

Windows® 7

Resource Kit

Mitch Tulloch, Tony Northrup, Jerry Honeycutt i Ed Wilson
oraz Microsoft Windows 7 Team

Przekład:

Leszek Biolik, Jakub Niedźwiedź, Krzysztof Szkudlarek

Windows® 7 Resource Kit
Edycja polska Microsoft Press
Original English language edition © 2010 by by Mitch Tulloch, Tony Northrup, and Jerry Honeycutt

Polish edition by APN PROMISE Sp. z o.o. Warszawa 2010

APN PROMISE Sp. z o.o., biuro: ul. Kryniczna 2, 03-934 Warszawa
tel. (022) 355-16-00; fax (022) 355-16-99
e-mail: mspress@promise.pl

Wszystkie prawa zastrzeżone. Żadna część niniejszej książki nie może być powielana ani rozpowszechniana w jakiegokolwiek formie i w jakikolwiek sposób (elektroniczny, mechaniczny), włącznie z fotokopiowaniem, nagrywaniem na taśmy lub przy użyciu innych systemów bez pisemnej zgody wydawcy.

Microsoft, Microsoft Press, Active Directory, ActiveX, Aero, Authenticode, BitLocker, ClearType, Direct3D, DirectX, ESP, Internet Explorer, MS, MSDN, MSN, OneNote, Outlook, SharePoint, SQL Server, SuperFetch, Visio, Visual Basic, Windows, Windows Media, Windows Mobile, Windows NT, Windows PowerShell, Windows Server, Windows Vista oraz Zune są zarejestrowanymi znakami towarowymi Microsoft Corporation.

Wszystkie inne nazwy handlowe i towarowe występujące w niniejszej publikacji mogą być znakami towarowymi zastrzeżonymi lub nazwami zastrzeżonymi odpowiednich firm odośnych właścicieli.

Przykłady firm, produktów, osób i wydarzeń opisane w niniejszej książce są fikcyjne i nie odnoszą się do żadnych konkretnych firm, produktów, osób i wydarzeń. Ewentualne podobieństwo do jakiegokolwiek rzeczywistej firmy, organizacji, produktu, nazwy domeny, adresu poczty elektronicznej, logo, osoby, miejsca lub zdarzenia jest przypadkowe i niezamierzone.

APN PROMISE Sp. z o.o. dołożyła wszelkich starań, aby zapewnić najwyższą jakość tej publikacji. Jednakże nikomu nie udziela się rękojmi ani gwarancji.
APN PROMISE Sp. z o.o. nie jest w żadnym wypadku odpowiedzialna za jakiegokolwiek szkody będące następstwem korzystania z informacji zawartych w niniejszej publikacji, nawet jeśli APN PROMISE została powiadomiona o możliwości wystąpienia szkód.

ISBN: 978-83-7541-059-4

Przekład: Leszek Biolik, Jakub Niedźwiedź, Krzysztof Szkudlarek
Redakcja: Marek Włodarz
Korekta: Ewa Swędrowska, Anna Wojdanowicz
Skład i łamanie: MAWart Marek Włodarz

Spis treści

Podziękowania	xxvii
Wstęp	xxix
Przegląd zawartości książki	xxix
Konwencje	xxx
Korzystanie z obrazu dysku CD	xxxii
Korzystanie z Windows 7 Resource Kit PowerShell Pack	xxxii
Korzystanie z przykładowych skryptów Windows PowerShell	xxxiii
Zastrzeżenie dotyczące zawartości płyty CD Windows PowerShell	xxxv
Zasady wsparcia dla pakietu Resource Kit	xxxvi

Część I Wprowadzenie

1 Przegląd uprawnień w systemie Windows 7	3
Usprawnienia w Windows 7 według rozdziałów	3
Interakcje z użytkownikiem	5
Wydajność	14
Mobilność	16
Niezawodność i możliwości wsparcia	19
Rozwiązywanie problemów	22
Wdrażanie	26
Wydania Windows 7	28
Windows 7 Starter	30
Windows 7 Home Basic	31
Windows 7 Home Premium	31
Windows 7 Professional	31
Windows 7 Enterprise	32
Windows 7 Ultimate	32
Wybieranie oprogramowania i sprzętu	33
Windows 7 Software Logo	33
Wymagania sprzętowe	34
Podsumowanie	35
Dodatkowe zasoby	35
Powiązane informacje	35
Na dołączonym nośniku	35
2 Bezpieczeństwo w systemie Windows 7	37
Odpowiedź na konkretne obawy związane z bezpieczeństwem	38
Prośby o pomoc związane ze szkodliwym oprogramowaniem	38
Kradzież danych	44
Funkcje zabezpieczeń wprowadzone wcześniej w systemie Windows Vista	47
Windows Defender	48
Zapora systemu Windows	50
Encrypting File System	52

Usprawnienia Menedżera poświadczeń	53
Usprawnienia zabezpieczeń architektonicznych i wewnętrznych	53
Nowe i poprawione funkcje zabezpieczeń Windows 7	63
BitLocker i BitLocker To Go	64
AppLocker	68
Wiele aktywnych profili zapory	69
Kontrola konta użytkownika	70
Funkcje zabezpieczeń programu Internet Explorer	76
Usprawnienia inspekcji	79
Bezpieczne odłączanie w puli jądra	81
Windows Biometric Framework	81
Karty inteligentne	82
Konta usług	82
Podsumowanie	83
Dodatkowe zasoby	84
Powiązane informacje	84
Na dołączonym nośniku	84

Część II Wdrażanie

3 Platforma wdrożeniowa	87
Wprowadzenie do narzędzi	87
Terminologia wdrażania Windows 7	90
Składniki platformy	91
Windows Imaging	93
Pliki odpowiedzi	93
Windows SIM	94
Windows Setup	95
Sysprep	96
Windows PE	97
Narzędzie Deployment Image Servicing and Management	98
Inne narzędzia	99
Usługi Windows Deployment Services	100
ImageX	101
Scenariusze wdrożeń	102
Aktualizacja komputera	102
Nowy komputer	102
Odświeżenie komputera	103
Wymiana komputera	103
Zrozumienie programu instalacyjnego	104
Faza instalacji wstępnej	105
Faza konfiguracji online	106
Faza Windows Welcome	107
Podstawowy proces wdrożeniowy	108
Proces Microsoft Deployment Toolkit	110
Podsumowanie	113
Dodatkowe zasoby	114
Powiązane informacje	114
Na dołączonym nośniku	114

4 Planowanie wdrożenia	115
Korzystanie z Microsoft Deployment Toolkit	115
Dokumentacja	117
Platforma rozwiązań	118
Planowanie wdrożeń na dużą skalę	119
Wizja	120
Planowanie projektu	121
Budowanie	122
Stabilizacja	123
Wdrażanie	124
Planowanie wdrożenia na małą skalę	124
Zakres i cele	125
Bieżące środowisko	125
Plan konfiguracji	126
Testowanie i pilotaż	127
Przeprowadzanie wdrożenia	127
Wymagania systemu Windows 7	128
Wymagania sprzętowe	128
Ścieżki aktualizacji	128
Przygotowanie do wdrożenia	129
Zarządzanie aplikacjami	130
Inżynieria obrazów	131
Wdrażanie	132
Naprawianie infrastruktury	133
Gotowość operacyjna	134
Zabezpieczenia	134
Migracja	135
Instalowanie Microsoft Deployment Toolkit	136
Uruchamianie narzędzia Deployment Workbench	138
Aktualizowanie składników pakietu Microsoft Deployment Toolkit	138
Podsumowanie	140
Dodatkowe zasoby	140
5 Testowanie zgodności aplikacji	141
Zrozumienie zgodności	142
Co oznacza zgodność	142
Dlaczego aplikacje przestają działać	143
Wybieranie najlepszego narzędzia	144
Asystent zgodności programów	144
Narzędzie do rozwiązywania problemów ze zgodnością programów	145
Application Compatibility Toolkit	146
Tryb Windows XP	147
Wirtualizacja aplikacji	147
Zrozumienie pakietu ACT	148
Wspierane topologie	149
Funkcje oceniające zgodność	150
Planowanie użycia ACT	151
Ukierunkowanie wdrożenia	152
Wybór metody wdrożeniowej	154
Wybór lokalizacji pliku dziennika	155

Przygotowanie do użycia ACT	156
Udostępnianie foldera przetwarzania dziennika	157
Przygotowywanie obsługi Microsoft Compatibility Exchange	157
Instalowanie ACT 5.5	157
Konfigurowanie ACM	158
Zbieranie danych na temat zgodności	159
Analizowanie danych na temat zgodności	161
Tworzenie i nadawanie kategorii	161
Określanie priorytetów danych dotyczących zgodności	163
Ocenianie zgodności aplikacji	164
Ustawianie statusu wdrożenia	165
Zarządzanie problemami ze zgodnością	166
Filtrowanie danych na temat zgodności	168
Synchronizowanie z usługą Compatibility Exchange Service	169
Racjonalizowanie zestawu aplikacji	170
Identyfikowanie brakujących aplikacji	170
Wybieranie określonych wersji aplikacji	170
Testowanie i rozwiązywanie problemów	171
Budowanie laboratorium testowego	172
Modelowanie środowiska produkcyjnego	173
Korzystanie z narzędzia Standard User Analyzer	174
Korzystanie z narzędzia Compatibility Administrator	175
Wdrażanie pakietów rozwiązujących problemy z aplikacjami	179
Podsumowanie	180
Dodatkowe zasoby	180
6 Przygotowywanie obrazów dysków	181
Zaczynamy	182
Wstępnie wymagane umiejętności	183
Wymagania dotyczące laboratorium	183
Przechwytywanie obrazów przy użyciu Microsoft Deployment Toolkit	186
Tworzenie i konfigurowanie udziału wdrożeniowego	187
Dodawanie systemów operacyjnych	190
Dodawanie aplikacji	192
Dodawanie pakietów	197
Dodawanie sterowników	201
Tworzenie sekwencji zadań	202
Edytowanie sekwencji zadań	206
Konfigurowanie właściwości grup i zadań	208
Konfigurowanie karty Options	209
Aktualizowanie udziału wdrożeniowego	213
Przechwytywanie obrazu dyskowego na potrzeby instalacji z niewielkim udziałem obsługi	220
Ręczne przygotowywanie obrazów	222
Dostosowywanie pakietu Microsoft Deployment Toolkit	224
Podsumowanie	225
Dodatkowe zasoby	225
7 Migrowanie danych stanu użytkowników	227
Ocena technologii migracji	228

Łatwy transfer w systemie Windows	228
Narzędzie User State Migration Tool	228
Microsoft IntelliMirror	229
Korzystanie z łatwego transferu w systemie Windows	230
Odświeżanie komputera	232
Zamiana komputera	233
Planowanie migracji stanu użytkowników przy użyciu USMT	236
Wybieranie ekspertów dziedzicznych	236
Identyfikowanie danych o stanie użytkowników	236
Ustalanie priorytetów zadań migracji	238
Wybieranie lokalizacji do przechowywania danych	238
Automatyzowanie narzędzia USMT	240
Testowanie migracji stanu użytkowników	241
Instalowanie USMT	242
Udział sieciowy	242
Nośnik Windows PE	243
Microsoft Deployment Toolkit	243
Configuration Manager	243
Zrozumienie składników USMT	243
Scanstate.exe	244
Loadstate.exe	245
Pliki migracyjne	246
Przygotowywanie plików migracyjnych	246
Dostosowywanie USMT	246
Składnia plików sterujących migracją	247
Wdrażanie plików migracyjnych	247
Korzystanie z USMT w Microsoft Deployment Toolkit	248
Określanie lokalizacji magazynów danych	248
Dodawanie niestandardowych plików migracyjnych	250
Podsumowanie	251
Dodatkowe zasoby	251
8 Rozpowszechnianie aplikacji	253
Przygotowywanie laboratorium	254
Planowanie wdrożenia	255
Priorytety	256
Kategorie	257
Metody instalacji	258
Eksperci dziedzicowi	258
Konfiguracje	259
Wybieranie strategii wdrażania	259
Grube obrazy	260
Cienkie obrazy	261
Obrazy hybrydowe	262
Automatyzowanie instalacji	263
Instalator systemu Windows (Windows Installer)	264
InstallShield	265
Starsze wersje InstallShield	266
Starsze wersje InstallShield – PackageForTheWeb	267
Starsze wersje Wise Installation System	267

Windows Script Host	267
Przepakowywanie starszych aplikacji	268
Proces przepakowywania	268
Narzędzia przepakowujące.	269
Wstawianie do obrazu dyskowego	270
Dodawanie aplikacji	271
Tworzenie zależności.	273
Instalowanie aplikacji	274
Podsumowanie	277
Dodatkowe zasoby	277
Powiązane informacje	277
Na dołączonym nośniku	278
9 Przygotowywanie środowiska Windows PE	279
Badanie środowiska Windows PE	280
Możliwości	282
Ograniczenia	284
Nowe funkcje środowiska Windows PE 3.0	285
Przygotowywanie środowiska	286
Instalowanie pakietu Windows AIK 2.0	286
Konfigurowanie środowiska budowania	287
Usuwanie środowiska budowania	288
Praca z Windows PE	288
Montowanie środowiska Windows PE	288
Dodawanie pakietów.	289
Kopiowanie aplikacji	291
Dodawanie sterowników urządzeń	291
Instalowanie aktualizacji	291
Zatwierdzanie zmian	291
Tworzenie nośnika rozruchowego	291
Dostosowywanie Windows PE	294
Automatyzowanie Windows PE	296
Automatyzacja przy pomocy Unattend.xml	296
Dodawanie obrazów do usług Windows Deployment Services.	296
Korzystanie z Windows PE w Microsoft Deployment Toolkit.	297
Podsumowanie	298
Dodatkowe zasoby	298
10 Konfigurowanie Windows Deployment Services	299
Wprowadzenie do usług Windows Deployment Services	300
Architektura usług	300
Tryby działania.	305
Planowanie usług Windows Deployment Services.	307
Wybór wersji usług Windows Deployment Services.	308
Wymagania serwerowe.	310
Wymagania dla komputerów klienckich	312
Wymagania DHCP.	312
Wymagania routingu	314
Wymagania wydajnościowe	314
Instalowanie usług Windows Deployment Services	315

Windows Server 2003	315
Windows Server 2008 R2	316
Konfigurowanie usług Windows Deployment Services	317
Przygotowywanie wykrywanych obrazów	319
Importowanie obrazów	321
Importowanie obrazów rozruchowych	321
Importowanie obrazów instalacyjnych	322
Wdrażanie pakietów sterowników	323
Wdrażanie pakietów sterowników na klientach	323
Zarządzanie grupami i pakietami sterowników	328
Dodawanie pakietów sterowników do obrazów rozruchowych	328
Zarządzanie zabezpieczeniami obrazów	329
Wstępne przygotowywanie komputerów klienckich	330
Konfigurowanie zatwierdzania przez administratora	331
Instalowanie systemu Windows 7	332
Przechwytywanie niestandardowych obrazów	333
Tworzenie transmisji multitemisyjnych	335
Wstępne wymagania dla multitemisji	335
Typy transmisji	336
Przeprowadzanie wdrażania multitemisyjnego	336
Korzystanie z Windows Deployment Services w Microsoft Deployment Toolkit	337
Podsumowanie	338
Dodatkowe zasoby	339
Powiązane informacje	339
Na dołączonym nośniku	339

11 Korzystanie z mechanizmu Volume Activation

Wstęp	341
Opcje aktywacji	342
Detal	342
Oryginalny producent sprzętu (OEM)	342
Volume Licensing	343
Key Management Service	344
Minimalne wymagania dla komputerów	345
Jak działa KMS	346
Planowanie wdrożenia KMS	347
Multiple Activation Key	350
Volume Activation Management Tool	350
Architektura MAK	351
Scenariusze Volume Activation	351
Sieć główna	353
Sieci izolowane	354
Pojedyncze komputery odłączone od sieci	356
Laboratoria testowe/projektowe	357
Co się stanie, jeśli systemy nie będą aktywowane?	358
Okres karencji	358
Wygaśnięcie okresu karencji	358
Klucze produktu	359
Podsumowanie	359
Dodatkowe zasoby	359

Powiązane informacje	359
Na dołączonym nośniku	360
12 Wdrażanie przy użyciu Microsoft Deployment Toolkit	361
Wprowadzenie do MDT 2010	361
Scenariusze wdrożeń	362
Dostęp do zasobów	362
Instalacji z niewielkim udziałem obsługi przy użyciu MDT 2010	363
Replikowanie udziału wdrożeniowego	364
Przygotowywanie usług Windows Deployment Services	366
Konfigurowanie zasobów	366
Konfigurowanie pliku CustomSettings.ini	367
Automatyzowanie procesu instalacji z niewielkim udziałem obsługi	369
Przeprowadzanie wdrożeń instalacji z niewielkim udziałem obsługi	371
Dostosowywanie pakietu MDT 2010	373
Konfigurowanie wielu komputerów	373
Konfigurowanie pojedynczych komputerów	376
Dostosowywanie pliku CustomSettings.ini	377
Dostosowywanie pliku BootStrap.ini	378
Korzystanie z bazy danych pakietu MDT 2010	379
Podsumowanie	384
Dodatkowe zasoby	384

Część III Zarządzanie komputerami biurowymi

13 Przegląd narzędzi zarządzania	387
Narzędzia dołączone do systemu	388
Zasady grupy	388
Windows Management Instrumentation	388
Windows PowerShell	389
Zdalne zarządzanie systemem Windows	390
Narzędzia wiersza polecenia	390
Pulpit zdalny	391
Narzędzia, które można pobrać	392
Microsoft Network Monitor	392
Microsoft Baseline Security Analyzer	393
Microsoft IPsec Diagnostic Tool	393
Windows NT Backup-Restore Utility	393
Windows Sysinternals Suite	394
System Windows 7 Enterprise i oprogramowanie Microsoft Desktop Optimization Pack	395
Microsoft Application Virtualization	396
Advanced Group Policy Management	396
Asset Inventory Service	397
Zestaw narzędziowy DaRT	397
Microsoft Enterprise Desktop Virtualization	397
Microsoft System Center Desktop Error Monitoring	398
Microsoft System Center	398
System Center Configuration Manager	398
System Center Operations Manager	399
System Center Data Protection Manager	400

System Center Virtual Machine Manager	400
System Center Essentials	401
Wprowadzenie do skryptów powłoki Windows PowerShell	401
Używanie poleceń cmdlet programu Windows PowerShell	402
Używanie przetwarzania potokowego do odczytu plików tekstowych	408
Dodatkowe metody przetwarzania potokowego	414
Działanie poleceń Cmdlet	419
Podstawy tworzenia skryptów	423
Używanie instrukcji <i>while</i>	429
Używanie instrukcji <i>do...while</i>	433
Używanie instrukcji <i>do...until</i>	436
Instrukcja <i>for</i>	439
Instrukcja <i>if</i>	445
Instrukcja <i>switch</i>	448
Działanie modułów	452
Dołączanie funkcji	452
Dodawanie funkcji Pomoc	457
Lokalizowanie i ładowanie modułów	464
Instalowanie modułów	467
Podsumowanie	473
Dodatkowe zasoby	474
Powiązane informacje	474
Na dołączonym nośniku	476
14 Zarządzanie środowiskiem pulpitu	479
Działanie zasad grupy w systemie Windows 7	479
Zasady grupy przed systemem Windows Vista	480
Zasady grupy w systemie Windows Vista i Windows Server 2008	482
Nowe funkcje zasad grupy w systemie Windows 7 i Windows Server 2008 R2	485
Ustawienia zasad grupy w systemie Windows 7	486
Działanie plików szablonów ADMX	494
Działanie wielu lokalnych zasad grupy	499
Zarządzanie zasadami grupy	502
Konfigurowanie magazynu centralnego	502
Dodawanie szablonów ADMX do magazynu	504
Tworzenie i zarządzanie obiektami GPO	505
Edytowanie obiektów GPO	511
Zarządzanie obiektami MLGPO	518
Migracja szablonów ADM do formatu ADMX	520
Konfigurowanie przetwarzania zasad grupy	522
Stosowanie narzędzia AGMP (Advanced Group Policy Management)	522
Rozwiązywanie problemów dotyczących zasad grupy	523
Korzystanie z programu Podgląd zdarzeń	524
Włączanie rejestrowania debugowania	526
Stosowanie narzędzia Group Policy Log View	527
Stosowanie narzędzia GPRresult	528
Podsumowanie	530
Dodatkowe zasoby	530
Informacje powiązane	530
Na dołączonym nośniku	532

15 Zarządzanie użytkownikami i ich danymi.	533
Działanie profili użytkowników w systemie Windows 7	533
Typy profili użytkownika	534
Obszar nazw profili użytkowników	536
Działanie bibliotek	548
Korzystanie z bibliotek	550
Zarządzanie bibliotekami	556
Implementowanie roamingu w korporacji	557
Działanie profili użytkowników mobilnych i funkcji Przekierowanie folderu	557
Implementowanie funkcji Przekierowanie folderu	563
Implementowanie profili użytkownika mobilnego	576
Praca z plikami trybu offline	587
Usprawnienia funkcji Pliki trybu offline wprowadzone w systemie Windows Vista	588
Dodatkowe usprawnienia funkcji Pliki trybu offline wprowadzone w systemie Windows 7	591
Działanie synchronizacji funkcji Pliki trybu offline	593
Zarządzanie funkcją Pliki trybu offline	596
Podsumowanie	611
Dodatkowe zasoby	612
Powiązane informacje	612
Na dołączonym nośniku	612
16 Zarządzanie dyskami i systemami plików.	613
Partycjonowanie dysku	614
Wybór pomiędzy rekordem MBR a tablicą GPT	614
Konwersja dysków MBR na dyski GPT	615
Partycje GPT	616
Wybór dysku podstawowego lub dynamicznego	617
Korzystanie z woluminów	617
Tworzenie woluminu prostego	617
Tworzenie woluminu łączonego	618
Tworzenie woluminu rozłożonego	619
Zmiana rozmiaru woluminu	620
Usuwanie woluminu	621
Tworzenie i używanie wirtualnych dysków twardych	622
Fragmentacja systemu plików	624
Tworzenie kopii zapasowej i przywracanie danych	626
Działanie kopii zapasowej plików	627
Struktura kopii zapasowej plików i folderów	628
Działanie kopii zapasowych Obraz systemu	630
Uruchamianie kopii zapasowej Obraz systemu z wiersza polecenia	630
Metoda przywracania kopii zapasowej Obraz systemu	631
Struktura kopii zapasowej obrazu systemu	633
Najlepsze rozwiązania dotyczące tworzenia kopii zapasowych komputerów	633
Zarządzanie kopiami zapasowymi za pomocą ustawień zasad grupy	634
Poprzednie wersje i kopie w tle	636
Funkcja Windows ReadyBoost	641
Szyfrowanie dysku za pomocą funkcji BitLocker	644
W jaki sposób funkcja BitLocker szyfruje dane	644
Ochrona danych za pomocą funkcji BitLocker	646

