaného zabalení aplikací od společnosti Veritas Software pro službu

			Windows Installer. Tento nástroj vám umožňuje rychle a jednoduše opakovaně zabalit existující aplikace (vzniklé před uvedením služby Windows Installer) do balíčků vhodných pro distribuci služnou Windows Installer.
* Winnt	Winnt.exe	Kapitola 13, „Automatizování instalace a inovace serveru“ Kapitola 25, „Automatizování instalace a inovace klientů“ Příloha B, „Příkazy instalačního programu“ Příloha C, „Příklady souborů odpovědí pro bezobslužnou instalaci“	Příkaz instalačního programu, který můžete použít pro čistou instalaci systému Microsoft Windows 2000 Server nebo Microsoft Windows 2000 Professional na počítač se systémem Microsoft MS-DOS nebo Microsoft Windows 3.x
* Winnt32	Winnt32.exe	Kapitola 13, „Automatizování instalace a inovace serveru“ Kapitola 25, „Automatizování instalace a inovace klientů“ Příloha B, „Příkazy instalačního programu“ Příloha C, „Příklady souborů odpovědí pro bezobslužnou instalaci“	Příkaz instalačního programu, který můžete použít pro čistou instalaci nebo inovaci na systém Windows 2000 Server či Windows 2000 Professional na počítači se systémem Windows NT 4.0, Windows 95 nebo Windows 98.

Další zdroje

- Další informace o sadě IEAK najdete v odkazu Microsoft Internet Explorer Administration Kit (IEAK) stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.
- Další informace o sadě Windows DNA Performance Kit najdete v odkazu Windows DNA Performance Kit stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

PŘÍLOHA E

Možnosti usnadnění pro postižené osoby

Společnost Microsoft se neustále snaží umožnit přístup ke svým produktům a službám a jejich používání všem uživatelům. Systém Microsoft Windows 2000 obsahuje nové a vylepšené možnosti usnadnění, které jsou užitečné uživatelům ve všech podnicích a všech profesích. Tyto funkce usnadňují úpravu nastavení počítače a umožňují uživatelům s postižením lepší přístup k programům a aplikacím, které potřebují pro svou práci.

V této příloze

Přehled možností usnadnění systému Windows 2000 869

Zavádění systému Windows 2000 s možnostmi usnadnění 872

Úprava počítače pro možnosti usnadnění 874

Konfigurace možností usnadnění v systému Windows 2000 877

Nastavení možností usnadnění podle typu postižení 879

Další zdroje 887

Cíle přílohy

Tato příloha vám pomůže s vývojem následujících dokumentů:

- Plán využití funkcí zabudovaných do operačního systému a doplňkových zařízení dalších výrobců pro uživatele s postiženími.
- Podle priority seřazený seznam součástí a funkcí, které lze zavést během inovace na systém Windows 2000.

Další informace v sadě Resource Kit

- Další informace o instalaci softwaru najdete v kapitole „Instalace a údržba softwaru“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.
- Další informace o používání zásad skupiny najdete v kapitole „Zásady skupiny“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.

Přehled možností usnadnění systému Windows 2000

Usnadnění znamená zajištění rovnocenného přístupu k počítačovému softwaru pro všechny uživatele včetně osob s postiženími zraku, sluchu, pohyblivosti či rozpoznávání. Postižení rozpoznávání zahrnuje omezení možností učení, jako je dyslexie, ztráta paměti, Downův syndrom a jazyková postižení, jako je negramotnost a neznalost jazyka.

Uživatelé s postižením sluchu jsou lidé neslyšící nebo s částečnou ztrátou sluchu. Fyzické postižení zahrnuje ochrnutí páteře, třas, záchvaty epilepsie, ztrátu údů nebo prstů a paralýzu. Za osoby s postiženou pohyblivostí lze považovat také osoby se zánětem šlach v prstech a s dalšími nemocemi způsobenými opakovaným namáháním. Mezi postižení zraku patří nevidomost a různé typy omezeného vidění, jako je barvoslepost nebo tunelové vidění. V systému Windows 2000 představuje pojem „usnadnění“ větší zpřístupnění počítačů prostřednictvím flexibilního upravitelného uživatelského rozhraní, alternativní metody vstupu a výstupu a lepší viditelnost prvků na obrazovce.

Výhody usnadnění v systému Windows 2000

Počet uživatelů s postiženími, kteří používají počítače, stále roste a s tímto růstem souvisí také nárůst potřeb vybavit zaměstnance pomocnými technologiemi. Nejnovější právní úpravy dokonce takovou povinnost stanovují. Zaměstnanci s postižením musí mít přístup k počítačům porovnatelný s přístupem k počítačům zaměstnanců, kteří nejsou postiženi. K tomu účelu slouží několik technologií zabudovaných do systému Windows 2000, které umožňují nakonfigurovat počítače s potřebnými možnostmi usnadnění.

Mnoho z těchto funkcí posunuje dále funkce operačních systémů Microsoft Windows 98 a Microsoft Windows NT. V této příloze jsou popsány nové i již existující funkce. Mezi nové a výrazně vylepšené funkce a nástroje systému Windows 2000 patří sada Active Accessibility (aktivní usnadnění), Průvodce funkcemi usnadnění (Accessibility Wizard), Lupa (Magnifier), Narrator (čtení obrazovky), Klávesnice na obrazovce (On-Screen Keyboard), Správce nástrojů (Utility Manager), dobře viditelné ukazatele myši, podpora formátu Synchronized Accessible Media Interchange (SAMI) a barevná schémata s vysokým kontrastem.

V systému Windows 2000 mohou uživatelé a správci vykonávat následující funkce:

Přepisovat výchozí nastavení upravená pro více uživatelů. Správci mohou nastavit velké množství možností usnadnění a dalších pro skupiny uživatelů pomocí ovládacích panelů, Průvodce funkcemi usnadnění a Správce nástrojů.

Rychle a snadno se pohybovat v systému Windows. Speciální funkce, jako jsou klávesové zkratky a systém Active Desktop, usnadňují přístup k objektům na ploše, v Průzkumníkovi Windows, na dalších serverech na síti a v aplikaci Internet Explorer, umožňují rychlý přístup k systému Windows a pomáhají uživatelům otevírat složky a vytvářet svá vlastní nastavení.

Používat širší rozsah pomocných technologií. Prostřednictvím funkce Active Accessibility fungují aplikace efektivněji s dalšími doplňky usnadnění od jiných společností, jako jsou systémy rozpoznávání řeči a další formy pomocných zařízení. I když je pro uživatele neviditelná, technologie Active Accessibility inovuje a rozšiřuje operační systém Microsoft Windows.

Upravit metody vstupu. Rozšířené konfigurace klávesnic včetně funkce Klávesnice na obrazovce, speciálních nastavení ukazatele myši a dalších možností umožňují uživatelům upravit si svá schémata uživatelského rozhraní (UI).

Konfigurovat možnosti z jediného místa. Průvodce funkcemi usnadnění, který se nachází v nabídce tlačítka Start, umožňuje správcům a uživatelům vybavit počítače těmi nejčastěji používanými funkcemi a tyto funkce nastavit podle potřeb jednotlivých uživatelů.

Zvětšovat část obrazovky. Několik funkcí, jako je například Lupa, umožňuje uživatelům pracovat na jiných počítačích, kde nemají instalovaná svá pomocná zařízení.

Pohybovat se v systému Windows. Klávesové zkratky a možnosti úpravy klávesnic pomáhají uživatelům, kteří pracují v programech a v aplikacích.

Nastavovat možnosti zvuku podle potřeb jednotlivců. Kromě upravitelných funkcí, jako je nastavení hlasitosti a možnosti multimédií, umožňují lidem s postižením sluchu řídit zvukové prostředí několik dalších funkcí usnadnění, jako jsou například Zobrazení zvuku (ShowSounds) a Popis zvuku (SoundSentry).

Nastavovat možnosti pro uživatele s postižením zraku. Mezi tyto funkce patří Narrator, což je nástroj převodu anglického textu do řeči zabudovaný do operačního systému, funkce Ozvučení kláves (ToggleKeys), což je funkce zajišťující zvuková upozornění na situaci, kdy uživatel stiskne určité klávesy, a oznámení událostí, která se nacházejí v ovládacím panelu Zvuky a multimédia (Sounds and Multimedia).

Používat filtry klávesnice a pomáhat tak různým rozpoznávacím, sluchovým, pohyblivostním a zrakovým potřebám uživatelů. Funkce Filtrování kláves (FilterKeys) upravuje čas reagování klávesnice a neregistruje náhodné stisky kláves.

Přiradit prvkům obrazovky schémata kontrastu, barvy, časování a velikosti. Rozšířený rozsah prvků obrazovky, jako jsou velké ukazatele myši a barevná schémata s vysokým kontrastem, a Průvodce funkcemi usnadnění dávají uživatelům možnost nastavit si vše podle svých potřeb a preferencí, jako je například vyšší viditelnost indikátoru textového kurzoru a možnost vypnout animace.

Získat větší kontrolu nad osobním počítačem použitím zařízení jiných výrobců. Funkce Posloupnost kláves (SerialKeys) je určena pro osoby, které nemohou používat standardní možnosti UI a potřebují další pomocná zařízení. Tato funkce umožňuje uživatelům připojit k sériovému portu počítače alternativní vstupní zařízení.

Úvahy před inovací na systém Windows 2000

Společnost Microsoft a další vývojáři funkcí softwaru a hardwaru neustále pracují na zlepšení možností pro osoby s postižením. Právě proto se některé funkce usnadnění ještě vyvíjejí nebo testují v okamžiku uvedení nové verze softwaru. Někdy jsou takové funkce dokončeny až po uvedení softwaru na trh a objeví se v následující verzi. Některé vytvořené technologie také ještě nejsou kompatibilní se systémem Windows 2000 nebo je do něj nelze zabudovat. Proto musí profesionálové oddělení informačních technologií pečlivě zjistit potřeby uživatelů, jejichž podporu zajišťují, ještě před zavedením nového systému. Jako součást vašeho plánování a testování zavádění nezapomeňte otestovat kompatibilitu všech potřebných pomocných zařízení se systémem Windows 2000.

Můžete také zvážit místo úplné instalace systému Windows 2000 inovaci jen vybraných existujících funkcí a programů na počítačích. Proces inovace lze automatizovat a s pomocí služby Active Directory můžete spravovat objekty aplikací zásad skupiny v organizační jednotce, doméně nebo síťovém sídle. Úplná instalace, která se také označuje za čistou instalaci, sice dovoluje instalaci konkrétních prvků, nepřebírá však nastavení z předchozího systému, což znamená, že uživatelé ztratí svá osobní nastavení a aplikace.

Poznámka Ať už budete vykonávat úplnou instalaci nebo inovaci, je důležité tak učinit s inovovaným systémem BIOS, který je kompatibilní s Windows 2000.

Pomocí přiřazených aplikací v zásadách skupiny mohou správci inzerovat objekty, aby si je mohl uživatel vybrat z nabídky tlačítka **Start** a aby následně došlo k jejich auto-

matické instalaci. Správci mohou odstranit aplikace přiřazené tímto způsobem. Jestliže budou správci místo přiřazování aplikace publikovat, uživatelé mají možnost instalovat si je pomocí ovládacího panelu Přidat nebo odebrat programy (Add/Remove Programs).

Funkce Active Accessibility je základní součástí operačního systému Windows, vychází z modelu Component Object Model (COM) a definuje, jak si mohou aplikace vyměňovat informace o prvcích uživatelského rozhraní (UI). Tato technologie omezuje nekompatibilitu s některými prostředky usnadnění, nenabízí však zatím úplnou kompatibilitu.

Další informace o aktuálních technologiích najdete v odkazu Microsoft Accessibility stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Další informace o instalování softwaru najdete v kapitole „Instalace a údržba softwaru“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.

Zavádění systému Windows 2000 s možnostmi usnadnění

Třebaže nástroje usnadnění, které jsou součástí systému Windows 2000, poskytují určité funkce pro uživatele se zvláštními potřebami, většina postižených uživatelů potřebuje pro svou každodenní práci pomocné nástroje s rozsáhlejší funkcí. Použitím hardwaru a softwaru vyvinutého nezávislými výrobci mohou uživatelé rozšířit své možnosti práce s operačním systémem Windows. Nezapomeňte otestovat kompatibilitu programů, aplikací a zařízení usnadnění s operačním systémem Windows a prověřit kompatibilitu ovladačů se systémem Windows 2000.

Technologie Active Accessibility

Rozhraní programování aplikací Active Accessibility je zabudováno do operačního systému Windows. Vychází z technologií OLE a COM a umožňuje nástrojům usnadnění pracovat s prvky uživatelského rozhraní. Pro uživatele je součástí Active Accessibility neviditelná. Tato technologie zlepšuje kompatibilitu s některými pomocnými nástroji usnadnění.

Výrobky a služby jiných společností

Společnost Microsoft pracuje ve spolupráci s nezávislými výrobci na výrobě kompatibilního softwaru a hardwaru pro uživatele s postižením. Jedním z účelů technologie Active Accessibility je vytvořit infrastrukturu pomáhající vzájemnému porozumění operačního systému a aplikací v zájmu zajištění větší kompatibility s těmito důležitými zařízeními. Pomocí Správce nástrojů (Utility Manager), což je nový prvek systému Windows 2000, mohou nyní výrobci přidávat do systému své výrobky usnadňující přístup. Nezávislí výrobci – obvykle malé společnosti vyrábějící specializovaná pomocná zařízení – pomáhají lidem s postižením lépe využívat operační systém Windows. Dále je uveden částečný seznam typů zařízení a funkcí, jaké tito nezávislí výrobci vytvářejí:

- Hardwarové a softwarové nástroje měnící chování myši a klávesnice
- Klávesnice na obrazovce
- Programy, které umožňují uživateli psát text pomocí myši nebo používat aktivaci hlasem
- Software, který předvídá slova nebo fráze, aby mohli uživatelé rychleji psát s méně stisky kláves
- Programy podporující titulkování
- Alternativní vstupní zařízení, jako jsou zařízení sledující pohyby hlavou, pohled očí, ovládání pomocí dechu a zařízení umožňující zadávání příkazů hlasem
- Programy, které zvětšují informace na obrazovce nebo mění jejich barvu
- Programy syntézy řeči nebo tiskárny Braillova písma, které tisknou informace uve-
dené na obrazovce

Logo „Certified for Windows“

Všichni výrobci hardwaru a softwaru spolupracují na úkolu vytvoření výrobků usnadnění pro všechny uživatele počítačů. Společnost Microsoft iniciovala program Certified for Windows (certifikováno pro systém Windows), který nyní platí pro systém Windows 2000. Tento program podporuje návrh prostředků usnadnění a obsahuje sadu požadavků a podmínek pro vývojáře aplikací. Hlavním cílem tohoto programu je zajistit kvalitu a konzistentnost výrobků, které pracují v operačním systému Windows 2000. Aby mohlo být aplikaci uděleno logo Certified for Windows, musí aplikaci otestovat společnost VeriTest a zaručit její soulad se specifikacemi aplikací pro systém Windows 2000.

Tyto specifikace se týkají takových požadavků, jako je titulkování a nikoli předávání informací výhradně pomocí zvuku, viditelnost indikátoru textového kurzoru a možnost řídit myš a klávesnici a vypínat animace. Jedním z cílů této spolupráce je zajistit kvalitu a konzistentnost pomocných zařízení pro uživatele s postiženími.

Další informace o programu Certified for Windows včetně specifikací aplikací najdete v odkazu Application Specification Download stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Důležité Většina pomocných nástrojů od jiných společností je kompatibilní s určitými verzemi nějakého operačního systému. Některé doplňkové nástroje jsou omezené tím, že se spoléhají na to, že formáty souborů a programovací rozhraní budou data uživateli správně interpretovat. Takové závislosti se v každém novém operačním systému mění. Proto ještě než se rozhodnete pro inovaci, musíte vytvořit inventář a vykonat testování kompatibility s novým operačním systémem a aplikacemi, které plánujete používat. Další informace o nových technologiích a kompatibilitě najdete v odkazu Microsoft Accessibility stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Použití funkce Posloupnost kláves s doplňkovým hardwarem a softwarem

Funkce Posloupnost kláves vám umožňuje připojit k sériovému portu počítače pomocná zařízení jiných společností. K sériovému portu osobního počítače tak můžete připojit například alternativní klávesnice nebo pomocná komunikační zařízení. Funkce Posloupnost kláves je určena lidem, kteří nemohou využívat standardní metody uživatel-

ského rozhraní (UI). Funkce Posloupnost kláves však umožňuje pomocnému zařízení také pracovat současně s místní klávesnicí a myší.

Úprava počítače pro možnosti usnadnění

Systém Windows 2000 instaluje možnosti usnadnění automaticky. Navíc uživatelé nemohou odstranit možnosti usnadnění z operačního systému po jejich instalaci – sem patří také možnosti Průvodce funkcemi usnadnění a ovládacích panelů. Instalační program nejen instaluje nové funkce, ale ponechává také při inovaci některé z dřívějších verzí systému Windows aktivní již instalované funkce. Možnosti usnadnění lze instalovat také na sdílené počítače, jako jsou například veřejné servery nebo servery pracovních skupin.

Vzdálená instalace a bezobslužná instalace z disku CD

Pomocí Průvodce klientskou instalací (Client Installation Wizard) můžete vzdáleně nakonfigurovat klientské počítače, které funkci vzdálené instalace podporují. Možnosti instalace nabízené uživatelům lze řídit pomocí zásad skupiny. Existují čtyři možnosti instalace: Automatická instalace (Automatic Setup), Vlastní instalace (Custom Setup), Opakované spuštění předchozí instalace (Restart a Previous Setup Attempt) a Údržba a řešení problémů (Maintenance and Troubleshooting).

Automatická instalace Při automatické instalaci používá výchozí možnost, služba vzdálené instalace (Remote Installation Services) systému Windows 2000, šablony pro bezobslužnou instalaci, takže můžete vytvořit potřebné možnosti v kategoriích obrazů (bitových kopií) operačního systému. Pomocí souboru odpovědí bezobslužné instalace lze zadat několik možností instalace, vybrat instalované položky a nakonfigurovat možnosti specifického klientského počítače.

Vlastní instalace Po volbě vlastní instalace můžete zadat název počítače a kontejner služby Active Directory, ve kterém vytvoříte objekt účtu daného počítače. Tato možnost také umožňuje nastavit počítač pro jednotlivé uživatele ve skupině a nastavit účet klientského počítače ve službě Active Directory ještě před dodáním počítače uživateli.

Opakované spuštění předchozí instalace Tato možnost opakovaně spustí předchozí nebo nezdařený pokus o instalaci. Je-li například spuštěna instalace obrazu operačního systému a dojde k přerušení spojení k serveru služby vzdálené instalace, můžete v instalaci pokračovat takto: Restartujte klientský počítač, po výzvě ke spuštění síťové služby stisknete klávesu F12 a pak zvolte možnost opakovaného spuštění předchozí instalace.

Údržba a řešení problémů Tato funkce umožňuje správcům přístup k diagnostickým nástrojům a dalším nástrojům údržby, které jsou zapotřebí k údržbě a řešení problémů klientských počítačů.

Služba Windows Installer

Technologie, která instaluje, udržuje a odstraňuje software z klientských počítačů. Služba Windows Installer podporuje aplikace, které se umějí samy opravit. Jestliže uživatel odstraní nějaký programový soubor, služba Windows Installer chybějící soubor při dalším spuštění dané aplikace znovu zavede do systému. Další informace o službě Windows Installer najdete v odkazu Windows Platform Software Development Kit (SDK)

stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Zásady skupiny

Zásady skupiny představují základní nástroj správce sítě pro správu skupin uživatelů a počítačů. Správce může určit možnosti správy a zabezpečení spravovaných skupin počítačů a uživatelů pomocí modulu snap-in Zásady skupiny (Group Policy) konzoly Microsoft Management Console (MMC). Systém Microsoft Windows 2000 Server obsahuje více než 200 výchozích nastavení zásad skupiny. Pomocí Průvodce klientskou instalací (Client Installation Wizard) můžete určit možnosti instalace uživatelů a povolit nebo zakázat uživateli přístup k určitým možnostem. Zásady skupiny jsou důležité pro podniky s postiženými uživateli, protože je můžete použít k úpravě nastavení skupin uživatelů se stejnými potřebami pomocných nástrojů. Navíc může více uživatelů jednoho počítače používat své přihlašovací informace a hesla k nastavení svých vlastních preferencí včetně určitých možností usnadnění.

Další informace o používání zásad skupiny najdete v kapitole „Zásady skupiny“ v knize *Microsoft Windows 2000 Server Distribuované systémy*.

Vytvoření více uživatelských profilů

Průvodce funkcemi usnadnění můžete použít k vytvoření více uživatelských profilů. Další uživatel, který se přihlásí do systému Windows, může sice nastavení změnit, přitom však nedojde k odstranění předchozích nastavení – jednotlivá nastavení se obnoví při příštím přihlášení uživatele. Tato funkce umožňuje uživatelům nebo správcům nastavit uživatelské volby. Systém Windows automaticky jiným uživatelům nabídne výchozí funkce. Jestliže jsou funkce usnadnění vypnuté, uživatelé, kteří je nepotřebují, si vůbec nevšimnou, že jsou takové funkce instalované. Proto mohou používat počítač jak lidé nepotřebující pomoc tak i lidé, kteří nějaké pomocné nástroje potřebují. Více uživatelů jednoho počítače může používat své přihlašovací informace a hesla k nastavení svých vlastních preferencí a pracovní plochy včetně potřebných možností usnadnění.

Možnosti správy

Pomocí Průvodce funkcemi usnadnění a ovládacích panelů můžete nastavit možnosti správy několika prvků. Mezi funkce, která lze zadat oběma prvky, patří nastavení automatického vypršení/automatického resetu a výchozí nastavení usnadnění. Chcete-li si tato nastavení uložit do souboru, aby je bylo možné použít i na jiném počítači, musíte však použít Průvodce funkcemi usnadnění.

Reset (vypršení) usnadnění

Další užitečnou funkcí pro počítače sdílené více uživateli je funkce vypršení časových limitů (resetu) možností usnadnění. Tato součást Průvodce funkcemi usnadnění i ovládacích panelů vypíná možnosti usnadnění po určité zadané době nečinnosti počítače. Operační systém se tak vrací ke svému výchozímu nastavení.

Poznámka Funkce automatického resetu (vypršení) nevypíná funkci Posloupnost kláves.

Systém Active Desktop

Prostřednictvím systému Active Desktop si může uživatel upravit prakticky všechny prvky pracovní plochy a navíc si tu může zobrazovat intranetový a internetový obsah. Průzkumník systému Windows 2000 umožňuje uživateli pohybovat se mezi prvky pracovní plochy, jako jsou ikony v hlavním panelu, soubory, ikony zástupců a další objekty, která se nacházejí na síti. Tato funkce dává všem kategoriím objektů konzistentní rozhraní – pro některé uživatele může být jednodušší pohybovat se přímo mezi objekty na pracovní ploše a nepoužívat myš.

Úprava pracovní plochy

Dále je uvedeno několik příkladů způsobů, jakými si uživatelé mohou upravit své pracovní plochy pomocí systému Active Desktop:

- Přidání webových stránek obsahujících aktivní obsah na plochu.
- Umístění panelu nástrojů na vhodnější místo pracovní plochy nebo hlavního panelu.
- Změna uspořádání často otevíraných souborů a programů a rychlý přístup k nim.
- Přidání panelu adresy na pracovní plochu nebo na hlavní panel. Uživatelé pak mohou zadávat internetovou adresu bez předchozího otevření prohlížeče.

Panely nástrojů pracovní plochy

Uživatelé si mohou vytvořit své vlastní panely nástrojů pracovní plochy s příkazy, které často používají. To je nejužitečnější pro uživatele, kteří dávají před klávesnici přednost myši. Uživatelé, kteří upřednostňují klávesnici, si obvykle přidávají příkazy do nabídky tlačítka **Start**.

Ikony stavu systému

Novinkou v systému Windows 2000 je zobrazování stavových ikon v systémové oblasti hlavního panelu. Jakmile uživatel aktivuje stavové ikony určitých často používaných funkcí usnadnění, objeví se v systémové oblasti hlavního panelu. Když navíc uživatel stiskne příslušnou klávesovou zkratku, ikona vyplní odpovídající obdélník a ukáže, která klávesa je aktivní. Tyto stavové ikony nahrazují indikátory stavu z předchozích verzí systému Windows.

Správce nástrojů

Novinkou v systému Windows 2000 je Správce nástrojů (Utility Manager), který uživatelům šetří mnoho času. Správce může určit, na kterých počítačích se automaticky otevrou po startu systému Windows 2000 nástroje usnadnění. Uživatelé mohou zastavit nebo restartovat nástroje podle svých potřeb. Pro některé uživatele je velmi důležitý okamžitý přístup k takovým funkcím, jako je Narrator, Lupa a Klávesnice na obrazovce.

Uživatelé a správci si mohou také pomocí Správce nástrojů upravit většinu programů usnadnění dostupných na počítači. Správci si mohou otevřít dialogové okno a podívat se, jaké nástroje usnadnění systému Windows 2000 jsou instalovány a jaký je jejich stav. Správci mohou také nastavit další aplikace nebo spouštět programy instalující doplňková zařízení. Správce nástrojů můžete sice otevřít pomocí nabídky tlačítka **Start**, rychlejší je však použít klávesovou zkratku Logo Windows+U.

Poznámka Zabudovanými programy, které si můžete otevřít ze Správce nástrojů, jsou Lupa, Narrator a Klávesnice na obrazovce. Kromě aplikací zabudovaných společností Microsoft do operačního systému se mohou ve Správci nástrojů objevovat také aplikace jiných výrobců.

Další informace o přidávání pomocných zařízení do Správce nástrojů najdete v dokumentaci daného nástroje nezávislého výrobce.

Konfigurace možností usnadnění v systému Windows 2000

Vytváření vlastních rozhraní umožňuje uživatelům s postižením řídit své počítačové prostředí, aby mohli úspěšně používat software, který potřebují ke své práci. V závislosti na konkrétních potřebách jednotlivých osob se uživatelé setkávají s problémy v různých aspektech systému Windows. I když se možnosti usnadnění instalují se systémem Windows 2000 automaticky, při čisté instalaci musí být znovu nastaveny již dříve nakonfigurované možnosti a volby a jednotlivým uživatelům je také zapotřebí nastavit nové možnosti.

Tabulka E.1 popisuje některé pomůcky zabudované do operačního systému Windows 2000 zajišťující jeho větší přístupnost. Protože některé funkce se používají pro více různých typů postižení, nejsou zde uvedeny podle konkrétního postižení, ale podle obtížnosti. Popisy funkcí podle kategorií postižení najdete v oddílu „Nastavení možností usnadnění podle typu postižení“ dále v této kapitole.

Tabulka E.1 Obvyklé potíže problémů a jejich řešení

Uživatel má problém s ...	Řešení systému Windows 2000
úpravou nastavení v síti s více uživateli.	Průvodce funkcemi usnadnění, Možnosti správy, ovládací panel Možnosti usnadnění (Accessibility Options)
těmito činnostmi: <ul style="list-style-type: none"> ■ otevření systému Windows nebo aplikací; ■ procházení prvky pracovní plochy a systémem Windows; ■ úprava nastavení klávesnice; ■ úprava nastavení zobrazení. 	Klávesové zkratky, Správce nástrojů, Narrator, Klávesnice na obrazovce, systém Active Desktop, ikony stavu systému
zapamatováním aktivace funkcí usnadnění.	Ovládací panel Možnosti usnadnění
vyhledáním potřebné funkce.	Průvodce funkcemi usnadnění se seznamem po-
dle postižení	
zapamatováním indikátorů navigace klávesnice.	Ovládací panely Možnosti usnadnění (Accessibility Options) a Zobrazení (Display), Průvodce funkcemi usnadnění
správným zápisem slov.	Automatická kontrola pravopisu, funkce automatického dokončování, funkce automatických oprav, klávesové zkratky

slyšením, například v následujících situacích:	Zobrazení zvuku, Popis zvuku, upravitelná zvuková schémata
■ poslech zvukových výzev;	
■ rozlišování zvuků;	
■ poslech zvukové nápovědy;	
■ práce v hlučném prostředí.	
použitím standardních konfigurací klávesnice.	Klávesnice Dvorak, Klávesnice na obrazovce, Myš klávesnicí (MouseKeys)
použitím klávesnici díky pomalé reakci.	Opakování kláves (RepeatKeys) a možnosti klávesnice
použitím klávesnice díky nechtěnému stisku kláves.	Pomalé klávesy (SlowKeys), Odskok kláves (BounceKeys), Opakování kláves (RepeatKeys) a Ozvučení kláves (ToggleKeys)
stiskem dvou kláves najednou.	Jedním prstem (StickyKeys)
použitím standardních metod uživatelského rozhraní včetně myši a klávesnice.	Zařízení ovládaní hlasem od jiných společností, Narrator, Klávesnice na obrazovce
prací s myší.	Myš klávesnicí
prací s blikajícími událostmi a dalšími schémata způsobujícími záchvaty.	Ovládací panel Možnosti usnadnění, který umožňuje uživatelům měnit časování, zvukové schémata a barevný kontrast, a Průvodce funkcemi usnadnění
hledáním nebo sledováním ukazatele myši.	Možnosti myši v Průvodci funkcemi usnadnění nebo ovládací panel
sledováním stavových světel klávesnice.	Ozvučení kláves
sledováním prvků na obrazovce.	Narrator, Lupa, ovládací panely a schémata velikost, barvy a kontrastu v Průvodci funkcemi usnadnění
dobou spoluprací se zabudovanými nástroji usnadnění (je zapotřebí doplňkové zařízení).	Active Accessibility, Posloupnost kláves pro zařízení nezávislých výrobců
vyhledáním pomocných zařízení nezávislých výrobců a dalších informací o usnadnění.	Webové sídlo Microsoft Accessibility (podrobnosti najdete v oddílu „Další zdroje“ v této příloze)

Uživatelé a správci mohou k úpravě mnoha funkcí usnadnění v systému Windows 2000 použít ovládací panel Možnosti usnadnění. Řadu často používaných funkcí nastavení však nyní můžete konfigurovat také pomocí Průvodce funkcemi usnadnění. Uvedeným ovládacím panelem nebo Průvodcem funkcemi usnadnění tak můžete nastavit například zobrazení, klávesnici, myš a zvukové funkce podle konkrétních potřeb uživatele. Obě cesty konfigurace možností jsou popsány v následujících pododdílech.

Konfigurace možností usnadnění pomocí Průvodce funkcemi usnadnění

Průvodce funkcemi usnadnění je novinkou v systému Windows 2000 a zjednodušuje nastavení voleb usnadnění podle konkrétních potřeb určitého uživatele – již není zapotřebí měnit číselné hodnoty nebo nastavení v ovládacích panelech. Tento průvodce je dostupný z nabídky tlačítka **Start** a představuje jediný vstupní bod nastavení mnoha často používaných funkcí. Uživatel si také může nastavení uložit do souboru a nakonfigurovat s jeho pomocí další počítače. Mezi možnostmi řízenými průvodcem jsou volby zvuku a zobrazení, jako je hlasitost a velikost písma, několik možností klávesnice, kam patří filtry klávesnice a funkce Myš klávesnicí, a možnost nastavovat volby správy.

Konfigurace možností usnadnění pomocí ovládacího panelu

Ikona Možnosti usnadnění (Accessibility Options) v ovládacích panelech dovoluje uživatelům jednoduše upravovat vlastnosti ovládající mnoho funkcí usnadnění systému Windows 2000. Uživatelé mohou zapínat a vypínat možnosti usnadnění a upravovat operace s klávesnicí, se zvuky a s myší podle svých konkrétních potřeb. Panel Možnosti usnadnění zajišťuje uživatelům přístup k těmto funkcím: Jedním prstem, Filtrování kláves, Ozvučení kláves, Popis zvuku, Zobrazení zvuku, Myš klávesnicí a Posloupnost kláves.

Kromě voleb pro uživatele s postižením v panelu Možnosti usnadnění nabízejí další ovládací panely jiné způsoby úpravy nastavení klientského počítače. Uživatelé mohou měnit nastavení v panelech Zobrazení (Display), Klávesnice (Keyboard), Myš (Mouse), Zvuky a multimédia (Sounds and Multimedia) a dalších. Následující oddíl popisuje mnoho dalších prvků i funkce určené přímo pro postižené uživatele.

Nastavení možností usnadnění podle typu postižení

Vytváření vlastních rozhraní dává uživatelům s postižením možnost řídit si své počítačové prostředí. Zjednodušené uživatelské rozhraní je nezbytnou podmínkou omezení množství nutných činností pohybu mezi prvky. Dále jsou uvedeny funkce a techniky systému Windows 2000, kterými mohou správci a uživatelé naplnit své specifické potřeby a preference. Mnoho z těchto možností platí pro více kategorií postižení, pro účely organizace jsou však rozčleněny do skupin podle kategorie postižení.

Možnosti pro uživatele s postižením rozpoznávání

Postižení rozpoznávání zahrnují vývojová postižení, jako je Downův syndrom, postižení schopnosti učit se, jakými jsou dyslexie, neznalost jazyka, negramotnost, nemožnost soustředit se a ztráta paměti, a postižení vnímání, jako jsou například pomalé reakce. Lidem s postižením rozpoznávání mohou být kromě pomocných zařízení jiných výrobců, jako jsou například prostředky hlasového vstupu, také velmi užitečné některé zabudované funkce systému Windows. Příklady jsou funkce sady IntelliSense, jako je automatická oprava (AutoCorrect), automatické dokončení (AutoComplete) a automatická kontrola pravopisu.

Funkci automatického dokončování můžete nastavit tak, aby obsahovala pouze informace, které uživatelé potřebují. Některým uživatelům mohou tyto funkce výrazně zjednodušit práci. V případě jiných uživatelů však může být lepší naopak tyto funkce zakázat, protože mohou představovat neustálá vyrušení, zejména pracuje-li uživatel s nástrojem převodu textu na mluvené slovo.

Lidem s postižením rozpoznávání bude užitečných několik funkcí usnadnění systému Windows 2000, které se nacházejí v Průvodci funkcemi usnadnění nebo v ovládacích panelech. Uživatelé, kteří pracovali se systémem Windows NT verze 4.0 nebo předchozím, si musí uvědomit, že v systému Windows 2000 se nacházejí speciální filtry klávesnice. Jak Průvodce funkcemi usnadnění tak i ovládací panely nyní umožňují uživatelům upravovat reakční časy klávesnice a ignorovat jejich náhodné stisky kláves a pomalou reakci.

Možnostmi klávesnice užitečnými pro osoby s postižením rozpoznávání jsou především klávesové zkratky. Pro tyto osoby jsou také užitečné následující funkce: Narrator, systém Active Desktop, ikony stavu systému zobrazující aktivované funkce a možnosti

zvuku umístěné v Průvodci funkcemi usnadnění a ovládacích panelech. Také zvuková schémata mohou pomoci upozornit uživatele na určité činnosti nebo je o nich dále informovat.

Formát Synchronized Accessible Media Interchange

Uživatelům s jazykovými problémy může usnadnit porozumění mluvenému slovu pomocí titulků formát Synchronized Accessible Media Interchange (SAMI). Tato funkce systému Windows 2000 je popsána v následujícím oddílu „Možnosti pro uživatele s postižením sluchu“.

Možnosti pro uživatele s postižením sluchu

Neslyšícím nebo špatně slyšícím uživatelům, kteří nedokáží dobře rozeznat zvuky, mohou být užitečné dále uvedené volby. Tyto funkce zahrnují úpravy zvukového schéma a náhradu zvuku vizuálními médii.

Upravitelná zvuková schémata

Uživatelé, kteří špatně slyší nebo kteří pracují v hlučném prostředí, si mohou nastavit výšku zvuků i hlasitost přiřazenou různým událostem na obrazovce, které pak snáze rozliší. Zvuky lze upravit buď pomocí Průvodce funkcemi usnadnění nebo příslušným ovládacím panelem.

Systém Windows nabízí zvuky, které mohou uživatelé přiřadit mnoha událostem. Může jít o události generované systémem Windows nebo jednotlivými programy. Jestliže mají uživatelé problémy s rozlišením výchozích zvuků, jako je pípnutí při signalizaci stisku neplatné klávesy, mohou si vybrat nové zvukové schéma nebo si vytvořit své vlastní, které jim pomůže s identifikováním zvuků. V systému Windows 2000 mohou uživatelé vypnout nahrání výchozích zvukových souborů.

Úprava hlasitosti

Má-li počítač zvukovou kartu, uživatelé mohou pomocí ovládacího panelu Zvuky a multimedia (Sounds and Multimedia) upravit hlasitost všech zvuků systému Windows. Hlasitost zvuku mohou také upravit pomocí ikony reproduktoru na hlavním panelu nebo nástrojem Ovládání hlasitosti (Volume Control).