Funkcja BitLocker To Go	649
Etapy działania funkcji BitLocker	651
Wymagania ochrony woluminu systemowego za pomocą funkcji BitLocker	652
Jak włączyć funkcję BitLocker na woluminie systemowym dla komputerów bez modułu TPM	654
Jak włączyć szyfrowanie funkcją BitLocker na woluminach systemowych	654
Jak włączyć szyfrowanie funkcją BitLocker na woluminach danych	656
Jak zarządzać kluczami funkcji BitLocker na komputerze lokalnym	656
Jak zarządzać funkcją BitLocker w wierszu polecenia	657
Jak odzyskać dane chronione przez funkcję BitLocker	658
Jak wyłączyć lub usunąć szyfrowanie dysku funkcją BitLocker	660
Jak trwale usunąć dysk BitLocker	660
Jak przygotować usługę AD DS pod kątem funkcji BitLocker	661
Jak konfigurować agenta odzyskiwania danych	662
Zarządzanie funkcją BitLocker za pomocą zasad grupy	662
Koszt funkcji BitLocker	665
System EFS (Encrypting File System)	666
Eksportowanie certyfikatów osobistych	667
Importowanie certyfikatów osobistych	667
Przydzielanie dostępu użytkownikom do zaszyfrowanego pliku	668
Łączy symboliczne	668
Tworzenie łączy symbolicznych	669
Tworzenie względnych i bezwzględnych łączy symbolicznych	670
Tworzenie łączy symbolicznych z folderami udostępnionymi	671
Stosowanie łączy stałych	673
Przydziały dysku	674
Konfigurowanie przydziałów dysku na pojedynczym komputerze	674
Konfigurowanie przydziałów dysku z wiersza polecenia	675
Konfigurowanie przydziałów dysku za pomocą ustawień zasad grupy	676
Narzędzia dyskowe	677
Disk Usage	677
EFSDump	677
SDelete	678
Streams	678
Sync	679
MoveFile i PendMoves	680
Podsumowanie	680
Dodatkowe zasoby	681
Powiązane informacje	681
Na dołączonym nośniku	682
17 Zarządzanie urządzeniami i usługami	683
Instalacja i zarządzanie urządzeniami	683
Usprawnienia w systemie Windows 7 dotyczące obsługi urządzeń	683
Instalacja urządzeń	688
Instalowanie i używanie urządzeń	699
Zarządzanie instalacją urządzeń za pomocą zasad grupy	714
Rozwiązywanie problemów instalacji urządzeń	726
Zarządzanie energią zasilania	732
Usprawnienia zarządzania energią w systemie Windows 7	733

Konfigurowanie ustawień zarządzania energią	738
Działanie usług	754
Usprawnienia usług w systemie Windows 7	754
Zarządzanie usługami	759
Podsumowanie	764
Dodatkowe zasoby	765
Powiązane informacje	765
Na dołączonym nośniku	766
18 Zarządzanie drukarkami	767
Usprawnienia drukowania w systemie Windows 7	767
Usprawnienia drukowania wprowadzone poprzednio w systemie Windows Vista	768
Dodatkowe usprawnienia drukowania w systemie Windows 7	770
Działanie drukowania w systemie Windows 7	771
XPS	771
Działanie podsystemu drukowania w systemie Windows	772
Działanie izolowania sterownika drukarki	775
Działanie konsoli Zarządzanie drukowaniem	778
Usprawnienia konsoli Zarządzanie drukowaniem wprowadzone w systemie Windows 7	778
Konsola Zarządzanie drukowaniem	780
Dodawanie i usuwanie serwerów wydruku	782
Konfigurowanie zabezpieczeń domyślnych dla serwerów wydruku	783
Dodawanie drukarek za pomocą programu Kreator instalacji drukarki sieciowej	784
Tworzenie i używanie filtrów drukarek	786
Tworzenie i używanie filtrów sterowników	787
Zarządzanie drukarkami przy użyciu konsoli Zarządzanie drukowaniem	788
Konfigurowanie właściwości drukarek	789
Publikowanie drukarek w usłudze AD DS	789
Zarządzanie sterownikami drukarek	790
Konfigurowanie trybu izolowania sterownika drukarki	793
Eksportowanie i importowanie konfiguracji serwera wydruku	795
Wykonywanie operacji grupowych za pomocą konsoli Zarządzanie drukowaniem	797
Zarządzanie drukarkami po stronie klienta	798
Instalowanie drukarek za pomocą Kreatora dodawania drukarki	798
Wyszukiwanie drukarek	799
Instalowanie drukarek za pomocą funkcji Wskaż i drukuj	802
Używanie folderu Urządzenia i drukarki	802
Korzystanie z drukowania z rozpoznawaniem lokalizacji	804
Używanie języka Color Management CPL	806
Zarządzanie obsługą drukarek po stronie klienta za pomocą zasad grupy	806
Konfigurowanie Kreatora dodawania drukarki	807
Wyłączenie wykonywania drukarki po stronie klienta	808
Konfigurowanie ograniczeń pakietowej funkcji wskazywania i drukowania	809
Rozszerzanie działania funkcji Wskaż i drukuj za pomocą usługi Windows Update	811
Instalowanie drukarek za pomocą zasad grupy	814
Przygotowanie instalacji drukarek	814
Instalowanie połączenia z drukarką	815
Ograniczenia instalowania drukarek za pomocą zasad grupy	818
Przypisywanie drukarek w oparciu o lokalizację	819

Migracja serwerów wydruku	819
Migracja serwerów wydruku za pomocą konsoli Zarządzanie drukowaniem.....	819
Migracja serwerów wydruku za pomocą narzędzia PrintBRM.....	822
Monitorowanie i rozwiązywanie problemów dotyczących drukarek	823
Konfigurowanie powiadomień e-mail	823
Konfigurowanie powiadomień serwera wydruku	824
Konfigurowanie akcji skryptów	824
Konfigurowanie szczegółowego rejestrowania zdarzeń.....	825
Podsumowanie	825
Dodatkowe zasoby	826
Powiązane informacje	826
Na dołączonym dysku CD.....	826
19 Zarządzanie wyszukiwaniem	827
Usprawnienia wyszukiwania i indeksowania	827
Wyszukiwanie w systemie Windows XP	828
Wyszukiwanie w systemie Windows Vista	828
Wyszukiwanie w systemie Windows 7	830
Wersje usługi Windows Search	832
Działanie usługi Windows Search	833
Terminologia mechanizmu wyszukiwania	833
Procesy mechanizmu usługi Windows Search.....	836
Włączanie usługi indeksowania	838
Architektura mechanizmu usługi Windows Search.....	838
Działanie wykazu	839
Działanie procesu indeksowania	846
Działanie wyszukiwania zdalnego	856
Zarządzanie indeksowaniem	857
Konfigurowanie indeksu	858
Konfigurowanie indeksowania plików trybu offline	861
Konfigurowanie indeksowania plików zaszyfrowanych	861
Konfigurowanie indeksowania podobnych słów.....	863
Konfigurowanie indeksowania tekstu w dokumentach obrazu formatu TIFF.....	863
Inne ustawienia zasad indeksu	865
Używanie funkcji wyszukiwania	869
Konfigurowanie wyszukiwania za pomocą opcji folderów	869
Korzystanie z funkcji wyszukiwania w menu Start	872
Biblioteki wyszukiwania.....	875
Korzystanie z wyszukiwania federacyjnego	884
Rozwiązywanie problemów funkcji wyszukiwania i indeksowania	887
Podsumowanie	889
Dodatkowe zasoby	889
Powiązane informacje	889
Na dołączonym nośniku	890
20 Zarządzanie przeglądarką Windows Internet Explorer	891
Usprawnienia przeglądarki Internet Explorer 8.	892
Przeglądanie w trybie InPrivate	892
Filtrowanie w trybie InPrivate.....	893
Widok zgodności	894

Filtr SmartScreen	895
Wyróżnianie domen	896
Izolacja kart	897
Akceleratorzy	898
Usprawnienia wprowadzone poprzednio w przeglądarce Internet Explorer 7.	899
Zmiany interfejsu użytkownika.	899
Przeglądanie na kartach	900
Pasek wyszukiwania.	900
Źródła RSS	902
Ulepszona obsługa standardów	903
Rozszerzone ustawienia zasad grupy.	904
Obrona przeciw złośliwym programom.	904
Ochrona przed kradzieżą danych.	913
Strefy zabezpieczeń.	922
Zarządzanie przeglądarką Internet Explorer za pomocą zasad grupy	926
Ustawienia zasad grupy dotyczące programu Internet Explorer 7 i Internet Explorer 8	8926
Nowe ustawienia zasad dla programu Internet Explorer 8.	930
Używanie zestawu narzędziowego IEAK (Internet Explorer Administration Kit).	932
Rozwiązywanie problemów dotyczących programu Internet Explorer	933
Program Internet Explorer nie uruchamia się	933
Dodatek nie funkcjonuje prawidłowo	933
Niektóre strony sieci Web nie są wyświetlane prawidłowo	934
Zapobieganie instalowaniu niepożądanych pasków narzędzi	936
Zmiana strony głównej i innych ustawień	937
Podsumowanie	937
Dodatkowe zasoby	938
Powiązane informacje	938
Na dołączonym nośniku	938

Część IV Konserwacja komputerów biurowych

21 Utrzymywanie kondycji systemu	941
Monitorowanie wydajności	941
Udoskonalenia procesu monitorowania wydajności wprowadzone w systemie Windows 7.	947
Korzystanie z przystawki Monitor wydajności.	948
Monitor zasobów	963
Zakładka Przegląd	964
Zakładka Procesor CPU.	965
Zakładka Pamięć	966
Zakładka Dysk	967
Zakładka Sieć.	968
Monitor niezawodności	969
Sposób działania monitora niezawodności	970
Pakiet narzędziowy Windows Performance Tools.	972
Monitorowanie zdarzeń	973
Omówienie architektury zdarzeń systemu Windows	973
Kanały.	974
Udoskonalenia w monitorowaniu zdarzeń, wprowadzone w systemie Windows 7	976
Korzystanie z przystawki Podgląd zdarzeń	976

Monitorowanie zdarzeń przy użyciu programu narzędziowego wiersza polecenia Weventutil	988
Monitorowanie zdarzeń przy użyciu programu Windows PowerShell	990
Używanie Harmonogramu zadań	993
Ulepszenia usługi Harmonogram zadań, wprowadzone w systemie Windows 7	994
Omówienie zadań	995
Omówienie architektury usługi Harmonogram zadań	996
Omówienie zabezpieczeń usługi Harmonogram zadań	997
Omówienie trybów zgodności z poleceniem AT oraz z usługą Harmonogram zadań w wersji 1.0.	999
Omówienie przystawki Harmonogram zadań	999
Omówienie zadań domyślnych	1000
Tworzenie zadań	1001
Zarządzanie zadaniami	1012
Tworzenie i zarządzanie zadaniami przy użyciu programu SchTasks.exe	1014
Zdarzenia harmonogramu zadań	1016
Rozwiązywanie problemów związanych z usługą Harmonogram zadań	1017
Interpretowanie kodów rezultatu i kodów powrotu	1019
Omówienie Narzędzia do oceny wydajności systemu Windows	1020
Omówienie testów wykonywanych przez narzędzie WinSAT	1020
Analiza wyników oceny funkcjonalności, przeprowadzonej przez program WinSAT . .	1021
Uruchamianie programu WinSAT z poziomu wiersza polecenia	1022
Omówienie kodów wyjścia zwracanych przez program WinSAT	1024
Uruchamianie programu WinSAT za pomocą elementu Informacje wydajności i narzędzia	1025
Omówienie funkcji raportowania błędów systemu Windows	1028
Przegląd funkcjonalności raportowania błędów systemu Windows	1029
Działanie systemu WER	1029
Omówienie cyklu raportowania błędów	1036
Omówienie danych WER	1037
Konfigurowanie systemu WER przy użyciu zasad grupy	1039
Konfigurowanie systemu WER przy użyciu Centrum akcji	1043
Podsumowanie	1047
Dodatkowe zasoby	1047
Powiązane informacje	1047
Na dołączonym dysku CD	1047

22 Zapewnianie wsparcia dla użytkowników przy użyciu Pomocy zdalnej . . 1049

Omówienie Pomocy zdalnej	1049
Udoskonalenia zdalnej pomocy, wprowadzone w systemie Windows 7	1050
Sposób działania Pomocy zdalnej	1052
Korzystanie z Pomocy zdalnej w środowisku korporacyjnym	1065
Współdziałanie z wersją Pomocy zdalnej systemu Windows Vista	1068
Współdziałanie z wersją Pomocy zdalnej systemu Windows XP	1068
Implementowanie i zarządzanie Pomocą zdalną	1069
Inicjowanie sesji Pomocy zdalnej	1070
Scenariusz 1: Wysyłanie zaproszenia Pomocy zdalnej przy użyciu funkcji łatwe połączenie	1076

Scenariusz 2: Zamawianie Pomocy zdalnej poprzez tworzenie biletów Pomocy zdalnej i zapisywanie ich w monitorowanych, udostępnionych folderach sieciowych	1081
Scenariusz 3: Oferowanie Pomocy zdalnej przy użyciu modelu DCOM	1084
Zarządzanie Pomocą zdalną przy użyciu zasad grupy	1086
Konfigurowanie Pomocy zdalnej w środowiskach niezarządzanych	1089
Dodatkowe ustawienia rejestru służące do konfigurowania Pomocy zdalnej.	1090
Podsumowanie	1097
Dodatkowe zasoby	1098
23 Zarządzanie aktualizacjami oprogramowania.	1099
Metody rozpowszechniania aktualizacji	1100
Klient Windows Update	1101
Usługa WSUS (Windows Server Update Services).	1103
System Center Configuration Manager 2007 R2.	1104
Ręczne instalowanie, skryptowanie i usuwanie aktualizacji.	1105
Omówienie plików aktualizacji w systemie Windows	1105
Instalowanie aktualizacji przy użyciu skryptów.	1106
Metody usuwania aktualizacji.	1107
Wdrażanie aktualizacji na nowych komputerach	1108
Zarządzanie usługą inteligentnego transferu w tle	1111
Zachowanie się usługi BITS.	1111
Ustawienia zasad grupy dotyczące usługi BITS.	1113
Zarządzanie usługą BITS przy użyciu programu Windows PowerShell	1115
Ustawienia zasad grupy, dotyczące klienta Windows Update.	1116
Konfigurowanie ustawień serwera proxy dla rozszerzenia Windows Update.	1118
Narzędzia służące do kontrolowania aktualizacji oprogramowania.	1119
Konsola MBSA	1120
MBSACL.	1122
Rozwiązywanie problemów związanych z funkcjonowaniem klienta Windows Update	1125
Proces aktualizowania oprogramowania sieciowego.	1127
Tworzenie zespołu odpowiedzialnego za aktualizowanie oprogramowania	1128
Przeprowadzanie inwentaryzacji oprogramowania	1129
Tworzenie procesu aktualizacji.	1130
Sposób dystrybuowania aktualizacji przez firmę Microsoft.	1137
Aktualizacje zabezpieczeń	1137
Aktualizacje zbiorcze.	1139
Pakiety serwisowe	1139
Cykl życia produktów firmy Microsoft	1141
Podsumowanie	1141
Dodatkowe zasoby	1142
Powiązane informacje	1142
Na dołączonym nośniku	1142
24 Zarządzanie ochroną klienta	1143
Omówienie zagrożeń płynących ze strony złośliwego oprogramowania.	1143
Kontrola konta użytkownika	1145
Kontrola konta użytkownika dla użytkowników standardowych.	1149
Kontrola konta użytkownika dla administratorów	1152
Interfejs użytkownika funkcji Kontrola konta użytkownika	1153

W jaki sposób system Windows sprawdza, czy dana aplikacja potrzebuje uprawnień administracyjnych	1154
Wirtualizacja zasobów przez funkcję Kontroli konta użytkownika	1157
Funkcja kontroli użytkownika a automatyczne uruchamianie programów.	1159
Problemy ze zgodnością i funkcją Kontroli konta użytkownika	1159
Sposób konfigurowania funkcji Kontrola konta użytkownika	1162
Sposób konfigurowania inspekcji podnoszenia uprawnień	1167
Inne dzienniki zdarzeń funkcji Kontrola konta użytkownika	1168
Wskazówki praktyczne dotyczące korzystania z funkcji Kontrola konta użytkownika	1169
Funkcja AppLocker	1170
Rodzaje reguł funkcji AppLocker	1172
Prowadzenie inspekcji reguł funkcji AppLocker	1175
Reguły bibliotek DLL	1177
Niestandardowe komunikaty błędów	1177
Korzystanie z funkcji AppLocker przy użyciu programu Windows PowerShell.	1178
Używanie programu Windows Defender	1178
Omówienie programu Windows Defender	1179
Poziomy alertów programu Windows Defender.	1182
Omówienie społeczności Microsoft SpyNet	1182
Konfigurowanie zasad grupy programu Windows Defender.	1184
Konfigurowanie programu Windows Defender na pojedynczym komputerze	1186
Jak sprawdzić, czy komputer został zainfekowany oprogramowaniem szpiegującym	1186
Wskazówki praktyczne dotyczące korzystania z programu Windows Defender	1187
Rozwiązywanie problemów związanych z niechcianym oprogramowaniem	1188
Ochrona dostępu do sieci	1189
Forefront	1191
Podsumowanie	1193
Dodatkowe zasoby	1195
Na dołączonym nośniku	1196

Część V Sieć

25 Konfigurowanie sieci	1199
Poprawiona użyteczność	1199
Centrum sieci i udostępniania	1200
Eksplorator sieci	1201
Jak system Windows odnajduje zasoby sieciowe	1202
Mapa sieci	1205
Kreator Skonfiguruj połączenie lub sieć	1206
Ulepszone możliwości zarządzania	1206
Typy lokalizacji sieciowych	1207
Zarządzanie mechanizmem QoS przy użyciu zasad grupy	1208
Zapora systemu Windows i protokół IPsec	1217
Kreator Połącz teraz w systemie Windows.	1218
Udoskonalenia podstawowych funkcji sieciowych	1219
Usługa BranchCache	1219
DNSsec	1225
GreenIT	1225
Efektywne wykorzystywanie sieci	1226
Skalowalne sieci	1232

Zwiększona niezawodność	1234
Obsługa protokołu IPv6	1235
Uwierzytelnianie sieciowe 802.1X.	1237
Protokół Server Message Block (SMB) 2.0.	1240
Silny model hosta	1241
Sieci bezprzewodowe	1242
Ulepszone interfejsy API.	1244
Rozpoznawanie sieci	1244
Ulepszenia sieci równorzędnych.	1245
Architektura EAPHost	1248
Architektura LSP	1249
Ścieżka WSD dla sieci SAN	1249
Sposób konfigurowania ustawień sieci bezprzewodowych	1250
Ręczne konfigurowanie ustawień sieci bezprzewodowej.	1251
Konfigurowanie ustawień sieci bezprzewodowej przy użyciu zasad grupy	1252
Konfigurowanie ustawień sieci bezprzewodowej z poziomu wiersza polecenia lub skryptu.	1254
Konfigurowanie protokołu TCP/IP.	1256
DHCP	1256
Ręczne konfigurowanie adresów IP	1260
Okno wiersza polecenia i skrypty.	1261
Sposób podłączania komputera do domeny usługi katalogowej Active Directory	1262
Sposób podłączania komputerów do domeny, gdy uwierzytelnianie 802.1X nie jest włączone	1262
Sposób podłączania komputerów do domeny, gdy uwierzytelnianie 802.1X jest włączone	1264
Podsumowanie	1265
Dodatkowe zasoby	1265
Powiązane informacje	1265
Na dołączonym nośniku	1266
26 Konfigurowanie Zapory systemu Windows oraz IPsec	1267
Omówienie Zapory systemu Windows z zabezpieczeniami zaawansowanymi	1267
Udoskonalenia zapory systemu Windows, wprowadzone wcześniej do systemu Windows Vista	1268
Dodatkowe udoskonalenia Zapory systemu Windows, wprowadzone w systemie Windows 7	1269
Omówienie platformy filtrowania systemu Windows	1272
Omówienie funkcji utwardzania usług systemu Windows	1276
Omówienie funkcjonalności kilku aktywnych profili zapory ogniowej	1282
Omówienie reguł.	1286
Zarządzanie Zaporą systemu Windows z zabezpieczeniami zaawansowanymi	1306
Narzędzia służące do zarządzania Zaporą systemu Windows z zabezpieczeniami zaawansowanymi	1306
Typowe zadania związane z zarządzaniem	1317
Podsumowanie	1337
Dodatkowe zasoby	1337
Powiązane informacje	1337
Na dołączonym nośniku	1338

27 Łączenie się ze zdalnymi użytkownikami i sieciami	1339
Ulepszenia w zakresie łączenia się ze zdalnymi użytkownikami i sieciami	
w systemie Windows 7	1339
Omówienie protokołu IKEv2	1340
Omówienie protokołu MOBIKE	1341
Omówienie funkcji wznawiania połączeń VPN	1342
Omówienie funkcji DirectAccess	1349
Omówienie funkcji BranchCache	1354
Obsługiwane rodzaje połączeń	1357
Rodzaje połączeń wychodzących	1357
Rodzaje połączeń przychodzących	1358
Przestarzałe rodzaje połączeń	1359
Konfigurowanie połączeń VPN	1359
Obsługiwane protokoły tunelujące	1359
Porównanie różnych protokołów tunelowania	1360
Omówienie udoskonaleń kryptograficznych	1362
Omówienie procesu negocjowania połączenia VPN	1369
Tworzenie i konfigurowanie połączeń VPN	1374
Konfigurowanie połączeń telefonicznych	1391
Tworzenie połączenia telefonicznego	1391
Konfigurowanie połączeń telefonicznych	1393
Zaawansowane ustawienia połączeń	1394
Konfigurowanie połączeń przychodzących	1394
Zarządzanie połączeniami przy użyciu zasad grupy	1396
Korzystanie z Pulpitu zdalnego	1400
Omówienie Pulpitu zdalnego	1400
Konfigurowanie i używanie Pulpitu zdalnego	1405
Konfigurowanie i używanie funkcji Połączenie programów RemoteApp i pulpitu	1423
Podsumowanie	1427
Dodatkowe zasoby	1428
Powiązane informacje	1428
Na dołączonym nośniku	1428
28 Wdrażanie IPv6	1429
Omówienie protokołu IPv6	1429
Omówienie terminologii związanej z protokołem IPv6	1431
Omówienie adresacji protokołu IPv6	1432
Omówienie routingu protokołu IPv6	1437
Omówienie komunikatów protokołu ICMPv6	1440
Omówienie procesu wykrywania sąsiadów	1441
Omówienie funkcji autokonfiguracji adresu	1444
Omówienie procesu tłumaczenia nazw	1446
Ulepszenia protokołu IPv6 w systemie Windows 7	1449
Podsumowanie ulepszeń protokołu IPv6 wprowadzonych w systemie Windows 7	1450
Konfigurowanie protokołu IPv6 w systemie Windows 7 i rozwiązywanie problemów	1454
Wyświetlanie ustawień adresowych protokołu IPv6	1454
Konfigurowanie protokołu IPv6 w systemie Windows 7 przy użyciu graficznego interfejsu użytkownika	1460
Konfigurowanie protokołu IPv6 w systemie Windows 7 przy użyciu programu Netsh	1462

Inne zadania związane z konfigurowaniem protokołu IPv6	1463
Rozwiązywanie problemów związanych z łącznością opartą na protokole IPv6	1467
Planowanie migracji do protokołu IPv6	1469
Omówienie technologii ISATAP	1471
Migracja sieci intranetowej do protokołu IPv6	1473
Podsumowanie	1479
Dodatkowe zasoby	1479
Powiązane informacje	1479
Na dołączonym nośniku	1480

Część VI Rozwiązywanie problemów

29 Konfigurowanie rozruchu i rozwiązywanie problemów z uruchamianiem	1483
Co nowego w rozruchu systemu Windows	1483
Dane konfiguracji rozruchu	1484
Odzyskiwanie systemu	1487
Windows Boot Performance Diagnostics	1489
Zrozumienie procesu uruchamiania	1489
Faza testu POST (Power-on self test)	1490
Faza wstępnego uruchamiania	1491
Faza Menedżera rozruchu systemu Windows	1494
Faza Modułu ładującego rozruchu systemu Windows	1495
Faza ładowania jądra	1496
Faza logowania	1501
Ważne pliki startowe	1502
Jak konfigurować ustawienia uruchamiania	1503
Jak korzystać z okna dialogowego Uruchamianie i odzyskiwanie	1504
Jak korzystać z narzędzia Konfiguracja systemu	1504
Jak korzystać z BCDEdit	1505
Rozwiązywanie problemów z rozruchem	1512
Rozwiązywanie problemów z rozruchem przed pojawieniem się logo	
Trwa uruchamianie systemu Windows	1513
Rozwiązywanie problemów z rozruchem po pojawieniu się logo Trwa	
uruchamianie systemu Windows	1522
Rozwiązywanie problemów z rozruchem po logowaniu	1533
Podsumowanie	1537
Dodatkowe zasoby	1537
Powiązane informacje	1537
Na dołączonym dysku CD	1538
30 Rozwiązywanie problemów dotyczących sprzętu, sterowników i dysków	1539
Usprawnienia dotyczące rozwiązywania problemów ze sprzętem i sterownikami	1540
Platforma rozwiązywania problemów w systemie Windows	1540
Monitor niezawodności	1543
Monitor zasobów	1544
Diagnostyka pamięci systemu Windows	1546
Diagnostyka awarii dyskowych	1546
Samo naprawiający się system NTFS	1547
Poprawiona niezawodność sterowników	1548

Usprawnione raportowanie błędów	1548
Proces rozwiązywania problemów sprzętowych	1548
Jak rozwiązywać problemy uniemożliwiające uruchomienie systemu Windows	1549
Jak rozwiązywać problemy z instalowaniem nowego sprzętu	1549
Jak rozwiązywać problemy z istniejącym sprzętem	1550
Jak rozwiązywać problemy z nieprzewidywalnymi symptomami	1551
Jak diagnozować problemy sprzętowe	1552
Jak korzystać z Menedżera urządzeń do identyfikowania wadliwych urządzeń.	1552
Jak sprawdzać fizyczny stan komputera	1553
Jak sprawdzić konfigurację sprzętu	1554
Jak sprawdzać, czy oprogramowanie firmowe systemu i urządzeń peryferyjnych jest aktualne	1556
Jak testować swój sprzęt, uruchamiając narzędzia diagnostyczne	1556
Jak diagnozować problemy związane z dyskami	1557
Jak korzystać z wbudowanej diagnostyki	1559
Jak korzystać z Monitora niezawodności.	1559
Jak korzystać z Podglądu zdarzeń	1559
Jak korzystać z zestawów modułów zbierających dane	1560
Jak korzystać z Diagnostyki pamięci systemu Windows.	1561
Jak rozwiązywać problemy dyskowe	1566
Jak przygotować się na awarie dysków	1567
Jak korzystać z ChkDsk	1568
Jak korzystać z kreatora Oczyszczanie dysku	1573
Jak wyłączyć nieuolną pamięć podręczną	1573
Jak rozwiązywać problemy ze sterownikami.	1574
Jak znaleźć zaktualizowane sterowniki	1574
Jak wycofywać sterowniki	1574
Jak korzystać z Weryfikatora sterowników	1575
Jak korzystać z Weryfikacji podpisu pliku	1577
Jak korzystać z Menedżera urządzeń do przeglądania i zmieniania wykorzystania zasobów	1578
Jak korzystać z Przywracania systemu.	1579
Jak rozwiązywać problemy z USB	1580
Jak rozwiązywać problemy ze sterownikami i sprzętem USB.	1580
Zrozumienie ograniczeń USB	1580
Jak identyfikować problemy z USB, korzystając z Monitora wydajności	1581
Jak badać koncentratory USB.	1583
Jak rozwiązywać problemy z Bluetooth.	1584
Narzędzia do rozwiązywania problemów	1585
DiskView.	1585
Handle	1586
Process Monitor.	1586
Podsumowanie	1587
Dodatkowe zasoby	1588
Powiązane informacje	1588
Na dołączonym dysku CD.	1588
31 Rozwiązywanie problemów sieciowych.	1589
Narzędzia do rozwiązywania problemów	1589
Arp	1592

Podgląd zdarzeń	1594
IPConfig	1595
Nblookup	1596
Nbtstat	1597
Net	1599
Netstat	1600
Network Monitor	1602
Nslookup	1603
PathPing	1606
Monitor wydajności	1609
Zestawy modułów zbierających dane	1612
Monitor zasobów	1613
Ping	1614
PortQry	1615
Route	1617
Menedżer zadań	1620
TCPView	1622
Klient Telnet	1623
Testowanie łączności z usługami	1624
Test TCP	1624
Diagnostyka sieci systemu Windows	1626
Proces rozwiązywania problemów sieciowych	1627
Jak rozwiązywać problemy z łącznością sieciową	1628
Jak rozwiązywać problemy z łącznością z aplikacjami	1633
Jak rozwiązywać problemy z tłumaczeniem nazw	1636
Jak rozwiązywać problemy wydajnościowe i sporadyczne problemy z łącznością	1639
Jak rozwiązywać problemy z przyłączaniem się do domeny lub logowaniem w niej	1642
Jak rozwiązywać problemy z odnajdowaniem sieci	1645
Jak rozwiązywać problemy z udostępnianiem plików i drukarek	1646
Jak rozwiązywać problemy z sieciami bezprzewodowymi	1648
Jak rozwiązywać problemy z zaporą	1650
Podsumowanie	1652
Dodatkowe zasoby	1652
Powiązane informacje	1652
Na dołączonym dysku CD	1652
32 Błędy stopu	1653
Przegląd komunikatów stopu	1653
Identyfikowanie błędu stopu	1654
Znajdowanie informacji pomagających rozwiązywać problemy	1654
Komunikaty stopu	1655
Typy błędów stopu	1657
Pliki zrzutów pamięci	1658
Konfigurowanie plików małych zrzutów pamięci	1660
Konfigurowanie plików zrzutów pamięci jądra	1661
Konfigurowanie plików pełnych zrzutów pamięci	1662
Jak ręcznie zainicjować błąd stopu i utworzyć plik zrzutu	1662
Korzystanie z plików zrzutów pamięci do analizowania błędów stopu	1663
Przygotowanie na błędy stopu	1667
Zapobieganie ponownym uruchomieniom systemu po błędzie stopu	1667

Rejestrowanie i zapisywanie informacji z komunikatu stopu	1668
Sprawdzanie wymagań oprogramowania odnośnie miejsca na dysku	1669
Instalowanie debugera jądra i plików symboli	1669
Typowe komunikaty stopu	1669
Błąd stopu 0xA lub IRQL_NOT_LESS_OR_EQUAL	1669
Błąd stopu 0x1E lub KMODE_EXCEPTION_NOT_HANDLED	1671
Błąd stopu 0x24 lub NTFS_FILE_SYSTEM	1674
Błąd stopu 0x2E lub DATA_BUS_ERROR	1675
Błąd stopu 0x3B lub SYSTEM_SERVICE_EXCEPTION	1676
Błąd stopu 0x3F lub NO_MORE_SYSTEM_PTES	1677
Błąd stopu 0x50 lub PAGE_FAULT_IN_NONPAGED_AREA	1678
Błąd stopu 0x77 lub KERNEL_STACK_INPAGE_ERROR	1679
Błąd stopu 0x7A lub KERNEL_DATA_INPAGE_ERROR	1681
Błąd stopu 0x7B lub INACCESSIBLE_BOOT_DEVICE	1682
Błąd stopu 0x7F lub UNEXPECTED_KERNEL_MODE_TRAP	1684
Błąd stopu 0x9F lub DRIVER_POWER_STATE_FAILURE	1686
Błąd stopu 0xBE lub ATTEMPTED_WRITE_TO_READONLY_MEMORY	1688
Błąd stopu 0xC2 lub BAD_POOL_CALLER	1688
Błąd stopu 0xCE lub DRIVER_UNLOADED_WITHOUT_CANCELLING_	
PENDING_OPERATIONS	1691
Błąd stopu 0xD1 lub IRQL_NOT_LESS_OR_EQUAL	1691
Błąd stopu 0xD8 lub DRIVER_USED_EXCESSIVE_PTES	1692
Błąd stopu 0xEA lub THREAD_STUCK_IN_DEVICE_DRIVER	1693
Błąd stopu 0xED lub UNMOUNTABLE_BOOT_VOLUME	1693
Błąd stopu 0xFE lub BUGCODE_USB_DRIVER	1694
Błąd stopu 0x00000124	1695
Błąd stopu 0xC000021A lub STATUS_SYSTEM_PROCESS_TERMINATED	1696
Błąd stopu 0xC0000221 lub STATUS_IMAGE_CHECKSUM_MISMATCH	1697
Komunikaty dotyczące błędnego funkcjonowania sprzętu	1698
Lista komunikatów stopu	1698
Sprawdzanie oprogramowania	1699
Sprawdzanie sprzętu	1701
Podsumowanie	1704
Dodatkowe zasoby	1704
Powiązane informacje	1704
Na dołączonym dysku CD	1704

Część VII Dodatki

A Ułatwienia dostępu w systemie Windows 7	1707
Centrum ułatwień dostępu	1707
Dodatkowe funkcje ułatwień dostępu	1710
Korzystanie z Centrum ułatwień dostępu	1711
Korzystanie z lupy	1712
Korzystanie z Narratora	1713
Korzystanie z klawiatury ekranowej	1714
Skróty klawiaturowe ułatwień dostępu	1715
Rozpoznawanie mowy w systemie Windows	1715
Produkty technologii wspomagających	1717
Centra zasobów ułatwień dostępu firmy Microsoft	1718

Dodatkowe zasoby	1718
B Słownik	1719
Indeks	1739
O autorach	1775
Wymagania systemowe	1780

Podziękowania

Autorzy książki Windows 7 Resource Kit chcieliby podziękować licznym członkom zespołu produktowego i innym ekspertom w firmie Microsoft, którzy poświęcili setki godzin cennego czasu na ten projekt, pomagając nam zaplanować zakres materiału, udostępniając specyfikacje produktu, sprawdzając rozdziały pod względem dokładności technicznej, pisząc teksty do ramek z uwagami, które dostarczyły cennych wskazówek, oraz oferując rady, zachęty i wsparcie podczas naszej pracy nad tym projektem. Chcielibyśmy szczególnie wyrazić swoje podziękowania następującym osobom, które pracują w firmie Microsoft, są to:

Aanand Ramachandran, Aaron Smith, Abhishek Tiwari, Adrian Lannin, Alan Morris, Alex Balcanquall, Alwin Vyhmeister, Andy Myers, Anirban Paul, Anjali Chaudhry, Anton Kucer, Ayesha Mascarenhas, Baldwin Ng, Bill Mell, Brent Goodpaster, Brian Lich, Chandra Nukala, Chris Clark, Connie Rock, Crispin Cowan, Darren Baker, Dave Bishop, Denny Gursky, Desmond Lee, Devrim Iyigun, George Roussos, Gerardo Diaz Cuellar, Gov Maharaj, James Kahle, James O'Neill, Jason Grieves, Jason Popp, Jez Sadler, Jim Martin, Joe Sherman, John Thekkethala, Jon Kay, Joseph Davies, Judith Herman, Katharine O'Doherty, Kathleen Carey, Kevin Woley, Kim Griffiths, Kukjin Lee, Kyle Beck, Lilia Gutnik, Lyon Wong, Mark Gray, Michael Murgolo, Michael Niehaus, Michael Novak, Mike Lewis, Mike Owen, Mike Stephens, Narendra Acharya, Nazia Zaman, Nils Dussart, Pat Stemen, Ramprabhu Rathnam, Richie Fang, Rick Kingslan, Scott Roberts, Sean Gilmour, Sean Siler, Sharad Kylasam, Steve Campbell, Thomas Willingham, Tim Mintner, Troy Funk, Varun Bahl, Vikram Singh i Wole Moses.

Dziękujemy też Billowi Noonanowi, Markowi Kitrisowi i zespołowi CTS Global Technical Readiness (GTR) w firmie Microsoft za wsparcie eksperckie dla tego projektu. Zespół GTR rozwija szkolenia dla inżynierów Microsoft Commercial Technical Support (CTS) we wszystkich działach produktowych, w tym Platforms, Messaging, Office Worker i Developer. GTR tworzy szczegółowe materiały techniczne „dla inżynierów przez inżynierów” z pomocą czołowych ekspertów, którzy są prawdziwymi inżynierami wspierającymi dla grup produktowych CTS.

Wreszcie specjalne podziękowania kierujemy do wspianalego zespołu redakcyjnego w Microsoft Press, w tym do takich osób jak Juliana Aldous, Karen Szall i Melissa von Tschudi-Sutton za niezmordowaną energię i poświęcenie pracy z nami nad tym ambitnym projektem oraz doprowadzenie go do sukcesu. Dziękujemy również Jean Findley z Custom Editorial Productions, Inc. (CEP), która zajmowała się aspektami produkcyjnymi tej książki oraz Susan McClung i Julie Hotchkiss, naszym redaktorkom, które zwracały baczną uwagę na szczegóły. Dziękujemy też Bobowi Deanowi, naszemu niezmordowanemu recenzentowi technicznemu.

Dziękujemy wszystkim!

—Autorzy

Wstęp

Zapraszamy do *Windows 7 Resource Kit* z Microsoft Press! *Windows 7 Resource Kit* jest wyczerpującym źródłem informacji technicznych, dotyczących wdrażania, konserwacji i rozwiązywania problemów z systemem Windows 7. Grupą docelową dla tego pakietu są doświadczeni profesjonaliści IT, którzy pracują w średnich i dużych organizacjach, ale każdy, kto chce nauczyć się, jak wdrażać, konfigurować, obsługiwać i rozwiązywać problemy z systemem Windows 7 w środowiskach usług Active Directory Domain Services (AD DS), uzna ten pakiet za nieoceniony.

Czytelnik znajdzie tu dogłębne informacje i oparte na zadaniach wskazówki dotyczące zarządzania wszystkimi aspektami systemu Windows 7, w tym zautomatyzowanym wdrażaniem, zarządzaniem środowiskiem pulpitu, wyszukiwaniem i organizacją, zarządzaniem aktualizacjami oprogramowania, ochroną klientów, sieciami, zdalnym dostępem i systematycznymi technikami rozwiązywania problemów. Można też będzie znaleźć tutaj liczne wtrącenia w ramach opracowane przez członków zespołu Windows w firmie Microsoft, które dają pełny wgląd w działanie systemu Windows 7, najlepsze praktyki zarządzania tą platformą i nieocenione wskazówki dotyczące rozwiązywania problemów. Wreszcie dołączony dysk zawiera *Windows 7 Resource Kit PowerShell Pack* oraz przykładowe skrypty Windows PowerShell, które można dostosowywać w celu automatyzowania różnych aspektów zarządzania klientami Windows 7 w środowiskach korporacyjnych.

Przegląd zawartości książki

Sześć części tej książki obejmuje następujące tematy:

- **Część I – Wprowadzenie** Zapewnia wstęp do funkcjonalności systemu Windows 7 oraz przegląd uprawnień dla tej platformy związanych z zabezpieczeniami.
- **Część II – Wdrażanie** Zapewnia dogłębne informacje i wskazówki dotyczące wdrażania systemu Windows 7 w środowiskach korporacyjnych ze szczególnym skupieniem się na wykorzystaniu narzędzia Microsoft Deployment Toolkit 2010 (MDT 2010).
- **Część III – Zarządzanie komputerami biurowymi** Opisuje, jak korzystać z zasad grupy do zarządzania środowiskiem pulpitu dla użytkowników komputerów działających pod kontrolą systemu Windows 7 i jak zarządzać konkretnymi funkcjami, takimi jak dyski i systemy plików, urządzenia i usługi, drukowanie, wyszukiwanie oraz Windows Internet Explorer.
- **Część IV – Konserwacja komputerów biurowych** Opisuje, jak utrzymywać kondycję komputerów działających pod kontrolą systemu Windows 7 poprzez korzystanie z infrastruktury, monitorowanie wydajności, zarządzanie aktualizacjami oprogramowania, zarządzanie ochroną klientów i korzystanie z Pomocy zdalnej.

- **Część V – Sieć** Zapewnia dogłębne informacje dotyczące podstaw sieci, sieci bezprzewodowych, zapory systemu Windows, Internet Protocol Security (IPsec), łączenia zdalnego przy użyciu wirtualnych sieci prywatnych (VPN), zdalnego pulpitu oraz protokołu Internet Protocol version 6 (IPv6).
- **Część VI – Rozwiązywanie problemów** Opisuje, jak rozwiązywać problemy z uruchamianiem systemu, sprzętem i siecią, a także jak interpretować komunikaty stopu.

Konwencje

W tej książce są stosowane następujące konwencje do wyróżniania specjalnych funkcji lub zastosowań.

Pomoce dla Czytelnika

W całej książce są używane następujące pomoce dla czytelnika w celu wskazywania przydatnych szczegółów:

Pomoc dla Czytelnika	Znaczenie
Uwaga	Podkreśla ważność określonego pojęcia lub wyróżnia specjalny przypadek, który nie musi mieć zastosowania w każdej sytuacji.
Ważne	Zwraca uwagę na podstawowe informacje, których nie należy ignorować.
Ostrzeżenie	Ostrzega, że brak wykonania lub uniknięcia określonego działania może spowodować poważne problemy dla użytkowników, systemów, spójności danych, itd.
Na dołączonym dysku	Zwraca uwagę na powiązany skrypt, narzędzie, szablon lub pomoc na dysku dołączonym do książki, który pomoże wykonać zadanie opisane w tekście.

Ramki

W tej książce są używane następujące ramki w celu zapewnienia dodatkowych wyjaśnień, wskazówek i porad dotyczących różnych funkcji systemu Windows 7:

Ramka	Znaczenie
Wskazówki ekspertów	Dostarczone przez ekspertów z firmy Microsoft w celu zapewnienia informacji „ze źródła” dotyczących działania Windows 7, najlepszych praktyk zarządzania klientami i rozwiązywania problemów.
Jak to działa	Zapewnia unikalny przegląd funkcji Windows 7 i sposobu ich działania.

Przykłady wiersza polecenia

W całej książce następujące są używane konwencje dotyczące stylów w celu dokumentowania przykładów wiersza polecenia.

Styl	Znaczenie
czcionka pogrubiona	Używana do wskazywania danych wejściowych od użytkownika (znaków, które wpisujemy dokładnie, tak jak pokazano).
<i>Czcionka pochyla</i>	Używana do wskazywania zmiennych, dla których musimy podać określoną wartość (na przykład <i>nazwa_pliku</i> może oznaczać dowolną, prawidłową nazwę pliku).
Czcionka o stałej szerokości znaków	Używana dla przykładów kodu i wyników działania wiersza polecenia.
<code>%SystemRoot%</code>	Używane dla zmiennych środowiskowych.

Korzystanie z obrazu dysku CD

Obraz dysku CD towarzyszący książce jest dostępny na stronie wydawcy przy opisie książki w zakładce Dodatkowe informacje, pod adresem:

<http://www.ksiazki.promise.pl/asp/produkt.aspx?pid=52475>

Na podstawie tego obrazu można wykonać fizyczny dysk CD lub zainstalować go jako napęd wirtualny. Dysk ten zawiera:

- **Windows 7 Resource Kit PowerShell Pack** Zbiór modułów Windows PowerShell, które możemy instalować w systemie Windows 7 w celu zapewnienia dodatkowej funkcjonalności poprzez przetwarzanie zadań administracyjnych Windows w skryptach wykorzystujących Windows PowerShell. Więcej informacji można znaleźć w części zatytułowanej „Korzystanie z Windows 7 Resource Kit PowerShell Pack” w dalszej części tego wprowadzenia.
- **Przykładowe skrypty Windows PowerShell** Dołączono prawie dwieście przykładowych skryptów Windows PowerShell, które przedstawiają, jak można administrować różnymi aspektami systemu Windows 7 przy wykorzystaniu Windows PowerShell. Więcej informacji można znaleźć w części zatytułowanej „Korzystanie z przykładowych skryptów Windows PowerShell” w dalszej części wprowadzenia.
- **Dodatkowa dokumentacja i pliki** Na dołączonym dysku zawarto dodatkową dokumentację i wspierające pliki dla kilku rozdziałów.
- **Dodatkowe materiały** Przykładowe rozdziały z innych tytułów Microsoft Press zamieszczono na dysku dołączonym do książki.
- **Windows 7 Training Portal** Łączy do produktów związanych z systemem Windows 7 przygotowanych przez Microsoft Learning.

- **Łącza autorów** Strona z linkami do witryn WWW każdego z autorów, gdzie można znaleźć więcej informacji dotyczących każdego autora i jego dokonań.
- **eBook** Elektroniczna wersja całej książki *Windows 7 Resource Kit* jest również zawarta na dołączonym dysku.

Dodatkowe informacje związane z zawartością dołączonego dysku można znaleźć w plikach *Readme.txt* w poszczególnych folderach.

DODATKOWA ZAWARTOŚĆ ONLINE W miarę pojawiania się nowych lub zaktualizowanych materiałów dodatkowych, uzupełniających tę książkę, będą one umieszczane w sieci na witrynie Microsoft Press Online Windows Server and Client. Wśród materiałów można znaleźć aktualizacje zawartości książki, artykuły, linki do dodatkowej zawartości, erratę, przykładowe rozdziały, itd. Dostępna pod adresem <http://microsoftpresssrv.libredigital.com/serverclient/> Witryna ta jest okresowo aktualizowana.

Korzystanie z Windows 7 Resource Kit PowerShell Pack

Windows 7 Resource Kit PowerShell Pack jest zbiorem modułów Windows PowerShell, które można zainstalować w systemie Windows 7, aby zapewnić dodatkową funkcjonalność związaną z przetwarzaniem zadań administracyjnych Windows w skryptach przy użyciu Windows PowerShell. *Moduły* – nowa funkcja Windows PowerShell 2.0 – pozwala ją organizować skrypty i funkcje Windows PowerShell w niezależne, samodzielne jednostki. Na przykład pojedynczy moduł może gromadzić razem wiele poleceń cmdlet, skryptów, funkcji i innych plików, które można rozpowszechniać wśród użytkowników. Więcej informacji można znaleźć w dalszej części tego wstępu pod nagłówkiem „Zastrzeżenie dotyczące zawartości płyty CD Windows PowerShell”.

PowerShell Pack zawiera dziesięć modułów, które można zainstalować, aby dodać dalsze możliwości tworzenia skryptów we własnym środowisku Windows PowerShell. Dodatkowa funkcjonalność zapewniana przez te moduły obejmuje:

- **WPK** Szybko i łatwo tworzy bogate interfejsy użytkownika z poziomu Windows PowerShell. Zawiera ponad 600 skryptów pomagających szybko budować interfejsy użytkownika. Jest podobna do aplikacji HTML (HTA), ale łatwiejsza.
- **FileSystem** Monitoruje pliki i foldery, wyszukuje zduplikowane pliki i sprawdza miejsce na dysku.
- **IsePack** Pozwala rozwinąć możliwości tworzenia skryptów w zintegrowanym środowisku skryptowym (ISE) dzięki ponad 35. skrótom.
- **DotNet** Bada przeładowane typy danych, znajduje polecenia operujące na danym typie i opisuje, jak możemy łącznie korzystać z Windows PowerShell, DotNet i COM.
- **PSImageTools** Konwertuje, obraca, skaluje i kadruje obrazy oraz pobiera metadane obrazów.