Někteří uživatelé potřebují místo zvuku vizuální upozornění. Pro neslyšící uživatele může být znaková řeč prvním jazykem a čeština druhým jazykem. Uživatelé mohou mít problémy se čtením stránek obsahujících zvláštní písma, která nesplňují typografické konvence a například slučují malá a velká písmena, nebo se zobrazováním animovaného textu. V takových případech se budou uživatelům hodit upravitelné zvuky a titulkování.

Následující funkce systému Windows 2000 jsou užitečné pro neslyšící nebo špatně slyšící uživatele.

Funkce Zobrazení zvuku

Zobrazení zvuku, funkce ovládacího panelu Možnosti usnadnění, instruuje aplikace používající titulkování, aby zobrazovaly vizuální nápovědu ve formě titulkování. V systému Windows 2000 si uživatelé mohou zvolit zobrazování titulkování.

Funkce Popis zvuku

V systému Windows 2000 podporuje funkce Popis zvuku pouze ty zvuky, které vytváří reproduktor počítače – nemůže detekovat zvuky vytvářené multimediální zvukovou kartou. Má-li počítač multimediální zvukovou kartu, uživatel nebo správce může tento hardware vypnout a vynutit si tak přehrávání zvuků reproduktorem počítače. Pak může funkce Popis zvuku detekovat uvedené události. Aby se taková změna uplatnila, musí uživatel restartovat systém Windows.

Formát Synchronized Accessible Media Interchange

Formát Synchronized Accessible Media Interchange (SAMI)/Direct Show se používá pro titulkování. SAMI je formát, který mohou používat vývojáři, instruktoři a autoři webových stránek k vytváření popisků a zvukových popisů v jediném dokumentu. SAMI vychází z formátu HTML a představuje podobný čitelný formát. Pomocí formátu SAMI mohou vývojáři a další osoby vytvářet otitulkované multimediální produkty. Nástroj Windows Media Player (Přehrávač záznamů) synchronizuje informace titulků a uživatel si dále může titulků upravit podle svých potřeb.

Další informace o formátu SAMI najdete v odkazu Microsoft Accessibility stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Možnosti pro uživatele s fyzickým postižením

Někteří uživatelé nemohou vykonávat určité manuální úkoly, jako je například použití myši nebo stisk dvou kláves najednou. Jiní uživatelé mají tendenci náhodně tisknout více kláves najednou nebo se některých kláves jen krátce nepředvídatelně dotýkat. Mezi fyzická postižení nebo postižení pohyblivosti patří paralýza, zranění z opakovaného namáhání, ochrnutí páteře, třas, kvadruplegie a chybějící údy či prsty. Mnoho uživatelů potřebuje klávesnici a myš upravené pro jejich konkrétní potřeby nebo se zcela spoléhají na alternativní vstupní zařízení. Naštěstí je uživatelům dostupné velké množství vstupních zařízení, včetně nástrojů hlasového vstupu sloužících k řízení počítače hlasem uživatele a filtrů klávesnice, klávesnic na obrazovce, menších a větších klávesnic, zařízení sledujících pohyb očí a systémů ovládaných dýcháním. Další informace o pomocných zařízeních a katalog zařízení usnadnění od nezávislých společností najdete v odkazu Microsoft Accessibility stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Možnosti klávesnice

Snížená hbitost může pro daného uživatele znamenat obtížné používání standardní klávesnice. Filtry klávesnice zabudované do systému Windows 2000 mohou takové problémy částečně kompenzovat tím, že berou v úvahu náhodný třas, pomalé reakce a podobné stavy. Mezi další druhý filtrů klávesnic patří nástroje pomáhající se psaním, jako jsou nástroje předvídání slov a umožňující zkrácený zápis slov a doplňkové kontroly překlepů. Následující oddíly popisují vstupní zařízení a funkce odlišné od standardní klávesnice. Tyto funkce představují možnosti upravující chování kláves podle konkrétních potřeb usnadnění.

Poznámka Ve většině případů není možné aplikovat stejné korekce chování klávesnice na ukazovací zařízení, jako je myš. To omezuje uživatele s postižením pohyblivosti na zadávání pomocí klávesnice.

Klávesnice na obrazovce

Někteří uživatelé mají problémy jak s myší tak i s klávesnicí. Mohou však používat klávesnici na obrazovce ve spojení s další metodou vstupu, jako je například ukazovací zařízení, pákový ovladač (joystick) připojený k sériovému portu nebo mezerník klávesnice používaný jako zařízení přepínání. Klávesnice na obrazovce je nástroj umožňující uživatelům vybírat klávesy pomocí režimu alternativního vstupu. Uživatelé, kteří dokáží ukazovat, ale nedokáží klepat, mohou využívat ukazovací zařízení, přepínače nebo vstupní systémy Morseova kódu.

Uživatelé mohou aktivovat a upravit funkci Klávesnice na obrazovce systému Windows 2000 pomocí nabídky tlačítka **Start**. Funkce Klávesnice na obrazovce poskytuje minimální úroveň funkčnosti uživatelům se středními postiženími pohyblivosti. Mnoho uživatelů s fyzickým postižením potřebuje k denní práci nějaký nástroj s vyšší funkčností. Další informace o klávesnicích na obrazovce pro systém Windows najdete v odkazu Microsoft Accessibility stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Poznámka Funkce Klávesnice na obrazovce slouží pouze jako dočasné řešení a nepředstavuje plnohodnotnou každodenně používanou klávesnici nahrazující obrazovkové klávesnice nezávislých výrobců.

Klávesnice Dvorak

Klávesnice Dvorak zpřístupňuje lidem, kteří mají potíže s psaním na standardní klávesnici QWERTZ, nejčastěji používané znaky. Existují tři rozložení Dvorak: jedno pro osoby používající ke psaní obě ruce, jedno pro osoby píšící pouze levou rukou a jedno pro osoby píšící pouze pravou rukou. Rozvržení Dvorak omezuje pohyby potřebné k zápisu obvyklého anglického textu, což může přispět k vyřešení určitých problémů se zraněními způsobenými opakovaným namáháním při psaní. Klávesnici Dvorak můžete přidat již při instalaci nebo i později. K nakonfigurování klávesnice Dvorak použijte ovládací panel Klávesnice (Keyboard).

Klávesové zkratky

Klávesové zkratky jsou pro postižené uživatele velmi důležité. Jsou nezměrně hodnotné pro uživatele s prakticky jakýmkoli kategoriemi postižení. Tyto příkazy kláves Alt a Ctrl mohou uživatelům pomoci ke snazšímu pohybu systémem Windows 2000. I bez konfigurace funkcí usnadnění může uživatel používat v dialogových oknech k přesunu mezi poli klávesu Tabulátor a k výběru položek seznamu kurzorové klávesy. V oknech vlastností s více kartami může uživatel vybírat jednotlivé vlastnosti zleva doprava. V systému Active Desktop může uživatel přidávat klávesové zkratky do nabídky **Start**. Další informace o klávesových zkratkách včetně jejich výčtu najdete v nápovědě systému Windows 2000.

Další informace o klávesových zkratkách včetně rozsáhlého výčtu klávesových zkratk usnadnění najdete v příloze H „Usnadnění (Accessibility)“ v sadě *Microsoft Windows 98 Resource Kit*.

Další informace o příkazech zadávaných jen pomocí klávesnice, klávesových zkratkách usnadnění a klávesách klávesnice Microsoft Natural Keyboard najdete v odkazu Microsoft Accessibility stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Klávesové zkratky možností usnadnění

Klávesové zkratky usnadnění představují metodu okamžité aktivace možností usnadnění pro uživatele, kteří nemohou používat počítač bez předchozí aktivace možností usnadnění. Tyto klávesové zkratky umožňují uživateli dočasně zapnout určitou funkci. Po zapnutí funkce mohou uživatelé k upravení funkce nebo její trvalé aktivaci použít Průvodce funkcemi usnadnění nebo ovládací panel Možnosti usnadnění. Stejná klávesová zkratka dočasně funkci vypíná, pokud překáží jinému uživateli, který chce pracovat s počítačem bez ní.

Klávesové zkratky jsou jedinečné kombinace kláves, které nesmí kolidovat s klávesami používanými programy. Jestliže se takový konflikt objeví, uživatel může klávesové zkratky vypnout a přesto nadále používat danou funkci podle potřeby. V typické instalaci systému Windows 2000 jsou klávesové zkratky usnadnění neaktivní, aby nekolidovaly s jinými programy.

Funkce Jedním prstem pro zápis jedním prstem nebo nástrojem drženým v ústech

Mnoho programů vyžaduje, aby uživatelé stisknuli dvě nebo více kláves najednou. V případě uživatelů píšících jedním prstem nebo nástrojem drženým v puse to není možné. Funkce Jedním prstem umožní uživateli tisknout klávesy postupně po jedné a přitom instruuje systém Windows tak, jako by byly požadované klávesy stisknuty najednou.

Pro sdílené počítače je vhodná volitelná funkce, která zajistí pro ostatní uživatele vypnutí funkce Jedním prstem. Je-li aktivována volba **Vypnout funkci Jedním prstem při stisknutí dvou kláves zároveň** (Turn StickyKeys Off If Two Keys Are Pressed at Once), funkce Jedním prstem detekuje současný stisk dvou kláves a automaticky se vypíná.

Někteří lidé nemají rádi zvuky klávesnice, zatímco jiným pomáhají. Uživatelé mohou tyto pomocné zvuky zapínat a vypínat ve vlastnostech funkce Jedním prstem volbou položky **Zvukový signál při stisknutí modifikační klávesy** (Make Sounds When Modifier Key Is Pressed).

Funkce Filtrování kláves pro uživatele s postižením pohyblivosti rukou

Systém Windows 2000 obsahuje filtry klávesnice, které samostatně nebo kombinovaně usnadňují zadání pro uživatele, kteří mají s klávesnicí problémy díky svým pomalým reakcím, náhodnému třasu nebo tendenci nechtěně se dotýkat a tisknout klávesy. Pomocí funkce Filtrování kláves mohou uživatelé upravovat reakční časy klávesnice a umožnit tak náhodný stisk kláves a pomalé reakce.

Funkce Ozvučení kláves pro uživatele náhodně tisknoucí přepínací klávesy

Funkce Ozvučení kláves říká systému Windows, aby po aktivování přepínacích kláves Num Lock, Caps Lock nebo Scroll Lock vygeneroval vysoký nebo nízký tón. Tento zvuk signalizuje uživateli, že došlo k aktivaci jedné z uvedených kláves.

Možnosti myši

Uživatelé s postižením pohyblivosti si nyní mohou nastavit schémata velikosti, barvy a animace. Pomocí ovládacího panelu Myš si mohou uživatelé upravit vlastnosti myši a zlepšit viditelnost ukazatele. Tato nastavitelná funkce je užitečná především pro uživatele s postižením zraku, i když není určena výhradně pro postižené uživatele.

Úprava vlastností myši

Pomocí ovládacího panelu Myš (Mouse) mohou uživatelé zadat automatické přesunutí ukazatele myši na výchozí tlačítka jako je **OK** nebo **Použít** v dialogových oknech a mohou tlačítka myši zaměnit tak, aby bylo výchozím tlačítkem to pravé. Uživatelé mohou nastavit také další možnosti myši, jako je rychlost a zrychlení ukazatele myši, orientace zleva doprava a velikost ukazatele, barvu, tvar, čas mezi klepnutími a animaci. Výběrem položek **Jsem nevidomý/nevidomá nebo mám potíže vidět objekty na obrazovce** (I am blind or have difficulty seeing things on screen) a **Mám potíže při používání klávesnice nebo myši** (I have difficulty using the keyboard or mouse) mohou uživatelé nastavovat několik možností usnadnění myši v Průvodci funkcemi usnadnění.

Funkce Myš klávesnicí pro zadávání pouze klávesnicí

I když je systém Windows 2000 vytvořen tak, aby bylo možné zadat všechny akce bez použití myši, některé programy myš vyžadují a pro některé úkoly je to také nejvhodnější nástroj. Funkce Myš klávesnicí ovládacího panelu je také užitečná pro grafiky a další uživatele, kteří potřebují umisťovat ukazatel myši s vysokou přesností. Uživatel nemusí mít k tomu, aby mohl tuto funkci používat, instalovanou myš. Pomocí funkce Myš klávesnicí mohou uživatelé také ovládat ukazatel myši jedním prstem nebo nástrojem drženým v ústech – k pohybu ukazatelem se používá numerická klávesnice. Při této metodě mohou uživatelé také klepat, poklepávat a přesunovat objekty oběma tlačítky myši. Je-li funkce Myš klávesnicí aktivní, vydává při zapnutých zvucích stoupající tón.

Možnosti pro uživatele se záchvaty

Abby mohli počítač používat také uživatelé s náhodnými záchvaty včetně epilepsie, je možné pomocí Průvodce funkcemi usnadnění nebo příslušného ovládacího panelu upravovat v systému Windows prvky obrazovky, jako je časování, barva a kontrast a zvuky. Rozsah výběru mnoha těchto funkcí byl v systému Windows 2000 rozšířen. Uživatelé mohou také omezit počet písem na jedno nebo více takových, které odpovídají jejich potřebám. Pro uživatele se záchvaty je možné upravit následující možnosti usnadnění.

Vzory časování

Vzory časování mohou ovlivnit uživatele mnoha různými způsoby. Uživatelé se záchvaty jako je epilepsie, mohou být citliví na obnovovací frekvence monitoru a blikající zobrazení. Nastavení ovládacích panelů systému Windows 2000 může zabránit výchozímu nahrání animací a videosekvencí. Uživatelé si mohou upravit rychlost blikání objektů na frekvenci, která jim nebude vadit. Uživatelé a správci také mohou změnit rychlost blikání indikátoru textového kurzoru a mohou také pro citlivé uživatele vypnout blikající obrázky.

Zvuková schémata

Uživatelé se záchvaty mohou být také citliví na určité zvuky. Nastavení v systému Windows 2000 mohou zabránit výchozímu nahrávání animací, videosekvencí a zvuků. Pomocí ovládacích panelů mohou uživatelé přiřazovat všem událostem vlastní zvukové soubory. Možnost upravit si zvuková schémata nebo zapínat a vypínat zvuk a upravovat hlasitost je pro uživatele velmi důležitá a v systému Windows 2000 nabývá mnoha různých forem při podpoře osob s různými typy postižení a potřeb.

Nastavení barvy a kontrastu

Pomocí ovládacího panelu Možnosti usnadnění a nástroje Lupa mohou uživatelé upravovat nastavení barvy a kontrastu. Novinkou v systému Windows 2000 je rozšířené spektrum barevných schémat, která lze dále upravit podle konkrétních potřeb uživatele. Podrobné informace najdete v následujícím oddílu o postižení zraku.

Možnosti pro uživatele s postižením zraku

Následující možnosti usnadnění jsou užitečné pro nevidomé uživatele nebo pro osoby, které trpí omezeným viděním, barvoslepostí, tunelovým viděním či jinými postiženími zraku: nástroje převodu textu na řeč, jako je Narrator, klávesové zkratky, Lupa (Magnifier) a upravitelné funkce, jako jsou ukazatele myši, barevná a kontrastní schémata a další prvky uživatelského rozhraní.

Narrator

Narrator je program převodu textu na mluvené slovo s minimálními funkcemi, který je součástí anglické (severoamerické) verze systému Windows 2000. Tato nová funkce spolupracuje s funkcí Active Accessibility při čtení objektů na obrazovce, jejich vlastností a jejich prostorových vztahů. Narrator má řadu možností umožňující uživatelům upravit si způsob, jakým zařízení čte prvky obrazovky. Volba Voice (hlas) dovoluje uživatelům upravit rychlost, hlasitost a výšku hlasu. Volba Reading (čtení) jim umožňuje vybírat zapisované znaky, které má zařízení číst nahlas, jako jsou klávesy Delete, Enter, tisknutelné znaky nebo modifikátory. Volba Mouse Pointer (ukazatel myši) způsobí, že ukazatel myši bude sledovat aktivní položku na obrazovce. Volba Announce events on screen (oznamovat události na obrazovce) dovoluje uživatelům přikázat zařízení oznamování zobrazení následujících položek: nové okno, nabídka, místní nabídka. Narrator poskytuje minimální úroveň funkčnosti pro uživatele se středními postiženími zraku. Mnoho uživatelů s omezeným viděním potřebuje ke každodennímu použití program převodu textu do mluveného slova s lepšími funkcemi. Další informace o nástrojích převodu textu na mluvené slovo fungujících v systému Windows najdete v odkazu Microsoft Accessibility stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.

Poznámka Narrator představuje jen dočasnou pomůcku a není tak náhradou plně funkčních nástrojů převodu textu na mluvené slovo jiných softwarových společností.

Zvuková signalizace klávesnice

Funkce Ozvučení kláves je užitečná zejména pro osoby, které často omylem tisknou místo klávesy Tab klávesu Caps Lock, protože je na to systém ihned upozorní. Funkce Ozvučení kláves také pracuje s klávesnicemi, na kterých není indikace stavu přepínačů Caps Lock, Num Lock a Scroll Lock.

Lupa

Lupa je nástroj zvětšování obrazovky s omezenými funkcemi, který zvětšuje část obrazovky systému Windows 2000 a usnadňuje její čtení osobám s menšími zrakovými postiženími. Zvětšení obrazovky lze použít také v jiných případech, například při grafických úpravách. Lupa zobrazuje zvětšenou část obrazovky v samostatném okně. Je-li Lupa aktivní, zvětšená oblast je pouze zobrazením – nejde o aktivní oblast. Lupa poskytuje minimální úroveň funkčnosti pro uživatele se středními postiženími zraku.

Mnoho uživatelů s omezením viděním potřebuje ke každodennímu použití program zvětšování obrazovky s lepšími funkcemi. Další informace o nástrojích zvětšování obrazovky fungujících v systému Windows najdete v odkazu Microsoft Accessibility stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/res-kit/webresources>.

Poznámka Lupa není náhradou plně funkčních nástrojů zvětšování obrazovky jiných softwarových společností.

Písma

Uživatelé mohou pomocí ovládacího panelu Písma (Fonts) odstranit ze systému Windows písma, která nechťejí používat. Jestliže odstraní všechna písma typu TrueType a ponechají instalovaná pouze rastrová písma, mohou také omezit jejich používané velikosti. Písma typu TrueType jsou nezávislá na zařízení, která jsou uložena ve formě obrysů a jejichž velikost lze libovolně měnit podle potřeby. Rastrová písma se vytvářejí jazykem tiskárny na základě bitových map. Odstraněním se písma nemažou z pevného disku, takže si je uživatelé mohou později znovu snadno nainstalovat.

Poznámka Odstranění písem v uvedeném ovládacím panelu omezuje také písma dostupná aplikacím. Tato operace výrazně ovlivňuje zobrazení dokumentů na obrazovce a jejich tisk, a proto musí být uživatelé při odstraňování písem opatrní.

Schémata velikosti a barvy

V Průvodci funkcemi usnadnění a také v ovládacích panelech si mohou uživatelé upravit velikost a barvu většiny prvků obrazovky, jako je text v oknech, nabídka, indikátor textového kurzoru, ukazatel myši, písma a záhlaví oken. Tato možnost může usnadnit používání systému a může omezit namáhání očí. V Průvodci funkcemi usnadnění mohou uživatelé měnit velikost ikon, velikost ukazatele myši a velikost textu. V ovládacích panelech je možné změnit šířku okraje oken. Poklepáním na ikonu Zobrazení (Display) a výběrem požadovaného schéma na kartě **Vzhled** (Appearance) lze také zadat velikost textu ve zprávách systému Windows a v okně příkazového řádku. Uživatelé mohou měnit velikost okna klávesnicí místo myši. Možnou také měnit velikost okna v Průvodci funkcemi usnadnění volbou položky **Jsem nevidomý/nevidomá nebo mám potíže vidět objekty na obrazovce** (I am blind or have difficulty seeing things on the screen). Pomocí Průvodce funkcemi usnadnění nebo ovládacími panely lze také změnit velikost písma ve zprávách systému Windows.

Před úpravou nastavení barvy zvažte tyto položky:

- Nastavení zobrazující velký počet barev vyžadují velké množství prostředků procesoru počítače.
- Nastavení High Color představuje více než 65 000 barev. Nastavení True Color představuje více než 16 miliónů barev.
- Maximální počet zobrazitelných barev určuje grafický adaptér (karta) a monitor.
- Aby bylo možné měnit nastavení jiného monitoru v systému s více monitory, musí správci zaškrtnout políčko **Rozšířit plochu i na tento monitor** (Extend My Windows Desktop onto this Monitor). Pak lze zadávat nastavení barev pro každý instalovaný monitor.

Barevná schémata s vysokým kontrastem

Úprava kontrastu a barvy usnadňuje rozeznání objektů na obrazovce o omezuje náma- hu očí. Funkce Vysoký kontrast se již neaktivuje jen pomocí ovládacích panelů, ale je to zabudovaná a rozšířená knihovna barevných schémat pro uživatele s omezeným vi- děním, kteří vyžadují vysoký kontrast mezi objekty popředí a pozadí. Tuto funkci mo- hou používat například uživatelé, kteří nedokáží jednoduše číst černý text na šedém pozadí nebo text napsaný přes obrázek. Po aktivaci režimu vysokého kontrastu se au- tomaticky vybere preferované barevné schéma uživatele. Prostřednictvím dialogového okna Lupa (Magnifier) mohou uživatelé invertovat barvy okna zvětšení nebo si obra- zovku zobrazovat s vysokým kontrastem. Aktivace režimu vysokého kontrastu může tr- vat několik sekund.

Nové ukazatele myši

Nové ukazatele myši upravované pomocí Průvodce funkcemi usnadnění nebo ovláda- cími panely umožňují uživatelům určit, který ukazatel myši je pro ně nejviditelnější. V zájmu zlepšení viditelnosti mohou nyní uživatelé nastavovat takové charakteristiky ukazatele myši, jako je jeho velikost, barva, rychlost, animace a viditelná stopa. Ukaza- telé mají nyní tři velikosti: velkou, zvláště velkou a výchozí. Možnosti ukazatelů zahr- nují černé, bílé a invertované ukazatele, které reagují na barvy obrazovky. (Poslední uvedený ukazatel má vždy barvu kontrastní k aktuálnímu pozadí.)

Další zdroje

- Další informace o možnostech usnadnění pro postižené uživatele včetně technické podpory, dokumentace a odkazů na další organizace najdete v odkazu Microsoft Accessibility stránky webových prostředků na adrese <http://windows.microsoft.com/windows2000/reskit/webresources>.
- Další informace o klávesových zkratkách včetně rozsáhlého seznamu klávesových zkratk usnadnění najdete v příloze H „Accessibility (Usnadnění)“ v knize *Microsoft Windows 98 Resource Kit*, Microsoft Corporation, 1998, Redmond, WA: Microsoft Press.
- Další informace o možnostech usnadnění pro uživatele s postiženími a katalog po- mocných nástrojů můžete získat telefonicky nebo poštou u společnosti Microsoft takto:
 - Využitím střediska telefonického prodeje společnosti Microsoft:
1 + (800) 426-9400
 - Využitím linky faxové služby telefonického prodeje sloužící pro zpětné faxování dokumentů: 1 +(800) 727-3351
 - Odesláním dopisu na adresu střediska informací o prodeji společnosti Microsoft na adresu: One Microsoft Way, Redmond, WA 98052-6393

Glosář

■

.adm

Přípona souborů šablon pro správu.

.msi

Přípona souborů balíčků služby Windows Installer.

A

Active Directory

Adresářová služba, která je součástí systému Windows 2000 Server. Ukládá informace o objektech v síti a poskytuje uživatelům a správcům sítě přístup k těmto informacím. Služba Active Directory poskytuje síťovým uživatelům přístup k povoleným prostředkům na libovolném místě sítě prostřednictvím jediného přihlášení. Správcům sítě poskytuje intuitivní hierarchické zobrazení sítě a centrální bod pro správu všech síťových objektů. Viz také adresář, adresářová služba.

Active Directory Connector (ADC)

Synchronizační agent systémů Windows 2000 Server, Windows 2000 Advanced Server a Windows 2000 Enterprise Server, který poskytuje možnost automatického udržování konzistentnosti adresářových informací dvou adresářů. Bez ADC by bylo nutné znovu ručně zadávat nové údaje a aktualizace v obou adresářových službách.

ActiveX

Sada technologií umožňující vzájemnou interakci softwarových součástí v síťovém prostředí bez ohledu na jazyk, v němž byly součásti vytvořeny.

adresa – address

V serveru System Management Server se adresy používají pro připojení sídel a jejich systémů. Odesílatelé používají adresy k odeslání instrukcí nebo dat na jiné počítače.

adresa IP – IP address

32bitová adresa sloužící k identifikaci uzlu v rámci propojení sítí IP. Každému uzlu v pro-

pojení sítí IP musí být přiřazena jedinečná adresa IP, která je tvořena identifikátorem sítě a identifikátorem hostitele. Adresa je obvykle reprezentována tečkovou desítkovou notací, v níž jsou desítkové hodnoty jednotlivých oktetů odděleny tečkou, například 192.168.7.27. V systému Windows 2000 lze adresy IP konfigurovat staticky nebo dynamicky prostřednictvím protokolu DHCP. Viz také protokol DHCP, uzel.

adresa IP třídy A – Class A IP address

Adresa IP jednosměrového vysílání v rozsahu od 1.0.0.1 do 126.255.255.254. První oktet indikuje síť a další tři oktety pak hostitele na síti. Viz také adresa IP třídy B, adresa IP třídy C, adresa IP.

adresa IP třídy B – Class B IP address

Adresa IP jednosměrového vysílání v rozsahu od 128.0.0.1 do 191.255.255.254. První dva oktety indikují síť a další dva oktety pak hostitele na síti. Viz také adresa IP třídy A, adresa IP třídy C, adresa IP.

adresa IP třídy C – Class C IP address

Adresa IP jednosměrového vysílání v rozsahu od 192.0.0.1 do 223.255.255.254. První tři oktety indikují síť a poslední oktet pak hostitele na síti. Služba Vyrovnávání zatížení sítě poskytuje volitelnou podporu relací pro adresy IP třídy C (kromě podpory jednotlivých adres IP) určenou klientům, kteří využívají více serverů proxy na straně klienta. Viz také adresa IP třídy A, adresa IP třídy B, adresa IP.

adresa IP třídy D – Class D IP address

Třída internetových adres určená pro adresy IP víceměrového vysílání. Hodnota prvního oktetu adresy IP a sítě třídy D je v rozsahu od 224 do 239.

adresa řízení přístupu k médiu

– media access control address

Adresa používaná pro komunikaci mezi síťovými adaptéry na jedné podsíti. Každý adaptér má přiřazenou adresu řízení přístupu k médiu.

adresář – directory

Zdroj informací (například telefonní adresář) obsahující informace o osobách, počítačových souborech či jiných objektech. V systému souborů jsou v adresářích ukládány informace o souborech. V distribuovaném prostředí (jako je například doména systému Windows 2000) jsou v adresářích uloženy informace o objektech, jako jsou tiskárny, aplikace, databáze a další uživatelé.

adresářová služba – directory service

Adresářový informační zdroj a služby, které činí informace dostupnými a využitelnými. Adresářová služba umožňuje uživateli vyhledat objekt podle libovolného z jeho atributů. Viz také Active Directory, adresář.

úložiště adresáře – directory store

Fyzické úložiště replik adresářového oddílu služby Active Directory na daném řadiči domény. Úložiště je zavedeno pomocí nástroje Extensible Storage Engine.

oddíl adresáře – directory partition

Souvislý podstrom Active Directory, který se replikuje jako jednotka do dalších řadičů domén ve struktuře obsahující repliku téhož podstromu. Ve službě Active Directory obsahuje jediný server vždy alespoň tři adresářové oddíly: schéma (definice třídy a atributu adresáře); konfiguraci (topologii replikace a další související informace); doménu (podstrom obsahující doménové objekty). Adresářové oddíly schématu a konfigurace se replikují do všech řadičů domén v dané doménové struktuře. Doménový adresářový oddíl se replikuje pouze do řadičů domén dané domény. Kromě úplné, zapisovatelné repliky svého vlastního doménového adresářového oddílu udržuje server globálního katalogu ještě částečné repliky všech dalších doménových adresářových oddílů ve struktuře. Tyto repliky jsou určeny pouze pro čtení. Viz také úplná replika; globální katalog; částečná replika.

adresářový strom – directory tree

Hierarchie objektů a kontejnerů v určitém adresáři, kterou si lze zobrazit jako obrácený strom, přičemž kořenový objekt je na vrcholu. Koncovými body ve stromu jsou obvykle jednotlivé objekty (listy). Uzly ve stromu neboli větve jsou kontejnerové objekty. Strom ukazuje, jak jsou objekty propojeny z hlediska cesty

z jednoho objektu na druhý. Jednoduchý strom je jediný kontejner a jeho objekty. Spojitý podstrom je libovolná nepřerušovaná část cesty ve stromu včetně všech členů všech kontejnerů v dané cestě.

agent

Aplikace spuštěná na zařízení spravovaném protokolem SNMP (Simple Network Management Protocol). Aplikace agenta je objektem aktivit správy. Také počítač se spuštěným softwarem agenta SNMP se někdy označuje za agenta.

aktivní oddíl – active partition

Oddíl, z něhož se počítač spouští. Aktivním oddílem musí být primární oddíl na základním disku. Pokud používáte výhradně systém Windows 2000, může se aktivní oddíl shodovat se systémovým oddílem. Používáte-li systém Windows 2000 a současně systém Windows 98 či dřívější nebo systém MS-DOS, musí aktivní oddíl obsahovat spouštěcí soubory pro oba operační systémy.

aktivní/aktivní – active/active

Klastrová konfigurace aplikace, při níž aplikace běží na všech uzlech zároveň. Viz také aktivní/pasivní.

aktivní/pasivní – active/passive

Klastrová konfigurace aplikace, při níž aplikace běží v jeden okamžik vždy jen na jednom uzlu. Viz také aktivní/aktivní.

aktualizace – refresh

Obnovení zobrazených informací aktuálními daty.

algoritmus – algorithm

Pravidlo nebo procedura pro řešení problému. Zabezpečený protokol IP používá k šifrování dat kryptografické algoritmy.

alokační tabulka souborů (FAT)**– file allocation table**

Systém souborů vycházející z alokační tabulky souborů (FAT) spravované některými operačními systémy (například Windows NT a Windows 2000). Tabulka sleduje stav různých segmentů místa na disku, které jsou použity pro uložení souborů.

alternativní vstupní zařízení**– alternative input devices**

Vstupní zařízení pro uživatele, kteří nemohou používat standardní vstupní zařízení, jako je myš nebo klávesnice.

API klastru – cluster API

Kolekce funkcí, které jsou implementovány softwarem klastru a používány klientskou nebo serverovou aplikací podporující klastry, aplikací správy klastrů nebo zdrojovou knihovnou DLL. API klastru se používá ke správě vlastního klastru, objektů klastru a databáze klastru. Viz také aplikace podporující klastry; knihovna DLL; uzel; prostředek; zdrojová knihovna DLL; klastr.

aplikace nepodporující klastry**– cluster-unaware application**

V klastru serverů je to aplikace, kterou lze spustit na uzlu klastru a kterou lze spravovat jako prostředek klastru, která však nepodporuje použití rozhraní API klastru, a proto neví nic o tomto prostředí. Aplikace nepodporující klastry fungují stále stejně bez ohledu na to, zda pracují na uzlu klastru serverů nebo na systému bez klastrů. Viz také aplikace podporující klastry; uzel.

aplikace podporující klastry**– cluster-aware application**

Aplikace nebo služba, kterou lze spustit na uzlu klastru a kterou lze spravovat jako prostředek klastru. Aplikace podporující klastry používají k příjmu informací o stavu a upozornění od serveru klastru rozhraní API klastru. Viz také API klastru; aplikace nepodporující klastry; uzel.

aplikace systému MS-DOS**– MS-DOS-based application**

Aplikace vytvořená pro prostředí MS-DOS, která proto nemusí využívat všech funkcí Windows 2000.

AppleTalk

Síťová architektura a síťové protokoly počítačů Apple Computer. Jako síť AppleTalk funguje i síť tvořená klientskými Macintoshi a počítačem se systémem Windows 2000 Server s aktivními funkcemi služby Services for Macintosh.

atribut (objekt) – attribute

Ve službě Active Directory je to jedna vlastnost objektu. Objekt je popsán hodnotami

svých atributů. V případě každé třídy objektu schéma definuje, jaké atributy musí nějaká instance dané třídy mít a jaké další atributy může mít.

atributy (soubor) – attributes

Informace indikující, zda je soubor určen pouze pro čtení, skrytý, připravený pro archivaci (zálohování), komprimovaný nebo zašifrovaný a zda se má obsah souboru indexovat v zájmu rychlého vyhledávání.

auditování – auditing

Sledování aktivit uživatelů zaznamenáváním vybraných typů událostí do protokolu zabezpečení serveru nebo pracovní stanice.

automatické použití privátních adres IP**– Automatic Private IP Addressing**

Funkce protokolu TCP/IP systému Windows 2000, která automaticky konfiguruje adresu IP v rozsahu 169.254.0.1 až 169.254.255.254 a masku podsítě o hodnotě 255.255.0.0 v případě, že je protokol TCP/IP nakonfigurován na dynamické adresování a protokol DHCP.

automatizovaná instalace – automated installation

Představuje spuštění bezobslužné instalace některou z metod, jako je služba Remote Installation Services, spustitelné CD a Sysprep.

autonomní systém (AS) – autonomous system

Skupina směrovačů vyměňujících si směrovací informace pomocí společného směrovacího protokolu.

autoritativní – authoritative

V rámci služby DNS jde o využití zón k registraci a překladu názvu domény DNS. Je-li server DNS konfigurován jako hostitel zóny, slouží jako autoritativní pro názvy v rámci této zóny. Serverům DNS je oprávnění udělováno na základě informací uložených v zóně. Viz také zóna.

autoritativní obnovení – authoritative restore

V rámci zálohování je to typ operace obnovení v řadiči domén systému Windows 2000, při němž jsou objekty v obnoveném adresáři považovány za autoritativní a nahradí (prostřednictvím replikace) všechny stávající kopie těchto objektů. Autoritativní obnovení lze použít pouze pro replikovanou stavová data systému, například pro data služby Active Directory či data služby File Replication Service. K provedení autoritativního obnovení je nutné po-

užít nástroj Ntdsutl.exe. Viz také neautoritativní obnovení; stav systému.

autorizace – authorization

V rámci vzdáleného přístupu nebo telefonických připojení je to proces ověřující, zda je pokus o připojení povolený. K autorizaci dochází po úspěšném ověření.

B

b/s – bps

Počet bitů přenesených za sekundu, který slouží jako ukazatel rychlosti, jakou je zařízení, například modem, schopno přenášet data. Jeden znak je tvořen 8 bity. Při asynchronní komunikaci je každý znak uveden start-bitem a ukončen stop-bitem. Pro každý znak je tedy přeneseno 10 bitů. Komunikuje-li například modem rychlostí 2 400 bitů za sekundu (b/s), je každou sekundu odesláno 240 znaků.

balíček – package

Ikona reprezentující vložené nebo propojené informace. Tyto informace mohou obsahovat celý soubor (například rastr programu Malování) nebo část souboru (například buňku tabulky). Pokud vyberete balíček, aplikace použítá k vytvoření tohoto objektu buď objekt přehraje (například zvukový soubor), nebo objekt otevře a zobrazí. Změníte-li původní informace, dojde k automatické aktualizaci propojených informací. Vložené informace je však nutné upravit ručně. V rámci serveru Systems Management Server je to objekt obsahující soubory a instrukce distribuce softwaru na distribuční bod. Viz také vložený objekt; propojený objekt; technologie OLE.

bezestavový – stateless

Ve vztahu k serverům to znamená nezahrnutí aktualizace serverové databáze na základě požadavku klienta. V případě práce se soubory to znamená, že obsah souboru nebyl změněn ani zachycen. U webových serverů je bezestavový požadavek klienta, který mohou členové klastru vyrovnávání zatížení sítě zpracovat, takový požadavek, jenž vrátí klientu statickou webovou stránku.

bezobslužná instalace – Unattended Setup

Automatizovaná, bezobslužná metoda instalace systému Windows 2000. Během instalace používá instalační program k získání potřeb-

ných údajů soubor odpovědí a nepožaduje interaktivní odpovědi od správce.

binární – binary

Numerický systém o základu 2, v němž jsou hodnoty vyjádřeny jako kombinace dvou čísel, 0 a 1.

bit

Nejmenší jednotka informací, kterou jsou počítače schopny zpracovat. Jeden bit představuje binární číslici 1 či 0 neboli logickou podmínku pravda či nepravda. Skupina 8 bitů tvoří jeden bajt, který může reprezentovat různé typy informací, například písmeno abecedy, číslo v desítkové soustavě nebo jiný znak. Zkratka bit byla vytvořena z anglických slov binary digit (binární číslice).

brána – gateway

Zařízení připojené k několika fyzickým sítím TCP/IP, které umožňuje doručovat mezi těmito sítěmi pakety IP. Brány provádějí překlady mezi různými transportními protokoly nebo formáty dat (například IPX a IP) a obecně je možno říci, že se k sítím přidávají právě kvůli možností překladu. Viz také adresa IP; směrovač IP.

brána sítě – network gateway

Zařízení, které připojuje síť používající různé komunikační protokoly tak, aby bylo možné předávat data mezi sítěmi. Brána sítě přenáší informace a převádí je do formy kompatibilní s protokoly používanými v přijímací síti.