- **PSRSS** Obsługuje FeedStore z poziomu Windows PowerShell.
- **PSSystemTools** Pozyskuje informacje o systemie operacyjnym lub sprzęcie.
- **PSUserTools** Uzyskuje dane o użytkownikach w systemie, sprawdza poziomy uprawnień i uruchamia procesy jako administrator.
- **PSCodeGen** Generuje skrypty Windows PowerShell, kod C# i Pinvoke.
- **TaskScheduler** Wyszczególnia zaplanowane zadania oraz tworzy i usuwa zadania.

Informacje, jak zainstalować PowerShell Pack w systemie Windows 7, można znaleźć w pliku ReadmePP.txt w folderze \PowerShellPack na dołączonym dysku.

Warto zwrócić uwagę, że moduły i towarzysząca im dokumentacja zawarte w PowerShell Pack są udostępniane bez gwarancji i nie są objęte wsparciem technicznym firmy Microsoft. Nie należy korzystać z tych modułów w środowisku produkcyjnym bez wcześniejszego przetestowania ich w środowisku nieprodukcyjnym. Więcej informacji można znaleźć w dalszej części wstępu pod nagłówkiem „Zastrzeżenie dotyczące zawartości płyty CD Windows PowerShell”.

Korzystanie z przykładowych skryptów Windows PowerShell

Na dołączonym dysku zawarto niemal dwieście przykładowych skryptów, które przedstawiają, jak można administrować różnymi aspektami Windows 7 przy wykorzystaniu Windows PowerShell. Te skrypty przykładowe są udostępniane bez gwarancji i są całkowicie pozbawione wsparcia technicznego firmy Microsoft. Nie należy z nich korzystać w środowisku produkcyjnym bez wcześniejszego przetestowania ich w środowisku nieprodukcyjnym. Konieczne może być dostosowanie niektórych skryptów, aby poprawnie działały w środowisku produkcyjnym. Więcej informacji można znaleźć w dalszej części wstępu pod nagłówkiem „Zastrzeżenie dotyczące zawartości płyty CD Windows PowerShell”.

Zanim skorzysta się ze skryptów, trzeba zrozumieć, w jaki sposób zasady wykonywania Windows PowerShell kontrolują uruchamianie skryptów na komputerze. Windows PowerShell może określać pięć wartości zasad wykonywania skryptów na komputerze:

- **Restricted** Jest to ustawienie domyślne i nie pozwala na uruchamianie żadnych skryptów.
- **AllSigned** To ustawienie oznacza, że skrypty muszą mieć podpis cyfrowy, zanim będą mogły zostać uruchomione.
- **RemoteSigned** To ustawienie oznacza, że podpisane muszą być tylko skrypty uruchamiane z udziałów plikowych, pobrane przy pomocy przeglądarki Internet Explorer lub otrzymane jako załączniki do poczty elektronicznej.
- **Unrestricted** To ustawienie oznacza, że można uruchamiać wszystkie skrypty.
- **Bypass** To ustawienie oznacza, że nic nie jest blokowane i nie ma żadnych komunikatów ani ostrzeżeń.

Aby zobaczyć aktualną zasadę wykonywania skryptów, otwórz wiersz polecenia Windows PowerShell i wpisz **Get-ExecutionPolicy**. Aktualną zasadę wykonywania w danym systemie można zmienić, wpisując **Set-ExecutionPolicy <wartość>**, gdzie <wartość> jest jedną z pięciu wymienionych powyżej wartości. Zmiana zasad wykonywania wymaga, aby Windows PowerShell był uruchomiony z poziomu administratora. Trzeba jednak zwrócić uwagę, że jeśli zasady wykonywania skryptów są ustawione przez administratora sieciowego przy pomocy zasad grupy, nie będzie można zmienić zasad wykonywania na danym komputerze.

Microsoft zaleca, aby zasady wykonywania były skonfigurowane jako *RemoteSigned* w środowisku produkcyjnym, chyba że istnieją istotne powody dla surowego lub łagodniejszego ustawienia. Informacje dotyczące podpisywania skryptów PowerShell można znaleźć pod adresem <http://technet.microsoft.com/en-us/magazine/2008.04.powershell.aspx>. Można też wpisać **Get-Help about_signing** w wierszu polecenia Windows PowerShell, aby uzyskać dodatkowe informacje dotyczące podpisywania skryptów.

Remoting, nowa funkcja Windows PowerShell 2.0, wykorzystuje protokół WS-Management pozwalający uruchamiać polecenia Windows PowerShell na jednym lub wielu komputerach zdalnych. Oznacza to, że wiele skryptów zawartych na dołączonym dysku będzie działać na komputerach zdalnych, nawet jeśli nie mają one parametru – *computer*, który pozwala określić nazwę komputera zdalnego. Aby remoting w Windows PowerShell działał, trzeba mieć zainstalowaną i skonfigurowaną wersję Windows PowerShell 2.0 zarówno na komputerze lokalnym, jak i na docelowym komputerze zdalnym. Trzeba też włączyć remoting na docelowych komputerach zdalnych, uruchamiając na nich polecenie **Enable-PSRemoting**, które skonfiguruje te komputery do odbioru poleceń zdalnych. Polecenie **Enable-PSRemoting** musi być uruchamiane z uprawnieniami administracyjnymi. Aby uzyskać więcej informacji na temat technologii dostępu zdalnego w Windows PowerShell, należy wpisać **Get-Help about_remoting** w wierszu polecenia Windows PowerShell.

Niektóre ze skryptów przykładowych wykorzystują Windows Management Instrumentation (WMI), Active Directory Services Interface (ADSI) lub interfejsy programowania aplikacji (API) Microsoft .NET Framework do łączenia się z komputerami zdalnymi. Skrypty te mogą operować na komputerach zdalnych, nawet jeśli Windows PowerShell nie będzie zainstalowany na tych komputerach. Jednakże zanim niektóre z tych skryptów będą mogły działać zdalnie, konieczne może być włączenie administracji zdalnej poprzez Zaporę systemu Windows zarówno na komputerze bazowym, jak i na komputerze docelowym dla odpowiedniego połączenia sieciowego. Trzeba też być członkiem grupy administratorów lokalnych na komputerze zdalnym.

Można użyć skryptu *EnableDisableRemoteAdmin.ps1*, aby umożliwić administrację zdalną poprzez Zaporę systemu Windows. Trzeba zwrócić uwagę, że działania wykonywane przez ten skrypt nie są odpowiednie dla maszyn połączonych bezpośrednio z Internetem i mogą nie być odpowiednie w przypadku pewnych klientów korporacyjnych. Przed uruchomieniem skryptu **EnableDisableRemoteAdmin.ps1** w środowisku produkcyjnym należy ocenić zmiany dokonywane przez ten skrypt, aby ustalić, czy są one odpowiednie w danym środowisku. Więcej informacji na temat działania WMI poprzez Zaporę systemu Windows można znaleźć pod adresem <http://msdn.microsoft.com/en-us/library/aa389286.aspx>.

Wszystkie skrypty przykładowe zawierają pomoc dla wiersza polecenia. Aby uzyskać podstawowe informacje dotyczące danego skryptu, wpisz **Get-Help nazwa_skryptu.ps1**,

gdzie *nazwa_skryptu.ps1* jest nazwą danego skryptu. Aby zobaczyć przykładową składnię użycia skryptu, a także szczegółowe informacje, wpisz **Get-Help *nazwa_skryptu.ps1* – Full**. Jeśli chcesz zobaczyć tylko przykłady użycia danego skryptu, wpisz **Get-Help *nazwa_skryptu.ps1* – Examples**.

Zastrzeżenie dotyczące zawartości płyty CD Windows PowerShell

Skrypty Windows PowerShell zawarte na dołączonym dysku są jedynie przykładami, a nie gotowymi narzędziami. Skrypty te są prezentowane jako przykłady użycia przy administrowaniu klientami Windows 7 przy pomocy Windows PowerShell. Chociaż podjęto wszelkie starania, aby zapewnić, że te skrypty przykładowe działają poprawnie, firma Microsoft nie ponosi żadnej odpowiedzialności za jakiegokolwiek szkody, które mogą wynikać z zastosowania tych skryptów. Skrypty przykładowe są udostępniane bez żadnych gwarancji dotyczących ich funkcjonalności, a firma Microsoft nie zapewnia dla nich żadnego wsparcia technicznego.

Pakiet Windows 7 Resource Kit PowerShell Pack zawarty na dołączonym dysku również nie jest wspierany przez firmę Microsoft i udostępniany bez gwarancji związanych z jego funkcjonalnością. Najnowsze informacje i wskazówki dotyczące użycia tego pakietu PowerShell Pack można znaleźć w blogu zespołu Windows PowerShell pod adresem <http://blogs.msdn.com/powershell/>.

Należy dokładnie zapoznać się z korzystaniem z tych skryptów i modułów Windows PowerShell w środowisku testowym przed podjęciem prób użycia ich w środowisku produkcyjnym. Ponieważ skrypty przykładowe są udostępniane jedynie jako przykłady, konieczne może być dostosowanie ich, jeśli zamierza się korzystać z nich w środowisku produkcyjnym. Na przykład skrypty zawierają jedynie minimalną obsługę błędów i zakładają, że docelowi klienci istnieją i są poprawnie skonfigurowani. W związku z tym autorzy zachęcają Czytelników do dostosowywania skryptów do własnych, konkretnych potrzeb.

Zasady wsparcia dla pakietu Resource Kit

Podjęto wszelkie starania w celu zapewnienia poprawności tej książki i zawartości dołączonego dysku CD. Microsoft Press zapewnia poprawki do tej książki przez Internet pod następującym adresem:

<http://www.microsoft.com/mspress/support/search.aspx>

Wszelkie komentarze, pytania lub pomysły dotyczące książki lub zawartości dołączonego dysku albo pytania, na które nie można znaleźć odpowiedzi, przeszukując bazę wiedzy, można przysyłać do Microsoft Press, korzystając z jednej z następujących metod:

E-mail:

rkinput@microsoft.com

Zwykła poczta:

Microsoft Press

Attn: Windows 7 Resource Kit Editor

One Microsoft Way

Redmond, WA 98052-6399

Należy zwrócić uwagę, że wsparcie techniczne dla produktów nie jest oferowane poprzez powyższe adresy pocztowe. W celu uzyskania informacji dotyczących wsparcia dla produktów firmy Microsoft należy odwiedzić witrynę Microsoft Product Support pod adresem:

<http://support.microsoft.com>

CZĘŚĆ I

Wprowadzenie

Przegląd uprawnień w systemie Windows 7

- Uprawnienia w Windows 7 według rozdziałów 3
- Wydania Windows 7 28
- Wybieranie oprogramowania i sprzętu 33
- Podsumowanie 35
- Dodatkowe zasoby 35

Windows 7 jest złożonym systemem operacyjnym z tysiącami funkcji. Całkowite zrozumienie go może wymagać wielu lat. Na szczęście większość profesjonalistów IT ma doświadczenie z wcześniejszymi wersjami systemu Windows, na których opiera się system operacyjny Windows 7, takimi jak Windows XP i Windows Vista. Ten rozdział zakłada podstawową znajomość funkcji Windows Vista i opisuje najbardziej znaczące uprawnienia, które nie są związane z zabezpieczeniami i nie będą omawiane w innych miejscach tej książki, różne wydania systemu Windows 7 oraz wymagania sprzętowe dla Windows 7.

UWAGA Zadaniem tego rozdziału jest przedstawienie profesjonalistom IT szerokiej perspektywy zmian w systemie Windows 7. Nadaje się on jednak również dla nie mających wykształcenia technicznego osób, które muszą zrozumieć nowe technologie.

Przegląd uprawnień systemu Windows 7 związanych z zabezpieczeniami można znaleźć w rozdziale 2, „Bezpieczeństwo w systemie Windows 7”.

Uprawnienia w Windows 7 według rozdziałów

Windows 7 zawiera setki uprawnień w stosunku do wcześniejszych klienckich systemów operacyjnych Windows. Ten rozdział przedstawia bardzo ogólny przegląd tych funkcji, skupiając się na tych, które nie są dogłębnie omawiane w innych miejscach książki. Tabela 1-1 wymienia kilka kluczowych uprawnień w systemie Windows 7, które będą interesujące dla

profesjonalistów IT i wskazuje rozdziały, które zapewniają szczegółowe informacje na temat każdego z tych usprawnień.

Tabela 1-1 Usprawnienia w systemie Windows 7

Usprawnienie	Rozdział
Usprawnienia zabezpieczeń	2
Usprawnienia wdrażania	3 do 12
Zgodność aplikacji	4
Windows PowerShell 2.0	13
Preferencje zasad grupy	14
Startowe obiekty zasad grupy (GPO)	14
Polecenia cmdlet w PowerShell dotyczące zasad grupy	14
Biblioteki	15
Usprawnienia plików offline	15
Usprawnienia Windows BitLocker	16
Usprawnienia Windows ReadyBoost	16
Device Stage i inne usprawnienia obsługi urządzeń	17
Wzbudzane uruchamianie usług	17
Korzystanie z Powercfg do oceny wydajności zasilania	17
Usprawnienia stosowania drukarek	18
Drukowanie zależne od lokalizacji	18
Izolowanie sterowników drukarek	18
Usprawnienia wyszukiwania	19
Tryb chroniony programu Internet Explorer	20
Monitor wydajności	21
Narzędzie do oceny wydajności systemu Windows (WinSAT)	21
Diagnostyka	21, 30, 31
Łatwe połączenie do Pomocy zdalnej	22
Windows AppLocker	24
Kontrola konta użytkownika (UAC)	24
Usprawnienia sieci	25
Jakość usług (QoS) oparta na adresach URL	25
Zabezpieczenia systemu DNS (DNSsec)	25
Profile wielu aktywnych zapór	26
Usprawnienia protokołu IPsec	26
BranchCache	27
Ponowne łączenie z siecią VPN	27
DirectAccess	27
Remote Desktop Protocol 7.0	27

Tabela 1-1 Usprawnienia w systemie Windows 7

Usprawnienie	Rozdział
Zmiany w IPv6	28
Rozwiązywanie problemów w systemie Windows	30
Monitor zasobów	30, 31
Zdalne rozwiązywanie problemów przy pomocy Windows PowerShell	30
Zaawansowane i niestandardowe rozwiązywanie problemów	30, 31
Monitor niezawodności	30
Rejestrator problemów	31, 31

UWAGA Systemy Windows Vista i Windows 7 zawierają znaczące usprawnienia zabezpieczeń w stosunku do poprzednich wersji Windows. Zmiany te są tak liczne, że poświęciliśmy osobny rozdział (2) na ich opisanie.

Książka nie omówia funkcji, które są używane głównie w środowiskach domowych, takich jak ochrona rodzicielska, gry, Windows Media Player, Windows Media Center, itd.

Interakcje z użytkownikiem

Dla użytkowników najważniejszymi usprawnieniami w Windows 7 będą widoczne zmiany interfejsu użytkownika. Ta część rozdziału omawia, jak zmienił się interfejs użytkownika systemu Windows 7. Podczas czytania warto rozważyć, które zmiany będą wymagały szkoleń dla użytkowników końcowych lub dokonania zmian w ustawieniach zarządzania komputerami biurowymi przed wdrożeniem.

Pasek zadań

Jak pokazano na rysunku 1-1, pasek zadań systemu Windows 7 znacząco się zmienił. Po pierwsze, jest wyższy, choć to domyślne ustawienie można na życzenie skonfigurować inaczej. Po drugie, Windows 7 wyświetla duże ikony dla działających aplikacji, zamiast małych ikon aplikacji wraz z tytułami okien używanych w poprzednich wersjach Windows. To ustawienie również można skonfigurować; użytkownicy mogą wybrać wyświetlanie tytułów okien razem z ikonami.



Rysunek 1-1 Nowy pasek zadań wyświetla ikony zamiast tytułów aplikacji i obsługuje przyczepianie aplikacji.

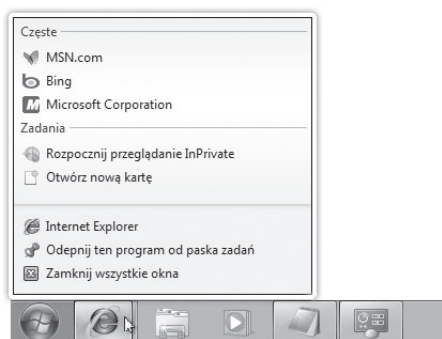
Pasek narzędzi Szybkie uruchamianie został usunięty. Użytkownicy mogą za to teraz przypinać aplikacje bezpośrednio do paska zadań. Gdy aplikacja jest przypięta do paska zadań, jej ikona zawsze pojawia się na pasku zadań, tak jakby aplikacja ta była uruchomiona. Użytkownicy mogą uruchomić tę aplikację, klikając jej ikonę.

Nowa funkcja – zwana Aero Peek – w systemie Windows 7 pozwala użytkownikom umieścić kursor nad prawym brzegiem paska zadań Windows, aby uczynić wszystkie otwarte okna przezroczystymi; tak żeby można było zobaczyć pulpit. Ta funkcja sprawia, że gadżety, które mogą być teraz umieszczane w dowolnym miejscu na pulpicie, są bardziej użyteczne. Użytkownicy mogą też podejrzeć otwarte okno lub działającą aplikację, zatrzymując kursor myszy nad elementem paska zadań w celu wyświetlenia miniaturki tego elementu, a następnie wskazując myszą tę miniaturkę.

Listy szybkiego dostępu

Użytkownicy mogą teraz otworzyć listę szybkiego dostępu, klikając prawym przyciskiem myszy ikonę aplikacji na pasku zadań lub wybierając ikonę aplikacji w menu Start. Jak pokazano na rysunku 1-2, listy szybkiego dostępu zapewniają dostęp do często używanych funkcji w aplikacji. Gdy w poprzednich wersjach systemu Windows klikaliśmy aplikację prawym przyciskiem myszy, zwykle widzieliśmy tylko standardowe elementy menu, w tym Maksymalizuj, Przywróć, Minimalizuj i Przenieś. W systemie Windows 7 aplikacje mogą dodawać zadania specyficzne dla aplikacji do menu kontekstowego okna.

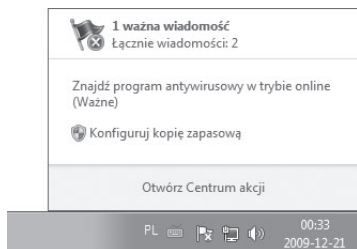
Na przykład lista szybkiego dostępu programu Windows Media Player pozwala użytkownikom odtworzyć muzykę lub wznowić ostatnią listę odtwarzania bez otwierania wcześniej programu Windows Media Player. Każda aplikacja zaprojektowana dla systemu Windows 7 może korzystać z list szybkiego dostępu, więc ta funkcja z czasem będzie coraz bardziej użyteczna.



Rysunek 1-2 Listy szybkiego dostępu zapewniają dostęp do często używanych aplikacji i plików.

Obszar powiadomień

W wersjach systemu Windows wcześniejszych niż Windows 7 obszar powiadomień (część paska zadań najbliżej zegara) mógł się zapychać niechcianymi ikonami dodawanymi przez różne aplikacje. W Windows 7 pojawiają się tutaj tylko ikony Sieć, Centrum akcji (które zastępuje Centrum zabezpieczeń dostępne w systemie Windows Vista) oraz ikona baterii (na komputerach mobilnych), chyba że użytkownicy wprost pozwolą na pojawianie się innych ikon. Rysunek 1-3 pokazuje obszar powiadomień z zaznaczoną ikoną Centrum akcji.



Rysunek 1-3 Obszar powiadomień jest uproszczony.

Gesty myszy

Aby poprawić produktywność użytkowników, Windows 7 dołącza dwa nowe gesty myszy:

- **Aero Snap** Użytkownicy mogą przeciągać okna do góry ekranu, aby je maksymalizować albo do lewego lub prawego brzegu ekranu, aby ustawić rozmiar okna, tak żeby zajmowało połowę ekranu. Pasek tytułu nadal zawiera przyciski Minimalizuj, Maksymalizuj i Zamknij. Zmiana rozmiaru okna poprzez przeciągnięcie jego narożnika do górnego lub dolnego brzegu ekranu automatycznie zwiększa rozmiar pionowy okna na pełną wysokość ekranu.
- **Aero Shake** Aby zmniejszyć chaos i bałagan powodowany przez aplikacje działające w tle, użytkownicy mogą zminimalizować wszystkie pozostałe okna, potrząsając oknem przy pomocy myszy. Ponowne potrząśnięcie oknem przywraca okna w tle do ich poprzednich pozycji.

Pomimo nazw oba te gesty działają niezależnie od tego, czy interfejs Aero jest włączony.

Poprawiony Alt + Tab

Przełączanie się między aplikacjami jest typowym, ale często zagmatwanym zadaniem wykonywanym przez użytkowników. W poprzednich wersjach Windows kombinacja Alt + Tab pozwalała użytkownikowi przełączać się pomiędzy aplikacjami. Jeśli użytkownik przytrzymał wciśnięty klawisz Alt i naciskał klawisz Tab, system Windows będzie przechodził pomiędzy kolejnymi aplikacjami, pozwalając użytkownikowi wybrać żadaną aplikację.

Windows 7 nadal obsługuje Alt + Tab. Ponadto gdy włączony jest interfejs Aero, Alt + Tab wyświetli miniaturową wersję każdej aplikacji, jak pokazano na rysunku 1-4. Jeśli użytkownik zatrzyma się podczas przeczucania aplikacji, pełne okno zostanie na krótko wyświetlone.



Rysunek 1-4 Gdy włączone jest Aero, Alt + Tab wyświetla miniaturę każdego okna.

Skróty klawiaturowe

Aby ograniczyć czas wymagany do wykonania typowych zadań, Windows 7 obsługuje skróty klawiaturowe wymienione w tabeli 1-2.

Tabela 1-2 Nowe skróty klawiaturowe Windows 7

Skrót klawiaturowy	DZIAŁANIE
 + strzałka w górę	Maksymalizuje bieżące okno.
 + strzałka w dół	Przywraca rozmiar lub minimalizuje bieżące okno.
 + strzałka w lewo	Przypina bieżące okno do lewej połowy ekranu.
 + strzałka w prawo	Przypina bieżące okno do prawej połowy ekranu.
 + Shift + strzałka w lewo	Przenosi bieżące okna do lewego ekranu podczas korzystania z dwóch monitorów.
 + Shift + strzałka w prawo	Przenosi bieżące okna do prawego ekranu podczas korzystania z dwóch monitorów.
 + Home	Minimalizuje lub przywraca rozmiar wszystkich okien oprócz bieżącego.
 + T	Uaktywnia pasek zadań, aby można było skorzystać z klawiszy ze strzałkami i klawisza Enter do wybierania elementu paska zadań. Kolejne naciśnięcia tego skrótu przechodzą cyklicznie przez kolejne elementy paska zadań.  + Shift + T przechodzi cyklicznie przez kolejne elementy w odwrotnym kierunku.
 + Tab	Przechodzi cyklicznie przez otwarte aplikacje w trybie trójwymiarowym.
Alt + Tab	Przechodzi cyklicznie przez otwarte aplikacje w trybie dwuwymiarowym.
 + spacja (przytrzymać klawisze wciśnięte)	Wyświetla podgląd pulpitu.
 + D	Pokazuje pulpit.
 + M	Minimalizuje bieżące okna.
 + G	Wyświetla gadżety ponad aplikacjami.
 + P	Pokazuje opcje prezentacji i monitorów zewnętrznych.
 + U	Otwiera Centrum ułatwień dostępu.
 + X	Otwiera Centrum mobilności, umożliwiając szybki dostęp do funkcji, takich jak WiFi.
 + [klawisz numeryczny 1–5]	Uruchamia program z paska zadań, który odpowiada danemu klawiszowi numerycznemu. Na przykład naciśnięcie  + 1 uruchamia pierwszą aplikację na pasku zadań.

Tabela 1-2 Nowe skróty klawiaturowe Windows 7

Skrót klawiaturowy	DZIAŁANIE
 + + (klawisz plus)	Powiększa fragment ekranu w programie Lupa.
 + - (klawisz minus)	Pomniejsza fragment ekranu w programie Lupa.
 + L	Blokuje komputer, wyświetlając ekran logowania.

Usprawnienia dla komputerów Tablet PC

Komputery Tablet PC są komputerami przenośnymi, które umożliwiają wprowadzanie danych przy użyciu specjalnego rysika. Korzystając z tego rysika, użytkownicy mogą pisać (lub rysować) bezpośrednio na ekranie komputera Tablet PC. Przed Windows Vista firma Microsoft zapewniała funkcje Tablet PC tylko w systemie Windows XP Tablet PC Edition. W systemie Windows 7 funkcje Tablet PC są zawarte w wersjach Windows 7 Home Premium, Windows 7 Professional, Windows 7 Enterprise i Windows 7 Ultimate.

Windows 7 zawiera kilka usprawnień interfejsu wpisywania danych używanego przez komputery Tablet PC. Rozpoznawanie pisma ręcznego zostało poprawione. Nowy Panel zapisu matematycznego pozwala użytkownikom wpisywać wyrażenia matematyczne, które mogą być następnie wykorzystywane przez aplikacje. Przewidywanie tekstu poprawia wprowadzanie tekstu w przypadku korzystania z klawiatury programowej i z biegiem czasu uczy się nowego słownictwa. Windows 7 obsługuje rozpoznawanie pisma odręcznego przy korzystaniu z większej liczby języków, w tym szwedzkiego, duńskiego, norweskiego, fińskiego, portugalskiego (Portugalia), polskiego, rosyjskiego, rumuńskiego, katalońskiego, serbskiego (zapis łaciński), serbskiego (zapis cyrylicą) i czeskiego. Tak jak w przypadku Windows Vista system Windows 7 nadal obsługuje języki angielski (U.S.), angielski (U.K.), niemiecki, francuski, hiszpański, włoski, holenderski, portugalski (Brazylia), chiński uproszczony, chiński tradycyjny, japoński i koreański.

Aby skonfigurować lub wyłączyć funkcje Tablet PC, należy skorzystać z ustawień zasad grupy znajdujących się zarówno w części Konfiguracja komputera, jak i Konfiguracja użytkownika w folderze Szablony administracyjne\Składniki systemu Windows\Komputer typu Tablet.

Interfejs dotykowy

Windows 7 zawiera poprawiony interfejs dotykowy dla komputerów z ekranami dotykowymi. Podczas gdy komputery Tablet PC wykorzystują rysik do wprowadzania danych, interfejs dotykowy wykorzystuje dotyk palca. Początkowe możliwości obejmują:

- Zaznaczanie tekstu poprzez przeciąganie nad nim palcem.
- Przewijanie w górę i w dół poprzez przeciąganie ekranu albo przewijanie w dowolnym kierunku poprzez przeciąganie ekranu dwoma palcami.
- Kliknięcie prawym przyciskiem myszy poprzez przytrzymanie jednego palca przez chwilę na ikonie albo poprzez przytrzymanie palca i puknięcie drugim palcem.
- Powiększanie i pomniejszanie przy użyciu dwóch palców i oddalanie ich lub zbliżanie.
- Obracanie obrazów poprzez ruch dwoma palcami po okręgu.

- Przerzucanie stron poprzez szybkie przesuwanie palcem po ekranie.
- Przeciąganie w górę na pasku zadań w celu uzyskania listy szybkiego dostępu.

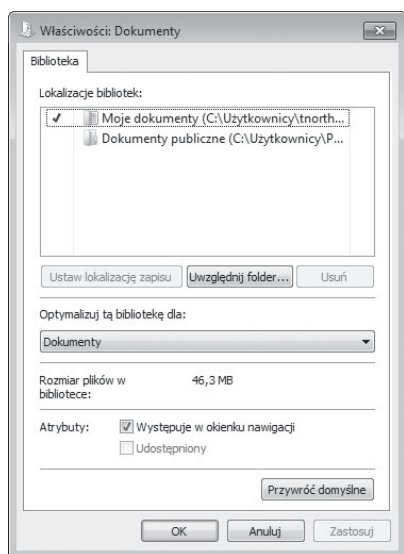
Przy odpowiednim sprzęcie te nowe funkcje sprawią, że system Windows 7 będzie bardziej intuicyjny w użyciu. Mają one potencjał poprawy produktywności użytkownika na komputerach mobilnych poprzez ograniczenie konieczności użycia klawiatury.

Biblioteki

Biblioteki działają jak foldery, ale wyświetlają pliki określonego typu z wielu komputerów. Na przykład można utworzyć bibliotekę do przechowywania wszystkich szkoleniowych filmów wideo dla pracowników z wielu serwerów w danej organizacji. Użytkownicy mogą następnie otwierać tę bibliotekę i mieć dostęp do filmów wideo bez interesowania się, na którym serwerze znajdują się poszczególne pliki. Biblioteki mogą być dostępne z menu Start, Eksploratora Windows oraz okien dialogowych Otwórz i Zapisz.

Biblioteki w systemie Windows 7 są podobne do folderów wyszukiwania w systemie Windows Vista. Jednakże użytkownicy mogą zapisywać pliki w bibliotece, natomiast foldery wyszukiwania są tylko do odczytu. Pliki zapisywane w bibliotece są zachowywane w folderze fizycznym, którego lokalizację można konfigurować. Windows 7 automatycznie indeksuje biblioteki, aby umożliwiać szybsze przeglądanie i wyszukiwanie.

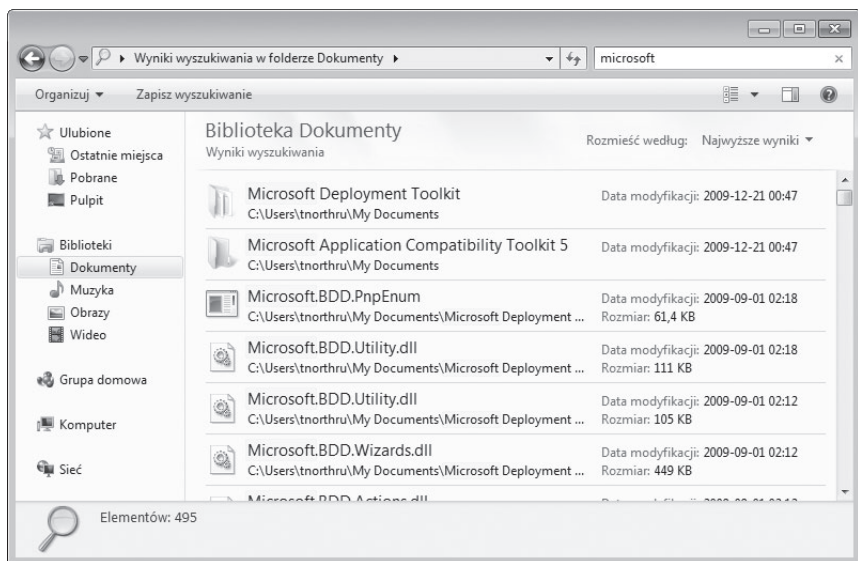
Na przykład domyślny widok Eksploratora Windows pokazuje bibliotekę Dokumenty zamiast foldera Dokumenty danego użytkownika. Jak widać w oknie dialogowym Właściwości: Dokumenty na rysunku 1-5, biblioteka Dokumenty zawiera zarówno folder Moje dokumenty dla danego użytkownika, jak i folder Dokumenty publiczne. Folder Moje dokumenty jest skonfigurowany jako lokalizacja zapisu, więc wszelkie nowe pliki będą umieszczane w tym folderze. Klikając przycisk Uwzględnij folder, użytkownicy mogą dodawać więcej folderów do biblioteki Dokumenty.



Rysunek 1-5 Właściwości biblioteki Dokumenty

Usprawnienia wyszukiwania

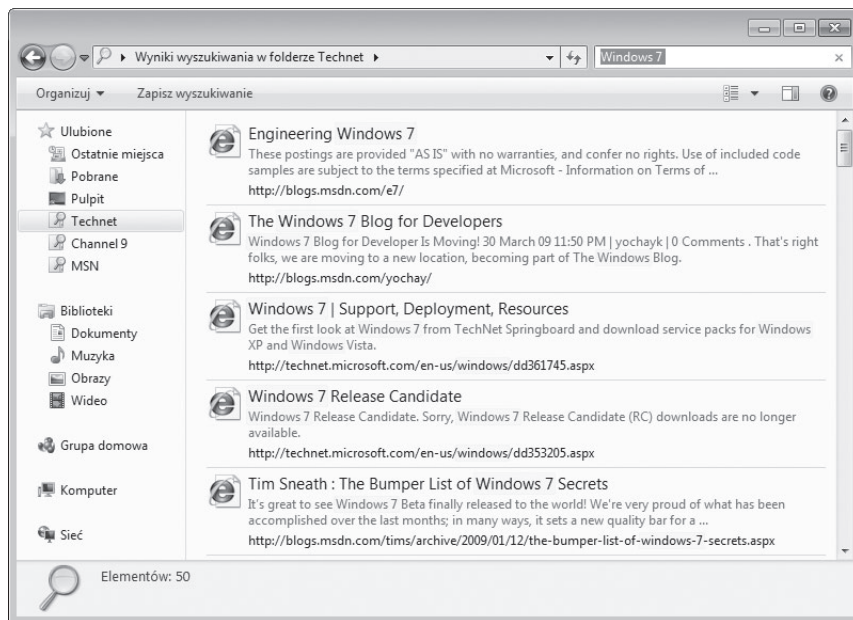
System Windows 7 zawiera usprawnione możliwości wyszukiwania, które wykorzystują inteligentniejszy algorytm do sortowania wyników wyszukiwania. Wyniki wyszukiwania pokazują fragmenty dokumentu i wyróżniają wyszukiwane słowa, jak widać na rysunku 1-6. Te wyróżnienia pomagają użytkownikom szybciej odnajdować dokumenty, wiadomości i obrazy, których potrzebują. Windows 7 ułatwia też dodawanie filtrów pozwalających użytkownikom łatwiej wyszukiwać określone foldery.



Rysunek 1-6 Funkcja wyszukiwania wyróżnia teraz słowa kluczowe w wynikach.

Federacja wyszukiwania

Federacja wyszukiwania umożliwia użytkownikom łatwe przeszukiwanie komputerów w swojej sieci oraz w Internecie, w tym witryn Microsoft SharePoint. Federacja wyszukiwania obsługuje otwartych dostawców federacji wyszukiwania, którzy wykorzystują standard OpenSearch. Umożliwia to użytkownikom (albo profesjonalistom IT poprzez zasady grupy) dodawanie połączeń wyszukiwania, które łączą się z witrynami WWW w intranecie lub Internecie. W momencie pisania tej książki wyszukiwanie w Internecie frazy „Windows 7 Search Federation providers” zwracało strony pozwalające użytkownikom instalować połączenia wyszukiwania dla wielu popularnych witryn WWW. Rysunek 1-7 pokazuje zainstalowane trzy łączniki wyszukiwania dla MSDN Channel 9, MSDN i Microsoft TechNet oraz wyświetla wyniki wyszukiwania w witrynie WWW TechNet.



Rysunek 1-7 Łączniki wyszukiwania umożliwiają użytkownikom przeszukiwanie witryn WWW z poziomu Eksploratora Windows.

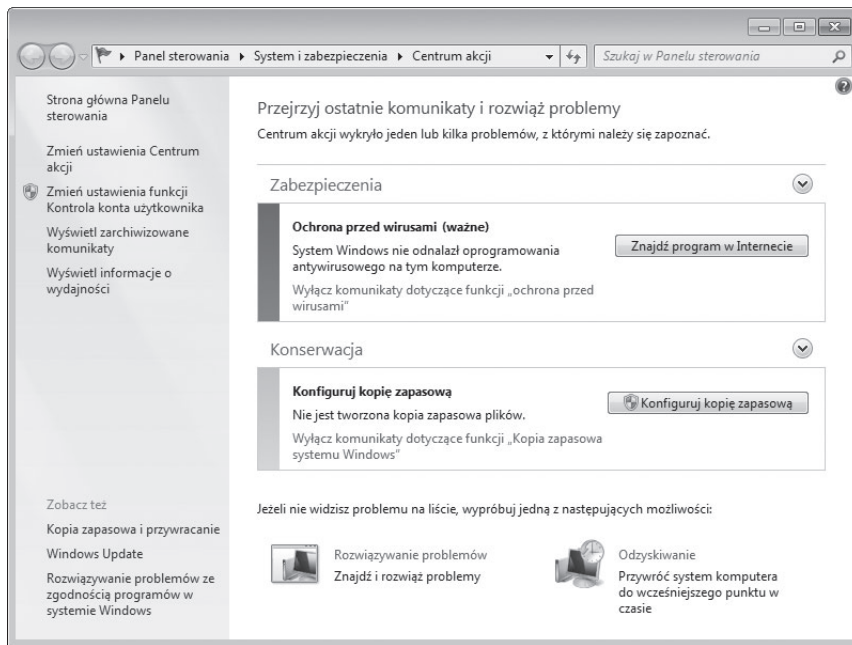
Centrum akcji

Windows Vista zawiera Centrum zabezpieczeń, zapewniające użytkownikom informacje dotyczące działań, które mogą oni podejmować, aby ochronić komputer. Na przykład Windows Vista wykorzystuje Centrum zabezpieczeń do ostrzegania użytkownika, że wyłączono program Windows Defender lub Zaporę systemu Windows.

Windows 7 zastępuje Centrum zabezpieczeń przez Centrum akcji, jak pokazano na rysunku 1-8. Centrum akcji powiadamia użytkownika o tych samych problemach z zabezpieczeniami co Centrum zabezpieczeń. Ponadto powiadamia użytkowników o problemach, które nie są związane z zabezpieczeniami, na przykład o problemie z wykonaniem zaplanowanej kopii zapasowej.

Centrum akcji konsoliduje alarmy z następujących funkcji systemu Windows:

- Centrum zabezpieczeń
- Raportowanie i rozwiązywanie problemów
- Windows Defender
- Windows Update
- Diagnostyka
- Ochrona dostępu do sieci (NAP)
- Tworzenie i przywracanie kopii zapasowej
- Przywracanie systemu
- Kontrola konta użytkownika (UAC)

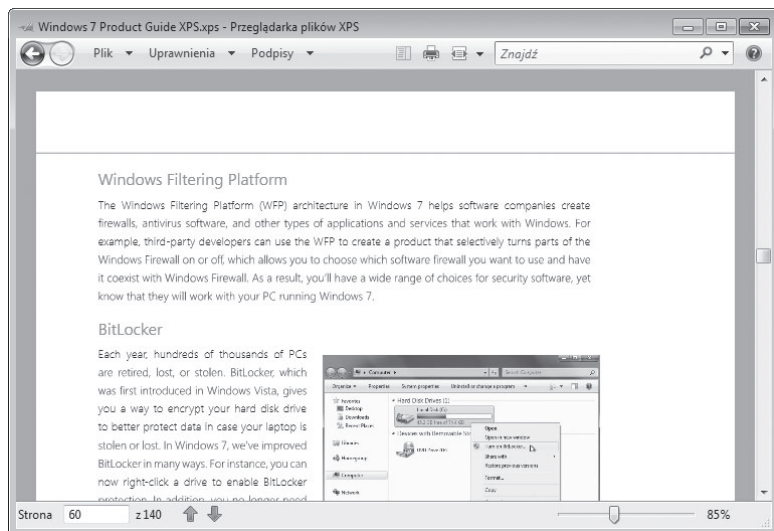


Rysunek 1-8 Centrum akcji konsoliduje komunikaty systemowe.

XML Paper Specification

Systemy Windows Vista i Windows 7 zawierają wbudowaną obsługę nowej specyfikacji XML Paper Specification (XPS). XPS jest formatem dokumentów, które można tworzyć z dowolnego dokumentu do wydrukowania, a następnie łatwo udostępniać na niemal dowolnej platformie. XPS zapewnia podobne możliwości co format Adobe PDF, ale ma tę przewagę, że jest wbudowany w system operacyjny.

Windows 7 zawiera poprawioną wersję Przeglądarki plików XPS, jak pokazano na rysunku 1-9, pozwalając otwierać i odczytywać dokumenty oparte na XPS bez narzędzia, które zostało użyte do utworzenia dokumentu. Użytkownicy mogą też korzystać z poprawionej Przeglądarki plików XPS do cyfrowego podpisywania dokumentów XPS. Jeśli organizacja wdroży usługi Windows Rights Management Services (RMS), użytkownicy mogą też ograniczać dostęp do otwierania i edytowania dokumentów XPS, korzystając z poprawionej Przeglądarki plików XPS.



Rysunek 1-9 Przeglądarka plików XPS

Windows Internet Explorer 8

System Windows 7 zawiera program Windows Internet Explorer 8, wysoko-wydajną przeglądarkę WWW zaprojektowaną z myślą o ochronie użytkowników przed internetowymi zagrożeniami. Chociaż przeglądarkę Internet Explorer 8 można instalować w systemach Windows XP i Windows Server 2003, zawiera ona ważne usprawnienie zabezpieczeń zwane trybem chronionym, które działa tylko w systemach Windows Vista, Windows 7 i Windows Server 2008. Tryb chroniony uruchamia Internet Explorer z minimalnymi uprawnieniami, co pomaga zapobiegać dokonywaniu trwałych zmian w konfiguracji komputera przez złośliwe witryny WWW.

Wydajność

Chociaż niektóre funkcje systemu Windows 7, takie jak Aero, wymagają wysoko wydajnego sprzętu, system Windows 7 zaprojektowano tak, by miał podobną wydajność do wcześniejszych wersji Windows podczas działania na tym samym sprzęcie, a często może działać wydajniej niż wcześniejsze wersje Windows. Kolejne części rozdziału opisują technologie zaprojektowane do poprawy wydajności Windows 7.

ReadyBoost

Technologia Windows ReadyBoost, pierwotnie wprowadzona w systemie Windows Vista, wykorzystuje napęd USB lub kartę pamięci SD do tymczasowego przechowywania danych, które w przeciwnym razie musiałyby być odczytywane ze znacznie wolniejszego twardego dysku. Windows Vista wykorzystuje technologię SuperFetch, żeby określać, które dane będą automatycznie przechowywane w pamięci podręcznej.

Po włożeniu napędu USB lub karty SD o rozmiarze większym niż 256 megabajtów (MB) system Windows Vista sprawdzi wydajność, żeby określić, czy to urządzenie jest wystarczająco

szybkie, aby współpracować z technologią ReadyBoost (urządzenia zaprojektowane dla technologii ReadyBoost mają na opakowaniu oznaczenie „Enhanced for Windows ReadyBoost”, ale inne urządzenia również mogą się do tego nadawać). Jeśli urządzenie jest wystarczająco szybkie, Windows Vista daje użytkownikowi możliwość włączenia technologii ReadyBoost. Ewentualnie użytkownicy mogą ręcznie włączać technologię ReadyBoost na kompatybilnych urządzeniach, zaglądając do właściwości danego napędu.

Windows 7 usprawnia technologię ReadyBoost, dodając obsługę jednoczesnego wykorzystania nawet do ośmiu urządzeń. Na przykład można włączyć ReadyBoost zarówno na kluczu USB, jak i na karcie SD, a system Windows 7 będzie korzystał z pamięci podręcznej na obu tych urządzeniach. Chociaż Windows Vista może tworzyć pamięć podręczną o wielkości maksymalnie 4 gigabajtów (GB), Windows 7 może tworzyć większe pamięci podręczne.

Jeśli urządzenie pamięci podręcznej zostanie usunięte, technologia ReadyBoost zostanie wyłączona, ale nie wpłynie to na stabilność komputera, ponieważ pliki przechowywane w tej pamięci są tylko kopiami tymczasowymi. Dane w pamięci podręcznej są szyfrowane, aby chronić prywatność.

BranchCache

BranchCache przechowuje lokalne kopie plików z korporacyjnego intranetu i przekazuje je na inne komputery w lokalnym oddziale, aby nie trzeba było ich przekazywać poprzez sieć rozległą (WAN). W ten sposób BranchCache może ograniczyć użycie sieci WAN i zwiększyć czas reakcji aplikacji sieciowych. BranchCache może zachowywać w pamięci podręcznej pliki z folderów udostępnianych i serwerów WWW, ale tylko wtedy, gdy serwer działa pod kontrolą systemu Windows Server 2008 R2.

BranchCache może działać w dwóch różnych trybach: Hosted Cache (który wymaga komputera działającego pod kontrolą systemu Windows Server 2008 R2 w każdym oddziale) oraz Distributed Cache (w którym klienci wewnątrz danego oddziału korzystają z sieci peer-to-peer do wymiany plików). Tryb Hosted Cache zapewnia lepszą wydajność, ale oddziały, które nie mają komputera działającego pod kontrolą systemu Windows Server 2008 R2, mogą korzystać z trybu Distributed Cache.

Dyski SSD

Windows 7 zawiera kilka usprawnień wydajności dysków SSD, takich jak napędy flash:

- Defragmentacja dysków jest wyłączona, ponieważ nie jest konieczna w napędach SSD.
- Windows 7 wykorzystuje polecenie SSD *TRIM*, aby wymazywać dane, które nie są już używane, co ogranicza czas wymagany do powtórного użycia tej samej lokalizacji.
- Windows 7 inaczej formatuje dyski SSD.

Połączenia programów RemoteApp i pulpitu

Po połączeniu z serwerem terminali działającym pod kontrolą systemu Windows Server 2008 R2 użytkownicy Windows 7 mają znacznie bardziej zintegrowane środowisko. Nie tylko interfejs użytkownika jest pełniejszy, ale aplikacje zdalne można uruchamiać bezpośrednio z menu Start. Gdy aplikacje zdalne są uruchomione, praktycznie są nie do rozróżnienia

od aplikacji lokalnych, co sprawia, że scentralizowane zarządzanie aplikacjami i architektury cienkich klientów są łatwiejsze we wdrażaniu i wykorzystaniu.

Pulpit zdalny w Windows 7 obsługuje wykorzystanie interfejsu użytkownika Aero i wielu monitorów, co zapewnia poczucie zbliżone do pracy na komputerze lokalnym. Również multimedia działają lepiej w pulpicie zdalnym, ponieważ Windows Media Player może teraz lepiej odtwarzać wideo poprzez połączenia pulpitu zdalnego, a pulpit zdalny zawiera obsługę mikrofonów. Użytkownicy mogą drukować na drukarce lokalnej bez konieczności instalowania sterowników drukarki na serwerze.

Nowa opcja PowerCfg –energy

Narzędzie Powercfg zostało usprawnione w systemie Windows 7 przez nową opcję wiersza polecenia (–energy) do włączania wykrycia typowych problemów z wydajnością zasilania. Do problemów tych może należeć nadmierne wykorzystanie procesora, zwiększona rozdzielczość zegara, nieefektywne ustawienia zasad oszczędności energii, nieefektywne stosowanie trybu uśpienia przez urządzenia USB oraz zmniejszenie pojemności baterii. Ta nowa opcja Powercfg może pomóc profesjonalistom IT w sprawdzaniu systemów przed wdrożeniem, zapewnianiu obsługi użytkownikom, którzy napotykają problemy z czasem działania baterii lub zużyciem energii, itd. Ponadto użytkownicy zaawansowani mogą korzystać z tej opcji do diagnozowania problemów z wydajnością energetyczną na własnych komputerach.