BUS

Viz všesměrové vysílání a neznámý server.

C

centrální síťové sídlo – central site

V rámci serveru Systems Management Server jde o hlavní síťové sídlo na vrcholu hierarchie SMS, jemuž všechna ostatní síťová sídla v systému System Management Server hlásí svůj inventář a události.

centrum distribuce klíčů (KDC)

– Key Distribution Center

Síťová služba, která vydává lístky služeb a dočasné klíče používané v protokolu ověření Kerberos. Ve Windows 2000 běží KDC jako privilegovaný proces na všech řadičích domén. Ke správě citlivých informací o účtech

uživatelů, jako jsou například hesla, používá KDC službu Active Directory. Viz také protokol ověření Kerberos; lístek připojení.

certifikační hierarchie – certification hierarchy

Model důvěryhodnosti certifikátů, v jehož rámci jsou cesty k certifikátům vytvářeny navázaním vztahu podřízený/nadřazený mezi certifikačními úřady. Viz také certifikační úřad; cesta k certifikátu.

certifikační úřad (CA) – certification authority

Entita zodpovídající za vytvoření a ručení za pravost veřejných klíčů patřících uživatelům (koncovým entitám) nebo jiným certifikačním úřadům. Mezi aktivity certifikačního úřadu může patřit vazba veřejných klíčů k identifikačním jménům prostřednictvím podepsaných certifikátů, správa pořadových čísel certifikátů a odvolávání certifikátů. Viz také certifikát; veřejný klíč.

certifikační úřad rozlehlé sítě

– enterprise certification authority

Certifikační úřad systému Windows 2000, který je plně integrován do služby Active Directory. Viz také certifikační úřad; samostatný certifikační úřad.

certifikát – certificate

Soubor používaný k ověřování a zabezpečení výměně informací v nezabezpečených sítích, jako je například síť Internet. Certifikát zabezpečeně váže veřejný šifrovací klíč k entitě, která uchovává odpovídající soukromý šifrovací klíč. Certifikáty jsou digitálně podepsány vydávajícím certifikačním úřadem a mohou být použity pro uživatele, počítač nebo službu.

certifikát veřejného klíče – public key certificate

Digitální doklad sloužící jako důkaz identity. Certifikáty veřejných klíčů vydává certifikační úřad (CA). Viz také certifikační úřad; protokol ověření Kerberos.

certifikát X.509v3 – X.509 version 3 certificate

Verze 3 doporučení X.509 organizace ITU-T pro syntaxi a formát. Tento standardní certifikační formát je používán certifikačními procesy systému Windows 2000. Certifikát X.509 obsahuje informace o osobě nebo entitě, které je certifikát vydán, informace o certifikátu a další volitelné informace o certifikačním úřadu, který tento certifikát vydal. Viz také certifikát; veřejný klíč.

cesta – path

Sekvence názvů adresářů (neboli složek) určující umístění adresáře, souboru nebo složky v adresářovém stromu systému Windows. Před každým názvem adresáře nebo souboru musí být znak zpětného lomítka (\). Chcete-li tedy například zadat cestu k souboru pojmenovanému Readme.doc v adresáři Windows na disku C, zapíšete C:\Windows\Readme.doc.

cesta k certifikátu – certification path

Nepřerušovaný řetěz důvěryhodnosti od certifikátu ke kořenovému certifikačnímu úřadu v certifikační hierarchii. Viz také certifikační hierarchie; certifikát.

cestovní profil – roaming profile

Sada uživatelských nastavení na jednom místě serveru umožňující uživateli přesun mezi počítači za současného zachování svého profilu.

cestovní profil uživatele – roaming user profile

Profil uživatele umístěný na serveru, který je při přihlášení uživatele stažen na místní počítač a po odhlášení uživatele aktualizován jak místně, tak na serveru. Cestovní profil uživatele je na serveru k dispozici při přihlášení k libovolnému počítači se systémem Windows 2000 Professional nebo Windows 2000 Server. Uživatel může při přihlášení použít místní profil uživatele, je-li aktuálnější než kopie na serveru.

klastr – cluster

Sada počítačů, které spolupracují při poskytování služby. Použití klastru zvyšuje dostupnost služby a škálovatelnost operačního systému, který tuto službu poskytuje. Služba Vyrovnání zatížení sítě poskytuje softwarové řešení pro podporu klastrů skládajících se z několika počítačů se systémem Windows 2000 Advanced Server, které poskytují síťové služby v rámci sítě Internet a privátních sítí intranet. Viz také dostupnost; škálovatelnost.

klastr serverů – server cluster

Klastr vytvořený a spravovaný službou Cluster Service a dalším softwarem (soubory .exe a .dll), mezi jehož uzly zajišťuje služba Cluster Service podporu trvalé dostupnosti aplikací spuštěných na serverech. Klastr serverů zahrnuje hardware a konfiguraci clusteru stejně jako službu Cluster Service. Viz také klastr; uzel.

klastr vyrovnávání zatížení sítě – network load balancing cluster

Dva až 32 serverů IIS, jejichž jedinou společnou adresu nabízí služba vyrovnávání zatížení sítě webovým klientům, a mezi něž rozdělují přicházející webové požadavky.

Cluster.exe

Alternativní způsob správy klastrů z příkazového řádku systému Windows 2000. Celou řadu úloh správy lze provést voláním programu Cluster.exe z příkazových skriptů. Viz také správce klastru.

částečná linka T1 – fractional T1

Linka T1 skládající se z 23 B-kanálů a jednoho D-kanálu. Jediný D-kanál se používá pro účely časování.

Č**částečná replika – partial replica**

Replika adresářového oddílu určená pouze pro čtení, která obsahuje podmnožinu atributů všech objektů v oddílu. Suma částečných replik v doménové struktuře se označuje za globální katalog. Atributy obsažené v částečné replice jsou ve schématu definovány jako atributy, jejichž objekty attributeSchema mají atribut isMemberOfPartialAttributeSet nastavený na hodnotu PRAVDA. Viz také úplná replika, globální katalog.

čistá instalace – clean installation

Proces instalace operačního systému na čistý neboli prázdný oddíl pevného disku počítače.

čítač výkonnosti – performance counter

V programu sledování systému je to datová položka přidružená k objektu sledování výkonu. Program sledování systému uvádí pro každý vybraný čítač hodnotu odpovídající určitému aspektu výkonnosti definovanému pro objekt sledování výkonu. Viz také objekt sledování výkonu.

členský server – member server

Počítač se systémem Windows 2000 Server, který není řadičem domény Windows 2000. Členské servery jsou účastníky domény, ale neobsahují kopii databáze adresářů. Pro členský server lze nastavit oprávnění týkající se prostředků, která uživatelům umožňují připojit se k serveru a využívat jeho prostředků. Oprávnění k prostředkům lze udělit globálním

skupinám domény a také místním skupinám a uživatelům. Viz také řadič domény; globální skupina; místní skupina.

členství ve skupině – group membership

Skupiny, do nichž patří uživatelský účet. Oprávnění a práva udělená skupině jsou rovněž poskytnuta jejím členům. Ve většině příkazů jsou akce, které uživatel může v systému Windows 2000 provést, určeny členstvím příslušného uživatelského účtu ve skupinách. Viz také skupina.

čtecí zařízení karet Smart Card**– smart-card reader**

Čtecí zařízení instalované na počítačích a umožňující používání karet Smart Card a tedy vyšší úroveň zabezpečení. Viz také karta Smart Card.

databáze WINS – WINS database

Databáze používaná k registrování a překladu názvů počítačů na adresy IP na sítích systému Windows. Obsah této databáze se replikuje v pravidelných intervalech v celé síti. Viz také partnerský server pro nabízenou replikaci; partnerský server pro vyžádanou replikaci; replikace.

D**datagram**

Nepotvrzený paket dat odeslaný na jiné místo sítě. Cílovým místem může být jiné zařízení přímo dosažitelné na místní síti (LAN) nebo vzdálené místo dosažitelné směrovanou dobou přes paketovou přepínanou síť.

DCOM

Viz model DCOM.

dědičnost – inheritance

Schopnost budovat nové třídy objektů na základě již existujících tříd objektů. Nový objekt je definován jako podtřída původního objektu. Původní objekt se stává nadřazenou třídou nového objektu. Podtřída dědí atributy nadřazené třídy, včetně pravidel struktury a pravidel obsahu.

defragmentace – defragmentation

Proces přepisování částí souboru do souvislých sektorů na pevném disku s cílem zvýšit rychlost přístupu a načítání. Při aktualizaci souborů mají počítače tendenci ukládat prove-

dené změny na největší souvislé volné místo na pevném disku, což je zpravidla jiný sektor než pro ostatní části souboru. Jsou-li soubory tímto způsobem fragmentovány, je nutné při každém otevření souboru projít pevný disk a vyhledat všechny části souboru, což zvyšuje dobu odezvy. V rámci služby Active Directory defragmentace mění uspořádání zápisu dat do souboru databáze adresáře a činí jej kompaktnějším. Viz také fragmentace.

delegování – delegation

Schopnost přidělit zodpovědnost za správu části oboru názvů jinému uživateli, skupině nebo organizaci. U služby DNS jde o záznam služby pojmenování v nadřazené zóně, který uvádí pojmenovávací server autoritativní pro delegovanou zónu. Viz také dědičnost; nadřazenost.

démon LPD – Line Printer Daemon

Služba tiskového serveru, která přijímá dokumenty (tiskové úlohy) od nástrojů LPR (Line Printer Remote) spuštěných na systémech klientů. Viz také nástroj LPR.

dešifrování – decryption

Proces přeměny zašifrovaných dat zpět do čitelné podoby. Viz také šifrovaný text; šifrování; prostý text.

detekce chyb – error detection

Technika detekce dat ztracených při přenosu. Umožňuje obnovení ztracených dat, neboť uvědomí vysílající počítač, že je nutné data přenést znovu.

DHCP

Viz protokol DHCP.

dialogové okno – dialog box

Okno zobrazující požadavek na zadání informací nebo o něčem informující. Mnoho dialogových oken má různé prvky, které je zapotřebí vybrat. Pak teprve dokáže systém Windows NT vykonat nějaký příkaz.

digitální certifikát – digital certificate

Viz certifikát.

disk

Zařízení pro fyzické ukládání dat připojené k počítači. Viz také základní disk; dynamický disk.

distribuce balíčku – package distribution

V rámci serveru Systems Management Server je to proces umístění dekomprimovaného ob-

rázku balíčku na distribuční body, sdílení daného obrázku a jeho zpřístupnění klientům. K tomuto procesu dojde, když zadáte distribuční body balíčku.

distribuční bod – distribution point

Na serveru Systems Management Server je to systém sídla s rolí distribučního bodu, který ukládá soubory balíčků přijaté ze serveru sídla. Klienty serveru Systems Management Server kontaktují distribuční bod za účelem získání programů a souborů v okamžiku, kdy detekují dostupnost inzerované aplikace z přístupového bodu klienta.

distribuční složka – distribution folder

Složka vytvořená na distribučním serveru systému Windows 2000, která obsahuje instalační soubory.

distribuovaný protokol DHCP – distributed DHCP

Scénář, v němž jsou adresy IP distribuovány v celé oblasti sídla.

dobu hledání – seek time

Čas nutný k umístění hlavičky disku na správnou část disku, aby mohl být zajištěn přístup k požadovaným datům.

dobu odezvy – response time

Čas potřebný k dokončení práce od jejího započetí. V prostředí klient/server se obvykle měří na straně klienta.

dohoda o připojení – connection agreement

Konfigurovatelná sekce v uživatelském rozhraní ADC obsahující informace, jako jsou názvy serverů kontaktovaných při synchronizaci, třídy objektů určené pro synchronizaci, cílové kontejnery a plán synchronizace. Viz také Active Directory Connector.

dohoda o servisních zásazích**– service level agreement**

Dohoda mezi vaší skupinou IT a uživateli specifikující, jaké úrovně omezení výkonnosti při servisních zásazích jsou přijatelné, například při náhradě zařízení nebo výpadku sítě.

doména – domain

V rámci systému Windows NT a Windows 2000 je to síťová sada počítačů se systémy Windows NT nebo Windows 2000, které sdílejí společnou databázi správce zabezpečení účtů (SAM) a které lze spravovat jako skupinu. Uživatel s účtem v určité doméně se může přihlásit ke svému účtu z libovolného počítače

v doméně. Doména je jedna zabezpečená oblast počítačové sítě systému Windows NT. V případě DNS jde o větev pod uzlem ve stroju DNS.

doména prostředku – resource domain

Doména systému Windows NT 4.0, která obsahuje data účtů pracovních stanic a počítačů s prostředky (například souborové a tiskové servery) přiřazené doméně účtů neboli hlavní doméně. Viz také hlavní doména.

doménová struktura – forest

Kolekce jednoho nebo více stromů služby Active Directory systému Windows 2000, které jsou si rovny a jejichž kořenové domény jsou propojeny obousměrnými tranzitivními vztahy důvěryhodnosti. Všechny stromy v doménové struktuře sdílejí společné schéma, konfiguraci a globální katalog. Obsahuje-li doménová struktura více stromů, tyto stromy netvoří spojitý obor názvů.

domény kombinovaného režimu

– mixed mode domains

Síťová sada počítačů, na nichž je spuštěno více operačních systémů, například jak Windows NT, tak i Windows 2000.

dostupnost – availability

Míra odolnosti počítače a programů proti chybám. Počítače s vysokou dostupností pracují 24 hodin denně 7 dní v týdnu. Viz také odolnost proti chybám.

důvěrnost – confidentiality

Zabezpečovací služba protokolu IP zajišťující pomocí šifrování dat, že se zpráva zobrazí pouze zadaným příjemcům.

důvěryhodná doménová struktura – trusted forest

Doménová struktura připojená k jiné doménové struktuře vztahem explicitní nebo tranzitivní důvěryhodnosti. Viz vztah explicitní důvěryhodnosti; doménová struktura; vztah tranzitivní důvěryhodnosti.

dynamická aktualizace – dynamic update

Aktualizovaná specifikace standardu systému DNS umožňující hostitelům, kteří si ukládají informace o názvech v DNS dynamicky registrovat a aktualizovat své záznamy v zónách spravovaných servery DNS, jež dokáží přijmout a zpracovat zprávy dynamické aktualizace.

dynamické směrování – dynamic routing

Použití protokolů směrování k aktualizaci směrovacích tabulek. Dynamické směrování reaguje na změny v topologii propojení sítí.

dynamický disk – dynamic disk

Fyzický disk, pro jehož správu je používán program Správa disků. Dynamické disky mohou obsahovat pouze dynamické svazky (to znamená svazky vytvořené programem správa disků). Dynamické disky nemohou obsahovat oddíly či logické jednotky a rovněž nejsou přístupné prostřednictvím systému MS-DOS. Viz také dynamický svazek; oddíl.

dynamický svazek – dynamic volume

Logický svazek vytvořený pomocí programu Správa disků. Mezi dynamické svazky patří jednoduché, prokládané, rozložené a zrcadlené svazky a svazky RAID-5. Dynamické svazky lze vytvářet pouze na dynamických discích. Viz také dynamický disk; svazek.

E

emulace místní sítě (LANE) – LAN emulation

Sada protokolů umožňujících použití stávajících síťových služeb ethernet a token ring v síti ATM. Emulace LANE umožňuje spojení mezi stanicemi připojenými k místním sítím a sítím ATM. Viz také režim asynchronního přenosu.

emulátor primárního řadiče domény

– primary domain controller emulator

První řadič domény Windows 2000 vytvořený v doméně. Kromě replikování data domény na další řadiče domén Windows 2000 také emulátor primárního řadiče domény funguje jako primární řadič domény Windows NT v tom smyslu, že vykonává povinnosti primárního řadiče domény včetně replikace dat domény na všechny záložní řadiče domény v doméně. Jestliže dojde k vypnutí emulátoru primárního řadiče domény, může roli emulátoru primárního řadiče domény převzít jiný řadič domény Windows 2000. Viz také primární řadič domény; záložní řadič domény.

emulovaná místní síť (ELAN)

– emulated local area network

Logická síť inicializovaná pomocí mechanismů definovaných emulací LAN. To může zahrnovat ATM a dříve připojené koncové stanice.

export

V systému NFS to znamená zpřístupnit klientu systém souborů serveru, aby se k němu mohl připojit.

externí síťové číslo – external network number

4bajtové hexadecimální číslo, které je používáno pro účely adresování a směrování. Externí síťové číslo je přidruženo k fyzickým síťovým adaptérům a sítím. Počítače v rámci téže sítě používající daný typ rámce musí mít stejné externí síťové číslo, jinak by nemohly vzájemně komunikovat. Všechna externí síťová čísla musí být v rámci propojení sítí IPX jedinečná. Viz také interní síťové číslo; protokol IPX.

externí trasy – external routes

Trasy, které se nenacházejí v rámci autonomního systému OSPF.

extranet

Omezená podmnožina počítačů nebo uživatelů na veřejné síti, obvykle na Internetu, kteří mají přístup k interní síti nějaké organizace. Tyto počítače nebo uživatelé většinou patří do partnerských organizací.

F**filtr – filter**

V rámci protokolu IPSec je to pravidlo umožňující spuštění vyjednávání o zabezpečení komunikace na základě zdroje, cíle a typu provozu IP.

filtrování kláves – FilterKeys

Funkce usnadnění systému Windows 2000 umožňující postiženým lidem nastavit čas reakce klávesnice. Viz také náhodné klávesy; opakování kláves; pomalé klávesy.

filtrování paketů – packet filtering

Zabránění určitým typům síťových paketů v odeslání nebo přijetí. Tuto funkci lze zavést v rámci zabezpečení (zabránění přístupu neoprávněných uživatelů) nebo ke zlepšení výkonosti tím, že se zbytečné pakety nebudou přenášet pomalým spojením. Viz také paket.

filtry – filters

V rámci filtrování paketů protokolů IP a IPX je to řada definic indikujících směrovači typ povoleného a zakázaného provozu na každém rozhraní.

filtry klávesnice – keyboard filters

Speciální časování a další zařízení kompenzující chvění prstů, jejich pomalý pohyb, náhodné stisky kláves a další postižení pohyblivosti.

formát SAMI – Synchronized Accessible Media Interchange

Formát optimalizovaný pro vytváření popisků a zvukových popisů v jediném dokumentu.

formulář – form

Specifikuje velikost papíru (např. A4 nebo letter) přiřazenou podavači v tiskárně. Formulář definuje fyzické charakteristiky, jako je velikost papíru a okraje tiskové oblasti papíru nebo jiného tiskového média.

FORTEZZA

Rodina zabezpečovacích produktů, včetně karet typu PCMCIA, kompatibilních zařízení sériových portů, kombinovaných karet (například FORTEZZA/Modem a FORTEZZA/Ethernet), desek serverů atd. FORTEZZA je registrovaná ochranná známka Národního bezpečnostního úřadu USA.

fragmentace – fragmentation

Rozptýlení jednotlivých částí diskového souboru na různá místa disku. K fragmentaci dochází při odstraňování starých souborů a přidávání nových. Zpomaluje přístup na disk a snižuje celkový výkon diskových operací, ovšem zpravidla nikoli závažně. Viz také defragmentace.

fronta – queue

Seznam programů nebo úloh čekajících na zpracování. V terminologii tisku systému Windows 2000 fronta označuje skupinu dokumentů čekajících na vytištění. V prostředí NetWare a OS/2 tvoří fronty primární softwarové rozhraní mezi aplikací a tiskovým zařízením a uživatelé odesílají dokumenty do fronty. V systému Windows 2000 je tímto rozhraním tiskárna. Dokumenty jsou odesílány na tiskárnu, nikoli do fronty.

FTP

Viz protokol FTP.

funkce IntelliMirror – IntelliMirror

Sada funkcí systému Windows 2000 používaná při změně počítačů a správě konfigurace. Je-li funkce IntelliMirror použita na serveru i klientu, pak data, aplikace a nastavení následují uživatele, když se přesune na jiný počítač.

Správci mohou pomocí funkce IntelliMirror zadávat vzdálené instalace systému Windows 2000.

funkce vizuálního upozornění – SoundSentry

Funkce Windows, která generuje místo zvuku nějaký vizuální efekt, například bliknutí obrazovky nebo blikání záhlaví.

G

gigabitový ethernet – Gigabit Ethernet

Standard sítě ethernet přenášející data rychlostí jedné miliardy bitů za sekundu nebo vyšší.

globálně jednoznačný identifikátor (GUID)

– globally unique identifier

16bajtová hodnota vytvořená z jednoznačného identifikátoru zařízení, aktuálního data a času a pořadového čísla. Identifikátor GUID se používá k identifikaci určitého zařízení nebo komponenty.

globální katalog – global catalog

Služba, která ukládá adresářové informace ze všech zdrojových domén na jediném místě instalacího stromu. Uživatelé mohou globálnímu katalogu předávat dotazy o objektech bez ohledu na jejich logické nebo fyzické umístění. Globální katalog je optimalizován na vysoký výkon při řešení dotazů.

globální skupina – global group

V systému Windows 2000 Server je to skupina, kterou lze používat v její vlastní doméně, na členských serverech a pracovních stanicích domény a v důvěřujících doménách. Na všech těchto místech lze zajistit globální skupině určitá práva a oprávnění a může se stát členem místních skupin. Globální skupina však může obsahovat pouze uživatelské účty z vlastní domény. Viz také skupina; místní skupina.

grafické uživatelské rozhraní (GUI)

– graphical user interface

Formát zobrazení, například systému Windows, představující funkce programů pomocí obrázků, jako jsou tlačítka a ikony. Grafická uživatelská rozhraní umožňují uživatelům vykonávat operace a volit různé funkce ukazováním a klepáním myši.

grafický adaptér – display adapter

Rozšiřující deska, která po zapojení do osobního počítače poskytuje možnosti zobrazení.

Grafické možnosti zobrazení počítače závisejí jednak na logických obvodech (které jsou zajištěny videoadaptérem) a jednak na monitoru. Jednotlivé adaptéry nabízejí několik různých grafických režimů. K dispozici jsou dva základní grafické režimy, text a grafika. V rámci těchto režimů nabízejí některé monitory možnost výběru rozlišení. Při nižším rozlišení je monitor schopen zobrazit více barev. Moderní adaptéry jsou vybaveny pamětí, a díky tomu není pro ukládání obrazu používána paměť RAM počítače. Většina adaptérů je navíc vybavena vlastními grafickými koprocesory pro provádění grafických výpočtů. Pro tyto adaptéry je často používán termín grafické akcelerátory. Viz také síťový adaptér.

H

hardwarový směrovač – hardware router

Směrovač vykonávající směrování jako jedinou funkci, pro níž je speciálně určen. Takový směrovač má specifický hardware vytvořený a optimalizovaný pro směrování.

heslo uživatele – user password

Heslo uložené v jednotlivých uživatelských účtech. Každý uživatel má jedinečné heslo uživatele a toto heslo musí zadat při přihlašování nebo přístupu k serveru.

hierarchická správa úložišť (HSM)

– hierarchical storage management

Technologie automatizující správu úložišť a snižující náklady na úložiště tím, že automaticky přesunuje méně používané soubory z místního úložiště na vzdálené úložiště a přenáší je zpět až v případě potřeby.

hlavní doména – account domain

Doména systému Windows NT, která je používána ke správě účtů uživatelů.

hlavní doména – master domain

Doména systému Windows NT, která je používána ke správě dat účtů uživatelů. Označuje se také za doménu účtů.

hlavní panel – taskbar

Panel, který obsahuje tlačítko Start a podle výchozího nastavení je umístěn v dolní části pracovní plochy. Klepnutím na tlačítka hlavního panelu lze přepínat mezi spuštěnými programy. Hlavní panel lze rovněž skrýt, přesunout na stranu nebo do horní části pracovní plochy

a dalšími způsoby upravit. Viz také plocha; tlačítko hlavního panelu; stavová oblast.

hlavní server – master server

V rámci přenosu zóny DNS je to počítač, který je zdrojem zóny. Hlavní servery mohou být různé a rozdělují se do dvou typů (primární a sekundární hlavní servery) v závislosti na tom, jakým způsobem získávají data zóny. Viz také primární server; sekundární server; zóna; přenos zóny.

hodnota TTL – Time To Live

Hodnota časovače, která je zahrnutá v pakechtech odesílaných sítěmi s podporou protokolu TCP/IP a která udává příjemci, jako dlouho může paket nebo informace v něm obsažené držet nebo používat před vypršením platnosti a zrušením paketu nebo dat. V rámci služby DNS jsou hodnoty TTL používány v záznamech o prostředcích v rámci zóny a určují, jak dlouho by měly klienty uchovávat tyto informace v mezipaměti a používat je, jsou-li uvedeny v odpovědi na dotaz, kterou poskytl server DNS pro tuto zónu.

host – guest

Uživatel služby Services for Macintosh, který nemá uživatelský účet nebo který nezadá heslo. Pokud uživatel počítače Macintosh přidělí oprávnění všem, jsou tato oprávnění dána hostům a uživatelům skupiny.

hostitel – host

Počítač se systémem Windows 2000, v němž je spuštěn serverový program nebo služba používaná síťovými nebo vzdálenými klienty. V rámci služby vyrovnávání zatížení sítě je klastr tvořen několika hostiteli připojenými v místní síti.

Hosts

Soubor obsahující seznam známých adres IP používaný protokolem TCP/IP k vyhledávání počítačů na síti nebo Internetu.

hromadné šifrování – bulk encryption

Proces, při němž jsou velké objemy dat, jako například soubory a zprávy elektronické pošty nebo online komunikační připojení, šifrovány, aby bylo dosaženo důvěrnosti. To se obvykle děje algoritmem symetrického klíče. Viz také šifrování; šifrování symetrickým klíčem.

chyba hardwaru – hardware failure

Chybná funkce nějaké fyzické součásti, například chyba hlavičky pevného disku nebo chyba paměti.

chyba stránky – page fault

Chyba, k níž dojde, když není možné ve fyzické paměti dostupné vykonávanému procesu najít požadovaný kód nebo data.

identifikátor hostitele – host ID

Číslo používané k identifikaci rozhraní na fyzické síti vymezené směrovači. Identifikátor hostitele musí být v síti jednoznačný.

identifikátor sítě – network ID

Číslo používané k identifikaci systémů umístěných na jedné fyzické síti vymezené směrovači. Identifikátor sítě musí být v rámci propojení sítí jednoznačný.

identifikátor zabezpečení (SID) – security identifier

Jednoznačné jméno identifikující uživatele přihlášeného do systému zabezpečení Windows NT nebo Windows 2000. Identifikátor zabezpečení může představovat jednoho uživatele, skupinu uživatelů nebo počítač.

IKE

Viz protokol IKE.

infračervený (IR) – infrared

Světlo, které je v barevném spektru za červenou. Toto záření je pro lidské oko neviditelné, avšak infračervené vysílače a přijímače jsou schopny infračervené signály odesílat a přijímat. Viz také zařízení s možností infračervené komunikace; port pro infračervený přenos; IrDA.

infrastruktura směrování – routing infrastructure

Struktura a topologie propojení sítí.

infrastruktura veřejných klíčů (PKI)**– public key infrastructure**

Termín obecně používaný pro popis zákonů, zásad, standardů a softwaru pro regulaci certifikátů a veřejných a soukromých klíčů a pro práci s nimi. V praxi se jedná o systém digitálních certifikátů, certifikačních úřadů a dalších registračních úřadů, které ověřují platnost jednotlivých účastníků elektronických transakcí. Standardy infrastruktury veřejných klíčů se stále vyvíjejí, přestože jsou v široké míře imple-

mentovány jako nezbytný prvek elektronické komerce.

inovice domény – domain upgrade

Proces náhrady starší verze operačního systému na počítačích v doméně novější verzí systému.

instalace na požádání – on-demand installation

Instalační volba poskytující softwaru kompatibilnímu se systémem Windows 2000 možnost instalovat nové funkce při jejich prvním použití a nikoli v okamžiku instalace celé aplikace.

instalace služeb vzdálené instalace (RISetup.exe)

– Remote Installation Services setup

Součást služeb vzdálené instalace používaná k nainstalování serveru RIS.

instalace systému Windows 2000

– Windows 2000 Setup

Program, který instaluje systém Windows 2000. Také se označuje jako instalační program, Winnt32.exe a Winnt.exe.

instalovat – install

Ve vztahu k softwaru to značí přidat programové soubory a složky na pevný disk a související data do registru, aby software správně fungoval. Instalace není totéž co inovace, při níž jsou stávající programové soubory, složky a položky registru aktualizovány na novější verzi. Ve vztahu k hardwaru to znamená fyzicky připojit zařízení k počítači, zavést do počítače ovladače zařízení a nakonfigurovat vlastnosti a nastavení zařízení. Viz také ovladač zařízení; registr.

integrita – integrity

Vlastnost zabezpečeného protokolu IP, která chrání data před neoprávněnou změnou během přenosu a zajišťuje, že přijatá data jsou přesně daty odeslanými. Každý paket je hašovacími funkcemi podepsán kryptografickým kontrolním součtem, který přijímací počítač ještě před otevřením paketu zkontroluje. Jestliže se paket (a tedy podpis) změnil, paket je ignorován.

Internet

Celosvětové veřejné propojení sítí TCP/IP skládající se z tisíců sítí propojujících výzkumné ústavy, univerzity, knihovny a soukromé společnosti.

interní obor názvů – internal namespace

Privátní obor názvů používaný pouze uživateli v rámci nějaké organizace.

interní síťové číslo – internal network number

4bajtové hexadecimální číslo, které je používáno pro účely adresování a směrování. Interní síťové číslo identifikuje virtuální síť v rámci počítače. Interní síťové číslo musí být v rámci propojení sítí IPX jedinečné. Pro interní síťové číslo je rovněž používán termín virtuální síťové číslo. Viz také externí síťové číslo; protokol IPX.

interval aktualizace – refresh interval

V rámci DNS je to 32bitový časový interval určující, jak často se mají data zóny aktualizovat. Po vypršení intervalu aktualizace sekundární hlavní server zkontroluje, zda jsou data zóny dosud aktivní nebo zda je nutná jejich aktualizace pomocí přenosu zóny. Tento interval je pro jednotlivé zóny nastaven v záznamu SOA (start-of-authority). Viz také záznam o prostředku; sekundární server; záznam SOA; zóna; přenos zóny.

interval vypršení platnosti – expire interval

V rámci služby DNS je to počet sekund, které servery DNS fungující jako sekundární hlavní servery pro zónu použijí k určení, zda platnost dat zóny bude ukončena, pokud zóna není aktualizována a obnovena. Viz také zóna.

intranet

Síť v rámci nějaké organizace používající internetové technologie a protokoly, dostupná je však jen určitým osobám, například zaměstnancům společnosti. Intranet se také označuje za privátní (soukromou) síť.

inventář – inventory

Informace o každém klientu v sídle sbírané agenty klienta inventáře serveru Systems Management Server. Inventář může v závislosti na konfiguraci definované správcem zahrnovat informace o hardwaru i softwaru a další soubory.

inventář hardwaru – hardware inventory

Automatizovaný proces používaný serverem Systems Management Server k získávání podrobných informací o hardwaru používaném na klientských počítačích v sídle Systems Management Server.

inzerování – advertisement

V serveru System Management Server jde o oznámení odeslané serverem sídla na body klientského přístupu (CAP) říkající, že klienty mohou používat program distribuce softwaru.

inzerovat – advertise

V serveru System Management Server to znamená učinit program dostupným členům nějaké kolekce (skupiny).

IPSec

Viz zabezpečený protokol IP

IrDA – Infrared Data Association

Síťový protokol používaný pro přenos dat vytvořených zařízeními s možností infračervené komunikace. IrDA je také organizace výrobců počítačů, součástí a telekomunikačních zařízení, která definuje standardy pro infračervenou komunikaci mezi počítači a periferními zařízeními, například tiskárnami. Viz také infračervený; zařízení s možností infračervené komunikace; port pro infračervený přenos.

J**jazyk HTML – Hypertext Markup Language**

Jednoduchý kódový jazyk sloužící k vytváření hypertextových dokumentů, které lze přenášet mezi platformami. Soubory HTML jsou jednoduché textové soubory ASCII, v nichž jsou vloženy kódy (speciální značky) určující formátování a hypertextové odkazy. Kód HTML se používá k formátování dokumentů na síti World Wide Web.

jazyk PCL – printer control language

Jazyk popisu stránek vyvinutý společností Hewlett Packard pro laserové a inkoustové tiskárny. Tento jazyk se vzhledem k rozšíření laserových tiskáren stal standardem pro celou řadu tiskáren. Viz také jazyk PDL; jazyk PostScript.

jazyk PDL – page-description language

Počítačový jazyk popisující uspořádání textu a obrázku na tištěné stránce. Viz také jazyk PCL; jazyk PostScript.

jazyk PostScript – PostScript

Jazyk popisu stránek vyvinutý společností Adobe Systems pro tisk na laserových tiskárnách, který umožňuje pružnou práci s písmy a nabízí grafiku ve vysoké kvalitě. Jazyk PostScript je standardem v oblasti DTP, neboť je podporován osvitovými jednotkami, zařízeními pro tisk ve vysokém rozlišení používanými v prostředí komerčních tiskáren. Viz také jazyk PCL; jazyk PDL.

jazyk SQL – Structured Query Language

Široce používaný standardní databázový podjazyk využívaný v dotazování, aktualizování a správě relačních databází.

jediný bod chyby – single point of failure

Libovolná komponenta v prostředí, která při své poruše způsobí zablokování dat nebo aplikací.

jednosměrové vysílání – unicast

Adresa specifikující určitého globálně jedinečného hostitele.

jednotka DFS domény – domain-based Dfs

Implementace jednotky DFS, v jejímž rámci jsou konfigurační informace jednotky DFS uloženy v adresáři služby Active Directory. Vzhledem k tomu, že tyto informace jsou k dispozici ve všech řadičích v rámci domény, poskytuje jednotka DFS domény odolnost proti chybám pro libovolný distribuovaný systém souborů v doméně. Kořenový adresář jednotky DFS domény má následující charakteristiky: musí být hostem na členském serveru domény, jeho topologie se automaticky publikuje do služby Active Directory, může mít sdílené složky na kořenové úrovni a podporuje replikaci kořenové složky a souborů pomocí systému FRS

název komitenta zabezpečení**– security principal name**

Název jednoznačně identifikující uživatele, skupinu nebo počítač v rámci jedné domény. Není zaručena jedinečnost tohoto názvu v rámci více domén. Viz také komitent zabezpečení.

K**kabelový modem – cable modem**

Modem poskytující širokopásmový přístup k Internetu v rozsahu 10 až 30 Mb/s.

karta PC – PC Card

Vyměnitelné zařízení, velikosti zhruba platební karty, které lze připojit do slotu PCMCIA (Personal Computer Memory Card International Association) v přenosném počítači. Mezi zařízení PCMCIA patří modemy, síťové karty a jednotky pevného disku.

karta Smart Card – smart card

Zařízení velikosti platební karty, které se používá s číslem PIN a umožňuje ověření na zá-

kladě certifikátu a jediného přihlášení. Tyto karty slouží k zabezpečenému ukládání certifikátů, veřejných a soukromých klíčů, hesel a dalších typů osobních informací. Chcete-li používat kartu Smart Card, musíte mít k dispozici čtecí zařízení karet Smart Card připojené k počítači. Viz také ověření; čtecí zařízení karet Smart Card.

kategorie každý – everyone category

V prostředí systému Macintosh je to jedna z uživatelských kategorií, jíž je přiřazeno povolení přístupu k nějaké složce. Povolení vydaná v kategorii každý platí pro všechny uživatele používající server, včetně hostů.

klávesnice Dvorak – Dvorak keyboard

Alternativní klávesnice s takovým rozmístěním, které usnadňuje používání nejčastěji zapisovaných znaků lidem, kteří mají problémy s psaním na standardní klávesnici.

klávesové zkratky – hot keys

Funkce Windows 2000 umožňující rychlou aktivaci určitých funkcí usnadnění použitím kombinací současně stisknutých kláves.

klávesy jedním prstem – StickyKeys

Funkce usnadnění zabudovaná do systému Windows, která zajišťuje aktivní stav kláves Shift, Ctrl a Alt po stisku a uvolnění, takže není nutné tisknout více kláves najednou. Tato funkce zpřístupňuje přepínací tlačítka i uživatelům, kteří nedokáží stisknout více kláves najednou.

klávesy po sobě – SerialKeys

Funkce Windows používající zařízení rozhraní pomocné komunikace a umožňující příjem stisknutých kláves a pohybu myši přes sériový port počítače.

klíč – key

Tajný kód neboli číslo potřebné ke čtení, úpravě nebo ověření zabezpečených dat. Klíče se používají ve spojení s algoritmy zabezpečení dat. O vytváření klíčů se automaticky stará systém Windows 2000. V případě registru je klíč zadán v registru, které může obsahovat podklíče i položky. Ve struktuře registru klíče odpovídají složkám a položky souborům.