Odzwierciedlanie procesów

Gdy aplikacje przestawały działać w systemie Windows Vista (i wcześniejszych wersjach Windows), użytkownicy czekali, podczas gdy narzędzie diagnostyczne zbierało informacje na temat awarii. To opóźnienie sprawiało, że awaria była jeszcze bardziej frustrująca dla użytkowników, obniżając dodatkowo ich wydajność. W systemie Windows 7 odzwierciedlanie procesów umożliwia systemowi podniesienie procesu, który uległ awarii i dalszą pracę, podczas gdy narzędzia diagnostyczne zbierają informacje o stanie aplikacji.

Mobilność

Coraz większą liczbę nowych komputerów stanowią laptopy lub komputery typu tablet, które są używane inaczej niż komputery biurkowe. Komputery mobilne muszą efektywnie zarządzać energią, a użytkownik powinien być w stanie łatwo monitorować zużycie energii i poziomy naładowania baterii. Komputery mobilne są również często używane na spotkaniach, co wymaga, aby były w stanie łatwo łączyć się z sieciami bezprzewodowymi i wyszukiwać zasoby sieciowe. Poniższe części tego rozdziału zapewniają ogólny przegląd usprawnień mobilności systemu Windows 7.

Poprawiony czas działania baterii

W systemie Windows Vista i wcześniejszych wersjach Windows można było konfigurować usługi, tak aby uruchamiały się automatycznie, a wtedy były one uruchamiane w tym samym czasie co system operacyjny lub z opóźnionym startem. W Windows 7 opcje te są nadal dostępne. Ponadto usługi mogą być uruchamiane lub zatrzymywane poprzez wyzwalacze.

We wcześniejszych wersjach systemu Windows po uruchomieniu usług musiały one rezerwować czas procesora w oparciu o zegar systemowy. Innymi słowy, usługa musi być aktywowana po upływie określonej liczby milisekund, nawet jeśli ta usługa nie ma nic do zrobienia. W Windows 7 usługi mogą być aktywowane przez rozmaite zdarzenia wyzwalające, w tym przez przychodzące komunikaty sieciowe lub zdarzenia inicjowane przez użytkownika. Pozwala to procesorowi komputera częściej przechodzić do stanu bezczynności, co zwiększa czas życia baterii.

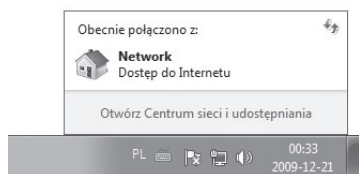
System Windows 7 jest efektywniejszy przy odtwarzaniu standardowych płyt wideo DVD poprzez wykorzystanie mniejszej mocy procesora i efektywniejsze obracanie dysku w napędzie. Podczas podróży użytkownicy mobilni będą mogli z większym prawdopodobieństwem obejrzeć cały film na płycie DVD na jednym ładowaniu baterii.

Adaptacyjna jasność monitora

Windows 7 automatycznie przyciemnia monitor po pewnym okresie bezczynności. Pozwala to systemowi Windows 7 ograniczać zużycie baterii bez pełnego przechodzenia do trybu uśpienia. Funkcja jasności adaptacyjnej inteligentnie reaguje też na działania użytkownika. Na przykład, jeśli funkcja jasności adaptacyjnej ściemnia monitor po 30 sekundach bezczynności, a użytkownik natychmiast poruszy myszą, aby rozjaśnić ekran, funkcja jasności adaptacyjnej odczeka teraz 60 sekund, zanim ponownie ściemni ekran.

Przeglądanie dostępnych sieci

Użytkownicy mobilni często muszą się łączyć z sieciami WiFi, sieciami szerokopasmowymi, wirtualnymi sieciami prywatnymi (VPN) i sieciami wdzwanianymi (dial-up). W systemie Windows 7 użytkownicy mogą łączyć się z sieciami bezprzewodowymi przy pomocy dwóch kliknięć – jedno kliknięcie ikony sieci w obszarze powiadomień i drugie kliknięcie danej sieci. Rysunek 1-10 pokazuje listę dostępnych sieci.



Rysunek 1-10 Lista dostępnych sieci

Inteligentne zasilanie sieci

Połączenia sieci przewodowych zużywają energię, gdy są włączone, nawet jeśli kabel sieciowy nie jest podłączony. Windows 7 oferuje możliwość automatycznego odcinania zasilania od kart sieciowych, gdy kabel jest odłączony. Gdy użytkownik podłączy kabel, zasilanie jest przywracane automatycznie. Ta funkcja oferuje korzyści związane z oszczędnością energii przez wyłączenie połączenia sieci przewodowej, a przy tym pozwala użytkownikom łatwo przyłączać się do sieci przewodowych.

Ponowne łączenie z siecią VPN

Łączność internetowa dla użytkowników mobilnych często jest zawodna. Na przykład użytkownicy sieci bezprzewodowej podróżujący pociągiem z Bostonu do Nowego Jorku mają łączność z Internetem przez większą część podróży. Jednakże mogą stracić połączenie z Internetem podczas przejeżdżania przez tunele lub tereny rolnicze.

Taka przerywana łączność jest szczególnie frustrująca, gdy użytkownik jest połączony z siecią VPN. W Windows Vista i wcześniejszych wersjach systemu Windows użytkownicy musieli ręcznie ponownie nawiązywać połączenie z VPN po powrocie połączenia internetowego. Dzięki funkcji ponownego łączenia z sieciami VPN system Windows 7 automatycznie wykryje, że znów jest połączony z Internetem i automatycznie ponownie połączy się z serwerem VPN działającym pod kontrolą systemu Windows Server 2008 R2.

DirectAccess

Ponowne łączenie z siecią VPN ułatwia utrzymywanie połączeń VPN, ale użytkownicy nadal muszą nawiązać początkowe połączenie z siecią VPN. Zwykle proces ten wymaga od użytkownika podania nazwy użytkownika i hasła, a następnie odczekanie kilku sekund (lub nawet minut) podczas ustanawiania połączenia VPN i sprawdzania stanu komputera. Z powodu tej uciążliwości użytkownicy mobilni często pomijają łączenie się z siecią VPN i zamiast tego korzystają jedynie z zasobów dostępnych w publicznej sieci Internet.

Jednakże użytkownicy mobilni, którzy nie łączą się z sieciami wewnętrznymi, nie wykorzystują swoich wewnętrznych zasobów. Z tego powodu nie są tak wydajni, jak mogliby być. Ponadto ich komputery nie uzyskują aktualizacji zabezpieczeń, czy zasad grupy, co może uczynić komputery podatnymi na atak i sprawić, że są niezgodne z zasadami firmy.

DirectAccess automatycznie łączy system Windows 7 z siecią wewnętrzną, gdy tylko komputer mobilny ma dostęp do Internetu. Funkcja ta jest bardzo podobna do VPN. Jednakże DirectAccess w ogóle nie pyta o nic użytkownika – połączenie jest całkowicie automatyczne. Z punktu widzenia użytkownika zasoby wewnętrzne są zawsze dostępne. Z punktu widzenia profesjonalistów IT można zarządzać komputerami mobilnymi, o ile tylko mają połączenie z Internetem bez konieczności wymagania od użytkownika łączenia się z siecią VPN.

DirectAccess ma więcej zalet, w tym możliwość pracy poprzez zapory, które ograniczają dostęp do VPN, oraz możliwość zapewniania uwierzytelniania i szyfrowania pomiędzy komputerami klienckimi a serwerami docelowymi w sieci wewnętrznej. DirectAccess wymaga serwera działającego pod kontrolą systemu Windows Server 2008 R2.

Wake on Wireless LAN

Użytkownicy mogą oszczędzać energię, przełączając komputery w tryb uśpienia, gdy nie są używane. We wcześniejszych wersjach systemu Windows użytkownicy i profesjonalści IT mogli korzystać z funkcji Wake on LAN (WOL), żeby budzić komputery, tak aby można było nimi zarządzać przez sieć. Jednakże WOL działa tylko wtedy, gdy komputery są połączone z siecią przewodową. Komputery bezprzewodowe w trybie uśpienia nie mogą być uruchamiane ani zarządzane przez sieć, co sprawia, że mogą nie nadążać za zmianami konfiguracji, aktualizacjami oprogramowania i innymi zadaniami zarządzającymi.

Windows 7 dodaje obsługę funkcji Wake on Wireless LAN (WoWLAN). Dzięki WoWLAN system Windows 7 może ograniczyć zużycie prądu, pozwalając użytkownikom i profesjonalistom IT na zdalne wybudzanie z trybu uśpienia komputerów połączonych z sieciami bezprzewodowymi. Ponieważ użytkownicy mogą budzić komputery, aby mieć do nich dostęp przez sieć, profesjonalści IT mogą skonfigurować je, tak aby przechodziły do oszczędnego trybu uśpienia, gdy nie będą używane.

Niezawodność i możliwości wsparcia

Chociaż użytkownicy końcowi zwykle skupiają się na zmianach interfejsu użytkownika, profesjonalści IT czerpią najwięcej korzyści z usprawnień związanych z niezawodnością i wsparciem. Te typy usprawnień mogą ograniczyć liczbę zgłoszeń do centrum wsparcia i znacznie poprawić skuteczność departamentów IT. Ponadto system Windows 7 może poprawić zadowolenie użytkowników z departamentów IT poprzez ograniczanie czasu poświęcanego na rozwiązywanie problemów z komputerem. Poniższe części tego rozdziału opisują ważne usprawnienia niezawodności i wsparcia w systemie Windows 7.

Startowe obiekty zasad grupy

Startowe obiekty zasad grupy (GPO) w systemie Windows 7 są zbiorami wstępnie skonfigurowanych szablonów administracyjnych, które mogą być wykorzystywane przez profesjonalistów IT jako standardowe, podstawowe konfiguracje do tworzenia faktycznych obiektów zasad grupy. Implementują one najlepsze praktyki firmy Microsoft, zawierając zalecane ustawienia zasad i wartości dla kluczowych scenariuszy korporacyjnych. Profesjonalści mogą również tworzyć i udostępniać własne startowe obiekty GPO w oparciu o wewnętrzne lub branżowe wymagania regulacyjne.

Preferencje zasad grupy

Preferencje zasad grupy rozszerzają zasięg możliwości zarządzania przez zasady grupy oraz sposoby stosowania ustawień. Dzięki preferencjom zasad grupy administratorzy systemowi mogą zarządzać funkcjami Windows, które nie obsługują zasad grupy, takimi jak mapowane dyski sieciowe i skróty na pulpicie.

Systemy Windows 7 i Windows Server 2008 R2 zawierają teraz domyślnie preferencje zasad grupy (w systemach Windows Vista i Windows Server 2008 trzeba było oddzielnie pobrać tę funkcję, aby z niej korzystać). Systemy Windows 7 i Windows Server 2008 R2 zawierają też nowe preferencje zasad grupy do elastycznego zarządzania zasilaniem i bardziej zaawansowanego harmonogramu zadań. Preferencje zasad grupy mogą być też używane do wdrażania ustawień rejestru w celu zarządzania aplikacjami. Administratorzy systemowi potrafią nawet tworzyć niestandardowe rozszerzenia preferencji zasad grupy.

W odróżnieniu od tradycyjnych ustawień zasad grupy preferencje zasad grupy nie są wymuszane. Są raczej traktowane jako ustawienia domyślne, które użytkownik może zmieniać. Preferencje można skonfigurować, tak aby stosować preferowane ustawienia za każdym razem, gdy uwzględniane są standardowe zasady grupy (jeśli użytkownik dokonał zmiany), albo aby używać ustawień preferowanych jako konfiguracji podstawowej, którą użytkownik może trwale zmieniać. Daje to profesjonalistom IT elastyczność pozwalającą

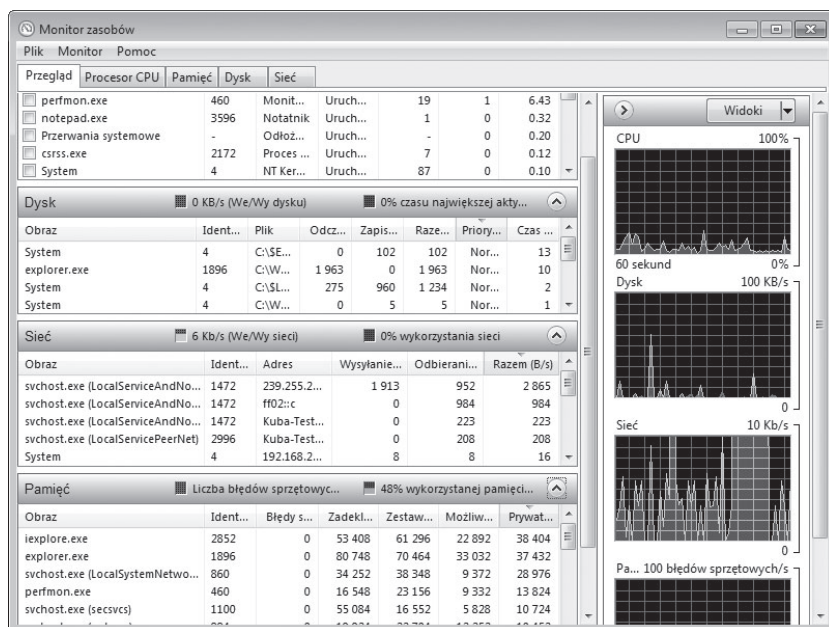
utrzymać optymalną równowagę pomiędzy kontrolą a wydajnością użytkowników. Preferencje zasad grupy zapewniają dodatkową elastyczność, umożliwiając administratorom systemowym konfigurowanie unikalnych ustawień dla różnych grup użytkowników lub komputerów w pojedynczym obiekcie zasad grupy, nie wymagając filtrów WMI (Windows Management Instrumentation).

Jakość usług w oparciu o adresy URL

Administratorzy systemowi obecnie ustalają priorytety ruchu sieciowego w oparciu o aplikację, numer portu i adres IP. Jednakże nowe inicjatywy, takie jak oprogramowanie jako usługa, wprowadzają konieczność szeregowania ruchu sieciowego w nowy sposób. Windows 7 zapewnia możliwość implementowania jakości usług (QoS) w oparciu o adresy URL. Jakość usług w oparciu o adresy URL można konfigurować poprzez zasady grupy, co daje profesjonalistom IT możliwości precyzyjniejszego dostrajania sieci.

Monitor zasobów

Windows 7 zawiera ulepszoną wersję Monitora zasobów, który wyświetla dane dotyczące wydajności procesora, pamięci, dysku i sieci w formacie pozwalającym na szybki dostęp do dużej liczby informacji, które możemy wykorzystać do łatwego zagłębiania się w szczególności specyficzne dla danego procesu. Jak pokazano na rysunku 1-11, Monitor zasobów jest użytecznym narzędziem do identyfikowania, które aplikacje, usługi i inne procesy zużywają zasoby. Podczas procesu rozwiązywania problemów profesjonalści IT mogą wykorzystywać te informacje do szybkiego identyfikowania podstawowych przyczyn problemów związanych z brakiem reakcji ze strony komputerów i aplikacji.



Rysunek 1-11 Monitor zasobów zapewnia szczegółowe informacje na temat działań aplikacji.

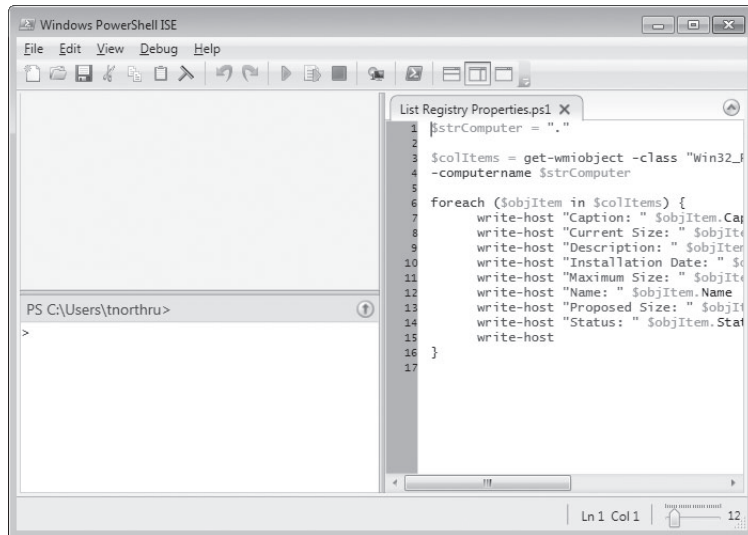
Windows PowerShell 2.0

Aby pomóc profesjonalistom IT w automatyzowaniu skomplikowanych lub monotonicznych zadań, system Windows 7 zawiera ulepszoną wersję środowiska skryptowego – Windows PowerShell 2.0. W odróżnieniu od tradycyjnych języków programowania projektowanych dla pełnoetatowych programistów Windows PowerShell jest językiem skryptowym, zaprojektowanym do stosowania przez administratorów systemowych. Ponieważ Windows PowerShell może korzystać z WMI, skrypty mogą wykonywać niemal dowolne zadania zarządzające, które profesjonalista IT chciałby zautomatyzować.

Do zadań, przy których profesjonalści IT wykorzystują Windows PowerShell 2.0 w systemie Windows 7, należą:

- Zdalne tworzenie punktu przywracania systemu przed rozwiązywaniem problemów.
- Zdalne przywracanie komputera do punktu przywracania systemu w celu rozwiązania problemu, którego nie można łatwo naprawić.
- Zdalne odpytywanie o zainstalowane aktualizacje.
- Edycja rejestru z użyciem transakcji, co zapewnia, że dana grupa zmian zostanie w całości zaimplementowana.
- Zdalne badanie danych o stabilności systemu z bazy danych niezawodności.

Windows 7 zawiera środowisko Windows PowerShell Integrated Scripting Environment (ISE), jak pokazano na rysunku 1-12. Windows PowerShell ISE umożliwia profesjonalistom IT tworzenie skryptów bez instalowania dodatkowych narzędzi.



Rysunek 1-12 Windows PowerShell 2.0 ISE

Sterta odporna na błędy

Wiele błędów aplikacji jest powodowanych przez złe zarządzanie pamięcią ze strony aplikacji. Choć za błędy te odpowiadają aplikacje, Windows 7 obsługuje stertę odporną na błędy. *Sterta* jest fragmentem pamięci wykorzystywanym przez aplikacje do tymczasowego przechowywania danych podczas działania aplikacji, zazwyczaj w formie zmiennych. Odporna na błędy sterata w systemie Windows 7 minimalizuje większość typowych powodów uszkodzenia sterty i może znacząco ograniczyć liczbę błędów aplikacji.

Rozwiązywanie problemów

Wbudowane mechanizmy diagnostyki i likwidowania awarii w systemie Windows Vista minimalizują wpływ występowania problemów na użytkownika, co ogranicza koszty wsparcia technicznego i zwiększa efektywność użytkowników oraz specjalistów od wsparcia. Poniższe części tego rozdziału opisują usprawnienia Windows Vista, które ułatwią użytkownikom rozwiązywanie swoich problemów, a departamentowi IT pozwolą rozwiązywać bardziej wymagające problemy, które nadal wymagają wsparcia.

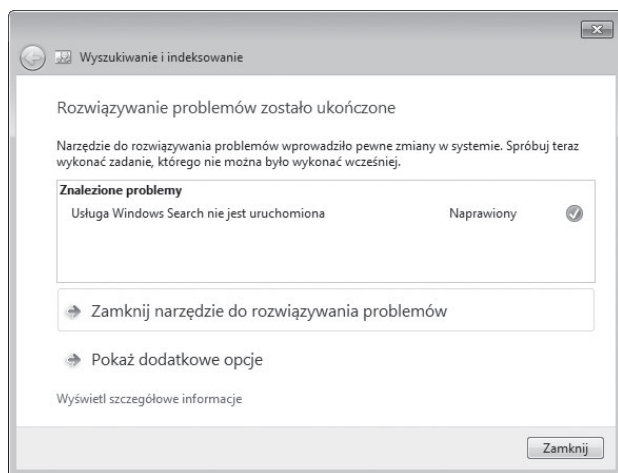
Platforma rozwiązywania problemów w systemie Windows

Windows Vista zawiera kilka zaawansowanych narzędzi do diagnostyki i rozwiązywania problemów zaprojektowanych, tak aby pozwalały użytkownikom rozwiązywać wiele typowych problemów bez wzywania centrum wsparcia IT. Windows 7 rozwija te narzędzia, wprowadzając platformę rozwiązywania problemów w systemie Windows. Platforma rozwiązywania problemów w systemie Windows obejmuje przyjazne dla użytkownika narzędzia, które mogą diagnozować a często też automatycznie rozwiązywać problemy w następujących kategoriach:

- Aero
- DirectAccess
- Sprzęt i urządzenia
- Sieć w grupie domowej
- Połączenia przychodzące
- Połączenia internetowe
- Wydajność programu Internet Explorer
- Zabezpieczenia programu Internet Explorer
- Karty sieciowe
- Wydajność
- Odtwarzanie dźwięku
- Zasilanie
- Drukarki
- Zgodność oprogramowania
- Nagrywanie dźwięku

- Wyszukiwanie i indeksowanie
- Foldery udostępnione
- Konserwacja systemu
- Dysk DVD programu Windows Media Player
- Biblioteka programu Windows Media Player
- Ustawienia programu Windows Media Player
- Windows Update

Rysunek 1-13 pokazuje, w jaki sposób pakiet rozwiązywania problemów Wyszukiwanie i indeksowanie jest w stanie zdiagnozować problem z wyszukiwaniem plików, mający wiele przyczyn.

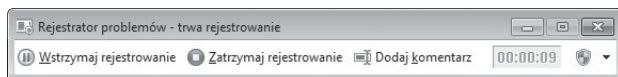


Rysunek 1-13 Pakiet rozwiązywania problemów automatycznie rozwiązujący złożony problem

Platforma rozwiązywania problemów w systemie Windows jest oparta na Windows PowerShell, więc departamenty IT mogą tworzyć własne pakiety rozwiązywania problemów dla aplikacji wewnętrznych. Oprócz uproszczenia rozwiązywania problemów dla użytkowników administratorzy mogą korzystać z narzędzi rozwiązywania problemów do przyspieszania skomplikowanych procedur diagnostycznych i testowych. Aby to umożliwić, administratorzy mogą uruchamiać narzędzia rozwiązywania problemów interaktywnie z wiersza polecenia lub w tle, wykorzystując plik odpowiedzi. Administratorzy mogą uruchamiać pakiety rozwiązywania problemów lokalnie lub zdalnie.