V okně Editoru registru se klíč zobrazuje jako složka v levém podokně. V rámci souboru odpovědi jsou klíče řetězce znaků určující para-

metry, které instalační program potřebuje pro bezobslužnou instalaci operačního systému.

klíč propojení – session key

Klíč používaný především k šifrování a dešifrování. Klíče propojení se obvykle používají v symetrických šifrovacích algoritmech, kde se pro zašifrování i dešifrování používá stejný klíč. Z tohoto důvodu obvykle označení klíč propojení a symetrický klíč označují stejný typ klíče. Viz také symetrické šifrování.

klíč registru – registry key

Identifikátor záznamu nebo skupiny záznamů v registru.

klient – client

Libovolný počítač nebo program připojující se k jinému počítači nebo programu a požadující od něj nějaké služby. Viz také server.

klient emulace LAN (LEC) – LAN emulation client

Klient v síti ELAN, který provádí předávání dat, překlad adresy a další řídicí funkce. Klient LEC je umístěn na koncových stanicích sítě ELAN. Viz také režim asynchronního přenosu; emulovaná místní síť; emulace místní sítě.

klient VPN – VPN client

Počítač iniciující připojení VPN k serveru VPN. Klientem VPN může být jednotlivý počítač, který získá připojení VPN vzdáleného přístupu, nebo směrovač, který získá připojení VPN mezi směrovači.

knihovna DLL – dynamic-link library

Funkce operačního systému Microsoft Windows a OS/2, která umožňuje uložit spustitelné rutiny do samostatných souborů s příponou DLL (tyto rutiny obvykle slouží jako specifické funkce nebo sada funkcí). Knihovny DLL jsou zavedeny pouze v případě, že je vyžaduje program, který je volá.

kód Unicode – Unicode

16bitový standard kódování znaků, který je schopen představovat písmena a znaky většiny světových jazyků. Kód Unicode byl vyvinut sdružením amerických počítačových společností.

kolekce – collection

V případě serveru Systems Management Server jde o sadu prostředků v sídle definovanou pravidly členství. Kolekce se používají k distribuci softwaru, zobrazení inventáře na klien-

tech a pro přístup ke klientům za účelem vzdáleného připojení nástrojů.

kombinovaný režim – mixed mode

Výchozí nastavení režimu domény v řadičích domén systému Windows 2000. Kombinovaný režim umožňuje, aby v jedné doméně existovaly záložní řadiče domény pro systémy Windows NT a Windows 2000 současně. Kombinovaný režim nepodporuje vylepšení univerzálních a vnořených skupin systému Windows 2000. Nastavení režimu domény lze změnit na nativní režim systému Windows 2000, jsou-li z domény odstraněny všechny řadiče domén systému Windows NT nebo jsou-li aktualizovány na Windows 2000. Viz také nativní režim.

komitent zabezpečení – security principal

Entita systému Windows 2000, které je automaticky přiřazen identifikátor zabezpečení pro přístup k prostředkům. Komitentem zabezpečení může být uživatel, skupina nebo počítač. Systém Windows 2000 používá ke správě účtů uživatelů a komitentů zabezpečení službu Active Directory. Viz také jméno komitenta zabezpečení.

koncové šifrování – end-to-end encryption

Šifrování dat mezi klientskou aplikací a serverem, který hostí prostředek nebo službu, k níž klientská aplikace přistupuje.

kontext zabezpečení – security context

Atributy nebo pravidla zabezpečení, která právě platí. Například pravidla řídící, co může uživatel dělat s chráněným objektem, jsou určena informacemi zabezpečení v tokenu přístupu uživatele a v popisovači zabezpečení objektu. Token přístupu a popisovač zabezpečení společně tvoří kontext zabezpečení akcí uživatele s objektem. Viz také token přístupu; popisovač zabezpečení.

konvergence – convergence

Proces stabilizace systému po provedení změn v síti. Pokud v případě směřování přestane být určitá trasa k dispozici, směrovače odešlou propojením sítí aktualizací zprávy, které znovu vytvoří informace o upřednostňovaných trasách. V rámci služby vyrovnávání zatížení sítě je konvergence proces, jehož prostřednictvím si hostitelé služby vyrovnávání zatížení sítě vyměňují zprávy s cílem určit nový, konzistentní stav klastru a zvolit hostitele s nejvyšší prioritou, tzv. výchozího hostitele. V průběhu

konvergence je pro hostitele sdílející zpracování provozu v síti pro specifické porty TCP či UDP určena nová distribuce zatížení. Viz také klastr; výchozí hostitel; hostitel; protokol UDP.

konzola MMC – Microsoft Management Console

Rámec pro hoštění konzol správy. Konzola je definována položkami svého stromu konzoly, což mohou být složky nebo další kontejnery, webové stránky a další nástroje pro správu. Konzola má jedno nebo více oken poskytujících zobrazení stromu konzoly a vlastností, služeb a událostí správy, které vyplývají ze stromu konzoly. Hlavní okno MMC poskytuje příkazy a nástroje pro vytváření obsahu konzoly. Je-li konzola v uživatelském režimu, tyto funkce konzoly MMC a vlastní strom konzoly mohou být skryté. Viz také strom konzoly.

konzoly – consoles

Rámec pro hoštění nástrojů správy v konzole Microsoft Management Console (MMC). Konzola je definována položkami svého stromu konzoly, což mohou být složky nebo jiné kontejnery, webové stránky a další nástroje pro správu. Konzola má okna poskytující zobrazení stromu konzoly a vlastností, služeb a událostí správy, které vyplývají z položek stromu konzoly.

kořen – root

Nejvyšší úroveň v hierarchicky uspořádané sadě informací. Kořen je místem, z něhož jsou v logické posloupnosti rozvětveny další dílčí sady, které představují bližší a podrobnější pohled.

kořenová doména – root domain

Začátek oboru názvů systému DNS. V rámci Active Directory je to počáteční doména ve stromu Active Directory. Zároveň je to počáteční doména doménové struktury.

kořenová složka systému – systemroot

Cesta a název složky, v níž jsou umístěny systémové soubory Windows 2000. Zpravidla se jedná o složku C:\Winnt, ovšem při instalaci systému Windows 2000 lze určit jinou jednotku či složku. K nahrazení aktuálního umístění složky obsahující systémové soubory systému Windows 2000 můžete použít hodnotu %systemroot%. Chcete-li určit kořenovou složku systému, klepněte na tlačítko Start, klepněte na příkaz Spustit a pak zadejte příkaz %systemroot%.

kořenový adresář jednotky DFS – DFS root

Sdílená součást Server Message Block na vrcholu topologie jednotky DFS, která je počátečním bodem propojení a sdílených souborů vytvářejících obor názvů DFS. Kořenový adresář jednotky DFS lze definovat (pro operace s doménami) na úrovni domény nebo (pro samostatné operace) na úrovni serveru. Systémy DFS vycházející z domén mají v doméně více kořenových adresářů, ale jen jeden kořenový adresář na každém serveru.

kořenový certifikační úřad**– root certification authority**

Certifikační úřad, který je v certifikační hierarchii na nejvyšší úrovni a požívá nejvyšší důvěry. Kořenový certifikační úřad má certifikát podepsaný sám sebou. Viz také certifikační úřad; cesta k certifikátu; certifikační hierarchie.

kořenový certifikát – root certificate

Certifikát certifikačního úřadu, který je podepsaný sám sebou. Je pro něj používán termín kořenový certifikát, protože je certifikátem pro kořenový certifikační úřad. Kořenový certifikační úřad musí podepsat vlastní certifikát, protože podle definice v certifikační hierarchii již neexistuje certifikační úřad vyšší úrovně. Viz také certifikát; certifikační úřad; kořenový certifikační úřad.

kryptografie – cryptography

Postupy a umění uchovávání zabezpečených zpráv a dat. Kryptografie slouží k zajištění čtyř hlavních funkcí zabezpečení informací: důvěrnosti, integrity, ověřování a neodvolatelnosti. Viz také důvěrnost; integrita; ověření; neodvolatelnost.

kvóta disku – disk quota

Maximální množství diskového prostoru dostupného uživateli.

L**L2PT**

Viz protokol Layer 2 Tunneling Protocol.

latence – latency

Viz latence replikace.

latence replikace – replication latency

V rámci replikace služby Active Directory je to zpoždění mezi dobou, kdy je provedena aktualizace dané repliky adresářového oddílu, a dobou, kdy je tato aktualizace provedena

v jiné replice stejného adresářového oddílu. Pro latenci je někdy rovněž používán termín zpoždění šíření. Viz také replikace.

LDAP

Viz protokol LDAP.

lístek propojení – session ticket

Informace předkládaná klientem službě v protokolu ověření Kerberos. Protože se lístky propojení používají k získání ověřených připojení ke službám, někdy se také označují termínem lístky služeb. Viz také protokol ověření Kerberos; centrum distribuce klíčů.

lístek služby – service ticket

Viz lístek propojení.

logická jednotka – logical drive

Svazek vytvořený v rámci rozšířeného oddílu na základním disku. Logickou jednotku lze formátovat a lze jí přiřadit písmeno jednotky. Logické jednotky mohou být obsaženy pouze na základních discích a nemohou zasahovat do několika disků. Viz také základní disk; základní svazek; rozšířený oddíl.

logická podsít' protokolu IP – logical IP subnet

Skupina hostitelů/členů IP, kteří patří do téže podsítě protokolu IP a jejichž adresa ATM hostitelského serveru ATMAPR je stejná.

logická tiskárna – logical printer

Softwarové rozhraní mezi operačním systémem a tiskárnou v systému Windows 2000. Zatímco tiskárna je zařízení provádějící vlastní tisk, logická tiskárna je jeho softwarové rozhraní na tiskovém serveru. Toto softwarové rozhraní určuje, jak je tisková úloha zpracována a jak je směrována na cíl (na místní nebo síťový port, do souboru nebo na vzdálenou sdílenou tiskárnu). Dokument je před skutečným odesláním na tiskárnu zařazen (neboli uložen) na logickou tiskárnu.

M**maska podsítě – subnet mask**

32bitová hodnota vyjádřená jako čtyři desítková čísla od 0 do 255 oddělená tečkami (například 255.255.0.0). Toto číslo umožňuje protokolu TCP/IP odlišit část identifikátoru sítě adresy IP od části identifikátoru hostitele. Identifikátor hostitele identifikuje jednotlivé počítače na síti. Hostitelé TCP/IP používají

masku podsítě k určení, zda se cílový hostitel nachází na místní nebo vzdálené síti.

metoda zabezpečení – security method

Proces určující služby zabezpečení, nastavení klíčů a algoritmy protokolu IP používané k ochraně dat během komunikace.

metrika – metric

Číslo indikující náklady trasy ve směrovací tabulce IP. Je tak možné vybrat si nejlepší z několika možných tras ke stejnému cíli.

mezipaměť – cache

Pro servery DNS a WINS je to místní úložiště záznamů o prostředcích pro nedávno přeložené názvy vzdálených hostitelů. Mezipaměť je obvykle vytvářena dynamicky v průběhu dotazování a překládání názvů. Pomáhá rovněž k optimalizaci času nutného k překládání požadovaných názvů. Viz také soubor mezipaměti; služba pojmenování; záznam o prostředku.

mezipaměť ARP – ARP cache

Tabulka adres IP a jim odpovídajících adres řízení přístupu k médiím. Každé rozhraní má samostatnou mezipaměť ARP.

migrace – migration

Proces kopírování objektu z místního úložiště na vzdálené úložiště.

migrace domény – domain migration

Proces přesunu účtů, prostředků a jim přiřazených zabezpečených objektů z jedné doménové struktury do druhé.

migrovat – migrate

Proces přechodu souborů nebo programů ze staršího systému souborů nebo protokolu na aktuálnější formát nebo protokol. Například databázové položky WINS lze převést ze statických databázových položek WINS na dynamicky registrované položky DHCP.

minimální délka hesla – minimum password length
Nejmenší počet znaků, které může heslo obsahovat.

minimální hodnota TTL – minimum TTL

Výchozí hodnota TTL (Time-To-Live) nastavená v sekundách, která je určena pro všechny záznamy o prostředcích v zóně. Tato hodnota je pro jednotlivé zóny nastavena v záznamu SOA (start-of-authority). Podle výchozího nastavení server DNS zahrnuje tuto hodnotu do odpovědi na dotazy a informuje tak příjemce,

jak dlouhou dobu mohou mít záznamy o prostředcích poskytnuté touto odpovědí uloženy v mezipaměti, než platnost dat těchto záznamů vyprší. Jsou-li hodnoty TTL nastaveny pro jednotlivé záznamy o prostředcích, přepíše tyto hodnoty minimální hodnotu TTL. Viz také hodnota TTL.

minimální verze instalačního programu

– Mini-Setup Wizard

Průvodce, který se rozběhne po prvním spuštění počítače z duplikovaného pevného disku. Průvodce zjistí všechny informace potřebné pro nově duplikovaný disk.

místní počítač – local computer

Počítač, k němuž jste právě přihlášení jako uživatelé. Obecněji je možné říci, že místní počítač je počítač, k němuž je možný přímý přístup bez použití komunikační linky nebo komunikačního zařízení, jako je síťová karta nebo modem. Podobně spuštění místního programu znamená spuštění programu na místním počítači (protikladem je spuštění ze síťového serveru).

místní síť (LAN) – LAN

Skupina počítačů, tiskáren a dalších zařízení umístěných v relativně omezené oblasti (například v budově), jež je propojená komunikačními linkami a umožňuje vzájemnou interakci jednotlivých zařízení v síti. Viz také rozsáhlá síť.

místní skupina – local group

Pro počítače se systémem Windows 2000 Professional a členské servery je to skupina, které lze udělit oprávnění a práva z vlastního počítače pouze k těm zdrojům na počítači, na němž je skupina vytvořena. Viz také globální skupina.

místní skupina domény – domain local group

Skupina Windows 2000 dostupná pouze v doménách pracujících v nativním režimu, která může obsahovat členy z libovolného místa doménové struktury, důvěryhodných doménových struktur a důvěryhodných domén s jinými systémy, než jsou Windows 2000. Místní skupina domény může zajistit oprávnění ke zdrojům v doméně, v níž existuje. Místní skupiny domény se obvykle používají k seskupení komitentů zabezpečení z celé doménové

struktury, aby bylo možné řídit přístup ke zdrojům v doméně.

místní tiskárna – local printer

Tiskárna, která je připojena přímo k jednomu z portů v počítači.

místní úložiště – local storage

V rámci systému Windows 2000 Server je to diskový svazek se systémem souborů NTFS, který slouží jako primární úložiště dat. Tyto diskové svazky mohou být spravovány programem Vzdálené úložiště, a to zkopírováním souborů s nízkou četností přístupu do vzdáleného (sekundárního) úložiště. Viz také vzdálené úložiště.

místo vložení – insertion point

Místo, kam se vloží text po zápisu na klávesnici. Místo vložení je obvykle v okně aplikaci nebo v dialogovém okně označeno blikající svislou čarou.

MMC

Viz konzola MMC.

mobilní uživatel – mobile user

Uživatel, který se pohybuje mimo rámec (budovu) organizace, jako je třeba prodejce nebo technik.

model COM – Component Object Model

Objektový programovací model vytvořený v zájmu podpory vzájemné využitelnosti softwaru. Model COM umožňuje dvěma nebo více aplikacím či komponentám jednoduše spolupracovat, i když byly vytvořeny různými producenty, v různých okamžicích, v různých programovacích jazycích nebo jsou-li spuštěny na jiných počítačích s různými operačními systémy. Model COM je základní technologií, na které lze stavět další technologie. Technologie společnosti Microsoft propojování a vkládání objektů (OLE) a ActiveX jsou vytvořeny na základě modelu COM.

model DCOM – Distributed Component Object Model

Specifikace Microsoft COM definující, jak komponenty komunikují na sítích systému Windows. K integraci aplikací klient/server na více počítačích použijte nástroj DCOM Configuration. Model DCOM lze také použít k integraci robustních aplikací webových prohlížečů. Viz také nástroj DCOM Configuration.

modul – module

Komponenta operačního systému Windows 2000, která sama jako jediná zodpovídá za své funkce. Aplikace běží v uživatelském režimu v samostatném modulu, odkud požaduje služby systému. Procesy aplikace se přenášejí do jednoho nebo více modulů v režimu jádra (chráněném), kde dojde k vlastnímu poskytnutí služby.

modul snap-in – MMC snap-in

Typ nástroje, který lze přidat do stromu konzoly podporované konzolou MMC (Microsoft Management Console), například správce zařízení. Modul snap-in může být samostatný nebo rozšiřující. Samostatný modul snap-in lze přidat odděleně, rozšiřujícím modulem snap-in lze pouze rozšířit funkce jiného modulu snap-in. Viz také konzola MMC.

myš klávesnicí – MouseKeys

Funkce systému Microsoft Windows umožňující používat k pohybu kurzorem myši numerickou klávesnici.

N**nadřazená doména – parent domain**

V rámci služby DNS a Active Directory jsou to domény, které jsou ve stromu oboru názvů umístěny přímo nad ostatními odvozenými doménami (podřízené domény). Například doména „microsoft.com“ je nadřazenou doménou pro doménu „example.microsoft.com“, což je doména podřízená. Viz také podřízená doména; doména; adresářový oddíl.

nadřazenost – parenting

Koncepce správy růstu a delegování nadřazené domény do dalších podřízených domén, které jsou delegovány a odvozeny od názvu nadřazené domény. Viz také podřízená doména; nadřazená doména.

nadřazený objekt – parent object

Objekt, v němž je umístěn jiný objekt. Nadřazený objekt implikuje relaci. Příkladem nadřazeného objektu je složka, v níž je umístěn soubor neboli podřízený objekt. Objekt může být současně objektem podřízeným i nadřazeným. Viz také podřízený objekt; objekt.

náhodné klávesy – BounceKeys

Filtr klávesnice pomáhající uživateli, náhodně nebo opakovaně tisknou klávesy.

náklady – cost

Bezrozměrná jednotka konfigurovaná na směrovačích OSPF indikující přednost použití určitého propojení.

nalezení – discovery

Proces, kterým se služba přihlášení do sítě systému Windows 2000 pokusí vyhledat řadič domény se systémem Windows 2000 Server v důvěryhodné doméně. Jakmile je řadič domény nalezen, použije se pro následné ověření účtu uživatele. V případě protokolu SNMP je dynamické nalezení identifikací zařízení připojených k síti SNMP.

nástroj ClonePrincipal – ClonePrincipal

Nástroj umožňující postupný přechod uživatelů do prostředí systému Windows 2000, aniž by to mělo vliv na existující prostředí Windows NT.

nástroj DCOM Configuration – DCOM Configuration tool

Nástroj systému Windows NT Server, který lze použít k nakonfigurování 32bitových aplikací na síťovou komunikaci DCOM. Viz také model DCOM.

nástroj LPR – Line Printer Remote

Nástroj umožňující připojení, který je spuštěn na klientských systémech a slouží k tisku souborů do počítače se serverem LPD. Viz také démon LPD.

nástroj sledování prostředků – Resource Monitor

Součást softwaru klastru, která spravuje komunikaci mezi klastrem serverů uzlu a jedním nebo více příslušnými prostředky. Viz také uzel; prostředek.

nástroj WinInstall LE – WinInstall LE

Nástroj úpravy balíčků, který je součástí systému Windows 2000 Server.

nástroje hlasového vstupu – voice input utilities

Typ programu pro rozpoznávání řeči, který umožňuje postiženým uživatelům ovládat počítač místo myši nebo klávesnicí vlastním hlasem.

nativní režim – native mode

Stav, kdy všechny řadiče domén v doméně byly inovovány na systém Windows 2000 a správce nastavil provoz v nativním režimu (prostřednictvím programu Uživatelé a počítače služby Active Directory). Viz také kombinovaný režim.

název domény – domain name

V rámci systému Windows 2000 a služby Active Directory je to název přidělený správcem kolekci síťových počítačů, které sdílejí společný adresář. V rámci služby DNS slouží jako názvy domén specifické názvy uzlů ve stromu oboru názvů DNS. Názvy domén DNS používají singulární názvy uzlů, takzvaná „označení“, které jsou spojeny tečkami (.) označujícími jednotlivé úrovně uzlů v oboru názvů. Viz také služba DNS; obor názvů.

název hostitele – host name

Název počítače v síti. V rámci sady Resource Kit systému Windows 2000 Server se název hostitele používá jako odkaz na první označení úplného doménového názvu. Viz také soubor Hosts.

název počítače – computer name

Jednoznačný název skládající se až z 15 znaků velkých písmen, který identifikuje počítač v síti. Tento název se nesmí shodovat s názvem jiného počítače nebo domény v síti.

název sítě – network name

V rámci klastru serverů je to název, kterým klienty přistupují k prostředkům klastru serverů. Název sítě se podobá názvu počítače. Je-li zahrnut do skupiny prostředků s nějakou adresou IP a umožněným přístupem klientů, pak představuje pro klienty virtuální server.

název služby – service name

Název, pod kterým je port znám.

název systému NetBIOS – NetBIOS name

Název rozpoznaný systémem WIS, který přeloží název na adresu IP.

název UNC – UNC name

Plný název prostředku v síti používaný systémem Windows 2000. Odpovídá syntaxi \\název_serveru\název_sdílené_položky, kde název_serveru je název serveru a název_sdílené_položky je název sdíleného prostředku. Názvy adresářů nebo souborů v konvenci UNC mohou rovněž v rámci názvu sdílené položky obsahovat název adresáře, a to s následující syntaxí: \\název_serveru\název_sdílené_položky\adresář\název_souboru.

názvový server – name server

V rámci modelu klient/server služby DNS jde o server obsahující informace o části databáze DNS. Server zpřístupňuje klientům, jež přes

Internet nebo intranet požadují překlad názvů, názvy počítačů a další informace. Viz také systém DNS.

neautoritativní obnovení – nonauthoritative restore

Obnovení záložní kopie řadiče domény Windows 2000, v jehož rámci nejsou objekty v obnoveném adresáři považovány za autoritativní. Obnovené objekty jsou aktualizovány změnami uloženými v ostatních replikách obnovené domény. Viz také autoritativní obnovení.

nejvyšší stáří hesla – maximum password age

Doba, po níž může být používáno heslo, aniž by systém od uživatele požadoval změnu hesla.

neodvolatelnost – nonrepudiation

Základní funkce zabezpečení kryptografie. Neodvolatelnost zaručuje, že žádná z komunikujících stran nemůže nepravdivě popřít, že došlo k určitému úseku komunikace. Bez principu neodvolatelnosti by někdo mohl komunikovat a později celou komunikaci popřít nebo tvrdit, že k ní došlo v jiném okamžiku. Viz také kryptografie; ověření; důvěrnost; integrita.

nepřerušitelný zdroj napájení (UPS) – uninterruptible power supply

Zařízení připojené mezi počítač a zdroj napájení s cílem zajistit, aby dodávka elektrické energie byla plynulá. Zařízení UPS používají baterie, aby po určitou dobu po přerušení dodávky energie udržely počítač v chodu. Zařízení UPS obvykle rovněž poskytují ochranu proti výkyvům a poklesům napájení.

nepřirazené místo – unallocated space

Dostupné místo na disku, které není přiřazeno žádnému oddílu, logické jednotce ani svazku. Typ objektu vytvořeného na volném místě závisí na typu disku (základní nebo dynamický). V případě základních disků lze volné místo mimo oddíly použít k vytvoření primárních nebo rozšířených oddílů. Volné místo v rámci rozšířeného oddílu lze použít k vytvoření logické jednotky. U dynamických disků lze volné místo použít k vytvoření dynamických svazků. Na rozdíl od základních disků se přesná používaná oblast disku při vytváření svazku nezadáva. Viz také základní disk; dynamický disk; rozšířený oddíl; logická jednotka; oddíl; primární oddíl; svazek.

Netdom

Nástroj umožňující správu domén a vztahů důvěryhodnosti Windows 2000 z příkazového řádku.

NetWare

Síťový operační systém společnosti Novell.

NNTP

Viz protokol NNTP.

O

obecná služba QoS – generic Quality of Service

Metoda, s jejíž pomocí mohou sítě TCP/IP zaručit služby Quality of Service pro multimediální aplikace. Obecná služba QoS přiřazuje spojením různé šířky pásem na základě jejich potřeb.

objekt – object

Entita, například soubor, složka, sdílená složka nebo objekt služby Active Directory, popsaná samostatnou pojmenovanou sadou atributů. Například mezi atributy objektu File patří název, umístění a velikost souboru, mezi atributy objektu Active Directory User může patřit jméno a příjmení uživatele a jeho elektronická adresa. V rámci technologií OLE a ActiveX může objektem být libovolná informace, kterou lze propojit či vložit do jiného objektu. Viz také atribut; objekt kontejneru; objekt jiného typu než kontejner; podřízený objekt; nadřazený objekt.

objekt jiného typu než kontejner

– noncontainer object

Objekt, který nemůže logicky obsahovat jiné objekty. Tímto typem objektu je například soubor. Viz také objekt kontejneru; objekt.

objekt kontejneru – container object

Objekt, který může logicky obsahovat další objekty. Příkladem objektu kontejneru je složka. Viz také objekt jiného typu než kontejner; objekt.

objekt sledování výkonu – performance object

V programu sledování výkonu je to logická kolekce čítačů přidružených k prostředku nebo službě, které lze sledovat. Viz také čítač výkonnosti.

objekt zásad skupiny – Group Policy object

Kolekce nastavení zásad skupiny. Objekty zásad skupiny jsou v podstatě dokumenty vytvo-

řené modulem snap-in zásady skupiny. Objekty zásad skupiny jsou uloženy na úrovni domény a mají vliv na uživatele a počítače, kteří jsou součástí sídel, domén a organizačních jednotek. Každý počítač se systémem Windows 2000 má navíc místně uloženou právě jednu skupinu nastavení, pro niž je používán termín místní objekt zásad skupiny.

objekty účtu počítače – computer account objects

Objekty používané k identifikaci určitého účtu počítače v systémech Windows NT 4.0 Server nebo Windows 2000 Server.

objekty uživatelských účtů – user account objects

Objekty používané k identifikaci účtu určitého uživatele v systémech Windows NT Server a Windows 2000 Server.

oblast – area

Skupina souvislých sítí v autonomním systému OSPF. Oblasti OSPF omezují velikost stavové databáze a nabízejí možnost sumarizace tras. Viz také autonomní systém; stavová databáze.

oblast zakázaného inzerování – stub area

Oblast OSPF, která neinzeruje jednotlivé externí sítě. Směrování do všech externích sítí v této oblasti prochází výchozí trasou (cíl 0.0.0.0 se síťovou maskou 0.0.0.0).

obnovení – recovery

Proces použití souboru protokolu s cílem zajistit konzistentní stav databáze po zhroutilí systému a obnovení databáze ze zálohy do posledního stavu zaznamenaného v souboru protokolu po chybě média. Viz také autoritativní obnovení.

obnovovací frekvence – refresh rate

Četnost, s jakou je překreslována obrazovka, aby obraz neblíkal. Celá obrazová oblast je u většiny monitorů aktualizována 60krát za sekundu.

obor názvů – namespace

Sada jedinečných názvů pro prostředky nebo položky používané ve sdíleném výpočetním prostředí. Názvy v oboru názvů lze přeložit na objekty, které představují. Pro konzolu MMC je obor názvů reprezentován stromem konzoly zobrazujícím všechny moduly snap-in a prostředky, které jsou pro konzolu k dispozici. V rámci systému DNS (Domain Name System) představuje obor názvů svislou nebo vodorovnou strukturu stromu názvů domény. Napří-

klad název domény, jako je „host1“ nebo „example“, použitý v úplném doménovém názvu „host1.example.microsoft.com“, určuje větev stromu oboru názvů domény. Ve službě Active Directory odpovídá obor názvů oboru názvů DNS ve struktuře, ale překládá názvy objektů služby Active Directory.

obor názvů domény – domain namespace

Databázová struktura používaná systémem DNS. Viz také služba DNS.

obor vícesměrového vysílání – multicast scope

Rozsah adres IP skupin vícesměrového vysílání v rozsahu 239.0.0.0 až 239.254.255.255. Adresám vícesměrového vysílání v tomto oboru lze zakázat šíření v obou směrech (odesílání nebo příjem) prostřednictvím určení hranic vícesměrového vysílání.

obousměrný vztah důvěryhodnosti**– two-way trust relationship**

Propojení mezi doménami, v němž každá z domén důvěřuje uživatelským účtům druhé domény a umožňuje jim využívat své prostředky. Uživatelé se mohou přihlašovat z počítačů v obou doménách k doméně obsahující jejich účet. Viz také vztah důvěryhodnosti.

oddíl – partition

Logická část pevného disku. Oddíly usnadňují organizování informací. Každý oddíl může být naformátován jiným systémem souborů. Oddíl musí být plně obsazen na jednom fyzickém disku a tabulka oddílů v hlavním spouštěcím záznamu fyzického disku může obsahovat až čtyři zadání oddílů.

odesílatel – sender

V rámci serveru Systems Management Server je to komponenta toku používající ke komunikaci mezi sídly existující systém připojení. Odesílatel spravuje připojení, zajišťuje integritu přenesených dat, obnovení po chybách a ukončuje spojení, když již není zapotřebí.

odhlášení – log off

Ukončení práce se sítí. Název uživatele se odstraní z aktivního používání až do doby, než se uživatel znovu přihlásí.

odkaz – referral

V rámci systému DFS je to informace připojující název DNS v logickém oboru názvů k ekvivalentnímu názvu UNC fyzického sdíleného média. Když klient DFS získá přístup ke sdíle-

né složce v oboru názvů DFS, kořenový server DFS vrátí odkaz, který bude klient používat při hledání dané sdílené složky. V systému DNS jde o ukazatel na server DNS, který je autoritativní pro nižší úroveň oboru názvů domény.

odolnost proti chybám – fault tolerance

Schopnost počítače nebo operačního systému zachovávat integritu dat při selhání hardwaru. Na platformách Windows NT a Windows 2000 zajišťuje odolnost proti chybám ovladač Ftdisk.sys.

offline

V rámci klastru serverů je to stav nějakého prostředku, skupiny nebo uzlu, kdy není klastru dostupný. V režimu offline rovněž mohou být prostředky a skupiny. Viz také skupina; uzel; online, pozastavený; prostředek.

OLE

Viz technologie OLE.

online

V rámci klastru serverů je to stav nějakého prostředku, skupiny nebo uzlu, kdy je klastru dostupný. Viz také prezenční signál; uzel; offline; pozastavený; prostředek.

opakování kláves – RepeatKeys

Funkce umožňující lidem se sníženou pohyblivostí přizpůsobit si nebo úplně zakázat použití funkce opakování kláves na klávesnici.

operátor zálohování – backup operator

Typ místní nebo globální skupiny obsahující uživatelská práva nutná k zálohování a obnovování složek a souborů. Členové skupiny Backup Operators mohou zálohovat a obnovovat soubory a složky bez ohledu na nastavení vlastnictví, oprávnění, šifrování či auditování. Viz také auditování; globální skupina; místní skupina; uživatelská práva.

oprávnění – permission

Pravidlo přiřazené objektu a určující, kteří uživatelé mohou získat přístup k danému objektu a jakým způsobem. Ve Windows 2000 patří mezi objekty soubory, složky, sdílené položky, tiskárny a objekty Active Directory. Služby pro Macintosh zajišťují překlad mezi oprávněními a privilegii přístupu systému Macintosh, takže oprávnění zadaná nějaké složce (jednotce) platí i pro uživatele počítačů Macintosh a privilegia přístupu vytvořená uživateli systému

Macintosh platí i pro uživatele počítačů PC připojené k počítači se spuštěným systémem Windows 2000 Server. Viz také objekt.

oprávnění tiskárny – printer permissions

Oprávnění specifikující, jaký typ přístupu k tiskárně má uživatel nebo skupina. K dispozici jsou oprávnění Tisk, Správa tiskáren a Správa dokumentů.

organizační jednotky – organizational units

Objekt kontejneru služby Active Directory používaný v rámci domén. Organizační jednotky jsou logické kontejnery, do nichž lze umístit uživatele, skupiny, počítače a další organizační jednotky. Mohou obsahovat pouze objekty z nadřazené domény. Organizační jednotka je nejmenší rozsah, pro nějž lze použít zásady skupiny nebo delegovat oprávnění.

osa a ramena – hub-and-spoke

Konfigurace serveru WINS používající centrální rozbočovač („osu“) jako místo kontaktování mnoha odlehklých „ramen“ serveru WINS v zájmu zkrácení času konvergence.

osobní identifikační číslo (PIN) – personal identification number

Tajný identifikační kód bránící ve zneužití „chytrých“ karet. Číslo PIN se podobá heslu a zná je pouze uživatel karty. Kartou tak může používat pouze ten, kdo ji vlastní a zná její PIN. Viz také karta Smart Card.

ověření – authentication

Proces IPsec, který kontroluje původ a integritu zprávy tím, že zaručí skutečnou identitu všech počítačů. Bez zaručeného ověření jsou neznámý počítač a všechna jím poslaná data považována za podezřelá. IPsec nabízí více metod ověření a zajišťuje tak kompatibilitu se systémy, na nichž běží dřívější verze Windows, počítači s jinými operačními systémy a se sdílenými počítači.

U přístupu k síti se jedná o proces, kterým systém vyhodnocuje přihlašovací informace uživatele. Jméno a heslo uživatele se porovnává se seznamem ověření. Jestliže systém najde shodu, povolí uživateli přístup v úrovni specifikované pro daného uživatele v seznamu oprávnění. Když se uživatel přihlásí k účtu na počítači se systémem Windows 2000 Professional, ověření vykoná klient. Když se uživatel připojí k účtu na doméně systému Windows 2000

Server, ověření může vykonat libovolný server dané domény. Viz také server; vztah důvěryhodnosti.

ovladač IPsec – IPsec driver

Mechanismus zabezpečeného protokolu IP aktivovaný v okamžiku konfigurace protokolu IPsec na počítači, který sleduje pakety a hledá shodu s filtrem IP v aktivních zásadách zabezpečeného protokolu IP na počítači. Ovladač IPsec má také na starosti vlastní šifrování a dešifrování dat. Viz také protokol IPsec. IPsec ovladač je ovladač používající seznam filtru IP aktivních zásad IPsec a hledající odcházející pakety, které je zapotřebí zabezpečit, a přicházející pakety, které je zapotřebí prověřit a dešifrovat.

ovladač tiskárny – printer driver

Program navržený tak, aby ostatním programům umožňoval využívat určitou tiskárnu, aniž by se musely zabývat specifickým hardwarem či vnitřním jazykem tiskárny. Díky využití ovladačů tiskáren, které řeší odlišnosti jednotlivých tiskáren, mohou programy správně komunikovat s celou řadou tiskáren. Viz také jazyk PCL; jazyk PostScript.

ovladač zařízení – device driver

Program, který umožňuje speciálnímu zařízení, jako je například modem, síťová karta nebo tiskárna, komunikovat se systémem Windows 2000. I v případě, že je zařízení v systému instalováno, může být systémem Windows 2000 využito až v okamžiku, kdy je nainstalován a nakonfigurován také příslušný ovladač. Je-li zařízení uvedeno v seznamu kompatibilního hardwaru (seznam HCL), je příslušný ovladač zpravidla součástí systému Windows 2000. Ovladače zařízení jsou zaváděny automaticky (pro všechna zařízení, jež to umožňují) při spuštění počítače a nejsou pro uživatele viditelné. Viz také seznam HCL.

ovladače miniportů – miniport drivers

Ovladač připojený na zprostředkovací ovladač a hardwarové zařízení.

označení – label

Viz označení názvu domény.

označení názvu domény – domain name label

Jednotlivé části úplného názvu domény DNS, které reprezentují uzel ve stromu oboru názvů domény. Názvy domén jsou tvořeny posloup-

ností označení, jako jsou tři označení (například „example“, „microsoft“ a „com“) tvořící název domény DNS „example.microsoft.com“. Jednotlivá označení použitá v názvu DNS nesmí být delší než 63 bajtů.

P**paket – packet**

Přenosová jednotka pevné maximální velikosti skládající se z binárních informací reprezentujících data a záhlaví obsahující identifikační číslo, zdrojovou a cílovou adresu a data pro řízení chyb.

paměť RAM – RAM

Paměť, z níž lze číst (či zapisovat) pomocí počítače či jiného zařízení. Informace uložené v paměti RAM jsou po vypnutí počítače vymazány. Viz také virtuální paměť.

paměť ROM – read-only memory

Polovodičový obvod obsahující informace, které nelze měnit.

pár klíčů – key pair

Soukromý klíč a jemu náležející veřejný klíč. Viz také pár kryptografických klíčů.

pár kryptografických klíčů – public/private key pair

Sada kryptografických klíčů používaných v šifrování s veřejným klíčem. Jeden klíč se používá k zašifrování a druhý k dešifrování. Viz také veřejný klíč; soukromý klíč.

partnerský server pro nabízenou replikaci**– push partner**

Služba WINS, která po příjmu požadavku odesílá repliky partnerskému serveru pro vyžádanou replikaci. Viz také partnerský server pro vyžádanou replikaci.

partnerský server pro vyžádanou replikaci**– pull partner**

Služba WINS, která vyžaduje repliky od partnerského serveru pro nabízenou replikaci a pak nabídnuté repliky přijímá. Viz také partnerský server pro nabízenou replikaci.

páteř vícesměrového vysílání – multicast backbone

Část sítě Internet určená k vícesměrovému vysílání.

páteřní spojení – backbone

V rámci OSPF je to oblast společná všem dalším oblastem OSPF, která se používá jako tranzitní oblast pro přenosy mezi oblastmi

a pro distribuci trasovacích informací mezi oblastmi. Pátevní spojení musí být souvislé. Viz také protokol OSPF.

ping

Nástroj, který ověřuje připojení k jednomu nebo několika vzdáleným hostitelům. Příkaz ping používá k určení, zda je určitý systém IP v síti funkční, požadavky o ozvěnu ICMP a pakety odpovědí na ozvěnu. Příkaz ping je vhodný pro diagnostiku selhání směrovače nebo sítě IP. Viz také protokol ICMP.

Plug-and-Play – Plug and Play

Sada specifikací vyvinutá společností Intel, která počítačům umožňuje automaticky zjistit a konfigurovat zařízení a nainstalovat příslušné ovladače.

počet přenosů – hop count

Pole řízení přenosu udávající počet směrovačů IPX, které daný paket IPX zpracovaly.

počítač s více adresami – multihomed

Počítač s více instalovanými síťovými adaptéry.

podepisování kódu – code signing

Digitální podepsání softwarového kódu, které zaručí jeho integritu a zjistí bezpečně jeho původ.

podpora velkých bloků dat – large window support

V rámci komunikací TCP je to největší množství dat, která lze přenést bez potvrzení. Blok dat má pevnou velikost. Podpora velkých bloků dat dynamicky přepočítává velikost bloku dat a umožňuje přenos větších množství dat najednou, což zvyšuje celkovou propustnost.

podporující klastry – cluster-aware

Klasifikace aplikace nebo služby, která běží na uzlu klastru serverů, je spravována jako prostředek klastru a je vytvořena tak, aby znala prostředí klastru serverů a mohla s ním pracovat.

podporující připojení – connection-oriented

Síťový protokol vyžadující před zahájením komunikace v rámci sítě koncové virtuální připojení mezi odesílatelem a příjemcem.

podřízená doména – child domain

V rámci serverů DNS a služby Active Directory je to doména umístěná ve stromu oboru názvů přímo pod jiným názvem domény (nadřazená doména). Například „example.microsoft.com“ je podřízená doména nadřazené domény „microsoft.com“. Pro podřízené domény je rovněž

používán termín subdomény. Viz také nadřazená doména; doména; adresářový oddíl.

podřízená doména – subdomain

Doména DNS umístěná ve stromu oboru názvů přímo pod jiným názvem domény (nadřazená doména). Například „example.microsoft.com“ je podřízená doména nadřazené domény „microsoft.com“.

podřízený objekt – child object

Objekt umístěný v jiném objektu. Podřízený objekt implikuje relaci. Například soubor je podřízený objekt umístěný ve složce, která je nadřazeným objektem. Viz také objekt; nadřazený objekt.

podsíť – subnet

Část sítě IP. Každá podsíť má své vlastní jednoznačné identifikační číslo podsítě.

pojmenovaný kanál – named pipe

Část paměti, kterou lze využít pro předání informací mezi procesy. Výstup jednoho procesu je potom vstupem jiného procesu. Druhý proces může být místní (na stejném počítači jako první proces) nebo vzdálený (na počítači v síti).

položka – entry

Položky jsou prvky nejnižší úrovně v registru. Zobrazují se v pravém podokně okna editoru registru. Každá položka se skládá z názvu, datového typu a hodnoty. Položky ukládají vlastní konfigurační data ovlivňující operační systém a programy, které na něm běží. Jako takové se liší od klíčů a podklíčů, což jsou kontejnery. Položky jsou odkazovány pomocí cesty v registru a názvem. Množství a typ dat, která lze uložit do nějaké položky, jsou dány datovým typem položky.

položka řízení přístupu (ACE) – access control entry

Položka v seznamu řízení přístupu (ACL) obsahující identifikátor zabezpečení (SID) a sadu oprávnění k přístupu. Procesu s odpovídajícím identifikátorem zabezpečení jsou přístupová práva buď zaručena, odepřena nebo zaručena s auditováním.

pomalé klávesy – SlowKeys

Funkce systému Windows říkající počítači, aby ignoroval klávesy, které nebyly stisknuté po určité minimální dobu. To umožňuje uživatelům náhodně nechtěně tisknout klávesy, aniž

by to mělo nějaký efekt. Viz také filtrování kláves.

popisovač – handle

V uživatelském rozhraní je to rozhraní objektu umožňující jeho přesun, změnu velikosti, změnu tvaru a další funkce, které se k danému objektu vztahují. V rámci programování jde o ukazatel na ukazatel, tedy token umožňující programu přístup k identifikovanému zdroji.

popisovač zabezpečení – security descriptor

Sada informací přiřazených nějakému objektu, která určuje oprávnění přiřazená uživatelům a skupinám i auditované bezpečnostní události. Viz také seznam řízení zabezpečeného přístupu; objekt; seznam pro řízení přístupu do systému.

port

Mechanismus umožňující více připojení. Vylepšení adresy IP. V rámci správce zařízení je to připojovací bod počítače, k němuž lze připojit zařízení předávající data do počítače a z počítače. Například tiskárna je obvykle připojena k paralelnímu portu (pro tento port je rovněž používán termín port LPT) a modem je zpravidla připojen k sériovému portu (pro nějž je rovněž používán termín port COM).

port pro infračervený přenos – infrared port

Optický port počítače, který komunikuje s ostatními počítači nebo zařízeními pomocí infračerveného světla. Komunikace se uskutečňuje bez kabelů. Porty pro infračervený přenos se používají v přenosných počítačích, tiskárnách, fotoaparátech a dalších zařízeních. Port pro infračervený přenos může rovněž být přidán na počítač s doplňkovým externím infračerveným zařízením, které je připojeno ke kartě PCI, k sériovému či paralelnímu portu nebo přímo k základní desce počítače. Viz také zařízení s možností infračervené komunikace.

poskytovatel služeb sítě Internet (ISP)**– Internet services provider**

Společnost poskytující jednotlivcům nebo společnostem přístup do sítě Internet a WWW. Podepíšete-li smlouvu s poskytovatelem služeb sítě Internet, získáte telefonní číslo, uživatelské jméno, heslo a další informace o připojení, které vám umožní připojení počítače k počítačům poskytovatele. Poskytovatel zpravidla za

připojení účtuje měsíční nebo hodinové poplatky.

postížení pohyblivosti – mobility impairments

Zmenšená schopnost vykonávat určité manuální úkony, jako je například používání myši nebo stisk více kláves najednou. Taková osoba má tendenci tisknout nekontrolovaně příliš mnoho kláves, nechtěně se jich dotýkat nebo nedokáže udržet vytištěnou knihu.

postížení poznávání – cognitive disabilities

Postížení, která jsou výsledkem poruch vnímání, ztráty paměti a omezené schopnosti učení a vývoje, jako je dyslexie nebo Downův syndrom.

povolit – enable

Nastavit zařízení jako funkční. Pokud například povolíte zařízení v hardwarové konfiguraci, budou moci uživatelé pracující s danou hardwarovou konfigurací toto zařízení využít.

pozastavený – paused

Stav uzlu, který je plně aktivním členem klastru, ale nemůže hostit skupiny. Pozastavený stav je určen pro správu. Viz také překlopení zpět; překlopení; uzlu; offline.

požadavek klienta – client request

Požadavek klientského počítače na server nebo, v rámci služby vyrovnávání zatížení sítě, na klastr počítačů. Služba vyrovnávání zatížení sítě předá jednotlivé požadavky klientů určitému hostiteli v rámci klastru, a to na základě zásad vyrovnávání zatížení, která stanovil správce systému. Viz také klient; klastr; hostitel; server.

práce ve virtuální privátní síti**– virtual private networking**

Akt konfigurace a vytvoření virtuální privátní sítě.

pracovní plocha – desktop

Pracovní plocha na obrazovce, kde se zobrazují okna, ikony, nabídky a dialogová okna.

pravidla – rules

Mechanismus zásad IPsec řídící, jak a kdy zásady IPsec chrání komunikaci. Pravidlo nabízí možnost spustit a řídit zabezpečenou komunikaci na základě zdroje, cíle a typu dopravy IP. Každé pravidlo obsahuje seznam filtrů IP a kolekci zabezpečovacích akcí, k nimž dojde při shodě se seznamem filtru.

pravidlo portu – port rule

V rámci služby vyrovnávání zatížení je to sada konfiguračních parametrů, které určují režim filtrování, jenž bude použit pro určitý rozsah portů. Viz také režim filtrování.

prezenční signál – heartbeat

V klastru serverů nebo klastru vyrovnávání zatížení sítě jde o periodickou zprávu odeslanou mezi uzly a detekující systémové chyby na všech uzlech.

primární oddíl – primary partition

Svazek vytvořený s využitím volného místa na základním disku. Z primárního oddílu lze spustit systém Windows 2000 a další operační systémy. Na základním disku lze vytvořit až čtyři primární oddíly, nebo tři primární oddíly a jeden oddíl rozšířený. Primární oddíly lze vytvářet pouze na základních discích a nelze je dále dělit na pododdíly. Viz také základní disk; dynamický svazek; rozšířený oddíl; oddíl.

primární řadič domény – primary domain controller

Řadič domény systému Windows NT 4.0 nebo 3.51, který je jako první v doméně vytvořen a obsahuje primární úložiště doménových dat. V doméně primární řadič domény pravidelně replikuje svá data na další řadiče domén, označované jako záložní řadiče domén. Viz také záložní řadič domény.

primární server – primary server

Autoritativní server DNS pro zónu, který může být použit jako místo aktualizace zóny. Pouze primární hlavní servery mají schopnost přímé aktualizace při zpracování aktualizací zóny, což zahrnuje přidávání, odstraňování a změny záznamů o prostředcích uložených jako data zóny. Primární hlavní servery rovněž slouží jako první zdroj při replikaci zóny na ostatní servery DNS.

primární token – primary token

Token přístupu přiřazený procesu, aby reprezentoval výchozí informace zabezpečení daného procesu. Je používán v zabezpečených operacích tokenem pracujícím jménem samotného procesu a nikoli jménem klienta. Viz také token přístupu; token zosobnění; proces.

priorita – priority

Úroveň upřednostnění určující pořadí, v jakém jsou toky procesu naplánovány pro zpracování procesorem.

priorita hostitele – host priority

V rámci služby vyrovnávání zatížení sítě je to pořadí hostitele při zpracování výchozího provozu sítě pro porty TCP a UDP. Používá se v případě, že hostitel v klastru přejde do režimu offline, a určuje, který hostitel v rámci klastru převeze zodpovědnost za provoz, který byl původně zpracováván hostitelem, jenž je nyní offline. Viz také protokol UDP.

privilegium – privilege

Právo uživatele vykonat určitý úkol, obvykle takový, který ovlivňuje celý počítačový systém a nikoli jen jeden určitý objekt. Privilegia přiřazují jednotlivým uživatelům nebo skupinám uživatelů správci jako součást nastavení zabezpečení počítače. Viz také lístek přístupu; oprávnění; uživatelská práva.

proces – process

Objekt operačního systému, který je tvořen spustitelným programem, sadou adres virtuální paměti a jedním nebo více toky. Po spuštění nějakého programu se vytvoří proces Windows 2000. Viz také tok.

profil uživatele – user profile

Soubor obsahující konfigurační informace určitého uživatele, jako jsou nastavení pracovní plochy, trvalá síťová připojení a nastavení aplikací. Nastavení každého uživatele se uloží do profilu uživatele, který systémy Windows NT a Windows 2000 použijí ke konfiguraci pracovní plochy po přihlášení uživatele.

prohlížeč – browser

Klientský nástroj navigace a přístupu k informacím na Internetu nebo intranetu. V kontextu práce v sítích systému Windows může „prohlížeč“ označovat také službu Computer Browser, která udržuje aktuální seznam počítačů na síti nebo části sítě a na požádání tento seznam předává aplikacím. Když se uživatel pokusí připojit k nějakému zdroji v doméně, kontaktuje se prohlížeč dané domény, který poskytne seznam dostupných zdrojů.

prokládaný svazek – striped volume

Svazek ukládající data v pružích na dvou nebo více fyzických discích. Data v prokládaném svazku jsou ve formě po sobě následujících logických bloků na tyto disky ukládána střídavě a pravidelně (v pružích). Každý „pruh“ dat se skládá z jednoho bloku dat na disk (včetně všech redundantních dat).

proměnná prostředí – environment variable

Řetězec tvořený nějakou informací o prostředí, například označení jednotky, cesty nebo názvu souboru, přiřazený určitému symbolickému názvu, který lze používat v systému Windows NT a Windows 2000. Proměnné prostředí se definují pomocí ovládacího panelu Systém nebo příkazem set příkazového řádku.

propojení – sessions

Více paketů odeslaných s potvrzením mezi koncovými dvěma body.

propojení sítě

Dvě nebo více fyzických sítí propojených směrovači. V rámci integrace služeb Services for Macintosh lze propojení sítí vytvořit připojením dvou nebo více sítí AppleTalk k počítači se systémem Windows 2000 Server. V rámci protokolu TCP/IP lze propojení sítí vytvořit připojením dvou nebo více sítí IP k počítači s více adresami a se systémem Windows 2000 Server nebo Windows 2000 Professional.

K efektivnímu směrování mezi propojeními sítí používajícími protokol TCP/IP je nutné povolit předávání IP.

propojený objekt – linked object

Objekt, který je vložen do dokumentu, ale zůstává zachován ve zdrojovém souboru. Jsou-li informace propojeny, je nový dokument při změně informací v původním dokumentu automaticky aktualizován. Viz také vložený objekt.

propustnost – throughput

U disků je to přenosová kapacita diskového systému.

prostředek – resource

Obecně libovolná část počítačového systému nebo sítě, například disková jednotka, tiskárna nebo paměť, kterou lze přidělit spuštěnému programu nebo procesu. Ve správci zařízení je to libovolná ze čtyř systémových komponent určujících způsob fungování zařízení na počítači. Jedná se o tyto čtyři systémové prostředky: linky požadavků přerušení (IRQ), kanály pro přímý přístup do paměti (DMA), vstupně-výstupní porty a adresy paměti. V rámci klastrů serverů jde o instanci nějakého typu prostředku. Služba klastrů spravuje různé fyzické nebo logické položky jako prostředky.

prostředí – shell

Interpreter příkazů, který se používá k předávání příkazů operačnímu systému.

prostý text – plaintext

Nezašifrovaná data. Viz také šifrovaný text; šifrování; dešifrování.

protokol – protocol

Sada pravidel a konvencí pro posílání informací mezi počítači v rámci sítě. Síťový software zpravidla implementuje více úrovní protokolů, které jsou ve vrstvách na sobě. Systémy Windows NT a Windows 2000 obsahují protokoly NetBEUI, TCP/IP a protokoly kompatibilní s IPX/SPX.

protokol alokace šířky pásma (BAP)**– Bandwidth Allocation Protocol**

Rídicí protokol PPP, který se při použití více-linkového připojení používá k dynamickému přidávání a odstraňování propojení.

protokol AppleTalk – AppleTalk protocol

Sada síťových protokolů, na nichž je založena síťová architektura AppleTalk. Zásobník protokolu AppleTalk musí být nainstalován na počítači se systémem Windows 2000 Server, aby se k němu mohly klienty systému Macintosh připojovat. Viz také AppleTalk.

protokol DHCP**– Dynamic Host Configuration Protocol**

Síťový protokol, k jehož výhodám patří bezpečnost, spolehlivost a jednoduchost konfigurace sítě TCP/IP. Protokol nabízí dynamickou konfiguraci adres IP počítačů. Protokol DHCP zabraňuje konfliktům adres a zajišťuje centralizovanou správu adres IP použitých v síti.

protokol EAP – Extensible Authentication Protocol

Rozšíření protokolu PPP, které umožňuje během ověřování připojení PPP použít mechanismus volného ověřování.

protokol FTP – File Transfer Protocol

Protokol definující, jak přenášet soubory z jednoho počítače na druhý přes Internet, a aplikace klient/server, která přesunuje soubory pomocí tohoto protokolu.

protokol HTTP – Hypertext Transfer Protocol

Protokol používaný k přenosu informací na síti World Wide Web. Adresa protokolu HTTP (jedna z forem jednotného ukazatele na zdroj

neboli URL) má tvar `http://www.microsoft.com`.

protokol CHAP

– Challenge Handshake Authentication Protocol

Ověřovací protokol používaný službami v připojeních PPP, který je dokumentovaný v RFC 1994 a který k hašování odpovědi na výzvu vydanou serverem pro vzdálený přístup používá standardní schéma jednosměrného šifrování MD-5.

protokol ICMP – Internet Control Message Protocol

Protokol údržby sady protokolů TCP/IP, který je vyžadován ve všech implementacích TCP/IP a umožňuje dvěma uzlům v síti IP sdílet informace o chybách a stavu sítě IP. Protokol ICMP je používán nástrojem ping k určení dostupnosti vzdáleného systému.

protokol IGMP

– Internet Group Management Protocol

Protokol sady TCP/IP zodpovědný za správu členství ve skupinách vícesměrového vysílání.

protokol IKE – Internet Key Exchange

Protokol vytvářející přiřazení zabezpečení a sdílené klíče nezbytné pro to, aby mohly dvě strany komunikovat zabezpečeným protokolem IP.

protokol IP – Internet Protocol

Směřovatelný protokol v sadě TCP/IP, který zodpovídá za adresování, směrování, fragmentaci a opětné složení paketů IP.

protokol IPX – Internetwork Packet Exchange

Síťový protokol systému NetWare, který řídí adresování a směrování paketů v rámci místních sítí i mezi nimi. Protokol IPX nezaručuje, že zpráva bude kompletní (bez ztracených paketů). Viz také protokol IPX/SPX; místní síť.

protokol IPX/SPX – Internetwork Packet Exchange/Sequenced Packet Exchange

Transportní protokoly používané v sítích Novell NetWare, které odpovídají kombinaci protokolů TCP a IP v sadě protokolů TCP/IP. V systému Windows 2000 je protokol IPX implementován prostřednictvím protokolu NWLink. Viz také protokol IPX; protokol TCP/IP; protokol NWLink.

protokol kvora – quorum log

Záznam změn, k nimž došlo v klastrovém podregistru od okamžiku uskutečnění poslední

kontroly podregistru. Tento protokol je uložený na disku kvora.

protokol Layer 2 Tunneling Protocol (L2TP)

– Layer 2 Tunneling Protocol

Protokol tunelových propojení zahrnující rámce odesílané přes síť IP, X.25, Frame Relay a ATM. Protokol L2TP je kombinací protokolů Point-to-Point Tunneling (PPTP) a specifikací L2F (Layer 2 Forwarding) navržených společností Cisco.

protokol LDAP

– Lightweight Directory Access Protocol

Protokol adresářové služby běžící přímo nad TCP/IP a primární přístupový protokol pro službu Active Directory. Protokol LDAP (Lightweight Directory Access Protocol) verze 3 je definován sadou dokumentů s navrhovanými standardy specifikace RFC 2251 sdružení IETF (Internet Engineering Task Force). Viz také rozhraní API protokolu LDAP

protokol MDHCP – multicast DHCP

Rozšíření protokolu DHCP, které poskytuje dynamické přiřazování a konfiguraci adres vícesměrového vysílání IP na sítích TCP/IP.

protokol MIME

– Multipurpose Internet Mail Extensions

Obecná metoda přenosu netextových dat internetovou poštou. Standard MIME zakóduje netextová data jako textové soubory a na straně příjemce je dekoduje zpět do původního formátu. K souboru se přidá hlavička MIME zahrnující typ obsažených dat a použitou metodu kódování. Viz také protokol S/MIME.

protokol NAT – Network Address Translation

Protokol umožňující síti s privátními adresami přistupovat k informacím na Internetu prostřednictvím procesu překladu IP.

protokol NCP – NetWare Core Protocol

Protokol sdílení souborů, který řídí komunikaci týkající se operací s prostředky (například s disky nebo tiskárnami), operací s vazebními databázemi a operací NDS mezi servery a klientskými počítači v síti Novell NetWare. Požadavky z klientských počítačů jsou předávány pomocí protokolu IPX. Servery reagují v souladu s pokyny protokolu NCP. Viz také vazební databáze; protokol IPX; služba NDS.

protokol NNTP – Network News Transfer Protocol

Člen sady protokolů TCP/IP, který slouží k distribuci zpráv diskusních příspěvků serverům a klientům NNTP (programům pro čtení diskusních příspěvků) v síti Internet. Protokol NNTP je navržen tak, aby články diskusních příspěvků byly uloženy v centrální databázi na serveru a uživatelé si tak mohli vybrat, které položky budou číst. Viz také protokol TCP/IP.

protokol NWLink – NWLink

Implementace protokolů IPX (Internetwork Packet Exchange), SPX (Sequenced Packet Exchange) a NetBIOS používaná v sítích Novell. Protokol NWLink je standardní síťový protokol, který podporuje směrování a je schopen podporovat aplikace NetWare typu klient/server, v jejichž rámci vzájemně komunikují aplikace založené na soketech NetWare s aplikacemi založenými na soketech IPX/SPX. Viz také protokol IPX/SPX; systém NetBIOS.

protokol OSPF – open shortest path first

Směrovací protokol používaný ve středních a velkých sítích. Tento protokol je složitější než protokol RIP, ale poskytuje vyšší kontrolu a je výkonnější při šíření směrovacích informací.

protokol ověření Kerberos**– Kerberos authentication protocol**

Ověřovací mechanismus používaný k ověření identity uživatele nebo hostitele. Protokol Kerberos v5 je výchozí ověřovací službou systému Windows 2000. Protokol Kerberos používají k ověřování také zabezpečený protokol IP a služba Admission Control QoS. Viz také služba Admission Control QoS; zabezpečený protokol IP.

protokol PAP – password authentication protocol

Jednoduché schéma ověření připojení PPP. Server vzdáleného přístupu požaduje zadání názvu a hesla uživatele, která mu klient vzdáleného přístupu předá ve formě prostého textu.

protokol počátečního zavedení (BOOTP)**– bootstrap protocol**

Sada pravidel neboli standardů umožňující vzájemné propojení počítačů. Používá se primárně v sítích TCP/IP ke konfiguraci pracovních stanic bez disků. Tento protokol je definován specifikacemi RFC 951 a 1542. Novějším protokolem konfigurace spouštění, který

tento protokol využívá, je protokol DHCP. Protokol BOOTP využívá například protokol DHCP konfigurace spouštění.

protokol PPP – Point-to-Point Protocol

Sada standardních protokolů používaných v propojení mezi dvěma body přenosu více-protokolových datagramů. Protokol PPP je dokumentován v RFC 1661.

protokol PPTP – Point-to-Point Tunneling Protocol

Tunelovací protokol, který zapouzdřuje rámce protokolu PPP do datagramů IP a přenáší je přes propojení sítí IP, například přes Internet nebo privátní (soukromý) intranet.

protokol překladu adres (ARP)**– Address Resolution Protocol**

V TCP/IP je to protokol, který pomocí omezeného vysílání do místní sítě překládá logicky přiřazené adresy IP. Adresa IP je převedena v softwaru jednotlivých hostitelských zařízení sítě IP na adresu jejich fyzického hardwaru nebo na adresu vrstvy řízení přístupu k médiu. V případě ATM se protokol ARP používá dvěma odlišnými způsoby. U protokolu CLIP se ARP používá k překladu adres na adresy hardwaru ATM. V případě emulace LAN sítě ATM se protokol ARP používá k překladu adres ethernet/802.3 nebo token ring na adresy hardwaru ATM. Viz také řízení přístupu k médiu; protokol TCP/IP.

protokol S/MIME**– Secure/Multipurpose Internet Mail Extensions**

Rozšíření standardu MIME s podporou zabezpečené pošty. Umožňuje původci zprávu digitálně podepsat, čímž dokáže její původ a zaručí integritu dat. Umožňuje také přenos zpráv v šifrovaném formátu, čímž se dosáhne důvěrné komunikace. Viz také protokol MIME.

protokol SMB – server message block

Protokol sdílení souboru, vytvořený tak, aby umožnil počítačům prostřednictvím různých typů sítí transparentní přístup k souborům, jež se nacházejí na vzdálených systémech. Protokol SMB, který společně vyvinuly společnosti Microsoft, Intel a IBM, definuje sérii příkazů, které předávají informace mezi počítači. Protokol SMB používá čtyři typy zpráv: řízení připojení, souboru, tiskárny a zprávy.

protokol SMTP – Simple Mail Transfer Protocol

Protokol používaný na Internetu ke spolehlivému a výkonnému přenosu pošty. Protokol SMTP není závislý na konkrétním vysílacím podsystému a vyžaduje pouze spolehlivý, uspořádaný kanál toku dat.

protokol SNMP**– Simple Network Management Protocol**

Síťový protokol pro správu sítí TCP/IP. Protokol SNMP přenáší informace správy a příkazy mezi programem správy obsluhovaný správcem a agentem správy sítě spuštěným na hostiteli. Agent SNMP odesílá stavové informace na jednoho nebo více hostitelů v okamžiku, kdy je hostitel požaduje nebo když dojde k významné události.

protokol TCP/IP – Transmission Control**Protocol/Internet Protocol**

Sada síťových protokolů používaných v síti Internet, která poskytuje komunikaci v rámci vzájemně propojených sítí tvořených počítači s různou hardwarovou architekturou a různými operačními systémy. Protokol TCP/IP zahrnuje standardy pro komunikaci počítačů a konvence propojování sítí a směrování provozu.

protokol TFTP – Trivial File Transfer Protocol

Protokol, který používá server IntelliMirror ke stažení počátečních souborů nutných k restartu nebo zahájení procesu instalace.

protokol TLS – Transport Layer Security

Standardní protokol poskytující zabezpečenou webovou komunikaci na Internetu nebo intranetech. Umožňuje klientům ověřovat servery nebo volitelně serverům ověřovat klienty. Také poskytuje zabezpečený kanál tím, že v zájmu zachování důvěrnosti komunikaci šifruje.

protokol událostí – Event Log

Soubor, do něhož se zaznamenávají události.

protokol UDP – User Datagram Protocol

Doplňk protokolu TCP nabízející službu datagramů bez připojení, která nezaručuje doručení ani správné uspořádání doručených paketů.

protokol změny – change log

Viz protokol kvora.

protokolování událostí – event logging

V systému Windows 2000 je to proces zaznamenávání položky auditu v auditovacím sledu při výskytu určitých událostí, jako je například

spuštění nebo ukončení služby, přihlášení či odhlášení uživatelů nebo přístup k prostředkům. Ke sledování událostí služby Services for Macintosh i událostí systému Windows 2000 lze využít program Prohlížeč událostí.

průvodce delegováním – delegation wizard

Průvodce používaný k rozdělení přesně určených prvků pracovní odpovědnosti správce na jiné uživatele.

průvodce instalací Active Directory**– Active Directory Installation Wizard**

Nástroj systému Windows 2000 Server umožňující během instalace instalovat službu Active Directory, vytvářet stromy v doménové struktuře, replikovat existující doménu, instalovat ověřovací software Kerberos a převádět servery na řadiče domén.

průvodce přípravou vzdálené instalace (RIPrep.exe)**– Remote Installation Preparation wizard**

Součást služeb vzdálené instalace, jež se používá k vytváření obrazů operačních systémů a jejich instalaci na servery RIS.

průvodce usnadněním – accessibility wizard

Interaktivní nástroj zjednodušující nastavení často používaných funkcí usnadnění. Tento průvodce dovoluje zadání podle typu postižení a nevyžaduje číselnou specifikaci jednotlivých nastavení.

přebalíčkování – repackaging

Proces převodu starší aplikace tak, aby mohla využít mnoha funkcí služby Windows Installer, včetně možnosti inzerování aplikace uživatelům, možnosti automatického opravení softwaru, došlo-li k poškození nebo smazání základních souborů, a umožnění uživatelům nainstalovat si aplikaci se zvýšenými privilegii.

předávací tabulka vícesměrového vysílání**– multicast forwarding table**

Tabulka používaná protokolem IP k předávání vícesměrového provozu IP. Zadání v tabulce vícesměrového vysílání se skládá z adresy skupiny vícesměrového vysílání, zdrojové adresy IP, seznamu rozhraní, na něž se provoz předává, a jediného rozhraní, na němž musí být provoz přijímán, aby mohl být předáván dále.

předmět – subject

Entita pracující s objektem. Když například tok vykonávání otevře soubor, tok je předmětem

a soubor je objekt jeho akce. Viz také objekt; tok.

předpona sítě – network prefix

Počet bitů v identifikátoru sítě IP začínající vyšším bitem. Předpona sítě je další možností vyjádření masky podsítě.

překlad názvu – name resolution

Proces softwarového překladu názvů, s nimiž se dobře pracuje uživateli, a číselných adres IP, které si uživatelé nezapamatují, ale jsou nezbytné pro komunikaci protokolem TCP/IP. Překlad názvů mohou zajišťovat softwarové součásti, například systém DNS nebo služba WINS. V adresářové službě jde o fázi zpracování operace adresáře LDAP, která zahrnuje vyhledání řadiče domény obsahujícího cílovou položku operace. Viz také služba DNS; protokol TCP/IP; služba WINS.

překlad názvů systému NetBIOS

– NetBIOS name resolution

Proces překladu názvu systému NetBIOS na jeho adresu IP.

překladač – resolver

Klientské programy DNS, které slouží k vyhledání informací o názvech DNS. Překladače mohou být malé programy (omezené sady programovacích rutin, které poskytují základní možnosti dotazování) nebo rozsáhlejší programy, které poskytují další funkce vyhledávání klientů DNS, například ukládání do mezipaměti. Viz také ukládání do mezipaměti; služba Caching Resolver.

překladač síťových adres

– network address translator

Směrovač IP definovaný v RFC 1631, který umí překládat adresy IP a čísla portů TCP/UDP předávaných paketů.

překlopení – failover

V klastru serverů je to prostředek zajištění vysoké dostupnosti. Během chyby nějakého prostředku ve skupině nebo uzlu, kde je skupina online, klastr převede skupinu na daném uzlu offline a pak ji převede do režimu online na jiném uzlu. Viz také uzel; prostředek.

překlopení zpět – failback

V klastru serverů je to přesun jedné překlopené skupiny na následující uzel určený na seznamu upřednostňovaných vlastníků dané skupiny. Viz také překlopení; uzel; prostředek.

přenos zóny – zone transfer

Proces, jímž servery DNS udržují a synchronizují data autoritativních názvů. Je-li server DNS konfigurován jako sekundární server zóny, posílá periodicky dotazy hlavnímu serveru DNS, který je konfigurován jako zdroj pro tuto zónu. Je-li verze uchovávaná hlavním serverem odlišná od verze na sekundárním serveru, přenesou sekundární server data zóny z hlavního serveru DNS a dojde tak k synchronizaci dat zóny. Viz také úplný přenos zóny; přírůstkový přenos zóny; sekundární server; zóna.

přenosový protokol – transport protocol

Protokol definující to, jak mají být data představena další přijímací vrstvě v síťovém modelu Windows NT a Windows 2000, a data podle toho zabalí. Přenosový protokol předá data přes rozhraní NDIS ovladači síťové karty a pomocí rozhraní TDI přesměrovávacímu zařízení.

přepínač – switch

Počítač nebo jiné síťové zařízení řídící směrování a funkci signální cesty. V rámci klastrů je přepínač používán k propojení hostitelů klastru se směrovačem nebo jiným zdrojem příchodního síťového připojení. Viz také směrování.

přepínaný virtuální okruh (SVC)

– switched virtual circuit

Připojení vytvořené dynamicky pomocí signálů mezi zařízeními v síti ATM.

přepnutí kláves – ToggleKeys

Funkce systému Windows způsobující pípnutí počítače při zapnutí nebo vypnutí jednoho z přepínacích kláves (Caps Lock, Num Lock, Scroll Lock).

přesměrování – redirection

V systému UNIX to znamená odeslat standardní výstup do souboru a nikoli na terminál nebo převzít standardní vstup ze souboru a nikoli z terminálu.

přesměrování složky – folder redirection

Volba skupinových zásad umožňující přesměrovat určené složky na síť.

přetěžované místo – bottleneck

Podmínka, obvykle zahrnující hardwarový zdroj, která způsobuje nízkou výkonnost celého systému.

přihlášení – log on

Započetí práce se sítí zadáním uživatelského jména a hesla, které uživatele v síti identifikují.

příkaz drain – drain

V rámci služby vyrovnávání zatížení sítě je to program, který zakazuje zpracování pro pravidla, jejichž rozsah portů obsahuje určený port. Ovlivněny budou všechny porty určené pravidlem portu. Je-li pro port použit argument „all“, bude tento příkaz použit pro všechny porty zahrnuté ve všech pravidlech portů. Nová připojení k určenému hostiteli nebo hostitelům nejsou povolena, ale všechna aktivní připojení jsou zachována. Chcete-li zakázat aktivní připojení, použijte příkaz disable. Pokud určení hostitelé nezahájili klastrové operace, nemá tento příkaz žádný vliv. Viz také příkaz drainstop; pravidlo portu.

příkaz drainstop – drainstop

V rámci služby vyrovnávání zatížení sítě jde o nástroj, který zakazuje nové zpracování provozu na určených hostitelích. Hostitelé potom přejdou do režimu vyprázdnění a ukončí stávající připojení. V průběhu této operace zůstávají hostitelé v klastru a zastaví klastrové operace v okamžiku, kdy již žádná připojení nejsou aktivní. Chcete-li režim vyprázdnění ukončit, explicitně ukončíte režim klastru příkazem stop, nebo spusťte nové zpracování provozu příkazem start. Chcete-li vyprázdnit připojení z určitého portu, použijte příkaz drain. Viz také příkaz drain.

připojení TCP – TCP connection

Logické připojení existující mezi dvěma procesy, která si data vyměňují pomocí TCP.

připojení virtuální privátní sítě**– virtual private network connection**

Propojení, v němž jsou soukromá data zapouzdřena a zašifrována.

připojení VPN – VPN connection

Část připojení, v němž jsou data zašifrována.

připojení vyžádaného volání**– demand-dial connection**

Připojení (obvykle uskutecněné pomocí přepinaného propojení rozsáhlé sítě), které se iniciuje v případě potřeby předání dat. Připojení vyžádaného volání se obvykle ukončí, pokud nedochází k žádnému přenosu.

připojovací body svazků – volume mount points

Nové systémové objekty v interním oboru názvů systému Windows 2000, které trvalým a robustním způsobem představují svazky úložišť.

přípona DNS – DNS suffix

U systému DNS je to volitelný název nadřazené domény, který lze připojit na konec relativního názvu domény použitý v dotazu na název nebo při vyhledávání hostitele. Příponu DNS lze použít k doplnění vyhledávaného alternativního plně zadaného názvu domény DNS, když první dotaz na název skončil chybou.

přírůstkový přenos zóny (IXFR)**– incremental zone transfer**

Alternativní typ dotazu, který může být použit některými servery DNS k aktualizaci a synchronizaci dat zóny při změně zóny. Je-li mezi servery DNS podporován přírůstkový přenos zóny, mohou servery sledovat a přenášet pouze přírůstkové změny záznamů o prostředcích mezi jednotlivými verzemi zóny. Viz také úplný přenos zóny; zóna; přenos zóny.

přirazení aplikace – application assignment

Proces, který pro přiřazení programů skupinám uživatelů využívá službu instalace softwaru (rozšíření zásad skupiny). Uživatelům se po přihlášení objeví tyto programy na pracovní ploše.

přirazení zabezpečení (SA) – security association

Šada parametrů definující služby a mechanismy nezbytné k ochraně zabezpečených komunikací IP. Viz také zabezpečený protokol IP.

přirazování – assigning

Na serveru System Management Server jde o zavedení určitého programu členům kolekce (skupiny), kde je přijetí programu povinné.

přístupový bod klienta – client access point

V případě serveru Systems Management Server je to systém sídla poskytující sadu sdílených adresářů a souborů, které vytvářejí společný komunikační bod mezi serverem a klientskými počítači.

publikované aplikace – published applications

Aplikace, které jsou dostupné uživatelům spravovaným prostřednictvím objektu skupinových zásad. Každý uživatel se může rozhodnout, zda si pomocí ovládacího panelu přidat nebo odebrat programy publikované aplikace na instaluje.