Rejestrator problemów

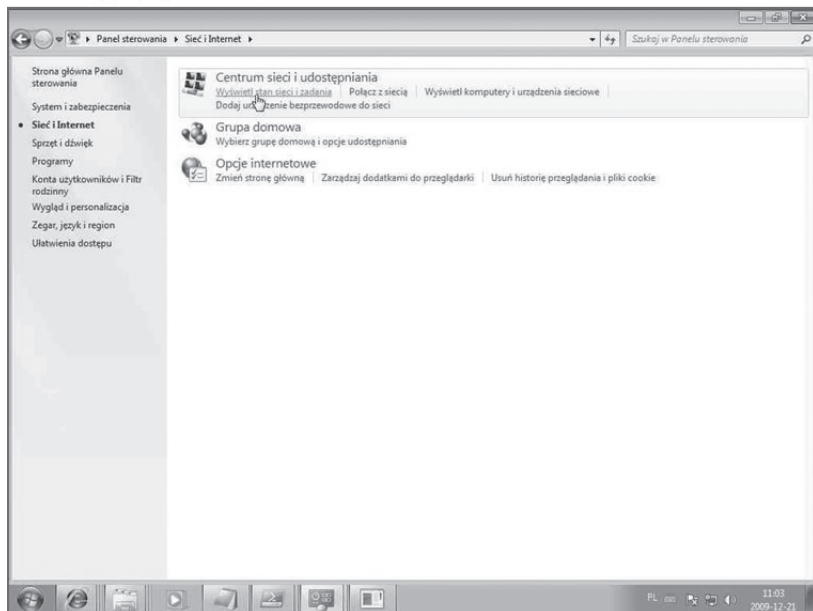
Jednym z największych wyzwań przy rozwiązywaniu problemów jest odtworzenie danego problemu. Jeśli profesjonalści IT nie mogą zduplikować danego problemu, nie mogą go zdiagnozować. Rejestrator problemów, pokazany na rysunku 1-14, jest narzędziem, które może być uruchamiane przez użytkowników w celu dokładnego udokumentowania okoliczności prowadzących do jakiegoś problemu. Użytkownicy rozpoczynają rejestrowanie, odtwarzają problem, a następnie przesyłają wynikowy raport HTML do profesjonalisty IT.



Rysunek 1-14 Rejestrator problemów

Raport HTML zawiera ciąg zrzutów ekranu, pokazujących dokładnie, co zrobił użytkownik, w tym każde naciśnięcie klawisza i kliknięcie myszą. Ponadto użytkownicy mogą dodawać komentarze opisujące szczegółowo każdy krok. Rysunek 1-15 pokazuje jeden krok z przykładowego raportu Rejestratora problemów. Warto zwrócić uwagę, że na górze strony opisane jest dokładnie, gdzie kliknął użytkownik.

Krok prowadzący do problemu 2: (2009-12-21 11:03:49) Kliknięcie lewym przyciskiem użytkownika na „Wyświetl stan sieci i zadania (łącznie)” w „Sieć i Internet”



Rysunek 1-15 Krok z przykładowego raportu Rejestratora problemów

Narzędzie do rozwiązywania problemów ze zgodnością programów

System Windows 7 usprawnia funkcję zgodności aplikacji z systemu Windows Vista. Jeśli aplikacja nie instaluje się, ponieważ nie rozpoznaje wersji systemu Windows, system Windows 7 prosi użytkownika o próbę ponownego zainstalowania aplikacji. Podczas tej następnej próby, system Windows 7 podaje inny numer wersji, który być może pozwoli na poprawne zainstalowanie aplikacji. W ten sposób system Windows 7 jest jeszcze bardziej zgodny z aplikacjami utworzonymi dla wcześniejszych wersji Windows, co minimalizuje czas poświęcany przez profesjonalistów IT na planowanie i rozwiązywanie problemów z aplikacjami.

Przekierowanie folderu i pliki trybu offline

Opcja przekierowania folderu i plików trybu offline zapewnia użytkownikom wygodny sposób dostępu do plików przechowywanych na serwerze centralnym, podczas gdy nie mają

połączenia z siecią korporacyjną. Windows 7 ogranicza początkowe czasy oczekiwania przyłączeniu się z folderami offline i pozwala profesjonalistom IT efektywniej zarządzać przekierowywaniem folderów i plikami trybu offline.

W systemie Windows 7 profesjonaliści IT mogą wykorzystywać zasady grupy, aby umożliwiać synchronizację określonych typów plików (na przykład plików muzycznych) z serwerem. Ponadto ponieważ funkcja plików trybu offline działa jako „zwykle offline”, gdy użytkownicy nie są połączeni z tą samą siecią LAN co serwer centralny, zwiększa się wydajność dla scenariuszy z oddziałami i dostępem zdalnym. Profesjonaliści IT mogą również kontrolować, kiedy pliki offline będą synchronizowane z serwerem, konfigurować określone przedziały czasowe dla synchronizacji, blokować inne godziny dla celów zarządzania szerokopasmowego i konfigurować maksymalny czas, po którym pliki muszą być ponownie zsynchronizowane.

Mobilne profile użytkowników

W systemie Windows Vista i wcześniejszych wersjach systemu Windows mobilne profile użytkowników były synchronizowane pomiędzy komputerem klienckim a serwerem, tylko gdy użytkownik się wylogowywał. W tym scenariuszu użytkownicy, którzy odłączali się od sieci bez wylogowywania (częsta czynność w przypadku użytkowników mobilnych), nie mieli synchronizowanego mobilnego profilu użytkownika.

W systemie Windows 7 mobilne profile użytkowników mogą być synchronizowane pomiędzy klientem a serwerem w czasie, gdy użytkownik jest nadal zalogowany. W efekcie użytkownik może być nadal zalogowany na komputerze, zalogować się na drugim komputerze i mieć odzwierciedlone najnowsze zmiany w profilu użytkownika.

Przywracanie systemu

Administratorzy mogą korzystać z Przywracania systemu do przywrócenia wcześniejszej konfiguracji systemu Windows. Przywracanie systemu jest niezbędne do rozwiązywania skomplikowanych problemów, takich jak instalacja złośliwego oprogramowania, ale przywracanie ustawień konfiguracyjnych do wcześniejszego stanu może spowodować awarie aplikacji zainstalowanych od momentu utworzenia danego punktu przywracania.

W systemie Windows 7 usprawniono funkcję Przywracania systemu, tak aby wyświetlała listę aplikacji, na które może mieć wpływ powrót do wcześniejszego punktu przywracania. Lista ta umożliwia administratorom oszacowanie potencjalnych problemów przed wykonaniem operacji przywracania systemu. Po przywróceniu administrator może sprawdzić te aplikacje i ponownie je zainstalować, jeśli to konieczne, aby przywrócić użytkownikowi w pełni funkcjonalny stan tych aplikacji.

Windows Recovery Environment

Podczas instalacji system Windows 7 automatycznie tworzy drugą partycję i instaluje na niej środowisko Windows Recovery Environment (Windows RE). Jeśli system Windows 7 nie może się uruchomić, użytkownik może otworzyć środowisko Windows RE i spróbować skorzystać z zawartych w nim narzędzi do rozwiązywania problemów. Narzędzie do naprawy systemu podczas uruchomienia (jedno z narzędzi do rozwiązywania problemów zawartych

w środowisku WinRE) może często automatycznie naprawić problem uniemożliwiający uruchomienie systemu Windows, co pozwala użytkownikowi szybko naprawić ów problem bez ponownego instalowania systemu Windows albo przywracania go z kopii zapasowej.

Zunifikowane śledzenie

Zunifikowane śledzenie zapewnia narzędzie do izolowania problemów w stosie sieciowym Windows 7. Zbiera ono dzienniki zdarzeń i przechwytyje pakiety we wszystkich warstwach stosu sieciowego, a następnie grupuje dane według działań.

Wdrażanie

Podobnie jak Windows Vista system Windows 7 obsługuje wdrażanie oparte na obrazach bez konieczności stosowania narzędzi firm trzecich. Profesjonaliści IT mogą całkowicie zautomatyzować wdrażanie, umieszczać niestandardowe sterowniki w obrazach, instalować aplikacje i aktualizacje systemu operacyjnego przed wdrożeniem oraz obsługiwać wiele języków i konfiguracji sprzętowych. System Windows 7 zawiera kilka nowych funkcji wdrożeniowych, które są opisane w kolejnych częściach rozdziału. Oprócz tych zmian instalator systemu Windows tworzy teraz automatycznie partycję dla narzędzia BitLocker (jak opisano w rozdziale 2) i dla środowiska Windows RE (jak opisano w rozdziale 29 „Konfigurowanie rozruchu i rozwiązywanie problemów z uruchamianiem”).

UWAGA W przypadku użytkowników indywidualnych, małych biur i jednorazowych aktualizacji funkcja Łatwy transfer w systemie Windows zapewnia prosty sposób transferu plików i ustawień z wcześniejszej wersji systemu Windows do nowego komputera działającego pod kontrolą systemu Windows 7. Poprawiono wydajność narzędzia Łatwy transfer w systemie Windows poprzez niezatrzymywanie transferu w celu poproszenia użytkownika o obsługę problemów z kopiowaniem plików. Tak jak w przypadku Windows Vista i wcześniejszych wersji systemu Windows, użytkownicy muszą ponownie zainstalować aplikacje na nowym komputerze. Jednakże system Windows 7 ułatwia proces ponownego instalowania aplikacji poprzez tworzenie spisu zainstalowanych programów na starym komputerze i przedstawianie tych informacji w raporcie pomiarowym, który zawiera łącza do informacji o produktach, aktualizacji oprogramowania i łącza do wsparcia technicznego dostarczone przez niezależnych dostawców oprogramowania.

Microsoft Deployment Toolkit 2010

MDT 2010, najnowsza wersja narzędzia Microsoft Deployment Toolkit, umożliwia szybkie wdrażanie systemów operacyjnych Windows 7, Windows Server 2008 R2, Windows Vista Service Pack 1 (SP1), Windows Server 2008, Windows XP SP3 i Windows 2003 SP2. MDT zapewnia zunifikowane narzędzia, skrypty i dokumentację dla wdrażania komputerów biurowych i serwerów przy użyciu zintegrowanej konsoli wdrożeniowej o nazwie Deployment Workbench. Korzystanie z MDT do wdrażania systemu Windows może pomóc ograniczyć czas wdrożenia, ułatwić tworzenie i zarządzanie ustandaryzowanymi obrazami komputerów biurowych i serwerów, zapewnić poprawę zabezpieczeń i ułatwić bieżące zarządzanie konfiguracją.

Windows Automated Installation Kit 2.0

Windows AIK 2.0, najnowsza wersja pakietu Windows Automated Installation Kit, zawiera nowe narzędzia wdrożeniowe i zaktualizowaną dokumentację do budowania niestandardowych rozwiązań związanych z wdrażaniem systemów Windows 7, Windows Server 2008 R2, Windows Vista SP1 i Windows Server 2008. Windows AIK 2.0 tworzy również podstawę dla MDT 2010, aby upraszczać automatyzację zadań związanych z wdrażaniem systemu Windows. Do nowych narzędzi zawartych w Windows AIK 2.0 należą:

- Narzędzie Deployment Image Servicing and Management (DISM)
- User State Migration Tool (USMT) 4.0
- Windows Preinstallation Environment (Windows PE) 3.0
- Volume Activation Management Tool (VAMT) 1.2.

Windows PE 3.0

Zaktualizowana wersja środowiska Windows PE jest oparta na jądrze systemu Windows 7, zamiast na jądrze Windows Vista. Nowe narzędzie DISM zastępuje narzędzia Pkgmgr, PEimg i Intlcfg. Windows PE 3.0 przejmuję również z systemu Windows 7 obsługę elementów interfejsu użytkownika, takich jak Aero Snap, które opisano w części dotyczącej gestów myszy.

Narzędzie Deployment Image Servicing and Management

Nowe narzędzie Deployment Image Servicing and Management (DISM) zapewnia profesjonalistom IT centralne miejsce do budowania i obsługi obrazów systemu Windows offline. DISM łączy funkcjonalność wielu różnych narzędzi Windows Vista, w tym International Settings Configuration (IntlCfg.exe), PEimg i Package Manager (Pkgmgr.exe). Przy pomocy DISM profesjonaliści IT mogą aktualizować obrazy systemów operacyjnych; dodawać funkcje opcjonalne; dodawać, wyliczać i usuwać sterowniki urządzeń pochodzące od firm trzecich; dodawać pakiety językowe i włączać ustawienia międzynarodowe; oraz utrzymywać magazyn obrazów offline zawierających sterowniki, pakiety, funkcje i aktualizacje oprogramowania. Możemy też korzystać z DISM do podwyższania poziomu obrazu Windows podczas wdrażania, na przykład z Windows 7 Professional do Windows 7 Ultimate Edition, co może ograniczyć liczbę oddzielnych obrazów, wymaganych do utrzymywania w danej organizacji.

Na przykład dana organizacja może utworzyć niestandardowy plik obrazu systemu Windows w formacie .wim. Moglibyśmy użyć narzędzia DISM do zamontowania tego niestandardowego obrazu, zbadania sterowników zawartych w tym obrazie, dodania plików niestandardowych i zapisania zaktualizowanego stanu obrazu, a następnie odłączyć ten obraz.

User State Migration Tool

Narzędzie User State Migration Tool (USMT) zostało zaktualizowane przez dodanie funkcji migracji przez sztywne łącze, która przenosi pliki z jednego systemu operacyjnego do innego na tym samym komputerze bez fizycznego przenoszenia tych plików na dysk, co zapewnia znaczący zysk wydajnościowy w porównaniu z wcześniejszymi metodami, które przenosiły pliki. Ponadto narzędzie USMT dla Windows 7 umożliwia migrację offline i zapewnia obsługę

Volume Shadow Copy, tak aby profesjonalści IT mogli migrować pliki, które są używane przez jakąś aplikację w momencie przechwytywania pliku. Można też migrować konta domenowe bez dostępności kontrolera domeny, co uprości wiele scenariuszy aktualizacyjnych.

Rozruch z pliku VHD

Można skonfigurować program rozruchowy Windows 7, aby uruchamiał system Windows z pliku wirtualnego dysku twardego (VHD) dokładnie tak samo jakby plik VHD był standardową partycją. Wystarczy po prostu skopiować plik VHD na komputer lokalny, a następnie użyć narzędzia BCDEdit.exe, aby dodać wpis dla pliku VHD do menu rozruchowego. System Windows 7 może również montować pliki VHD w konsoli Zarządzanie dyskami, tak jakby były normalnymi partycjami.

Dynamiczne dostarczanie sterowników

Funkcja dynamicznego dostarczania sterowników przechowuje sterowniki w centralnej lokalizacji, co oszczędza czas profesjonalistom IT, gdyż nie wymaga aktualizowania obrazów systemów operacyjnych, kiedy wymagane są nowe sterowniki (na przykład, gdy departament IT kupi nowy sprzęt). Sterowniki mogą być instalowane dynamicznie w oparciu o identyfikatory Plug and Play sprzętu komputerowego lub jako z góry określone zestawy w oparciu o informacje zawarte w systemie BIOS.

Multicast Multiple Stream Transfer

Funkcja Multicast Multiple Stream Transfer w systemie Windows 7 umożliwia bardziej efektywne wdrażanie obrazów na wielu komputerach w sieci. Zamiast wymagać oddzielnych połączeń bezpośrednich pomiędzy serwerami wdrożeniowymi a każdym klientem pozwala serwerom wdrożeniowym przysyłać dane o obrazach do wielu klientów jednocześnie. Windows 7 zawiera usprawnienie, które pozwala serwerom grupować klientów o podobnej przepustowości sieci i strumieniowe przysyłanie danych z różnymi prędkościami do każdej grupy, tak aby całkowita przepustowość nie była ograniczana przez najwolniejszego klienta.

Wydania Windows 7

Tak jak w przypadku wcześniejszych wersji systemu Windows, firma Microsoft wypuściła kilka różnych wersji (zwanych również SKU) systemu Windows 7, aby spełniać potrzeby różnych typów klientów, co opisano w tabeli 1-3.

Tabela 1-3 Oferta Windows 7 dla różnych segmentów klientów

Dla konsumentów	Dla małych firm	Dla średnich i dużych firm	Dla rynków wschodzących
Windows 7 Home Premium	Windows 7 Professional	Windows 7 Professional	Windows 7 Starter
Windows 7 Ultimate	Windows 7 Ultimate	Windows 7 Enterprise	Windows 7 Home Basic

Mimo dostępności kilku różnych wydań systemu Windows 7, dysku z produktem Windows 7 zawiera każdą wersję. Konkretnie wydanie, które będzie instalowane, zależy od klucza produktu użytego do zainstalowania oprogramowania. Użytkownicy mają opcję przejścia do wyższego wydania, korzystając z Windows Anytime Upgrade. Na przykład, jeśli użytkownik Windows 7 Home Basic uzna, że chce skorzystać z funkcjonalności Media Center, może użyć Windows Anytime Upgrade, aby zaktualizować system do wersji Windows 7 Home Premium lub Windows 7 Ultimate Edition.

Tabela 1-4 przedstawia zestawienie różnic pomiędzy wydaniem Windows 7 (z wyjątkiem wydania Windows 7 Starter Edition, które jest omawiane w dalszej części). Kolejne podrozdziały opisują bardziej szczegółowo każde wydanie.

Tabela 1-4 Funkcje różnych wydań systemu Windows 7

Funkcja	Home				
	Home Basic	Premium	Professional	Enterprise	Ultimate
Tworzenie grup domowych	Tylko dołączanie	X	X	X	X
Wielodotyk		X	X	X	X
Drukowanie zależne od lokalizacji			X	X	X
Udostępnianie pulpitu zdalnego			X	X	X
Tryb prezentacji			X	X	X
BranchCache				X	X
DirectAccess				X	X
Rozruch z pliku VHD				X	X
Przylączanie do domen			X	X	X
AppLocker				X	X
Zaplanowane kopie zapasowe		X	X	X	X
Pełna kopia zapasowa komputera			X	X	X
Interfejs użytkownika Aero	Częściowo	X	X	X	X
Obsługa dwóch procesorów (nie licząc poszczególnych rdzeni procesorów)			X	X	X
Lata wsparcia dla produktu	5	5	10	10	5
Windows Media Center		X	X	X	X

Tabela 1-4 Funkcje różnych wydań systemu Windows 7

Funkcja	Home				
	Home Basic	Premium	Professional	Enterprise	Ultimate
Windows DVD Maker		X			X
Kontrola rodzicielska	X	X			X
Faksowanie i skanowanie w systemie Windows			X	X	X
Centrum sieci i udostępniania			X	X	X
Inicjowanie sieci bezprzewodowych			X	X	X
Przychodzące połączenia udostępniania plików i drukarek	5	10	10	10	10
Tablet PC		X	X	X	X
Encrypting File System			X	X	X
Narzędzia do wdrażania na komputerach biurowych			X	X	X
Sieciowe ustawienia QoS oparte na zasadach			X	X	X
Kontrola nad instalacjami sterowników			X	X	X
Klient NAP			X	X	X
Szyfrowanie dysków funkcją BitLocker				X	X
Jednoczesna instalacja wielu języków interfejsu użytkownika				X	X
Podsystem aplikacji systemu UNIX				X	X

Windows 7 Starter

Chociaż wersja systemu Windows Vista Starter była dostępna tylko na rynkach wschodzących, wydanie Windows 7 Starter jest dostępne na całym świecie. To wydanie systemu Windows 7 zapewnia podstawowy zestaw funkcji i jest oferowane tylko w formie wstępnie instalowanej przez producentów sprzętu (OEM). Użytkownicy mogą skorzystać z usprawnień zabezpieczeń, wyszukiwania i organizacji. Jednakże interfejs Windows 7 Aero nie jest dostępny, a wydanie Windows 7 Starter istnieje tylko w wersjach 32-bitowych; brak wersji

64-bitowej. Wszystkie pozostałe wydania systemu Windows 7 są dostępne zarówno w wersjach 32-bitowych, jak i 64-bitowych.

Windows 7 Home Basic

Edycja Windows 7 Home Basic, dostępna jedynie na rynkach wschodzących, została zaprojektowana, aby spełniać potrzeby użytkowników domowych szukających taniego systemu operacyjnego. Windows 7 Home Basic jest wystarczającą wersją dla użytkowników, którzy używają komputerów głównie do odblokowania i wysyłania poczty elektronicznej, wiadomości błyskawicznych i przeglądania WWW. Do funkcji tego wydania należą:

- Natychmiastowe wyszukiwanie
- Internet Explorer 8
- Windows Defender
- Galeria fotografii systemu Windows
- Łatwy transfer w systemie Windows

Podobnie do wydania Windows 7 Starter, Windows 7 Home Basic nie zawiera interfejsu użytkownika Aero.

Windows 7 Home Premium

Jako preferowane wydanie konsumenckie Windows 7 Home Premium zawiera wszystkie funkcje Windows 7 Home Basic oraz następujące:

- Interfejs użytkownika Aero
- Windows Media Center
- Obsługę komputerów typu tablet
- Windows DVD Maker
- Planowane wykonywanie kopii zapasowych
- Obsługa Windows SideShow

Windows 7 Professional

Windows 7 Professional będzie odpowiadać potrzebom większości użytkowników biznesowych, w tym firmom małej i średniej wielkości. Windows 7 Professional zawiera wszystkie funkcje zawarte w Windows 7 Home Basic oraz następujące:

- Interfejs użytkownika Aero
- Obsługę komputerów typu tablet
- Możliwości tworzenia i przywracania kopii zapasowych (w tym kopii zapasowej całego komputera, automatycznej kopii zapasowej plików i kopii zapasowej woluminu dyskowego)
- Podstawowe funkcje biznesowe, w tym przyłączanie do domen, obsługa zasad grupy i system plików EFS

- Faksowanie i skanowanie
- Zasoby dla małych firm.

Podobnie jak zastępowana edycja Windows Vista Business Edition edycja, Windows 7 Professional jest dostępna poprzez licencje hurtowe.

Windows 7 Enterprise

Windows 7 Enterprise bazuje na zestawie funkcji Windows 7 Professional, dodając następujące funkcje:

- **Szyfrowanie napędów przez Windows BitLocker** Szyfruje wszystkie pliki na dysku systemowym, pomagając chronić użytkownika przed kradzieżą danych, jeśli napastnik uzyska fizyczny dostęp do twardego dysku
- **Wszystkie języki interfejsu użytkownika** Ułatwia wdrażanie w przedsiębiorstwach mających biura w różnych krajach i kulturach.
- **Uprawnienia licencyjne dla czterech wirtualnych systemów operacyjnych** Umożliwia uruchamianie wielu wersji systemu Windows w maszynach wirtualnych – co nadaje się idealnie do testowania oprogramowania lub uruchamiania aplikacji wymagających wcześniejszych wersji systemu Windows.
- **Podsystem dla aplikacji opartych na systemie UNIX (SUA)** Może być używany do kompilowania i uruchamiania aplikacji POSIX (Portable Operating System Interface for UNIX) w Windows.

Podobnie jak Windows Vista Enterprise wydanie Windows 7 Enterprise jest dostępne poprzez programy licencjonowania Software Assurance i Enterprise Advantage udostępniane przez firmę Microsoft.

Windows 7 Ultimate

Windows 7 Ultimate zawiera każdą funkcję zapewnianą przez wszystkie inne wersje systemu Windows, w tym zarówno Windows 7 Home Premium, jak i Windows 7 Enterprise. Użytkownicy, którzy wykorzystują komputery zarówno do pracy, jak i do użytku osobistego, powinni wybrać Windows 7 Ultimate. Podobnie użytkownicy, którzy nie chcą znaleźć się w sytuacji, gdy zabraknie im w przyszłości jakiejś funkcji Windows, powinni wybrać system Windows 7 Ultimate.

Klienci biznesowi, którzy wybiorą Windows 7 Ultimate napotkają kilka niedogodności:

- **Wdrażanie** Klucze licencjonowania hurtowego nie są dostępne dla Windows 7 Ultimate. Wdrażanie i obsługa tej edycji w scenariuszu korporacyjnym nie mogą być wydajnie przeprowadzane przez profesjonalistów IT, ponieważ każda instalacja wymaga ręcznej implementacji. Co więcej, jeśli klienci uzyskają Windows 7 Ultimate poprzez producenta OEM, nie będą mieli dostępu do pozostałych uprawnień, które pozwalają klientom instalować standardowy obraz korporacyjny zamiast wykorzystania systemu operacyjnego wstępnie zainstalowanego przez firmę OEM.