R

RAID

Viz svazek RAID.

rámec – frame

V rámci synchronní komunikace jde o balíček informací odvyšlaný jako jedna jednotka z jednoho zařízení do druhého. Rámec je termín nejčastěji používaný v sítích ethernet. Rámec se podobá paketu používanému v jiných sítích. Viz také paket.

rastrová písma – raster fonts

Písma, která jsou ukládána ve formě rastrových obrázků. Rastrová písma jsou navržena s určitou velikostí a rozlišením pro specifické tiskárny a nelze je otočit ani změnit jejich měřítko. Pokud tiskárna nepodporuje rastrová písma, nemůže je vytisknout.

registr – registry

V systému Windows 2000, Windows NT a Windows 98 je to databázové úložiště informací o konfiguraci počítače. Registr je uspořádán hierarchicky jako strom a skládá se z klíčů, podklíčů, podregistrů a položek hodnot.

relativní identifikátor (RID) – relative identifier

Část identifikátoru zabezpečení (SID) identifikující účet nebo skupinu. Identifikátory RID jsou v rámci domény, v níž je daný účet nebo skupina vytvořena, jednoznačné. Viz také identifikátor zabezpečení.

replika – replica

V rámci replikace Active Directory je to kopie logického oddílu Active Directory, která je synchronizována pomocí replikace na různých doménových řadičích, které obsahují kopie téhož adresářového oddílu. Replika může také označovat složenou sadu adresářových oddílů udržovanou na jednom řadiči domény.

replikace – replication

Proces kopírování dat z úložiště dat nebo systému souborů na několik počítačů uchovávajících táž data za účelem synchronizace dat. V systému Windows 2000 dochází k replikaci Active Directory prostřednictvím služby Directory Replicator Service a k replikaci systému souborů pomocí replikace systému DFS.

replikace Active Directory

– Active Directory replication

Replikace, k níž dochází díky službě replikace adresářů zajišťující replikaci adresářových oddílů mezi řadiči domén. Repliky adresářových oddílů lze zapsat na všechny řadiče domén. Replikační služba zkopíruje změny z dané repliky adresářového oddílu do všech ostatních řadičů domén obsahujících repliku téhož adresářového oddílu. Viz také adresářový oddíl; služba replikace souborů.

replikace s více hlavními servery

– multimaster replication

Model replikace, v němž libovolný řadič domény přijímá a replikuje změny adresářů do libovolného jiného řadiče domény. Liší se tedy od ostatních replikačních modelů, v jejichž rámci jeden počítač ukládá jednu modifikovatelnou kopii adresáře a v ostatních počítačích jsou ukládány pouze kopie. Viz také řadič domény; replikace.

replikace správce LAN – LAN manager replication

Služba replikace souborů používaná ve Windows NT. Viz služba replikace souborů.

restrukturalizace domény – domain restructure

Proces změny organizace jedné doménové struktury do druhé struktury, což má obvykle za následek změnu účtů, skupin a důvěryhodností.

režim asynchronního přenosu (ATM)

– Asynchronous Transfer Mode

Vysokorychlostní připojovací protokol sloužící k přenosu různých typů provozu v síti.

režim filtrování – filtering mode

V rámci služby Vyrovnávání zatížení sítě je to metoda, při níž je přichodící síťový provoz v klastru zpracováván hostiteli v tomto klastru. Provoz může být zpracováván buď jedním serverem, rozdělen metodou vyrovnávání zatížení mezi hostitele v rámci klastru nebo úplně zakázán. Viz také server.

režim GUI – GUI mode

Část instalačního programu využívající grafické uživatelské rozhraní (GUI).

rozbočovač – hub

Síťové zařízení, které spojuje komunikační linky na jednom místě a poskytuje společné připojení ke všem zařízením v síti.

rozdělení do podsítí – subnetting

Akt rozdělení adresového prostoru identifikátoru sítě TCP/IP do menších síťových segmentů, každý z nichž má svůj vlastní identifikátor podsítě.

rozhraní – interface

V rámci sítí jde o logické zařízení, přes něž lze odesílat a přijímat pakety. V nástroji správy Routing and Remote Access je to vizuální reprezentace síťového segmentu, k němuž lze přistoupit přes adaptéry místní nebo rozlehlé sítě. Každé rozhraní má jednoznačný název. Viz také místní síť; síťový adaptér; směrování; rozsáhlá síť.

rozhraní Active Directory Service Interface (ADSI) – Active Directory Service Interfaces

Jedná se o model adresářové služby a sadu rozhraní modelu COM. ADSI umožňuje aplikacím systémů Windows 95, Windows 98, Windows NT a Windows 2000 získat přístup k několika síťovým adresářovým službám, včetně služby Active Directory. Rozhraní se dodává jako sada SDK (Software Development Kit).

rozhraní Advanced Configuration and Power Interface (ACPI) – Advanced Configuration and Power Interface

Otevřená specifikace, která definuje řízení spotřeby u celé řady mobilních a stolních počítačů, serverů a periferních zařízení. Rozhraní ACPI je základem iniciativy OnNow umožňující vyrábět počítače, jež lze spustit pomocí tlačítka na klávesnici. Rozhraní ACPI je nezbytností pro plné využití výhod řízení spotřeby a technologie Plug-and-Play v systému Windows 2000. Pokud si nejste jisti, zda váš počítač vyhovuje standardu ACPI, najdete potřebné informace v dokumentaci od výrobce. Viz také Plug-and-Play.

rozhraní API protokolu LDAP – Lightweight Directory Access Protocol Access Programming Interface

Sada rozhraní API protokolu LDAP nízké úrovně vytvořená v jazyce C.

rozhraní API s více jazyky – multilingual API

Rozhraní API používaná k podpoře více jazyků v systému Windows 2000.

rozhraní CGI – common gateway interface

Serverové rozhraní inicializace softwarových služeb. Sada rozhraní popisující, jak webový server komunikuje se softwarem na tomtéž

počítači. Programem CGI může být libovolný software za předpokladu, že zpracovává vstup a výstup podle standardu CGI.

rozhraní CryptoAPI – CryptoAPI

Rozhraní pro programování aplikací (API), které je poskytováno jako součást systému Windows 2000. Rozhraní CryptoAPI nabízí sadu funkcí, které aplikacím umožňují flexibilní šifrování nebo digitální podepisování dat a současně poskytují ochranu dat soukromých klíčů. Vlastní kryptografické operace jsou prováděny nezávislými moduly, pro něž je používáno označení zprostředkovatelé kryptografických služeb (CSP). Viz také zprostředkovatel kryptografických služeb; soukromý klíč.

rozhraní FDDI – Fiber Distributed Data Interface

Určitý typ síťového média navržený tak, aby mohl používat optické kabely. Viz také LocalTalk; token ring

rozhraní NetBEUI**– NetBIOS Enhanced User Interface**

Síťový protokol sítě Microsoft. Zpravidla se používá v malých místních sítích (LAN) s 1 až 200 klienty. Jako jedinou metodu směrování může využívat zdrojové směrování token ring. Jedná se o implementaci standardu NetBIOS, kterou realizovala společnost Microsoft.

rozhraní ODBC – open database connectivity

Programovací rozhraní aplikace (API) umožňující databázovým aplikacím přistupovat k datům v různých existujících zdrojích dat.

rozhraní PCI – peripheral component interconnect

Specifikace společnosti Intel definující systém místní sběrnice dovolující instalaci až 10 rozšiřujících karet odpovídajících standardu PCI do počítače.

rozhraní programování aplikací (API)**– application programming interface**

Sada podprogramů, které aplikace používá k zadání požadavku vykonání služeb nízké úrovně poskytovaných operačním systémem počítače. Tyto podprogramy se obvykle starají o úkoly podpory, jako je správa souborů a zobrazování informací.

rozhraní SCSI – Small Computer System Interface

Standardní vysokorychlostní paralelní rozhraní definované výběrem X3T9.2 organizace ANSI (American National Standards Institute). Rozhraní SCSI slouží k připojování mikropočítačů

k periferním zařízením, jako jsou pevné disky či tiskárny, a k dalším počítačům a místním sítím (LAN).

rozhraní vyžádaného volání

– demand-dial interface

Logické rozhraní představující připojení vyžádaného volání (spojení PPP) nakonfigurované na volajícím směrovači. Rozhraní vyžádaného volání obsahuje konfigurační informace, jako je použitý port, adresování potřebné k vytvoření spojení (například telefonní číslo), metody ověření a šifrování a oprávnění k ověření.

rozhraní Winsock – Windows Sockets

Standard rozhraní API používaný v systému Windows a zajišťující obousměrný, spolehlivý, řezaný a neduplikovaný tok dat.

rozsáhlá síť (WAN) – WAN

Komunikační síť propojující geograficky vzdálené počítače, tiskárny a další zařízení. Rozsáhlá síť umožňuje všem připojeným zařízením na síti vzájemně komunikovat. Viz také místní síť.

rozšíření na straně klienta – client-side extensions

Komponenty skupinových zásad, které jsou v některých případech zodpovědné za zavedení skupinových zásad na klientském počítači.

rozšíření správce klastru

– Cluster Administrator extension

Dynamická knihovna (DLL), která umožňuje správcí klastru konfigurovat nový typ prostředí. Rozšíření správce klastru používá API rozšíření správce klastru. Viz také správce klastru; prostředek; klastr.

rozšířený oddíl – extended partition

Část základního disku, která může obsahovat logické jednotky. Rozšířený oddíl použijte v případě, že chcete na základním disku používat více než čtyři svazky. Rozšířeným oddílem může být pouze jeden ze čtyř oddílů, které jsou povoleny pro fyzický disk; k vytvoření rozšířeného oddílu není nutný primární oddíl. Rozšířené oddíly lze vytvářet pouze na základních discích. Viz také základní disk; logická jednotka; oddíl; primární oddíl; volné místo.

rozšiřující komunikační zařízení

– augmentative communication devices

Doplňkový software a hardware, který pomáhá uživatelům s nějakým postižením řídit počítač pomocí asistenční technologie. Příklady

jsou systémy rozpoznávání řeči a čtečky obrazovky.

ručně vytvořený vztah důvěryhodnosti

– shortcut trust

Obousměrný vztah důvěryhodnosti, který je explicitně vytvořen mezi dvěma doménami systému Windows 2000 v různých stromech v rámci jedné doménové struktury. Smyslem ručně vytvořeného vztahu důvěryhodnosti je optimalizovat proces ověření probíhající mezi doménami. Ručně vytvořený vztah důvěryhodnosti lze vytvořit pouze mezi dvěma doménami systému Windows 2000 v jedné doménové struktuře. Všechny ručně vytvořené vztahy důvěryhodnosti jsou tranzitivní. Viz také strom domén; doménová struktura; vztah tranzitivní důvěryhodnosti.

Ř

řadič domény – domain controller

V rámci domény systému Windows NT Server a Windows 2000 Server je to počítač, který ověřuje přihlášení k doméně a spravuje zásady zabezpečení a hlavní databázi domény. Přihlášení uživatele mohou ověřovat servery i řadiče domén, změny hesel se však vykonávají pomocí řadiče domény.

řečový syntetizátor – speech synthesizer

Pomocné zařízení vytvářející mluvená slova buď řazení předem nahraných slov nebo na programováním počítače takovým způsobem, aby vytvářel zvuky tvořící mluvená slova.

řízení přístupu – access control

Bezpečnostní mechanismus v systému Windows NT a Windows 2000 určující, které objekty může komitent zabezpečení používat a jak je může používat. Viz také ověření; komitent zabezpečení.

řízení přístupu – admission control

Služba používaná ke správě síťových zdrojů sdílených síťových segmentů.

řízení přístupu k médiu – media access control

Vrstva v síťové architektuře systému Windows NT a Windows 2000, která se stará o přístup k síti a detekci kolizí.

S

sada svazků – volume set

Kombinace oddílů na jednom fyzickém disku, které se jeví jako jedna logická jednotka. Viz také odolnost proti chybám; sada svazků stripe set.

sada svazků stripe set – stripe set

Ukládání dat přes identické oddíly na různých oddílech. Sada stripe set nezajišťuje odolnost proti chybám, což dokáží sady stripe set s paritou. Viz také odolnost proti chybám; oddíl; sada svazků stripe set s paritou; sada svazků.

sada svazků stripe set s paritou

– stripe set with parity

Metoda ochrany dat, kdy jsou data rozložena do pruhů velkých bloků na všech discích v poli. Redundantnost dat zajišťují informace o paritě. Tato metoda zajišťuje odolnost proti chybám. Viz také sada svazků stripe set; odolnost proti chybám.

sada zrcadlení – mirror set

Plně redundantní neboli zrcadlová kopie dat. Sada zrcadlení poskytuje identickou kopii vybraného disku. Všechna data zapisovaná na primární disk se zapíše také na zrcadlový disk. Tím získáte okamžitý přístup k jinému disku s kopií informací. Sady zrcadlení zajišťují odolnost proti chybám. Viz také sada svazků stripe set s paritou; sada svazků.

samostatný certifikační úřad

– stand-alone certification authority

Certifikační úřad systému Windows 2000, který není integrován do služby Active Directory. Viz také certifikační úřad; certifikační úřad rozlehlé sítě.

sběrnice – bus

Komunikační linka používaná k přenosu dat mezi komponentami počítačového systému. Sběrnice je v zásadě dálnice umožňující různým částem systému sdílet data.

sdílená tiskárna – shared printer

Tiskárna přijímající vstup z více než jednoho počítače. Například tiskárnu připojenou k počítači v síti lze sdílet tak, aby byla k dispozici i uživatelům ostatních počítačů. Pro sdílenou tiskárnu je rovněž používán termín síťová tiskárna.

sdílení tisku – print sharing

Schopnost počítače se systémem Windows NT Workstation nebo Windows NT Server sdílet tiskárnu na síti. Lze toho dosáhnout poklepnutím na ovládací panel Tiskárny nebo zadáním příkazu síťového sdílení na příkazovém řádku.

sdružení IETF – Internet Engineering Task Force

Otevřená komunita návrhářů sítí, operátorů, dodavatelů a výzkumníků, kteří se zabývají vývojem architektury sítě Internet a bezproblémovým provozem sítě Internet. Technické práce jsou prováděny pracovními skupinami, které jsou uspořádány podle jednotlivých oblastí (například směrování, přenos nebo zabezpečení), a prostřednictvím diskusních skupin. Standardy sítě Internet jsou vyvíjeny ve formě specifikací RFC (Requests for Comments), což jsou posloupnosti poznámek věnující se celé řadě aspektů počítačového zpracování a počítačové komunikace se zvláštním zřetelem na síťové protokoly, programy a koncepce.

sekundární server – secondary server

Autoritativní server DNS pro zónu, který slouží jako zdroj pro replikaci zóny na ostatní servery. Sekundární hlavní servery aktualizují data zóny pouze přenosem dat zóny z ostatních serverů DNS. Nemají schopnost provádět aktualizace zóny přímo. Viz také hlavní server; přenos zóny.

sekundární úložiště – secondary storage

Zařízení pro ukládání, které se používá k ukládání dat migrovaných ze spravovaných svazků. Sekundární úložiště zahrnují části pevného disku používané k migraci pracovní oblasti.

server

Počítač zajišťující sdílené zdroje pro uživatele sítě.

server DNS – DNS server

Počítač, na kterém běží programy serveru DNS obsahující překlad názvů na adresy IP, překlad adres IP na názvy, informace o struktuře doménového stromu a další informace. Servery DNS se také pokoušejí vyřešit požadavky klientů.

server emulace LAN (LES) – LAN emulation server

Centrální řídicí bod sítě ELAN. Server emulace místní sítě umožňuje klientům emulace LAN připojit se k síti ELAN a překládat adresy místní sítě na adresy ATM. Viz také režim asyn-

chronního přenosu; emulovaná místní síť; emulace místní sítě.

server firewall – firewall

Kombinace hardwaru a softwaru, která poskytuje systém zabezpečení, zpravidla s cílem zabránit neoprávněnému přístupu zvnějšku do vnitřní sítě nebo do sítě intranet. Server firewall zabráňuje přímé komunikaci mezi sítí a externími počítači, a to směrováním komunikace přes server proxy umístěný mimo síť. Server proxy určuje, zda je bezpečné předat soubor do sítě. Pro server firewall je rovněž používán termín brána zabezpečení.

server komponent – Component Server

Server poskytující platformu pro spouštění služeb komponent, jako jsou vyrovnávání zatížení aplikací, transakční služby a správa aplikací.

server pro vzdálený přístup – remote access server

Libovolný počítač se systémem Windows 2000 Server, na němž je nakonfigurován příjem připojení vzdáleného přístupu.

server proxy WINS – WINS proxy

Počítač, který naslouchá vícesměrovému vysílání dotazů na názvy a odpovídá pro ty názvy, které nejsou v místní podsíti. Server proxy komunikuje při překladu názvů s názvovým serverem a zjištěné názvy uchovává po určitou dobu v mezipaměti. Viz také služba WINS.

server předmostí – bridgehead server

Server, který přijímá a posílá dál komunikaci elektronické pošty na obou koncích spojení, což je podobné funkci vykonávané branou.

server síťového sídla – site server

Počítač se spuštěným systémem Windows NT server, na němž byla spuštěna instalace sídla Systems Management Server (SMS). Jakmile je na počítači instalován server SMS, počítač přejímá roli serveru sídla. Server sídla, který hostí komponenty SMS potřebné ke sledování a správě sídla SMS, obvykle vykonává několik dalších rolí SMS, takže pracuje jako server komponent, bod přístupu klientů a distribuční bod.

server SMS – Systems Management Server

Součást sady Windows BackOffice. Server SMS zahrnuje kolekci inventáře a nástroje zavedení a diagnostiky. Server SMS může výrazným způsobem zautomatizovat úlohy inovace softwaru, umožnit vzdálené řešení problémů,

správu licencí softwaru a sledování počítačů a sítí.

server VPN – VPN server

Počítač přijímající připojení VPN od klientů VPN. Server VPN může zajistit připojení VPN vzdáleného přístupu nebo připojení VPN mezi směrovači.

servery vysílání datových proudů

– streaming media servers

Software (například Microsoft Media Technology) poskytující podporu multimédiím a umožňující předávání obsahu přes Internet nebo intranet ve formátu ASF (Advanced Streaming Format).

seznam důvěryhodných certifikátů (CTL)

– certificate trust list

Podepsaný seznam certifikátů kořenového certifikačního úřadu, které správce považuje pro určené účely (například ověřování klientů nebo zabezpečení elektronické pošty) za důvěryhodné. Viz také certifikát; certifikační úřad; kořenový certifikát; kořenový certifikační úřad.

seznam HCL – Hardware Compatibility List

Seznam všech zařízení podporovaných systémem Windows 2000.

seznam odvolaných certifikátů (CRL)

– certificate revocation list

Dokument spravovaný a publikovaný certifikačním úřadem, v němž jsou uvedeny odvolané certifikáty. Seznam CRL je podepsán soukromým klíčem certifikačního úřadu, aby byla zajištěna jeho integrita. Viz také certifikát; certifikační úřad.

seznam pro řízení přístupu do systému (SACL)

– system access control list

Představuje část popisovače zabezpečení nějakého objektu určující, které události se budou auditovat podle uživatelů nebo skupin. Příklady auditovaných událostí jsou přístup k souboru, pokusy o přihlášení a ukončení systému. Viz také položka řízení přístupu; seznam řízení zabezpečeného přístupu; objekt; popisovač zabezpečení.

seznam procházení – browse list

Libovolný seznam položek, kterým lze procházet, jako například seznam serverů v síti nebo seznam tiskáren zobrazený Průvodcem přidání tiskárny.

seznam řízení přístupu (ACL) – access control list

Část popisovače zabezpečení, která vyhodnocuje ochrany aplikované na nějaký objekt. Vlastník objektu má k dispozici volné řízení přístupu k objektu a může změnit seznam ACL objektu a umožnit tak nebo zakázat ostatním uživatelům přístup k objektu. Seznamy ACL jsou tvořeny položkami řízení přístupu (ACE). Každý popisovač zabezpečení objektu v systému Windows NT nebo Windows 2000 obsahuje čtyři komponenty zabezpečení: tvůrce (vlastníka), skupinu (pro kompatibilitu se systémem POSIX, která je navíc je spojena s „primární skupinou“ nastavenou v jednotlivých objektech uživatelů ve správci uživatelů), seznam řízení zabezpečeného přístupu (DACL, často označovaný jen za ACL, který určuje oprávnění objektu) a seznam pro řízení přístupu do systému (SACL, který určuje auditování). Viz také seznam řízení zabezpečeného přístupu.

seznam řízení zabezpečeného přístupu (DACL)**– discretionary access control list**

Část popisovače zabezpečení nějakého objektu, která zaručuje nebo odpírá specifickým uživatelům a skupinám oprávnění k přístupu k danému objektu. Pouze vlastník objektu může změnit oprávnění k přístupu v DACL, a proto je přístup k objektu rozhodnutím jeho vlastníka. Viz také položka řízení přístupu; objekt; seznam pro řízení přístupu do systému; popisovač zabezpečení.

shrnutí tras – route sumarization

Praxe kombinování více identifikačních čísel sítí do jediné trasy ve směrovací tabulce. Shrnování tras lze používat, jsou-li infrastruktury hierarchického směrování dobře naplánovány.

schéma – schema

Popis atributů a tříd objektů uložených v adresáři služby Active Directory. Pro každou třídu objektů schéma definuje atributy, které třída objektů musí mít, další atributy, které může mít, a třídu objektů, která může být této třídě nadřazena. Schéma služby Active Directory lze aktualizovat dynamicky. Aplikace například může rozšířit schéma o nové atributy a třídy a tato rozšíření okamžitě použít. Aktualizace schématu jsou prováděny vytvořením nebo změnou objektů schémat uložených v adresáři služby Active Directory. Objektům schématu je

stejně jako ostatním objektům v adresáři služby Active Directory přiřazen seznam řízení přístupu, a proto mohou schéma změnit pouze ověření uživatelé.

síť LocalTalk – LocalTalk

Síťový hardware Apple vestavěný do všech počítačů Macintosh. Síť LocalTalk zahrnuje kabely a konektory pro připojení součástí a síťových zařízení, které jsou částí síťového systému AppleTalk. Pro síť LocalTalk byl původně používán termín AppleTalk Personal Network.

síť token ring – Token Ring

Určitý typ síťového média, který propojuje klienty v uzavřeném prstenci a klientům zaručuje možnost používat síť prostřednictvím předávání tokenů. Viz také síť LocalTalk; rozhraní FDDI.

síť všesměrového vysílání – broadcast network

Síť, která podporuje více než dva připojené směrovače a má možnost adresovat jednu fyzickou zprávu všem připojeným směrovačům (všesměrové vysílání). Příkladem sítě všesměrového vysílání je síť ethernet.

síťová adresa – network address

Viz identifikátor sítě.

síťová vrstva – network layer

Vrstva adresující zprávy a překládající logické adresy a názvy na fyzické adresy. Také určuje trasu od zdrojového k cílovému počítači a řeší problémy s přenosem, jako je přepínání, směrování a řízení zahlcení sítě datovými pakety.

síťové médium – network media

Typ fyzického propojení kabely a protokolů nižší úrovně používaný k vysílání a příjmu rámců. Například ethernet, FDDI a token ring.

síťové sídlo – site

Místo v síti obsahující servery služby Active Directory. Síťové sídlo je definováno jako jedna nebo více dobře propojených podsítí TCP/IP. („Dobře propojený“ znamená, že připojení k síti je vysoce spolehlivé a rychlé.) Protože počítače v jednom sídle k sobě mají z hlediska sítě blíž, komunikace mezi nimi je spolehlivá, rychlá a výkonná. Definování sídla jako sady podsítí umožňuje správcům nakonfigurovat topologii replikace a přístup ke službě Active Directory při využití fyzické sítě. Když se uživatel přihlásí do sítě, klienty Active Directory najdou servery Active Directory ve stej-

ném sídle, jako je klient. V rámci serveru Systems Management Server jsou to servery síťových sídel a klientské počítače svázané skupinou podsítí, například jako podsítí IP nebo síťové číslo IPX. Viz také služba Locator; podsítí; topologie replikace.

síťový adaptér – network adapter

Software nebo zásuvná karta, která připojuje uzel neboli hostitele k místní síti (LAN). Je-li uzel členem klastru serverů, je síťový adaptér objektem klastru serverů (objektem síťového rozhraní).

skript – script

Určitý typ programu skládající se ze sady instrukcí pro aplikaci nebo nástroj. Skript obvykle vyjadřuje příkazy pomocí pravidel a syntaxe příslušné aplikace či nástroje v kombinaci s jednoduchými řídicími strukturami, jako jsou smyčky a výrazy podmínek. V prostředí Windows je často možné setkat se místo termínu „skript“ s označením „dávkový program“.

skupina – group

Kolekce uživatelů, počítačů, kontaktů a dalších skupin. Skupiny lze používat jako kolekce zabezpečení nebo jako kolekce pro distribuci elektronické pošty. Distribuční skupiny jsou používány pouze pro elektronickou poštu. Zabezpečené skupiny slouží k udělení přístupu k prostředkům a také jako seznamy pro distribuci elektronické pošty. V klastrech serverů je to kolekce prostředků a základní jednotka převedení. Viz také doménová místní skupina; globální skupina; nativní režim; univerzální skupina.

skupina distribučních bodů

– distribution point group

Na serveru Systems Management Server je to sada distribučních bodů, které lze spravovat jako jednu entitu.

skupina vícesměrového vysílání – multicast group

Skupina členských hostitelů TCP/IP nakonfigurovaná tak, aby sledovala a přijímala datagramy odeslané na zadanou cílovou adresu IP. Cílová adresa skupiny je sdílenou adresou IP v oblasti adres třídy D (224.0.0.0 až 239.255.255.255). Viz také datagram.

skupiny zabezpečení – security groups

Skupiny, které lze použít ke správě oprávnění uživatelů a dalších objektů domény.

sledovací program – sniffer

Aplikace nebo zařízení, které dokáže číst, sledovat a zachytávat výměnu síťových dat a čist síťové pakety. Nejsou-li pakety zašifrované, poskytuje takový program úplný pohled na data v paketu.

sledování sítě – Network Monitor

Nástroj zachytávání a analýzy paketů používaný k zobrazování provozu sítě. Tento nástroj je součástí systému Windows 2000 Server, server Systems Management Server však obsahuje jeho úplnější verzi.

sledování softwaru – software metering

V rámci serveru Systems Management Server je to proces, kterým SMS sleduje a spravuje použití softwarových aplikací s cílem zajištění naplnění licenčních požadavků nebo pochopením použití softwaru.

sloučení domén – domain consolidation

Proces zkombinování dvou nebo více domén do jedné větší domény.

složka Sysvol – Sysvol

Sdílený adresář, v němž je uložena kopie veřejných souborů domény, které jsou v rámci domény replikovány mezi všemi řadiči domény. Viz také doména; řadič domény.

složka Tiskárny – printers folder

Složka ovládacích panelů obsahující průvodce přidáním tiskárny a ikony všech tiskáren instalovaných na počítači.

služba Admission Control QoS

– QoS Admission Control Service

Softwarová služba umožňující řídit přidělování šířky pásma a síťové zdroje přiřazené části sítě. Je možné přidělit důležitým aplikacím větší šířku pásma a méně důležitým menší. Službu Admission Control QoS lze instalovat na libovolném do sítě zapojeném počítači s Windows 2000.

služba Caching Resolver – caching resolver

V rámci systému Windows 2000 je to služba překladu adres IP na straně klienta DNS, která v mezipaměti uchovává nedávno zjištěné informace o názvech domén DNS. Tato služba poskytuje systémový přístup programům spolupracujícím se servery DNS pro záznamy o prostředcích získané ze serverů DNS v průběhu zpracování dotazů na názvy. Data v mezipaměti jsou používána po omezenou dobu

a stárnou v závislosti na aktivní hodnotě TTL (Time To Live). Hodnotu TTL lze nastavit pro každý záznam o prostředku (RR) individuálně. V opačném případě je výchozí hodnotou minimální hodnota TTL nastavená v záznamu SOA RR zóny. Viz také mezipaměť; ukládání do mezipaměti; interval vypršení platnosti; minimální hodnota TTL; překladač; záznam o prostředku; hodnota TTL.

služba Call Manager – Call Manager

Softwarová součást ustanovující, spravující a ukončující spojení mezi dvěma počítači.

služba Certificate Services – certificate services

Služba Windows 2000 vydávající certifikáty pro určitý certifikační úřad. Poskytuje управительné služby vydávání a správy certifikátů. Viz také certifikát; certifikační úřad.

služba Client Service for Netware

– Client Service for Netware

Služba, která je součástí systému Windows 2000 Professional a umožňuje klientským počítačům provádět přímá připojení k prostředkům v počítačích se softwarem serveru NetWare 2.x, 3.x nebo 4.x nebo 5.x.

služba Cluster Service – Cluster Service

Clussvc.exe, základní spustitelný soubor komponenty práce s klastry Windows, která vytváří klastr serverů, řídí všechny aspekty provozu klastru serverů a spravuje databázi klastru. Na každém uzlu v klastru serverů je spuštěna jedna instance služby Cluster Service.

služba DHCP – DHCP Service

Služba umožňující počítači fungovat jako server DHCP a konfigurovat klientské síťové počítače podporující DHCP. Protokol DHCP běží na serverovém počítači a umožňuje automatickou a centralizovanou správu adres IP a dalších konfiguračních nastavení protokolu TCP/IP klientských počítačů na síti.

služba DNS – Domain Name System

Hierarchický systém pojmenování používaný k vyhledávání názvů domén na Internetu nebo privátních sítí TCP/IP. Služba DNS zajišťuje připojování názvů domén DNS k adresám IP a naopak. To dovoluje uživateli, počítačům a aplikacím využívat službu DNS a zadávat vzdálené systémy plně kvalifikovanými názvy domén a nikoli adresami IP. Viz také doména; ping.

služba Gateway Service for Netware

– Gateway Service for Netware

Služba, která vytváří bránu a umožňuje klientským počítačům, na nichž je spuštěn pouze klientský software Microsoft, získat přes server se systémem Windows 2000 přístup k prostředkům NetWare, jako jsou například souborové a tiskové služby.

služba Locator – domain controller locator

Algoritmus běžící v kontextu služby Netlogon, který vyhledává řadiče domén na síti systému Windows 2000. Služba Locator dokáže vyhledat řadiče domén pomocí názvů DNS (v případě počítačů podporujících IP/DNS) nebo pomocí názvů NetBIOS (v případě počítačů se systémy Windows 3.x, Windows for Workgroups, Windows NT 3.5 nebo novějším, Windows 95 či Windows 98, nebo ji lze použít na síti, kde není k dispozici komunikace IP).

služba Microsoft Component Services

– Microsoft Component Services

Program spuštěný na internetovém nebo jiném serveru, který spravuje požadavky na aplikace a databázové transakce ze strany klientského uživatele. Služba Microsoft Component Services zbavuje uživatele a klientský počítač nutnosti formulovat dotazy do neznámých databází a předává dotazy databázovým serverům. Zároveň se stará o zabezpečení, připojení k jiným serverům a integritu transakcí.

služba NDS – Novell Directory Services

V sítích se systémem Novell NetWare 4.0 a 5.0 je to distribuovaná databáze, v níž jsou uchovávány informace o všech prostředcích v síti a která poskytuje přístup k těmto prostředkům.

služba pojmenování – naming service

Služba, která je obdobou služeb WINS nebo DNS a umožňuje překlad popisných názvů na adresy nebo jiná speciálně definovaná data prostředků, které slouží k vyhledání síťových prostředků různých typů a účelů.

služba překladu názvů – name resolution service

Služba vyžadovaná propojenými sítěmi TCP/IP překládající názvy počítačů na adresy IP a adresy IP na názvy počítačů. (Lidé používají pro připojení k počítačům „přátelské“ názvy, programy používají adresy IP.) Viz také propojení sítí; protokol TCP/IP.

služba QoS – Quality of Service

Sada standardů zajištění kvality a mechanismů pro přenos dat, která je implementována v systému Windows 2000.

služba replikace souborů – File Replication service

Služba používaná distribuovaným systémem souborů (DFS) k synchronizaci obsahu mezi přiřazenými replikami a službou Active Directory Sites and Services k replikaci topologických informací a informací globálního katalogu do řadičů domén.

služba Time Service – Time Service

Prostředek klastru serverů, který je v čase konzistentní na všech uzlech.

služba vzdáleného přístupu (RAS)**– Remote Access Service**

Služba Windows NT 4.0 poskytující možnosti vzdáleného připojení k síti pro mobilní pracovníky a správce systému, kteří sledují a spravují servery v různých kancelářích.

služba Windows Installer – Windows Installer

Komponenta systému Windows 2000 standardizující způsob, jakým se aplikace instalují na více počítačů. Požaduje, aby měla každá aplikace svůj vlastní instalační program nebo skript.

služba WINS – Windows Internet Name Service

Softwarová služba, která dynamicky mapuje adresy IP na názvy počítačů (názvy pro rozhraní NetBIOS). Umožňuje tak uživatelům přístup k prostředkům na základě názvu (není tedy nutné používat adresy IP, jejichž zapamatování je složité). Servery WINS podporují klienty se systémem Windows NT 4.0 a s dřívějšími verzemi operačních systémů společnosti Microsoft. Viz také služba DNS.

služba WMI**– Windows Management Instrumentation**

Technologie společnosti Microsoft, která reprezentuje fyzické a logické objekty existující v prostředí spravovaném systémem Windows konzistentním a jednotným způsobem. Služba WMI má za úkol zjednodušit vývoj dobře integrovaných aplikací správy a umožnit výrobcům poskytovat vysoce výkonná a škálovatelná řešení správy pro podniková prostředí.

služby IIS – Internet Information Services

Softwarové služby, které kromě dalších funkcí sítě Internet podporují vytváření, konfiguraci

a správu stránek WWW. Služby IIS (Internet Information Services) zahrnují protokol NNTP (Network News Transfer Protocol), protokol FTP (File Transfer Protocol) a protokol SMTP (Simple Mail Transfer Protocol). Viz také protokol FTP; protokol NNTP; protokol SMTP.

služby vzdálené instalace (RIS)**– Remote Installation Services**

Volitelná součást systému Windows 2000, která vzdáleně instaluje systém Windows 2000 Professional. Instaluje operační systémy na vzdálené počítače umožňující restart tím, že daný počítač připojí k síti, spustí jej a přihlásí se platným uživatelským účtem.

směrovací protokol – routing protocol

Sada periodických nebo vyžádaných zpráv obsahujících směrovací informace, které si směrovače vyměňují v zájmu sdílení směrovacích informací a zajištění odolnosti proti chybám. Kromě počáteční konfigurace vyžadují dynamické směrovače jen malou následnou obsluhu, a proto je lze použít i ve větším propojení sítí.

směrovací tabulka – routing table

Databáze směrovačů obsahující informace o identifikačních číslech sítě, adresách pro předávání a metrikách dosažitelných síťových segmentů na propojených sítích.

směrovač – router

Síťový počítač pomáhající místním a rozsáhlým sítím získat možnosti interakce a propojitelnosti, který také může propojovat místní síť s různou topologií (například ethernet a token ring).

směrovač IP – Internet Protocol router

Systém připojený k několika fyzickým sítím TCP/IP, který umožňuje doručovat mezi těmito sítěmi pakety IP. Viz také paket; směrovač; směrování; protokol TCP/IP.

směrovač okraje oblasti (ABR) – area border router

Směrovač, který je připojen k více oblastem. Směrovače okraje oblasti mají samostatné stavové databáze pro každou oblast. Viz také stavová databáze.

směrování – routing

Proces předávání paketu na základě cílové adresy IP.

směrování CIDR – classless interdomain routing

Metoda přiřazování adres IP, které nevycházejí z původních tříd adres IP. Směrování CIDR bylo vytvořeno, aby se zabránilo plýtvání veřejnými adresami IP a aby byla minimalizována velikost internetových směrovacích tabulek.

SMTP

Viz protokol SMTP.

SOA

Viz záznam SOA.

softwarový inventář – software inventory

V rámci serveru Systems Management Server je to automatizovaný proces, který SMS používá ke sběru informací o softwaru na klient-ských počítačích.

SOHO – Small Office/Home Office

Kancelář s několika počítači, kterou lze považovat za samostatně fungující nebo za součást větší sítě.

soubor adres – address pool

Skupina adres IP v nějakém rozsahu. Soubory adres pak může server DHCP dynamicky přiřazovat klientům DHCP.

soubor Hosts – hosts file

Místní textový soubor ve stejném formátu jako soubor /etc/hosts systému 4.3 Berkeley Software Distribution (BSD) UNIX. Tento soubor převádí názvy hostitelů na adresy IP. V systému Windows 2000 je tento soubor uložen ve složce %Systemroot%\System32\Drivers\Etc. Viz také kořenová složka systému.

soubor mezipaměti – cache file

Soubor používaný serverem DNS k předzavedení mezipaměti názvů při spuštění služby. Pro soubor mezipaměti je rovněž používán termín soubor „odkazů na kořenové servery“, protože server DNS používá záznamy o prostředcích uložené v tomto souboru k vyhledání kořenových serverů poskytujících odkazy na autoritativní servery pro vzdálené názvy. Pro servery DNS systému Windows je soubor mezipaměti pojmenován Cache.dns a je umístěn ve složce %Systemroot%\System32\Dns. Viz také autoritativní; mezipaměť; kořenová složka systému.

soubor odpovědí – answer file

Textový soubor, který lze použít pro automatické zadávání vstupů v rámci bezobslužné instalace Windows 2000. Tento vstup zahrnuje

parametry odpovídající na otázky instalačního programu konkrétní instalace. V některých případech lze tento textový soubor použít k zajištění vstupů pro průvodce, například průvodce instalací služby Active Directory, který pomocí instalačního programu přidává v systému Windows 2000 Server službu Active Directory. Výchozí soubor odpovědí pro instalační program se označuje jako Unattend.txt.

soubor protokolu – log file

Soubor, který slouží k ukládání zpráv generovaných aplikací, službou nebo operačním systémem. Tyto zprávy jsou používány ke sledování prováděných operací. Například servery WWW uchovávají soubory protokolů obsahující všechny požadavky vznesené na příslušný server. Soubory protokolů jsou obvykle běžné textové soubory ve formátu ASCII s příponou LOG. V rámci zálohování je to soubor obsahující záznam data, kdy byly vytvořeny pásky, a seznam názvů souborů a adresářů, které byly úspěšně zálohovány a obnoveny. Soubory protokolů jsou rovněž vytvářeny službou výstrahy a protokolování výkonu.

soubor výpisu – dump file

Soubor používaný k ukládání dat paměti pro případ poruchy.

soubor ZAP (.zap) – ZAP file

Soubor aplikačního balíčku nulové správy systému Windows. Je to textový soubor (podobný souboru .ini) popisující, jak se má nainstalovat nějaká aplikace (jaký příkazový řádek se má použít), vlastnosti aplikace (název, verze a jazyk) a jaké vstupní body má aplikace automaticky nainstalovat (pro přípony názvů souborů, CLSID a ProgID). Soubor .zap je obvykle uložen na stejném místě na síti, jako je instalační program, na který se odkazuje.

souborový server – file server

Server poskytující v rámci celé organizace přístup k souborům, programům a aplikacím.

soukromé adresy – private addresses

Adresy IP v rámci soukromého adresovacího prostoru určené pro používání organizacemi k adresování soukromého intranetu. Soukromá adresa IP je v jednom z následujících bloků adres: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16.

soukromý klíč – private key

Tajná polovina páru kryptografických klíčů, která se používá v algoritmu veřejného klíče. Soukromé klíče se zpravidla používají k digitálnímu podepisování dat nebo dešifrování dat, která byla zašifrována pomocí odpovídajícího veřejného klíče. Viz také veřejný klíč.

specifikace RFC – Request for Comment

Dokument definující standard protokolu TCP/IP. Specifikace RFC publikuje organizace IETF (Internet Engineering Task Force) a další pracovní skupiny.

spojení mezi směrovači na požádání – on-demand router-to-router connection

Spojení VPN mezi směrovači, které je skutečně zavoláním směrovače s telefonickým připojením k Internetu.

spouštěcí disketa vzdálené instalace (RBFG.exe) – remote installation boot floppy

Součást služeb vzdálené instalace používaný k vytvoření spouštěcí diskety, která je zapotřebí k instalaci operačních systémů pomocí služby RIS na určité klientské počítače.

správa klíčů – key management

Zabezpečená správa soukromých klíčů používaných v šifrování s veřejným klíčem. Systém Windows 2000 spravuje soukromé klíče a udržuje jejich důvěrnost pomocí rozhraní CryptoAPI a zprostředkovatelů kryptografických služeb poskytovatelů (CPS). Viz také soukromý klíč; rozhraní CryptoAPI; zprostředkovatel kryptografických služeb.

správce klastru – Cluster Administrator

Aplikace (Cluadmin.exe), která slouží ke konfiguraci klastru a jeho uzlů, skupin a prostředků. Správce klastru lze spustit na libovolném členu důvěryhodné domény bez ohledu na to, zda se jedná o uzel klastru. Viz také rozšíření správce klastru; cluster.exe; uzel; prostředek; klastr.

správce DHCP – DHCP Manager

Základní nástroj správy serverů DHCP. Správce DHCP je nástroj konzoly MMC, který se přidává do nabídky nástrojů správy po instalaci služby DHCP.

správce nástrojů – Utility Manager

Funkce systému Windows 2000 umožňující správcům zobrazovat si stav aplikací a nástrojů a snáze přizpůsobovat další funkce.

správce sítě – network administrator

Osoba odpovídající za nastavení a správu řadičů domén či místních počítačů a jejich účtů uživatelů a skupin. Správce sítě také přiřazuje hesla a oprávnění a pomáhá uživatelům s problémy práce v síti. Správci jsou členy skupiny Administrators a mají plnou kontrolu nad doménou nebo počítačem.

správce synchronizace – Synchronization Manager

Ve Windows 2000 je to nástroj používaný k zajištění, že soubor nebo adresář na klientském počítači obsahuje stejná data jako odpovídající soubor a adresář na serveru.

správce zabezpečení – security administrator

Uživatel, který má práva spravovat auditování a protokol zabezpečení. Standardně jsou tato práva přiřazena skupině Administrators. Viz také auditování; seznam pro řízení přístupu do systému; uživatelská práva.

spustitelný disk CD-ROM – bootable CR-ROM

Metoda automatizované instalace, která spouští instalační program z disku CD-ROM. Tato metoda je užitečná u vzdálených počítačů s pomalým připojením a bez oddělení IT. Viz také automatizovaná instalace.

spuštění – boot

Proces zapnutí nebo resetování počítače. Při prvním zapnutí nebo resetování počítač vykoná software, který zavede a spustí operační systém počítače a připraví jej k použití.

statické směrování – static routing

Směrování omezené na pevné směrovací tabulky, protiklad dynamicky aktualizovaných směrovacích tabulek. Viz také dynamické směrování; směrování; směrovací tabulka.

stav systému – system state

V rámci zálohování je to kolekce dat specifických pro systém, která lze zálohovat a obnovit. U všech operačních systémů Windows 2000 mezi stavová data systému patří registr, registrační databáze tříd a spouštěcí soubory systému. V systému Windows 2000 Server mezi stavová data systému patří rovněž databáze služby Certificate Services (pokud je server používán jako certifikační). Je-li server řadičem domény, patří mezi stavová data systému rovněž databáze služby Active Directory a adresář Sysvol. Viz také Active Directory; řadič domény; registr; složka Sysvol.

stavová databáze (LSDB) – link state database

Mapa oblastí udržovaná směrovači OSPF. K její aktualizaci dochází při každé změně topologie sítě. Stavová databáze slouží k výpočtu tras IP, které musí být po každé změně topologie vypočteny znovu. Viz také protokol OSPF.

stavová oblast – status area

Oblast na hlavním panelu napravo od tlačítek. Ve stavové oblasti se zobrazuje čas a rovněž ikony poskytující rychlý přístup k programům, například ovládání hlasitosti a možnosti napájení. Dočasně se zde mohou objevovat i další ikony poskytující informace o stavu aktivit. Například po odeslání dokumentu na tiskárnu se zde zobrazí ikona tiskárny a po dokončení tisku zase zmizí.

stránkovací soubor – paging file

Skrytý soubor na pevném disku, který systém Windows 2000 používá k ukládání částí programu a datových souborů, které se nevejdou do paměti. Stránkovací soubor a fyzická paměť, neboli paměť RAM, tvoří virtuální paměť. Systém Windows 2000 podle potřeby přesune data ze stránkovacího souboru do paměti a rovněž z paměti do stránkovacího souboru, pokud je vyžadován prostor pro nová data. Pro stránkovací soubor je rovněž používán termín odkládací soubor. Viz také paměť RAM; virtuální paměť.

stránkování – paging

Proces přesunu virtuální paměti mezi fyzickou pamětí a diskem. Ke stránkování dochází v okamžiku dosažení limitů fyzické paměti a to pouze pro data, která ještě nejsou na prostoru disku „zálohována“. Například data souborů se nestránkují, protože již mají vymezený prostor v rámci systému souborů. Viz také virtuální paměť.

strom domén – domain tree

V rámci služby DNS je to invertovaná hierarchická stromová struktura, která se používá k indexování názvů domén. Stromy domén jsou, co se účelu a koncepce týče, obdobou adresářových stromů používaných počítačovými systémy pro diskovou paměť. Viz také název domény; obor názvů.

strom konzoly – console tree

Podokno konzoly MMC (Microsoft Management Console), které zobrazuje hierarchicky

uspořádaný obor názvů. Podle výchozího nastavení se jedná o levé podokno okna konzoly, které však může být skryté. Položky ve stromu konzoly (například webové stránky, složky a ovládací prvky) a jejich hierarchické uspořádání určují možnosti správy konzoly. Viz také konzola MMC.

svazek – volume

Část fyzického disku, která funguje jako samostatný fyzický disk. Ve složce Tento počítač a v Průzkumníku Windows se svazky zobrazují jako místní disky, například C: nebo D:.

svazek RAID**– redundant array of independent disks**

Metoda používaná ke standardizaci a kategorizaci diskových systémů odolných proti chybám. K dispozici je šest úrovní, které se vzájemně liší výkonem, spolehlivostí i náklady. Systém Windows 2000 poskytuje tři úrovně RAID: úroveň 0 (rozkládání), úroveň 1 (zrcadlení) a úroveň 5 (sady stripe sets s paritou). Viz také odolnost proti chybám; zrcadlený svazek; svazek RAID-5; prokládaný svazek.

svazek RAID-5 – RAID-5 volume

Svazek odolný proti chybám, v němž jsou data a parita rozloženy do pruhů na třech nebo více discích. Parita je vypočítávanou hodnotou, která slouží k rekonstrukci dat po selhání. Pokud část fyzického disku selže, lze na základě zbylých dat a parity zrekonstruovat chybějící data.

symetrické šifrování – symmetric key encryption

Šifrovací algoritmus, který pro šifrování i dešifrování vyžaduje stejný tajný klíč, což se často také označuje za šifrování s tajným klíčem. Díky své rychlosti je symetrické šifrování obvykle upřednostňováno před asymetrickým šifrováním v případech, že odesílatel zprávy potřebuje zašifrovat velký objem dat. Viz také šifrování s veřejným klíčem.

symetrické víceprocesorové zpracování (SMP)**– Symmetric Multiprocessing**

Počítačová architektura, ve které více procesorů sdílí stejnou paměť obsahující jedinou kopii operačního systému, jedinou kopii každé používané aplikace a jedinou kopii dat. Protože operační systém rozděluje zatížení na úlohy a přiřazuje tyto úlohy dostupným procesorům, technologie SMP snižuje čas transakcí.

symetrický klíč – symmetric key

Jediný klíč používaný v algoritmech symetrického šifrování pro kódování i dekódování. Viz také hromadné šifrování; šifrování; dešifrování; klíč propojení.

synchronní zpracování – synchronous processing

Výchozí režim zpracování skupinových zásad v systému Windows 2000. V tomto výchozím režimu se uživatelé nemohou přihlásit, dokud nejsou zpracovány všechny objekty skupinových zásad počítačů, a nemohou začít pracovat na svých počítačích, dokud nejsou zpracovány všechny objekty skupinových zásad uživatelů.

Syspart

Proces vykonávaný volitelným parametrem souboru Winnt32.exe. Používá se pro čistou instalaci na počítače s nepodobným hardwarem. Tato metoda automatizované instalace omezuje čas zavedení systému, protože odstraňuje část kopírování souborů instalačního programu. Viz automatizovaná instalace.

Sysprep

Nástroj, který připraví pevný disk zdrojového počítače pro duplikaci na cílové počítače, a pak spustí proces přenosu obrazu disku zajištěný nějakým samostatným programem. Tato metoda automatické instalace se používá, když je disk na hlavním počítači shodný s disky na cílových počítačích. Viz také automatizovaná instalace.

systém DFS – Distributed File System

Služba Windows 2000 skládající se ze softwaru umístěného na síťových serverech a klientech, která transparentně propojuje sdílené složky umístěné na různých souborových serverech do jednoho oboru názvů, jejímž účelem je zlepšit rozdělování zatížení a dostupnost dat.

systém FAT32 – FAT32

Odvozenina systému souborů s alokační tabulkou souborů. Systém FAT32 podporuje menší velikost klastrů než systém FAT, a následkem toho je přidělování místa na jednotkách FAT32 efektivnější. Viz také alokační tabulka souborů; systém souborů NTFS.

systém NetBIOS – network basic input/output system

Rozhraní API (Application Programming Interface), které mohou využívat programy v místní

síti nebo na počítačích se systémy Microsoft-DOS, OS/2 a některými verzemi systému UNIX. Systém NetBIOS poskytuje jednotnou sadu příkazů pro požadování síťových služeb nižší úrovně.

systém NetBIOS přes protokol TCP/IP – NetBIOS over TCP/IP

Funkce zajišťující dostupnost programovacího rozhraní NetBIOS přes protokol TCP/IP. Používá se ke sledování serverů na trasách, které používají překlad názvů systému NetBIOS.

systém souborů – file system

V operačním systému je to celková struktura, v níž jsou soubory pojmenovány, uloženy a organizovány. Mezi systémy souborů patří systémy NTFS, FAT a FAT32.

systém souborů CIFS**– Common Internet File System**

Protokol a odpovídající rozhraní API používané aplikačními programy k odesílání požadavků aplikačním službám na vyšší úrovni. Systém CIFS byl dříve označován jako SMB (Server Message Block).

systém souborů NTFS – NTFS file system

Obnovitelný systém souborů navržený speciálně pro použití v rámci operačního systému Windows NT a Windows 2000. Systém NTFS používá databázi, zpracování transakcí a paradigma objektů, čímž zaručuje zabezpečení dat, spolehlivost systému souborů a další pokročilé funkce. Systém také podporuje zotavení, rozsáhlá paměťová média a různé funkce podsystému POSIX. Díky tomu, že tento systém zpracovává všechny soubory jako objekty s atributy definovanými uživateli a systémem, podporuje rovněž objektově orientované aplikace.

systémové soubory – system files

Soubory používané systémem Windows k zavedení, konfiguraci a spuštění operačního systému. Systémové soubory nelze odstraňovat ani přesouvat.

systémové zásady – system policy

V rámci správy sítě je to část skupinových zásad, která se zabývá nastavením aktuálního uživatele a místního počítače v registru. V systému Windows 2000 se někdy systémová politika označuje za softwarovou politiku a je jednou ze služeb poskytovaných modulem snap-in

skupinových zásad konzoly MMC. Pro zajištění zpětné kompatibility je součástí Windows 2000 Editor systémových zásad Poledit.exe. Tento nástroj potřebují správci k nastavení systémové politiky na počítačích se systémy Windows NT 4.0 a Windows 95. Viz také konzola MMC; registr.

Š

šablona certifikátu – certificate template

Konstrukce systému Windows 2000, která předem specifikuje formát a obsah certifikátů v závislosti na jejich předpokládaném použití. Vyžadujete-li certifikát od certifikačního úřadu systému Windows 2000, má žadatel o certifikát (v závislosti na přístupových právech) možnost výběru z celé řady různých typů certifikátů založených na šablonách certifikátů, například „Uživatel“ a „Podpis kódu“. Viz také certifikát; certifikační úřad.

šablony pro správu (soubory .adm)

– administrative templates

Soubor ACII označovaný za šablonu pro správu (soubor .adm), kterou používají skupinové zásady jako zdroj při vytváření nastavení uživatelského rozhraní, jež může správce určit.

šestnáctkový – hexadecimal

Číselný systém se základem 16, jehož čísla jsou představována číslicemi 0 až 9 a písmeny A (odpovídá desítkové hodnotě 10) až F (odpovídá desítkové hodnotě 15).

šifra – cipher

Metoda vytváření skryté zprávy. Šifra se používá k přeměně čitelné zprávy v prostém textu na nečitelnou, zakódovanou neboli skrytou zprávu označovanou za šifrovaný text. Pouze osoba s určitým tajným dekodovacím klíčem může převést zašifrovaný text zpět na původní prostý text. Viz také šifrovaný text; prostý text; šifrování.

šifrovací deska – crypto-accelerated board

Hardwarové zařízení urychlující šifrovací operace jejich převedením na speciální procesor na desce.

šifrovací klíč – encryption key

Hodnota použitá určitým algoritmem k zakódování nebo dekodování zprávy.

šifrované heslo – encrypted password

Heslo, které je zakódováno pomocí šifrování. Šifrovaná hesla jsou zabezpečenější než hesla nešifrovaná, jejichž zjištění je snazší.

šifrování – encryption

Proces změny zpráv nebo dat takovým způsobem, aby byla skryta jejich podstata.

šifrování s veřejným klíčem – public key encryption

Metoda šifrování používající dva šifrovací klíče: veřejný klíč pro zašifrování dat a soukromý klíč pro dešifrování dat. Šifrování veřejným klíčem se také označuje za asymetrické šifrování.

šifrovaný text – ciphertext

Text zašifrovaný pomocí šifrovacího klíče. Zašifrovaný text nemá žádný význam pro někoho bez dešifrovacího klíče. Viz také dešifrování; šifrování; šifrovací klíč; prostý text.

šířka pásma – bandwidth

V analogových komunikacích rozdíl mezi nejvyšší a nejnižší frekvencí v daném rozsahu. Například analogová telefonní linka využívá šířku pásma 3 000 Hz, což je rozdíl nejnižší (300 Hz) a nejvyšší (3 300 Hz) frekvence, kterou je schopna přenášet. V počítačových sítích znamená větší šířka pásma schopnost rychlejšího přenosu dat. Šířka pásma vyjádřena v bitech za sekundu (b/s).

škálování – scaling

Proces přidávání procesorů k systému za účelem získání vyšší propustnosti.

škálovatelnost – scalability

Měřítko, do jaké míry může počítač, služba nebo aplikace splňovat zvyšující se požadavky na výkon. V rámci klastřů serverů je termínem škálovatelnost označována možnost přidat ke stávajícímu klastru postupně jeden nebo více systémů, pokud celkové zatížení klastru přesáhne jeho možnosti.

T

T1

Přenosový kanál vysílající data rychlostí 1 544 Mb/s.

T3

Přenosový kanál vysílající data rychlostí 44 736 Mb/s ve stejném formátu jako DS3.

tabulka oddílů – partition table

Oblast hlavního spouštěcího záznamu, kterou počítač používá u rčení, jak přistupovat k disku. Tabulka oddílů může obsahovat až čtyři oddíly pro každý fyzický disk.

tajný klíč – secret key

Šifrovací klíč, které dvě strany sdílejí vzájemně a s nikým jiným. Viz také symetrické šifrování.

TCP/IP

Viz protokol TCP/IP.

technika round robin – round robin

Jednoduchý mechanismus používaný servery DNS při sdílení a rozdělení zatížení síťových prostředků. Používá se k otáčení pořadí dat záznamů o prostředcích vrácených v reakci na dotaz v případě, kdy v rámci dotazovaného názvu domény DNS existuje více záznamů o prostředcích stejného typu.

technologie OLE – object linking and embedding

Metoda sdílení informací mezi aplikacemi. Propojením objektu, například grafiky, z jednoho dokumentu se do jiného dokumentu vloží odkaz na objekt ve výchozím dokumentu. Všechny změny objektu v prvním dokumentu se projeví také ve druhém dokumentu. Vložení znamená vytvoření kopie objektu z jednoho dokumentu ve druhém dokumentu. Změny zadané objektu v prvním dokumentu se neprojeví v druhém dokumentu, pokud vložený objekt nebudete specificky aktualizovat. Viz také ActiveX.

telnet – Telnet

Protokol emulace terminálu široce používaný na Internetu pro přihlášení k síťovým počítačům. Telnet také označuje aplikaci, která používá protokol telnet pro uživatele, kteří se přihlašují za vzdálených míst.

tenký klient – thin client

Síťový počítač bez pevného disku.

terminál – terminal

Zařízení skládající se z obrazovky a klávesnice, jež se používá ke komunikaci s počítačem.

terminál systému Windows**– Windows-based terminal**

Terminál, který používá operační systém Windows.

textový režim – text mode

Část instalačního programu, která používá textové rozhraní.

tiskové zařízení – print device

Hardwarové zařízení používané pro tisk, obecně nazývané tiskárna. Viz také logická tiskárna.

tiskový server – print server

Počítač vyhrazený ke správě tiskáren v síti. Tiskovým serverem může být libovolný počítač v síti.

tlačítko hlavního panelu – taskbar button

Tlačítko zobrazené na hlavním panelu a odpovídající spuštění aplikace. Viz také hlavní panel.

tok – thread

Typ objektu v procesu, který vykonává instrukce programu. Použitím více toků lze vykonávat více různých operací v jednom procesu najednou a je také možné, aby jeden proces spouštěl různé části svého programu na různých procesorech zároveň. V adresovém prostoru svého procesu má tok vlastní sadu registrů, vlastní zásobník jádra, blok prostředí toku a uživatelský zásobník.

token přístupu – access token

Objekt obsahující informace zabezpečení pro dobu přihlášení. Systém Windows 2000 vytváří token přístupu v okamžiku přihlášení uživatele a každý proces vykonaný jménem uživatele má kopii tohoto tokenu. Tento token identifikuje uživatele, skupiny uživatele a privilegia uživatele. Systém používá tento token pro řízení přístupu k zabezpečeným objektům a pro řízení možností uživatele vykonávat na místním počítači různé operace související se systémem. Existují dva druhy tokenu přístupu: primární a zosobnění. Viz také primární token; token zosobnění; privilegeum; proces; identifikátor zabezpečení.

token zosobnění – impersonation token

Token přístupu vytvořený v zájmu zachycení informací zabezpečení nějakého klientského procesu, který tak umožňuje službě „zosobnit“ klientský proces v zabezpečených operacích. Viz také token přístupu; primární token.

topologie – topology

V systému Windows je to vztah mezi sadou síťových součástí. V kontextu replikace adresářů služby Active Directory se termín topologie vztahuje na sadu připojení, které řadiče domén používají k replikaci informací mezi sebou. Viz také řadič domény; replikace.

topologie jednotky DFS – DFS topology

Logická struktura distribuovaného systému souborů, včetně různých položek, jako je kořenový adresář jednotky DFS, propojení jednotky DFS, sdílené složky a sady replik, jak je určeno v konzole správy DFS. Tento pojem nelze zaměňovat s oborem názvů DFS, což je logické zobrazení sdílených prostředků viděné uživateli.

topologie replikace – replication topology

V rámci replikace Active Directory je to sada připojení, které používají řadiče domén při vzájemné replikaci informací v rámci sídel i mezi nimi. Viz také řadič domény; replikace Active Directory.

transformace – transform

Vlastní skript vytvořený za účelem úpravy chování instalace přímou změnou instalačního skriptu bez opakovaného zabalíčkování aplikace.

trvalý virtuální okruh (PVC)**– permanent virtual circuit**

Virtuální okruh přiřazený předkonfigurované statické trase.

třída objektu – object class

Třída objektu je formální definice určitého druhu objektu, který lze uložit do adresáře. Třída objektu je jednoznačná, pojmenovaná sada atributů představující něco konkrétního, například uživatele, tiskárnu nebo aplikaci. Tyto atributy obsahují data popisující věc, která je identifikována objektem adresáře. Atributy uživatele mohou zahrnovat dané jméno uživatele, jeho příjmení a adresu elektronické pošty. Termíny třída a třída objektu lze zaměňovat. Atributy, které lze použít k popisu objektu, jsou určeny pravidly obsahu.

TTL

Viz hodnota TTL.

tunel – tunnel

Logická cesta, kterou zapouzdřené pakety putují tranzitními propojenými sítěmi.

tunelové propojení – tunneling

Metoda využití infrastruktury propojení sítí k přenosu dat (rámců nebo paketů) jiného protokolu.

tunelový protokol – tunneling protocol

Komunikační standard používaný ke správě tunelů a zapouzdření soukromých dat. Tune-

lovaná data musí být také zašifrována, aby se stala připojením VPN. Systém Windows 2000 obsahuje protokol PPTP a protokol L2TP.

typ hardwaru – hardware type

Klasifikace podobných zařízení. Například pro digitální fotoaparáty a skenery je typem hardwaru zařízení pro zpracování obrázků.

typy událostí – event types

Chyby, základní akce s označením nebo problémy se zařízeními.

U**účet Guest – guest account**

Vestavěný účet používaný pro přihlášení k počítači se systémem Windows 2000 v případě, že uživatel nemá v tomto počítači, v příslušné doméně a ani v žádné z důvěryhodných domén svůj účet.

událost – event

Libovolná významná situace v systému nebo aplikaci, která vyžaduje, aby na její výskyt byl uživatel upozorněn, nebo pro niž musí být přidána nová položka do protokolu.

UDP

Viz protokol UDP.

ukazovací zařízení směru pohledu – eye-gaze pointing device

Vstupní zařízení, které umožňuje ovládat obrazovkový kurzor pomocí vidění a které umožňuje uživateli tisknout obrazovková tlačítka v dialogových oknech, vybírat položky nabídek a vybírat buňky nebo text.

ukládání do mezipaměti – caching

V rámci serverů DNS jde obvykle o schopnost serverů DNS ukládat informace zjištěné o oboru názvů domény v průběhu zpracování a překládání dotazů na názvy. V systému Windows 2000 je ukládání do mezipaměti k dispozici rovněž prostřednictvím služby klienta DNS jako způsob uchovávání mezipaměti informací o názvech zjištěných v průběhu nedávných dotazů. Viz také služba Caching Resolver.

úložiště certifikátů – certificate stores

Systém Windows 2000 ukládá objekty veřejných klíčů, jako jsou certifikáty a seznamy odvolaných certifikátů, v logických a fyzických úložištích. Logická úložiště seskupují objekty

veřejných klíčů pro uživatele, počítače a služby. Fyzickými úložišti jsou místa, kde jsou objekty veřejných klíčů skutečně uloženy v registru místních počítačů (nebo v Active Directory v případě některých certifikátů uživatelů). Logická úložiště obsahují ukazatele na objekty veřejných klíčů ve fyzických úložištích. Uživatelé, počítače a služby sdílejí mnoho objektů veřejných klíčů, takže logická úložiště umožňují sdílení objektů veřejných klíčů, aniž by bylo nutné ukládat duplikáty objektů pro každého uživatele, počítač nebo službu.

univerzální sériová sběrnice (USB)

– Universal Serial Bus

Obousměrná, izochronní, dynamicky připojitelná sériová rozhraní sloužící k přidávání periferních zařízení, jako jsou pákové ovladače, sériové či paralelní porty a vstupní zařízení na jedinou sběrnici.

univerzální skupina – universal group

Skupina Windows 2000 dostupná pouze v nativním režimu, která je platná kdekoli v doménové struktuře. Univerzální skupiny jsou uváděny v globálním katalogu, ale obsahují především globální skupiny z domén doménové struktury. To je nejjednodušší forma skupiny, která může obsahovat další univerzální skupiny, globální skupiny a uživatele z libovolné části doménové struktury. Viz také místní skupina domény; doménová struktura; globální katalog.

UNIX

Výkonný, víceuživatelský operační systém s podporou multitaskingu (zpracování více úloh najednou) původně vyvinutý v roce 1969 ve společnosti AT&T Bell Laboratories pro mikropočítače. UNIX je považován za portovatelnější (méně závislý na konkrétním počítači) než jiné operační systémy, protože je napsán v jazyce C. Novější verze systému UNIX byly vyvinuty na kalifornské univerzitě v Berkeley a společností AT&T.

úplná replika – full replica

Replika adresářového oddílu určená pro čtení i zápis, která obsahuje všechny atributy všech objektů v oddílu. Úplná replika se také označuje za hlavní repliku. Viz také částečná replika.

úplný doménový název (FQDN)

– fully qualified domain name

Název domény DNS, který byl jednoznačně určen tak, že s naprostou jistotou určuje odpovídající umístění ve stromu oboru názvů domény, například „host.example.microsoft.com“. Pro úplný doménový název je rovněž používán termín plně kvalifikovaný doménový název.

úplný přenos zóny (AXFR) – full zone transfer

Standardní typ dotazu podporovaný všemi servery DNS, který slouží k aktualizaci a synchronizaci dat zóny při změně zóny. Je-li jako typ dotazu DNS použit přenos AXFR, je jako odpověď přenesena celá zóna. Viz také přírůstkový přenos zóny; zóna; přenos zóny.

úřad IANA – Internet Assigned Numbers Authority

Organizace delegující adresy IP a jejich přiřazení organizacím, jako je InterNIC.

usnadnění – accessibility

Kvalita systému zahrnující hardware a software ve smyslu zavedení upravitelného uživatelského prostředí, alternativních metod vstupu a výstupu a zvětšení prvků obrazovky, aby počítač mohli využívat i lidé s postižením fyzickým, rozpoznávání, sluchu či zraku.

uzamčení účtu – account lockout

Funkce zabezpečení systému Windows 2000, která uzamkne uživatelský účet, pokud dojde v zadaném čase k několika neúspěšným pokusům o přihlášení. Tato funkce vychází z nastavení uzamčení zásad zabezpečení. (Uzamčené účty nelze používat k přihlášení.)

uzamknout – lock

Učinit soubor nedostupným. Když může s nějakým souborem pracovat více uživatelů, tento soubor se po přístupu jednoho uživatele uzamkne, aby jej nemohlo změnit více uživatelů najednou.

uzavřené zachytávání – closed captioning

Alternativní reprezentace (obvykle text) zvukových nebo obrazových médií, které si lze zobrazit pouze na speciálně vybaveném přijímači.

uzel – node

V rámci stromových struktur jde o umístění v rámci stromu, které může být propojeno s jednou nebo několika položkami níže. V rámci místních sítí je to zařízení, které je

připojeno k síti a je schopno komunikace s ostatními síťovými zařízeními, v rámci klastru serverů s instalovaným softwarem služby Cluster Service, který je členem klastru. Viz také místní síť.

uživatelé – users

Speciální skupina obsahující všechny uživatele, kteří mají oprávnění uživatele na serveru. Když uživatel systému Macintosh přiřadí oprávnění všem, tato oprávnění platí pro uživatele skupiny a hosty. Viz také kategorie každý; host.

uživatelská maska podsítě – custom subnet mask

Maska podsítě, která nevychází z internetových tříd adres. Uživatelské masky podsítí se v práci s podsítěmi užívají velmi často.

uživatelská práva – user rights

Oprávnění vydané uživateli centrem distribuce klíčů (KDC) v okamžiku přihlášení uživatele. Uživatel musí při požadování lístků připojení služeb předložit KDC lístek TGT. Protože je lístek TGT obvykle platný po celou dobu připojení uživatele, někdy se také označuje za uživatelský lístek. Viz také protokol ověření Kerberos, centrum distribuce klíčů, lístek připojení.

uživatelské jméno – user name

Jedinečné jméno identifikující uživatelský účet v systému Windows 2000. Název uživatelského účtu musí být v rámci názvů ostatních skupin a uživatelských jmen v příslušné doméně či pracovní skupině jedinečný.

V

vazba – binding

Proces, kterým jsou softwarové komponenty a vrstvy vzájemně propojeny. Po instalaci síťové součásti se vytvoří vztahy vazby a závislosti mezi komponentami. Vazby umožňují komponentám vzájemně komunikovat.

vazební databáze – bindery

Databáze systému Novell NetWare 2.x a 3.x obsahující organizační a bezpečnostní informace o uživateli a skupinách.

veřejné adresy – public addresses

Adresy IP přiřazené organizací InterNIC, u nichž je zaručena celosvětová jednoznačnost a dosažitelnost na Internetu.

veřejný klíč – public key

Netajná polovina páru kryptografických klíčů, který se používá v algoritmu veřejného klíče. Veřejné klíče se zpravidla používají k ověřování digitálních podpisů nebo k dešifrování dat zašifrovaných odpovídajícím tajným klíčem. Viz také soukromý klíč.

vícejazyčná verze systému Windows 2000

– Windows 2000 MultiLanguage Version

Verze systému Windows 2000 rozšiřující podporu jazyků tím, že umožňuje změnu jazyka uživatelského prostředí podle uživatelů. Tato verze také minimalizuje počet jazykových verzí, které musí být v síti použity.

víceměrové vysílání – multicast

Síťový provoz určený k odeslání na více hostitelů patřících do skupiny víceměrového vysílání. Viz také skupina víceměrového vysílání.

virtuální obvod (VC) – Virtual Circuit

Propojení mezi dvěma body za účelem přenosu dat. To umožňuje větší možnosti řízení atributů volání, jako je šířka pásma, latence, změny zpoždění a řazení.

virtuální paměť – virtual memory

Místo na pevném disku, které systém Windows 2000 používá jako paměť. Díky virtuální paměti může být množství dostupné paměti z hlediska nějakého procesu mnohem větší než skutečná fyzická paměť v počítači. Operační systém virtuální paměť obsluhuje způsobem, který je pro aplikace transparentní. Stránkuje totiž data, která se nevejdou do fyzické paměti, z disku a na disk podle potřeby.

virtuální privátní síť (VPN) – virtual private network

Rozšíření privátní sítě, které obsahuje propojení přes sdílené nebo veřejné síť, jako je například Internet.

virtuální připojení – virtual link

Logické propojení mezi hraničním směrovačem páteřní oblasti a hraničním směrovačem oblasti, který není k páteři připojen.

virtuální server – virtual server

V klastru serverů je to sada prostředků včetně prostředku Network Name a prostředku adresy IP, která je obsažena ve skupině prostředků. Pro klienty představuje virtuální server počítač se spuštěným systémem Windows NT Server nebo Windows 2000 Server.

virtuální síť – virtual network

Logická síť, která existuje v rámci serverů a směrovačů Novell NetWare a serverů a směrovačů kompatibilních se systémem NetWare, ale není přidružena k fyzickému adaptéru. Virtuální síť se uživateli jeví jako samostatná síť. V počítači se systémem Windows 2000 Server jsou umístění programů uvedena v rámci virtuální, nikoli fyzické sítě. Interní síťové číslo identifikuje virtuální síť v rámci počítače. Viz také externí síťové číslo; interní síťové číslo.

vložené skupiny – nested groups

Funkce Windows 2000 dostupná pouze v nativním režimu umožňující vytváření skupin ve skupinách. Viz také univerzální skupina; globální skupina; místní skupina domény; doménová struktura; důvěryhodná doménová struktura.

vložený objekt – embeded object

Informace vytvořené v jiné aplikaci, které byly vloženy do dokumentu. Jde-li o vložené informace, můžete je v novém dokumentu upravit pomocí panelů nástrojů a nabídek původního programu. Chcete-li vložené informace upravit, poklepejte na ně a použijte panely nástrojů a nabídky původního programu, který se zobrazí. Vložené informace nejsou propojeny s původním souborem. Změníte-li informace na jednom místě, nedojde na druhém místě k jejich aktualizaci. Viz také propojený objekt.

volba blokování zásad – block policy option

Volba, která zabráňuje objektům skupinových zásad specifikovaným v kontejnerech služby Active Directory na vyšší úrovni v aplikování na počítač nebo uživatele.

volba pevného pořadí zpracování – loopback option

Volba umožňující správci aplikovat nastavení skupinových zásad podle počítače, k němuž se uživatel přihlásí, dokonce i po zpracování nastavení uživatele.

volné místo – free space

Dostupný prostor používaný k vytvoření logických jednotek v rámci rozšířeného oddílu. Viz také rozšířený oddíl; logická jednotka; nepřiražené místo.

vrstva abstrakce hardwaru (HAL)**– hardware abstraction layer**

Tenká vrstva softwaru dodaná výrobcem hardwaru, která skrývá neboli činí abstraktní-

mi rozdíly hardwaru z hlediska vyšších úrovní operačního systému. Přes filtr zajištěný vrstvou HAL vypadají různé typy hardwaru pro zbývající část operačního systému stále stejně. To dovoľuje přenositelnost systémů Windows NT a Windows 2000 na různé hardwarové platformy. Vrstva HAL také poskytuje rutiny umožňující jednomu ovladači zařízení podporovat určité zařízení na všech platformách. Vrstva HAL úzce spolupracuje s jádrem systému.

vrstva SSL – Secure Sockets Layer

Navrhovaný otevřený standard vyvinutý společností Netscape Communications sloužící k vytvoření kanálu zabezpečené komunikace, který zabráňuje zjištění kritických informací, například čísel kreditních karet. Tato vrstva především umožňuje zabezpečené finanční transakce na síti WWW, i když dokáže pracovat také s jinými internetovými službami.

vstupní zařízení na ústa – mouthstick

Alternativní asistenční vstupní zařízení pro uživatele s fyzickým postižením.

všesměrové vysílání – broadcast

Adresa určená pro všechny hostitele na dané síti. Viz také síť všesměrového vysílání.

všesměrové vysílání a neznámý server (BUS) – broadcast and unknown server

Služba vícesměrového vysílání v emulované místní síti (ELAN), která předává data jednosměrového, vícesměrového a všesměrového vysílání odesílaná klientem emulace místní sítě. Viz také emulovaná místní síť.

výchozí brána – default gateway

Konfigurační položka protokolu TCP/IP, která je adresou IP přímo dosažitelného směrovače IP. Konfigurace výchozí brány vytvoří výchozí trasu ve směrovací tabulce IP.

výchozí hostitel – default host

Hostitel s nejvyšší hostitelskou prioritou, pro nějž není použit příkaz drainstop. Po dokončení konvergence výchozí hostitel zpracuje veškerý síťový provoz pro porty TCP a UDP, které nejsou jinak zahrnuty v pravidlech portů. Viz také konvergence; příkaz drainstop; priorita hostitele; pravidlo portu; protokol UDP.

výchozí maska podsítě – default subnet mask

Maska podsítě, která se používá na sítích pracujících s internetovými třídami adres. Masku podsítě pro třídu A je 255.0.0.0. Masku podsítě

pro třídu B je 255.255.0.0. Masku podsítě pro třídu C je 255.255.255.0.

výchozí síť – default network

V prostředí počítačů Macintosh je to fyzická síť, v níž jsou procesy serveru umístěny jako uzly a v níž se server zobrazuje uživateli. Výchozí síť serveru musí být jedna ze sítí, k nimž je server připojen. Výchozí sítě jsou určeny pouze pro servery v propojení sítí AppleTalk Phase 2.

výchozí trasa – default route

Trasa, která se použije v okamžiku, kdy nejsou v tabulce směrování nalezeny žádné jiné trasy k cílovému místu. Když například směrovač nebo koncový systém nemůže najít síťovou nebo hostitelskou trasu k cíli, použije se výchozí trasa. Výchozí trasa se používá pro zjednodušení konfigurace koncových systémů nebo směrovačů. V případě tabulek trasování IP je výchozí trasa trasou s cílovým místem 0.0.0.0 a maskou 0.0.0.0.

výměna klíčů – key exchange

Důvěrná výměna tajných klíčů v režimu online, což se zpravidla uskutečňuje za pomoci šifrování s veřejným klíčem. Viz také šifrování s veřejným klíčem.

výrobce OEM – original equipment manufacturer

Výrobce části zařízení. Při výrobě počítačů a dalšího počítačového zařízení výrobci originálních součástí obvykle kupují komponenty od jiných výrobců originálních zařízení a pak je integrují do svého vlastního výrobku.

vyrovnávací paměť – buffer

Oblast paměti používaná k dočasnému uložení dat, kde čekají na další použití.

vyrovnávání zatížení – load-balancing

Technika používaná službou Windows Clustering k rozložení výkonu serverového programu (například serveru WWW), a to distribucí požadavků klientů mezi více serverů v rámci klastru. Každý hostitel může určit procento zatížení, které zpracuje, nebo je možné rozdělit zatížení rovnoměrně mezi všechny hostitele. Pokud hostitel selže, služba Windows Clustering provede dynamickou redistribuci zatížení mezi zbývajícím hostitelům. Viz také požadavek klienta; klastr; hostitel; škálovatelnost; server.

vyrovnávání zatížení sítě – network load ballancing

Technika používaná službou Windows Clustering k rozložení výkonu serverového programu (například serveru WWW), a to distribucí požadavků klientů mezi více serverů v rámci klastru.

vysoká dostupnost – high availability

Schopnost udržet po většinu času aplikaci nebo službu ve funkčním stavu a použitelnou klienty.

vzájemné ověření – mutual authentication

Proces, kdy volající směrovač ověří sám sebe odpovídajícím směrovačem a odpovídající směrovač ověří sám sebe volajícím směrovačem. Oba konce spojení tak ověří identitu druhého konce linky. Vzájemné ověření poskytují ověřovací metody MS-CHAP v2 a EAP-TLS.

vzdálené úložiště – remote storage

V rámci systému Windows 2000 Server jde o vyměnitelné pásky v knihovně používané jako sekundární úložiště dat. Určené pásky používané jako sekundární úložiště dat jsou spravovány programem Vzdálené úložiště a obsahují data, která buď jsou uložena na místním úložišti nebo byla odstraněna z místního úložiště z důvodu uvolnění místa na disku. Viz také místní úložiště.

vzdálené volání procedur – remote procedure call

Způsob předávání zpráv, který distribuovaným aplikacím umožňuje volat služby dostupné v různých počítačích v rámci sítě. Používá se při vzdálené správě počítačů.

vzdálený počítač – remote computer

Počítač, k němuž lze získat přístup pouze pomocí komunikační linky nebo komunikačního zařízení, jako je síťová karta nebo modem.

vztah důvěryhodnosti – trust relationship

Logický vztah navázaný mezi doménami a umožňující předávací ověřování, v jehož rámci důvěřující doména uděluje přihlašovací ověřování důvěryhodné domény. Uživatelským účtům a globálním skupinám definovaným v důvěryhodné doméně lze udělit práva a oprávnění v důvěřující doméně, a to i v případě, že tyto uživatelské účty nebo skupiny v adresáři důvěřující domény nejsou uvedeny. Viz také ověření; doména; obousměrný vztah důvěryhodnosti.

vztah explicitní důvěryhodnosti**– explicit trust relationship**

Vztah důvěryhodnosti systému Windows NT, při němž se vytvoří explicitní propojení pouze v jednom směru. Explicitní důvěryhodnosti mohou existovat také mezi doménami Windows NT a doménami Windows 2000, a také mezi doménovými strukturami.

vztah tranzitivní důvěryhodnosti**– transitive trust relationship**

Vztah důvěryhodnosti, který standardně existuje mezi doménami Windows 2000 v doménovém stromě či struktuře, mezi stromy v doménové struktuře nebo mezi doménovými strukturami. Pokud se doména připojí ke stávající doménové struktuře nebo stromu doménové struktury, je tranzitivní vztah důvěryhodnosti vytvořen automaticky. Viz také strom domén; doménová struktura.

W**webový server – Web server**

Server poskytující možnost vyvíjet aplikace COM a vytvářet rozsáhlá webová sídla pro Internet a intranetové sítě.

WINS

Viz služba WINS.

Z**zabezpečená dynamická aktualizace****– secure dynamic update**

Proces, při kterém klient zabezpečené dynamické aktualizace předá požadavek na dynamickou aktualizaci serveru DNS a server se pokusí o aktualizaci, pouze pokud může klient prokázat svou identitu a má příslušná oprávnění pro aktualizaci. Viz také dynamická aktualizace.

zabezpečený protokol IP (IPSec)**– Internet Protocol security**

Sada standardních ochranných služeb a protokolů založených na šifrování. IPSec chrání všechny protokoly v sadě TCP/IP a internetové komunikace uskutečněné pomocí L2TP. Viz také protokol Layer 2 Tunneling Protocol.

záchranná opravná disketa (ERD)**– emergency repair disk**

Disketa vytvořená nástrojem Zálohování, která obsahuje informace o aktuálním nastavení systému Windows. Pomocí této diskety lze opravit počítač v případě, že jej nelze spustit nebo že dojde k poškození či vymazání systémových souborů.

zakázat – disable

Učinit zařízení nefunkčním. Například je-li v profilu hardwaru zakázáno nějaké zařízení, dané zařízení nelze při použití tohoto profilu hardwaru používat. Zákaz zařízení uvolňuje prostředky, které mu byly přiřazeny.

základní disk – basic disk

Fyzický disk obsahující primární oddíly nebo rozšířené oddíly s logickými jednotkami používanými systémem Windows 2000 a všemi verzemi systému Windows NT. Základní disky rovněž mohou obsahovat rozložené, zrcadlené a prokládané svazky a svazky RAID-5 vytvořené pomocí systému Windows NT 4.0 nebo dřívějšího. Je-li použit kompatibilní systém souborů, k základním diskům lze přistupovat prostřednictvím systému MS-DOS, Windows 95, Windows 98 a všech systémů Windows NT.

základní svazek – basic volume

Svazek na základním disku. Základní svazky zahrnují primární oddíly, logické jednotky s rozšířenými oddíly stejně jako svazky rozložené, zrcadlené, prokládané nebo RAID-5, které byly vytvořeny pomocí systému Windows NT 4.0 nebo dřívějšího. Základní svazky lze vytvářet pouze na základních discích. Na jednom disku nemohou existovat základní a dynamické svazky.

zálohovací sklad – backup set

Kolekce souborů, složek a dalších dat, které byly zálohovány a uloženy v souboru nebo na jedné či několika páskách.

záložní řadič domény (BDC)**– backup domain controller**

V systému Windows NT Server 4.0 nebo dřívějším je to počítač se systémem Windows NT Server, který přijímá kopii databáze adresářů domény (obsahující všechny informace o účtech a zásadách zabezpečení pro danou doménu). Kopie je pravidelně a automaticky synchronizována s hlavní kopíí na primárním řadiči domény (PDC). Záložní řadič domény

může rovněž ověřovat přihlašovací informace uživatele a v případě potřeby může být povýšen na primární řadič domény. V rámci domény může existovat několik záložních řadičů. Záložní řadiče domén systému Windows NT 3.51 a 4.0 mohou být součástí domény Windows 2000 v případě, že doména je nakonfigurována v kombinovaném režimu. Viz také kombinovaný režim; primární řadič domény.

zápis předpony sítě – network prefix notation

Praxe vyjádření masky podsítě ve formě předpony sítě a nikoli v tečkovém desítkovém zápisu.

zařazovací služba pro tisk – print spooler

Počítačový software, který přijme dokument odeslaný uživatelem na tiskárnu a uloží jej na disk nebo do paměti až do okamžiku, kdy bude tiskárna připravena na jeho zpracování. Tato kolekce dynamických knihoven (DLL) přijímá, zpracovává, plánuje a distribuuje tištěné dokumenty. Termín „spooler“ (zařazovací služba) vznikl jako zkratka slov „simultaneous print operations on line“ (současné tiskové operace online). Viz také zařazování.

zařazování – spooling

Proces na serveru, v jehož rámci jsou tištěné dokumenty ukládány na disk, dokud tiskárna není připravena je zpracovat. Zařazovací služba přijímá od klientů jednotlivé dokumenty, ukládá je a ve vhodný okamžik je posílá na tiskárnu.

zařízení – device

Libovolné vybavení, které lze připojit k síti nebo k počítači, například počítač, tiskárna, pákový ovladač, adaptérová či modemová karta, nebo libovolné jiné periferní zařízení. Zařízení zpravidla k zachování funkce v rámci systému Windows 2000 vyžadují ovladač zařízení. Viz také ovladač zařízení.

zařízení s možností infračervené komunikace

– infrared device

Počítač nebo počítačové periferní zařízení, například tiskárna, které je schopno komunikovat pomocí infračerveného světla. Viz také infračervený.

zásady skupiny – Group Policy

Nástroj správce systému používaný k definování a řízení funkcí programů, síťových pro-

středků a fungování operačního systému z hlediska uživatelů a počítačů v organizaci. V prostředí služby Active Directory se zásady skupin aplikují na uživatele nebo počítače podle jejich členství v sídlech, doménách nebo organizačních strukturách.

zásady vzdáleného přístupu – remote access policy

Sada podmínek a parametrů připojení definující charakteristiky příchodného připojení a omezení pro něj platná. Zásady vzdáleného přístupu určují, zda je určitý pokus o připojení oprávněný a zda může být přijat.

závislost – dependency

Stav, při kterém jeden prostředek musí být online, než může druhý prostředek přejít do stavu online.

závislostní strom – dependency tree

Oddělená sada prostředků, které jsou vzájemně propojeny vztahy závislosti. Všechny prostředky v daném závislostním stromu musí být členy jediné skupiny. Viz také závislost; prostředek.

záznam o prostředku (RR) – resource record

Informace v databázi DNS, které lze použít při zpracovávání dotazů klienta. Každý server DNS obsahuje záznamy o prostředcích, které potřebuje k zodpovězení dotazů dané části oboru názvů DNS, pro něž je autoritativní.

záznam SOA – start of authority

Záznam určující výchozí bod nebo původní bod autority pro informace uložené v zóně. Záznam SOA je prvním záznamem o prostředku, který je vytvořen při vytvoření nové zóny. Obsahuje několik parametrů používaných ostatními počítači k určení, jak dlouho budou ostatní servery DNS využívat informace zóny a jak často je nutné tyto informace aktualizovat. Viz také autoritativní; sekundární server; zóna.

zdrojová knihovna DLL – resource DLL

Dynamická knihovna definující výchozí vlastnosti a chování určitého typu prostředku. Zdrojová knihovna DLL obsahuje implementaci rozhraní API (Application Programming Interface) pro specifický typ prostředku a zavádí se do adresního prostoru příslušného nástroje Sledování prostředků. Viz také knihovna DLL; prostředek; nástroj Sledování prostředků.

zobrazení zvuku – ShowSounds

Globální příznak instruující programy tak, že mají místo zvuku používat grafická upozornění pro uživatele se sluchovým postižením nebo pro pracovníky v hlučném prostředí.

zóna – zone

V databázi DNS je zónou souvislá část stromu DNS, který je serverem DNS spravován jako samostatná entita. Zóna obsahuje zdrojové záznamy všech názvů v zóně. V prostředí počítačů Macintosh je to logické seskupení, které v síti zjednodušuje procházení prostředků, například serverů a tiskáren. Je obdobou domény v sítích systému Windows 2000 Server. Viz také služba doména; server DNS.

zóna zpětného vyhledávání – reverse lookup zone

Zóna obsahující informace potřebné pro zpětné vyhledávání. Viz také zpětné vyhledávání.

zosobnění – impersonation

Akce, při níž systém Windows 2000 Server umožní jednomu procesu převzít atributy zabezpečení jiného procesu.

zpětné vyhledávání – reverse lookup

Dotaz, při němž se adresa IP použije k určení názvu DDNS počítače.

zpracování přes pomalou linku**– slow link processing**

Nastavitelná součást skupinových zásad umožňující správcům definovat, která nastavení skupinových zásad se nebudou zpracovávat přes pomalá síťová propojení.

zprostředkovatel kryptografických služeb (CSP)**– cryptographic service provider**

Nezávislý softwarový modul provádějící šifrování, jako jsou výměny tajných klíčů, digitální podepisování dat a ověřování veřejných klíčů. Od CSP může požadovat šifrovací operace libovolná služba nebo aplikace Windows 2000. Viz také rozhraní CryptoAPI.

zrcadlený svazek – mirrored volume

Svazek odolný proti chybám, který duplikuje data na dvou fyzických discích. Zrcadlový obraz je vždy umístěn na jiném disku. Pokud jeden z fyzických disků selže, přestanou být data na tomto disku dostupná, ale systém je bude mít k dispozici na druhém, nepoškozeném disku. Zrcadlené svazky jsou ve srovnání se svazky RAID-5 pomalejší v operacích čtení, ale rychlejší při zápisu. Zrcadlené svazky lze vytvářet pouze na dynamických discích.

V systému Windows NT 4.0 byl pro zrcadlené svazky používán termín zrcadlené sady. Viz také dynamický disk; dynamický svazek; odolnost proti chybám; svazek RAID; svazek.

Rejstřík

\$\$Rename.txt 391, 756
 [GuiRunOnce], oddíl 399, 763
 \OEM\$ 386, 751
 \OEM\$\\$ 388, 752
 \OEM\$\\$1 388, 752
 \OEM\$\\$1\Pnpdrivers 388, 752
 \OEM\$\\$1\Sysprep 388, 753
 \OEM\$\Písmoeno_jednotky 388, 753
 \OEM\$\Textmode 388, 752
 \i386 386, 751

A

abstrakce hardwaru 754
 ACL seznamy 296, 323
 - fungování 323
 - implementace 323
 Active Directory, služba 10, 50, 51, 153,
 161, 257, 396, 463, 595, 610, 655, 684, 820
 - funkce 208
 - infrastruktura 205
 - návrh infrastruktury 207
 - plánování 210
 - principy návrhu 211
 - přehled služby 208
 adaptéry ATM 184
 ADC, služba 598, 601, 605
 adresářová služba Exchange Server 595
 administrační nástroje 93
 aktivování licenčního serveru 484
 analýza infrastruktury sítě 187, 188
 analýza rozdílů 64
 aplikace
 - zajištění dostupnosti 529
 aplikační server 464

aplikování řízení přístupu 322
 aplikování správy změn 707
 AppleTalk protokol 175
 architektura adresářových služeb 138
 architektura informací 63
 architektura sítě
 - příprava 140
 architektura technologií 63
 Asynchronous Transfer Mode (ATM),
 protokol 180
 - adaptéry 184
 - emulace LAN 182
 - výhody užití 181
 auditování 349
 - implementace 349
 Authenticode 344
 - implementace 345
 automatizovaná instalace
 Windows 2000 766
 - metody 767
 automatizování instalace 381
 autonomní systémy 171
 autoritativní server 237

B

Bandwidth Allocation Protocol (BAP) 162
 BDC řadič 283
 bezpečnostní rizika 311
 Bootstrap Protocol 179

C

centralizovaná správa 168
 Certificate Services, služba 357
 certifikační postup (CPS) 362

certifikační úřad 356, 361, 368
- hierarchie důvěryhodnosti 363
- instalace 372
- kompromitovaný 369
certifikát 359
- obnovení 367
- odvolání 367
- správa 357
- zásady 362
- životní cyklus 366
cestovní uživatelské profily 11, 489
Challenge Handshake Authentication Protocol (CHAP) 161
ClonePrincipal, nástroj 305
cluster 546
- obnovení 566
- optimalizace 564
Cluster Service, služba 545, 561, 563
- plánování 557
clustering 532
clusteringový systém Windows 581
Cmdlines.txt 398, 762
COM aplikace 797
COM+ aplikace 540
Component Object Model (COM) 22
Connection Manager 523

Č

čistá instalace 382, 814
členský server 145, 809
- inovace 451, 452, 809
- instalace 451, 452, 809

D

databázový server 465
definice eskalace plánů 106
definování sídel 251
definování typů uživatelů 674

defragmentace disku 577
delegování 348
- průvodce 348
delegování plného řízení 244
demilitarizovaná zóna 514
Deployment Planning Guide 4
detekce neautorizovaných serverů DHCP 178
DHCP protokol Windows 2000 177
- integrace 178
- návrh 179
- nové funkce 177
- výhody použití 177
diagram laboratoře 99
- fyzický 100
- logický 99
diagram sítě
- fyzický 134
- logický 134
disková kvóta
- nastavení 736
diskové prostředky 574
- správa 574
distribuce
- problémy 439
- rozšíření 435
- sledování 436
- testování 435
distribuce balíčků 434
distribuční body 434
distribuční zabezpečení 309
distribučované zabezpečení 315, 806
distribučovaný systém souborů 584
DNS, systém 153
dokumentování konfigurace laboratoře 98
dokumenty zavádění 67
- analýza rozdílů 67
- návrh zavádění 67
- plán eskalace problémů 67

- plán kapacity 67
- vyhodnocení rizik 67
- doména
 - hierarchie 229
 - inovace domény 267
 - migrace 259
 - model správy 138
 - názvy domén 232
 - plán domén 218
 - restrukturalizace 265, 292
 - stromy 230
 - typ struktury 91, 138
 - řadič 139
- doménová důvěryhodnost 329
- doménová struktura 212, 269
 - nárůst nákladu 215
 - plánování 214
 - určení počtu 214
 - zásady řízení změn 217
- domovský adresář 490
- duplicitní zásady 688
- duplikování disků 404
- důvěryhodnost 213, 237, 328
 - doménová 329
 - vytvoření vztahů 328
- dvoufaktorové ověřování 313
- dvouvrstvé delegování 244
- dynamická úložiště 575

E

ELAN, síť 184, 185

elektronická pošta

- fungování 346
- zabezpečení 345

emulace LAN 182

Encrypting File System (EFS) 331, 332

Ethernet, rámce 174

Exchange Server 51, 820

- integrování systému 51

Exchange Server 595, 602

Extensible Authentication Protocol (EAP) 161

externí konektivita 156

F

failback timing 549

failover timing 549

festival testování 637

File and Print Services for NetWare 656

formát souboru odpovědí 841

FRS, služba 289

funkce zabezpečení 21, 796

funkční specializace 68

fyzický diagram laboratoře 100

fyzický diagram sítě 134

G

Gateway Services klient

globální katalog 213

- umístění serverů 255

globální skupina 284

- přesun 298

grafické symboly xxxi

H

Hardware Abstraction Layer (HAL) 390

hardwarové profily 694

hierarchie domén 229

- vytvoření 229

hranice varování kvóty 584

hranice zabezpečení 513

I

identifikátor zabezpečení 277

IIS/ASP aplikace 540

Indexing Service 586

Infrared Data Association 660
infrastruktura sítě 129, 133
- dokumentování prostředí 131
- příprava 131, 149
infrastruktura směrování protokolu IP 169
infrastruktura veřejných klíčů 358
infrastruktura zabezpečení
- příprava 146
inovace členského serveru
- časový plán 453
- příprava 454
- vykonání 457
inovace domény 267, 278
- určení pořadí 278
inovace serveru 381
inovace Windows 2000 379
inovované počítače
- výběr 441
instalace klientů
- automatizování 745
instalace licencí 485
instalace Windows 2000 379
- distribuční složky 384
- metody 383
- příprava 384
integrita dat 314
IntelliMirror, funkce 10, 209, 728
Internet Authentication Service 168
Internet Connection Sharing (ICS) 162
inventář
- použití 196
- vytvoření 192
inventarizace hardwaru 455
inzeráty
- hlášení stavu 446
- problémy 447
- sledování 444
inzerování balíčku 439
IP
- automatické privátní adresování 157

- infrastruktura směrování 169
- RIP protokol 170
- třídy adres 158
IP/ATM 183
IPSec protokol 164, 334, 335
- implementace 334
IPX protokol 174, 656
- struktura směrování 174
IT 10, 12, 13, 16

K

kapacita, plánování 70
Kerberos protokol 281, 317, 318
klíč souboru odpovědí 842
klíčové obchodní procesy 63
klíčové výrobní procesy 63
klient, příprava 147
klientská licence 474
klientské počítače 93
- hardware 93
- software 93
kombinovaný režim 273
kompaktní disk sady Resource Kit xxxii
kompatibilita aplikací 201, 265
kompatibilita softwaru 456
koncept migrace 262
koncept zabezpečení 312
konektivita klientů 651
- definování strategie 651
- přehled 651 základ 653
konektivita sídel organizace 155
konektivita sítě 151
- přehled konektivity 152
- určení strategií 151
- vzdálená konektivita 152
konektivita sítě SOHO 663
konektivita vzdálených klientů 156
konfigurace instalace 414
konfigurace klientů 671

konfigurace sítě 136
konfigurování hardwaru 693
konsolidace adresářů 209
kontakty synchronizování adresářů 824
kontejner konfigurace 213
konvence dokumentů xxxi
konzola MMC 686

L

laboratoř viz testovací laboratoř
laboratorní model 85
- výběr modelu 86
laboratorní prostředí, distribuované 89
laboratorní testování
- seznam úkolů 114
LAN Manager, systém 288, 290
LAN, síť
- konektivita 152
Layer 2 Tunneling
Protocol (L2TP) 162, 164
- příklady 165, 521
licenční server 473 486
listy plánování 791
logický diagram laboratoře 99
logický diagram sítě 134
logistika softwaru 50
lokátor řadiče domény 236

M

manažer oddělení 10
masky podsítí 159
maximální kvóta 583
metodologie testování 636
mezinárodní finanční služby 36
- druhotný cíl 38
- hlavní cíl 38
- migrace 40
- návrh 38

- technické řešení 38
- testování 40
- vyhodnocení 36
mezinárodní výrobce spotřebního
a průmyslového zboží 41
Microsoft Clearinghouse 473
Microsoft Proxy Server 515
Microsoft TCP/IP, protokol 158
migrace domén 259
- cíl 260
- koncept 262
- nástroje 305
- postupná migrace 260
- seznam úkolů 307
místní skupina 284
MMC, konzola 686
model správy 63
model správy domén 138
Multicast and Address Resolution Service
(MARS) 183

N

načasování překlopení 549
načasování překlopení zpět 549
nástroje zavádění 859
nativní režim 283
návrh laboratoře - předpoklady 90
nekompatibilita aplikací 647
NetBIOS 287
NetBIOS/IPX, provoz 175
Netdom, program 306
Network Address Translation (NAT) 162
nodvolatelnost 314
Novell NetWare 461
Novell NetWare 657
NTFS soubory 491, 582
NTLM protokol 280

O

obchodní aplikace 137, 632
 obnovení systému 593
 ochrana dat 588
 - zavedení 331
 odolnost proti chybám 589
 odvolání certifikátů 367, 368
 Open ShortestPath First (OSPF) 171
 - návrh oblasti 172, 173
 optimalizace správy dat 580
 organizační jednotka viz OU
 Organizational Unit (OU) 239
 - plánování 241
 - struktura 240
 - určení 243
 - vytváření 242, 247, 248
 ověřování 313
 - dvoufaktorové 313
 ověřování kódu 314

P

PDC řadič 275
 - emulace řadiče PDC 276
 periferie 92, 95
 periodická aktualizace 689
 personál 512
 pilotní plán
 - cíl 131
 - časový plán 123
 - plán 122, 123
 - podpora 122
 - rozsah 120
 - sídla 121
 - uživatelé 121
 - vytvoření 120
 pilotní proces 118
 pilotní program
 - přehled vykonání 118

- příprava 124
 - sledování 127
 - vyhodnocení 126
 - zavádění 126
 pilotní sídlo 124
 pilotní uživatel 125
 - příprava 125
 PKI
 - implementace 355, 356
 - plánování 354
 plán
 - spuštění 4
 plán domén 218
 - proces plánování 219
 plán projektu
 - příprava 31
 - určení cílů 33
 - vytvoření 30
 plán vzdělávání a školení 69
 plánování kapacity 70
 plánování zavádění Windows 2000 793
 plánování zavedení 57
 Plug-and-Play 391, 755
 podrobnosti plánu projektu 58
 - cíle 58
 - personální požadavky 59
 - rozsah 58
 podsít
 - masky 159
 - používání 159
 Point-to-Point Tunneling Protocol 164, 521
 pokročilá správa 507
 postupné zavádění
 - vytvoření cesty 29
 posudek fyzické infrastruktury 142
 požadavky na aplikace 63
 PPP/ATM 183
 práce v síti 800
 pracovní list plánování 810
 pravidla laboratoře 104

preferovaný uzel 549
preferred node 549
priority aplikací 634
připojitelnost sítě 95
prodejce 11
produkční prostředí 35
prostor názvů domén 50
protokolární událost 340
proxy-server 466
průvodce delegováním zařízení 348
předpoklady infrastruktury sítě 129
přehled plánování 1
přesměrování složek 734
přesun počítačů 300
příklady instalačního programu 835

Q

Quality of Service, služba 185

R

RAID, pole 564, 589
Resource Kit 57, 207, 309, 671
- CD xxxii
- podpora xxxiv
restrukturizace domén 265, 292
- důvody 293
- scénář 301
- určení okamžiku 294
- zkoumání dopadu 294
režim asynchronního přenosu (ATM) 660
režim nahrazení 688
režim sloučení 688
RIP protokol 170
RIS server 779, 781
rizika
- časový plán 73
- řízení 71
- vyhodnocení 70

Ř

řadič domén 139, 227
- lokátor 236
- příprava 144
- umístění 223
řešení správy počítačů 795
řízení laboratoře 102
řízení přístupu 314
řízení správy 347
řízení testů 110

S

serverový cluster 546
servery
- aplikační 464
- členský 145
- databázový 465
- licenční 473, 486
- proxy-server 466
- síťový 468
- souborový 137, 460
- terminálový 473
- tiskový 137, 462
- webový 137, 466
Setupcl.exe 408
seznam úkolů testování 115
SID identifikátor 295
SIDhistory atribut 297, 298
sídlo
- definování 251
- topologie 249
- umístění sídel 254
- vytváření 251
šifrování 493
simulování navrhovaného serverového prostředí 91
sít malé kanceláře 662
síťová pozice 152

- síťové adresy, překlad 176
 - síťové protokoly 95
 - síťové riziko 542
 - identifikace 548
 - určení 542
 - síťový server
 - ladění 468
 - síťový tisk 463
 - skupiny 284
 - globální skupina 284
 - místní 284
 - místní skupina domény 284
 - univerzální skupina 284
 - vkládání 286
 - sledování sítě 201
 - služby
 - zajištění dostupnosti 529
 - služby infrastruktury správy 793
 - Smart Card 319, 320
 - Směrování, služba 160
 - SMS balíčky 421, 423
 - snížená dodatečná správa 163
 - SOHO, síť 663
 - příklady
 - soubor odpovědí 392, 393
 - formát 841
 - klíč 842
 - soubor 842
 - ukázkové 842
 - souborový server 137, 460
 - současné počítačové prostředí 62
 - správa disků 574
 - správa klientských systémů 672
 - pomocí zásad skupiny 680
 - správa kvót 583
 - správa počítačů 19
 - správa služeb infrastruktury 18
 - správa ukládání 26
 - správa úložišť 801
 - správce IT 10
 - správce synchronizace 11
 - správní dokument 66
 - celkový odhad rizika 67
 - fáze 66
 - personál 66
 - prostory 66
 - rozpočet 66
 - rozsah 66
 - strategie komunikace 67
 - stabilizace existující sítě 142
 - standarta správy 671
 - standardní klientské konfigurace 49
 - standards a pravidla
 - vytvoření 64
 - stolní počítače
 - konfigurace 96
 - strategie komunikace 68
 - strategie laboratoře 82
 - strategie migrace domén 805
 - stromy domén 230
 - struktura domén 91, 488
 - synchronizace adresářů 596, 823
 - časový plán 823
 - kontakty 824
 - Syspart, nástroj 403, 405, 406, 409
 - duplikování disků 404
 - Syspart, nástroj 768
 - Sysprep, nástroj 769, 770
 - Sysprep.exe 406, 771
 - Sysprep.inf 406, 771
 - Systém Status 436
 - Systems Management Server 184, 413, 425, 448
 - distribuce softwaru 420
 - zavádění Windows 2000 419
-
- ## Š
- šablony zabezpečení 341
 - fungování 341

- implementace 342
- požadavky 342
- škálovatelnost 23, 169, 293, 798

T

- TCP/IP Windows 2000 157, 160
- telefonické připojování k síti 137
- terminálová služba 465
- terminálové služby 471
 - licenční komponenty 473
 - požadavky 477
 - přehled 471
- terminálové služby 9
- terminálové služby 93
- terminálové služby přes Internet 494
- terminálový server 473
- testovací laboratoř 77
 - diagram 99
 - návrh 90
 - použití 83
 - pravidla laboratoře 104
 - předběžná 82
 - řízení laboratoře 102
 - strategie laboratoře 82
 - účelové laboratoře 85
 - výběr umístění 87
 - vybudování laboratoře 102
 - změny managementu 85
- testovací případy, návrh 109
- testovací proces 81
- testovací prostředí 78
 - použití 78
 - proces vývoje 79
 - vytvoření 78
- testovací sídlo 434
- testování 105
 - metodologie 107
 - po zavedení systému 111
 - testovací případy 109
 - vytvoření plánu testování 106
- testování aplikací 630
- správa 631
- testování kapacity serveru 565
- testování tisku 643
- testy
 - řízení 110
 - výsledky 110
- testy jednotek 105
- tisk přes síť WAN 501
- tisk z terminálových služeb 500
- tiskárny
 - sdílení 463
- tiskový server 137, 462
- topologie sídel 249
 - vytvoření plánu 249
 - změna topologie 256
- topologie sítě 222
- týmy Windows 59, 60, 61
- týmy zavádění 42, 48
- typ struktury domén 138

U

- ukázkové soubory odpovědí 842
- úložiště
 - dynamická 575
 - vyměnitelná 578
 - vzdálené 579
 - základní 575
- úložiště systému
 - určení strategie správy 569
- univerzální skupina 284
- UNIX
 - síťoví klienti 658
- uživatelské rozhraní
 - definice standardů 696
- uživatelské účty 91

V

veřejný klíč 341, 353

- návrh infrastruktury 359
- plánování infrastruktury 353
- vytváření infrastruktury 358
- zavedení infrastruktury 371

vícejazyčná verze 700, 701

virtuální privátní síť 519

VPN síť 163, 164, 166

- zabezpečení 163

vybudování laboratoře 102

vyhodnocení rizik 70

vyměnitelná úložiště 578

výsledky testů 110

vysoká dostupnost 815

vytváření sídel 251

vzdálená instalace 10, 51

vzdálená konektivita 152

- model 152

vzdálené monitorování 169

vzdálené připojování k síti 137

vzdálené úložiště 579

vzdálený přístup 162, 321

- návrh 163

W

WAN spojení 92

webová sídla

- zabezpečení 346

webový server 137, 466

Windows 2000

- ATM, technologie 180
- DHCP, protokol 177
- instalace 379
- inovace 379
- pilotní program 117
- produkty 6
- konfigurace 7

- System Management Server 187
- TCP/IP 157
- úkoly plánování
- zavádění 52, 65, 74, 75

Windows 2000 Advanced Server 530

Windows 2000 Advanced Server 8

Windows 2000 Professional 6, 147

- automatizování instalace 766

Windows 2000 Server 7

- automatizování instalace 401

Windows 2000 Server Standard 8

Windows 95 147

Windows 98 147

Windows CE 496

Windows Installer 765

Windows Internet Name Service 160

- návrh systému 160

Windows NT 3.51 Workstation 147

- inovace 431

Windows NT 4.0 Workstation 147

- inovace 431

Winnt.exe 397, 761, 839

Winnt32.exe 397, 761, 836

Z

zabezpečená elektronická pošta 345

zabezpečené aplikace 343

zabezpečení 13

zabezpečení 21

zabezpečení sítě

- distribuované 315
- model 312
- plán 310
- správa důvěryhodnosti 312
- zásady 312

zabezpečení sítě 509

- plánování 510
- určení strategie 509
- zavádění technologií 516

zachytávání dat 646
základní úložiště 575
zásady místního počítače 339
zásady protokolární události 340
zásady registru 340
zásady skupin s omezeným členstvím 340
zásady skupiny 337
zásady systémových služeb 340
zásady systému souborů 341
zásady účtů 339
zásady veřejných klíčů 241
zásady zabezpečení protokolu IP 341
zatížení sítě 535 - vyrovnávání 535
zavádění klientů 627
životní cyklus certifikátu 366
změnové řízení 112
změnový management 111
zotavení po havárii 591, 592



Microsoft® Windows Server 2000

Plánování a implementace sítě

Kniha *Plánování a implementace sítě* vás vybaví všemi potřebnými informacemi potřebnými pro úspěšné naplánování, návrh a zvládnutí implementace Windows 2000 Serveru a Windows 2000 Professional ve vaší organizaci.

Z obsahu:

- Vytvoření plánu zavádění systému v organizaci, včetně zajištění souladu funkcí systému s jejími obchodními a provozními požadavky, pilotních projektů a postupů při testování.
- Příprava potřebné síťové infrastruktury, stanovení strategie pro konektivitu a bezpečnost sítě.
- Navržení infrastruktury Active Directory™ a strategie migrace domén.
- Automatizace instalace serverů a klientských stanic.
- Testování kompatibility aplikací, optimalizace jejich dostupnosti pomocí Windows Clusteringu.
- Vymezení problému správy klientských stanic a strategie řízení změn a konfigurace.
- Usnadnění zaváděcího procesu vývojovými diagramy a plánovacími tabulkami.



**Vydalo vydavatelství
a nakladatelství
Computer Press®**

Hornocholupická 22,
143 00 Praha 4,
<http://www.cpress.cz>

Distribuce:

Computer Press Brno,
náměstí 28. dubna 48,
635 00 Brno-Bystřec,
tel. (05) 46 12 21 11,
fax: (05) 46 12 21 12,
e-mail: distribuce@cpress.cz

Computer Press Bratislava,
Hattalova 12
831 03 Bratislava, SR,
tel.: +421 (7) 44 45 20 48,
44 25 17 20,
fax: +421 (7) 44 45 20 46,
e-mail: distribucia@cpress.sk

Publikaci lze objednat
také na adrese
<http://www.vltava.cz>



VŠECHNY CESTY
K INFORMACÍM

Microsoft®