- **Możliwość zarządzania** Windows 7 Ultimate zawiera funkcje konsumenckie, takie jak Windows Media Center, którymi nie można łatwo zarządzać poprzez zasady grupy.
- **Wsparcie** Wydanie Windows 7 Ultimate nie jest objęte programem wsparcia Premium. Firmy, które zainstalowały Windows 7 Ultimate, muszą korzystać ze wsparcia bezpośrednio u dostawców sprzętu. Ponadto polityka serwisowania dla konsumenckiego systemu operacyjnego, takiego jak Ultimate, jest ograniczona do pięciu lat zamiast 10 lat dla biznesowej polityki serwisowania stosowanej w przypadku Windows 7 Enterprise.

Pomimo tych wad wydanie Windows 7 Ultimate jest dostępne poprzez program Software Assurance bez dodatkowych opłat. Klienci biznesowi powinni wybierać Windows 7 Enterprise dla większości komputerów i instalować Windows 7 Ultimate tylko na określonych komputerach, które wymagają funkcji domowych lub związanych z multimediami.

Wybieranie oprogramowania i sprzętu

Windows 7 zaprojektowano do współpracy ze sprzętem komputerowym, który obsługuje Windows Vista i może nawet osiągać lepszą wydajność niż Windows Vista na tym samym sprzęcie. Windows 7 zaprojektowano też z myślą o wykorzystaniu nowoczesnych możliwości sprzętowych. Poniższe podrozdziały opisują wymagania sprzętowe i dla logo Windows 7, co pomoże wybrać sprzęt pozwalający zapewnić potrzebne funkcje systemu Windows 7.

Windows 7 Software Logo

Microsoft zapewnia producentom sprzętu i oprogramowania logo systemu Windows 7 pokazujące, że dany program został przetestowany pod kątem działania z Windows 7. Aby aplikacja zakwalifikowała się do programu Windows 7 Logo, musi spełniać następujące kryteria:

- Być zgodna ze wskazówkami koalicji anty-spyware
- Nie próbować obchodzić ochrony zasobów Windows
- Zapewniać stałą jakość
- Zapewniać czystą, odwracalną instalację
- Domyślnie instalować się w poprawnych folderach
- Cyfrowo podpisywać pliki i sterowniki
- Obsługiwać wersje x64 systemu Windows
- Nie blokować instalacji lub uruchamiania aplikacji w oparciu o sprawdzanie wersji systemu operacyjnego
- Stosować się do zaleceń UAC
- Przestrzegać komunikatów menedżera ponownego uruchamiania
- Nie łądować usług i sterowników w trybie chronionym
- Obsługiwać sesje wielu użytkowników

Więcej informacji można przeczytać w dokumencie „The Windows 7 Client Software Logo Program”, który jest dostępny na witrynie Microsoft Download Center pod adresem www.microsoft.com/downloads/.

Wymagania sprzętowe

Windows 7 ma takie same wymagania sprzętowe jak Windows Vista. Dla podstawowego środowiska Windows 7 komputer musi spełniać następujące wymagania:

- Nowoczesny procesor (co najmniej 800 MHz)
- 512 MB pamięci systemowej
- Karta graficzna z możliwością obsługi DirectX 9

Dla rozszerzonego środowiska Windows 7 komputer musi spełniać następujące wymagania:

- 1-GHz procesor 32-bitowy (x86) lub 64-bitowy (x64)
- 1 GB pamięci systemowej
- Obsługa grafiki DirectX 9 przy pomocy sterownika Windows Display Driver Model (WDDM) driver, 128 MB pamięci graficznej (minimum), Pixel Shader 2.0 i 32 bity na piksel
- 40 GB pojemności dysku twardego z 15 GB wolnego miejsca
- Napęd DVD-ROM
- Możliwość wyjścia dźwiękowego
- Możliwość dostępu do Internetu

Rysunek 1-16 pokazuje logo sprzętowe Windows 7, które oznacza, że komputer został przetestowany z Windows 7. Oprogramowanie i sprzęt bez logo też będą prawdopodobnie działać na komputerach z Windows 7. Jednakże instalacja może być trudniejsza – konieczne może być ręczne wyszukiwanie sterowników, a aplikacje mogą mieć problemy ze zgodnością. Odmienne logo Windows Touch jest używane dla komputerów, które uzyskały certyfikat współpracy z interfejsem dotykowym Windows Touch.



Rysunek 1-16 Logo sprzętowe Windows 7

Podsumowanie

Windows 7 zawiera wiele znaczących usprawnień w stosunku do poprzednich wersji systemu Windows. Użytkownicy natychmiast zauważą ulepszony interfejs użytkownika, który został specjalnie zaprojektowany w celu poprawienia wydajności użytkowników. Usprawnienia wydajności pomogą ograniczyć uciążliwe opóźnienia i maksymalnie wykorzystają większość starszego sprzętu komputerowego. Użytkownicy mobilni odkrywają, że znacznie łatwiej jest zarządzać zasilaniem i możliwościami sieci bezprzewodowych, a użytkownicy komputerów typu tablet skorzystają z ulepszonej obsługi rysika i rozpoznawania pisma odręcznego.

Większość usprawnień systemu Windows 7 ma jednak na celu poprawę wydajności departamentów IT. Windows 7 oferuje wydajność wdrażania opartego na obrazach bez wymagania użycia narzędzi firm trzecich. Ulepszona niezawodność, możliwości wsparcia i rozwiązywania problemów mogą ograniczyć liczbę telefonów do centrum pomocy technicznej i pozwolą profesjonalistom IT szybciej rozwiązywać problemy, które nadal wymagają ich interwencji.

System Windows 7 jest dostępny w kilku różnych wydaniach; jednakże większość profesjonalistów IT wybierze Windows 7 Professional lub Windows 7 Enterprise. Prawdopodobnie można będzie wdrożyć system Windows 7, wykorzystując istniejący sprzęt komputerowy bez konieczności jego ulepszania. Jeśli trzeba zakupić dodatkowe komputery, należy zrozumieć różne wymagania sprzętowe dla różnych funkcji systemu Windows 7.

Ten rozdział przedstawił jedynie przegląd najważniejszych usprawnień. Pozostałe rozdziały tej książki omówią dogłębnie różne usprawnienia i podadzą szczegółowe informacje na temat tego, jak zarządzać systemem Windows 7 w środowiskach korporacyjnych.

Dodatkowe zasoby

Następujące zasoby zawierają dodatkowe informacje i narzędzia związane z tym rozdziałem.

Powiązane informacje

- Główna strona systemu Windows 7 w witrynie Microsoft.com pod adresem <http://www.microsoft.com/windows/windows-7/default.aspx>.
- Artykuł „What’s New for IT Pros in Windows 7 Release Candidate” w dziale Windows Client TechCenter na witrynie Microsoft TechNet pod adresem <http://technet.microsoft.com/en-us/library/dd349334.aspx>.

Na dołączonym nośniku

- Get-ProcessorArchitecture.ps1
- Get-WindowsEdition.ps1
- DisplayProcessor.ps1

- ListOperatingSystem.ps1
- Test-64bit.ps1
- Get-OSVersion.ps1

Bezpieczeństwo w systemie Windows 7

- Odpowiedź na konkretne obawy związane z bezpieczeństwem 38
- Funkcje zabezpieczeń wprowadzone wcześniej w systemie Windows Vista 47
- Nowe i poprawione funkcje zabezpieczeń Windows 7 63
- Podsumowanie 83
- Dodatkowe zasoby 84

System Windows Vista drastycznie zmienił zabezpieczenia systemu operacyjnego Windows. Przede wszystkim system Windows Vista domyślnie wykorzystywał mniej uprzywilejowane konta standardowych użytkowników dla większości zadań. Funkcjonalność ta zaimplementowana jako część kontroli konta użytkownika (UAC) i trybu chronionego programu Windows Internet Explorer dała w efekcie zmniejszenie infekcji szkodliwym oprogramowaniem, ograniczając zmiany, które mogły być dokonywane przez aplikacje w systemie operacyjnym bez ich zatwierdzania przez użytkowników.

System Windows 7 udoskonala usprawnienia z systemu Windows Vista. Kontrola konta użytkownika jest teraz domyślnie mniej nachalna. Funkcja Windows BitLocker jest bardziej elastyczna i została rozszerzona na współpracę z pamięciami wymiennymi. Funkcja Windows AppLocker zapewnia więcej elastyczności przy ograniczaniu, które aplikacje mogą być uruchamiane przez użytkownika. Zapora systemu Windows obsługuje teraz oddzielne profile dla sieci fizycznej i wirtualnej sieci prywatnej (VPN). Podczas gdy system Windows Vista silnie zmienił zabezpieczenia klienckiego systemu operacyjnego Windows, to Windows 7 skupia się na maksymalnym wykorzystaniu podstaw zabezpieczeń ustanowionych w Windows Vista.

Ten rozdział zapewnia przegląd najważniejszych usprawnień zabezpieczeń w Windows Vista i Windows 7 i wyjaśnia, jak mogą one poprawić bezpieczeństwo w typowych scenariuszach oraz oferuje informacje dotyczące tego, jak możemy wykorzystać te usprawnienia zabezpieczeń, aby spełnić wymagania zabezpieczeń w danej organizacji. W większości przypadków bardziej szczegółowe informacje dotyczące każdej funkcji zabezpieczeń można znaleźć w innych rozdziałach tej książki. Rozdział 2 zawiera odsyłacze do bardziej szczegółowego omówienia w innych rozdziałach.

Odpowiedź na konkretne obawy związane z bezpieczeństwem

System Windows 7 zawiera wiele nowych i poprawionych technologii zabezpieczeń. Choć zrozumienie technologii zabezpieczeń często wymaga bardziej szczegółowej wiedzy, scenariusze zabezpieczeń, którym służą te technologie, są praktyczne i jasne. Kolejne części tego rozdziału opisują, w jaki sposób funkcje zabezpieczeń w Windows Vista i Windows 7 współpracują ze sobą, aby poprawić bezpieczeństwo w trzech głównych obszarach: sieciach bezprzewodowych, oprogramowaniach szpiegowskich i innych rodzajach szkodliwego oprogramowania oraz robakach sieciowych. Każda technologia zabezpieczeń jest omówiona bardziej szczegółowo w dalszej części tego rozdziału i gdzie indziej w tej książce.

Prośby o pomoc związane ze szkodliwym oprogramowaniem

Zagrożenia bezpieczeństwa stale się zmieniają, przystosowując się do nowych generacji systemu operacyjnego. W kilku ostatnich latach gwałtownie wzrosło występowanie *szkodliwego oprogramowania* (szeroki termin obejmujący wirusy, robaki, konie trojańskie i rootkity, jak również programy szpiegowskie i inne potencjalnie niechciane oprogramowanie).

UWAGA Microsoft wykorzystuje termin *programy szpiegujące i inne potencjalnie niechciane oprogramowanie* w stosunku do oprogramowania, które jest niechciane, ale niekoniecznie jednoznacznie szkodliwe. W tej książce definicja *szkodliwego oprogramowania* obejmuje zarówno bezpośrednio szkodliwe wirusy i robaki, jak również niejednoznaczne programy szpiegowskie i inne potencjalnie niechciane oprogramowanie.

Wirusy, robaki i konie trojańskie mogą rozprzestrzeniać się z komputera na komputer, wykorzystując luki w oprogramowaniu, odgadując poświadczenia użytkowników lub oszukując użytkowników przy pomocy technik socjotechniki. Programy szpiegowskie i potencjalnie niechciane oprogramowanie rozprzestrzenia się tymi technikami, ale również poprzez uprawnione instalacje inicjowane przez użytkowników. Użytkownicy mogą zainstalować aplikację nieświadomi niepożądanego funkcjonalności programu albo obecności dodatkowego programu instalowanego razem z daną aplikacją.

Z powodu wyzwań związanych z identyfikowaniem szkodliwego oprogramowania, całkowite wyeliminowanie tego zagrożenia może być niemożliwe. Jednakże systemy Windows Vista i Windows 7 mają wiele nowych funkcji zabezpieczających, pomagających chronić komputery przed szkodliwym oprogramowaniem.

Wielu infekcjom szkodliwego oprogramowania można zapobiegać, instalując aktualizacje na komputerze mobilnym lub dostosowując konfigurację zabezpieczeń. Zasady grupy, usługi Windows Server Update Services (WSUS) i inne technologie zarządzające znacząco uprościły zadanie szybkiej dystrybucji aktualizacji i zmian zabezpieczeń. Jednakże zmiany te odnoszą skutek, tylko gdy komputery klienckie łączą się z siecią wewnętrzną. Gdy użytkownicy podróżują, komputery mobilne mogą pozostawać przez dni, tygodnie lub miesiące bez połączenia z siecią wewnętrzną. DirectAccess, nowa technologia wprowadzona w systemach

Windows 7 i Windows Server 2008 R2, automatycznie łączy komputery z siecią wewnętrzną za każdym razem, gdy mają one połączenie internetowe. Dlatego DirectAccess może aktualizować mobilne komputery klienckie z Windows 7 bardziej regularnie niż wcześniejsze wersje systemu Windows, co daje działowi IT potrzebną kontrolę, pozwalającą zmniejszać nowo odkryte zagrożenia poprzez dystrybucję aktualizacji lub zmian konfiguracji.

Pierwotnie wprowadzona w Windows Vista funkcja UAC (Kontrola konta użytkownika) ogranicza możliwości instalowania szkodliwego oprogramowania, umożliwiając profesjonalistom IT konfigurowanie użytkowników jako użytkowników standardowych, a nie administratorów. Pomaga to uniemożliwiać użytkownikom dokonywanie potencjalnie niebezpiecznych zmian na komputerach bez ograniczania ich możliwości kontroli nad innymi aspektami komputerów, takimi jak strefa czasowa lub ustawienia zasilania. W przypadku każdego, kto jednak loguje się jako administrator, funkcja UAC utrudnia oprogramowaniu szkodliwemu wpływ na cały komputer. Windows 7 zawiera ulepszenia funkcji UAC poprzez ograniczanie liczby komunikatów wyświetlanych użytkownikom. Dodatkowo administratorzy mogą dostosować zachowanie w przypadku zatwierdzania komunikatu. Czyniąc funkcję UAC wygodniejszą w użyciu, system Windows 7 ogranicza koszt wdrażania systemu Windows przy użyciu chronionego środowiska.

Podobnie tryb chroniony programu Internet Explorer powoduje jego działanie bez uprawnień koniecznych do instalowania oprogramowania (lub nawet zapisywania plików poza katalogiem Temporary Internet Files), ograniczając w ten sposób ryzyko, że Internet Explorer zostanie wykorzystany do zainstalowania szkodliwego oprogramowania bez zgody użytkownika.

Windows Defender wykrywa wiele typów programów szpiegowskich i innego potencjalnie niechcianego oprogramowania oraz informuje użytkownika, zanim aplikacje będą mogły dokonać potencjalnie szkodliwych zmian. W systemie Windows 7 Windows Defender ma znacznie poprawioną wydajność monitorowania w czasie rzeczywistym. Dzięki ograniczeniu kosztów wydajnościowych monitorowania w czasie rzeczywistym, więcej departamentów IT może pozostawić monitorowanie w czasie rzeczywistym włączone, czerpiąc w ten sposób korzyści z dodatkowych zabezpieczeń. Ponadto Windows Defender wykorzystuje Centrum akcji do powiadamiania użytkowników o potencjalnych problemach.

Funkcja hartowania usług systemu Windows ogranicza szkody, jakie może wyrządzić napastnik w przypadku, gdy będzie w stanie skutecznie skompromitować usługę, co redukuje ryzyko dokonania trwałych zmian w systemie operacyjnym przez napastnika lub przeprowadzenia ataku na inne komputery w sieci. Chociaż system Windows 7 nie może wyeliminować szkodliwego oprogramowania, te technologie mogą znacząco ograniczyć wpływ takiego oprogramowania.

System Windows 7 zaprojektowano, tak aby blokował wiele typów powszechnych technik instalowania szkodliwego oprogramowania. Kolejne części tego rozdziału opisują, jak systemy Windows Vista i Windows 7 chronią się przed szkodliwym oprogramowaniem, które próbuje zainstalować się bez wiedzy użytkownika poprzez przyłączanie się do innych programów oraz socjotechnikę, luki w przeglądarce i robaki sieciowe.

Ochrona przed dołączaniem oprogramowania i socjotechniką

Dwoma najpowszechniejszymi sposobami używanymi przez szkodliwe oprogramowanie do instalowania na komputerze jest dołączanie do innego oprogramowania i socjotechnika. W pierwszym przypadku szkodliwe oprogramowanie jest spakowane razem z jakimś przydatnym. Często użytkownik nie jest świadomy negatywnych aspektów powiązanego oprogramowania. W przypadku socjotechniki użytkownik jest podstępem zachęcany do zainstalowania oprogramowania. Zwykle użytkownik otrzymuje mylącą wiadomość pocztą elektroniczną lub komunikat z przeglądarki zawierający instrukcje otwarcia załącznika lub odwiedzenia jakiejś witryny WWW.

Systemy Windows Vista i Windows 7 oferują znacznie poprawioną ochronę zarówno przed dołączaniem szkodliwego oprogramowania, jak i socjotechniką. Przy domyślnych ustawieniach szkodliwe oprogramowanie próbujące zainstalować się poprzez dołączanie do innego oprogramowania lub socjotechnikę musi obejść dwa poziomy ochrony: UAC oraz Windows Defender.

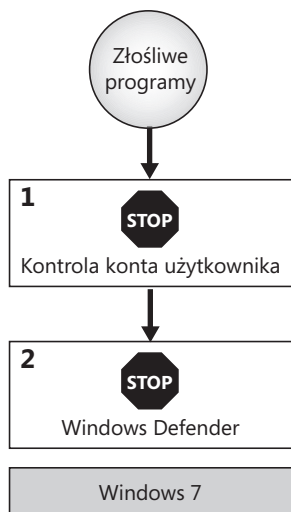
UAC albo poprosi użytkownika o potwierdzenie chęci zainstalowania oprogramowania (jeśli użytkownik jest zalogowany na koncie administracyjnym), albo poprosi użytkownika o podanie poświadczeń administracyjnych (jeśli użytkownik jest zalogowany na koncie standardowym). Ta funkcja uświadamia użytkowników, że jakiś proces próbuje dokonać znaczących zmian i pozwala zatrzymać ten proces. Standardowi użytkownicy muszą skontaktować się z administratorem, aby kontynuować instalację. Więcej informacji można uzyskać pod nagłówkiem „Kontrola konta użytkownika” w dalszej części tego rozdziału.

Ochrona w czasie rzeczywistym przez Windows Defender blokuje aplikacje, które są identyfikowane jako szkodliwe. Windows Defender wykrywa również i zatrzymuje zmiany, które szkodliwe oprogramowanie próbuje wykonać, na przykład konfigurowanie automatycznego uruchomienia szkodliwego oprogramowania przy ponownym rozruchu systemu. Windows Defender powiadamia użytkownika, że aplikacja próbowała dokonać zmiany i daje użytkownikowi możliwość zablokowania lub kontynuowania instalacji. Więcej informacji można uzyskać pod nagłówkiem „Windows Defender” w dalszej części rozdziału.

UWAGA Windows Defender dodaje zdarzenia do systemowego dziennika zdarzeń. W połączeniu z subskrypcją zdarzeń lub narzędziem, takim jak Microsoft Systems Center Operations Manager (SCOM), możemy łatwo agregować i analizować zdarzenia programu Windows Defender w swojej organizacji.

Te poziomy ochrony zilustrowano na rysunku 2-1.

W systemie Windows XP i wcześniejszych wersjach Windows instalacje szkodliwego oprogramowania przez dołączanie do innego oprogramowania i socjotechnikę miały szanse powodzenia, ponieważ nie było tego typu ochrony zawartej w systemie operacyjnym ani w zestawach poprawek serwisowych do systemu.



Rysunek 2-1 Systemy Windows Vista i Windows 7 wykorzystują ochronę przed atakami szkodliwych programów poprzez dołączanie do innego oprogramowania i socjotechnikę.

Dogłębna obrona

Dogłębna obrona jest sprawdzoną techniką warstwowej ochrony, która ogranicza podatność na luki. Na przykład moglibyśmy zaprojektować sieć z trzema warstwami filtrowania pakietów: routerem filtrującym pakiety, zaporą sprzętową i zaporami programowymi (takimi jak Zapora systemu Windows) po obu stronach połączenia. Jeśli napastnikowi uda się obejść jedną lub dwie warstwy ochrony, komputery będą nadal chronione.

Prawdziwą korzyścią z dogłębnej obrony jest jej możliwość ochrony przed błędem ludzkim. Podczas gdy pojedyncza warstwa obrony jest wystarczającą ochroną w normalnych okolicznościach, wyłączenie jej przez administratora podczas rozwiązywania problemów, przypadkowej zmiany konfiguracji lub przez nowo odkrytą lukę, może całkiem wyłączyć taką jednowarstwową obronę. Dogłębna obrona zapewnia ochronę nawet w przypadku, gdy pojawi się pojedyncza luka.

Chociaż większość nowych funkcji zabezpieczeń systemu Windows stanowią środki prewencyjne, które skupiają się na bezpośrednim przeciwdziałaniu ryzyku przez blokowanie możliwości wykorzystania luk, strategia dogłębnej obrony powinna również obejmować środki wykrywające i reagujące. Inspekcja i zewnętrzne systemy wykrywania włamań mogą pomóc w zanalizowaniu ataku po fakcie, umożliwiając administratorom zablokowanie kolejnych ataków i być może zidentyfikowanie napastnika. Kopie zapasowe i plany odbudowy po awarii pozwalają zareagować na atak i ograniczyć potencjalną utratę danych.

Ochrona przed instalacjami szkodliwego oprogramowania przez luki w przeglądarce

Historycznie wiele instalacji szkodliwego oprogramowania było dokonywanych, ponieważ użytkownik odwiedził szkodliwą witrynę WWW, a witryna ta wykorzystywała lukę w przeglądarce WWW do zainstalowania szkodliwego oprogramowania. W niektórych przypadkach użytkownik nie otrzymywał żadnego ostrzeżenia o tym, że instalowane jest oprogramowanie. W innych sytuacjach użytkownicy byli proszeni o potwierdzenie instalacji, ale komunikat ten mógł być mylący lub niekompletny.

Windows 7 zapewnia cztery warstwy ochrony przed instalowaniem tego typu szkodliwego oprogramowania:

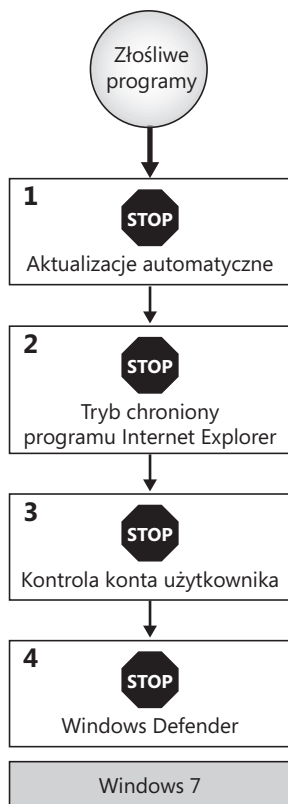
- Domyślnie włączone aktualizacje automatycznie pomagają utrzymać program Internet Explorer i pozostałe części systemu operacyjnego „na czasie” poprzez instalowanie łatek, które mogą naprawiać wiele luk zabezpieczeń. Aktualizacje automatyczne mogą uzyskiwać poprawki zabezpieczeń z witryny Microsoft.com lub z wewnętrznego serwera WSUS. Więcej informacji można znaleźć w rozdziale 23 „Zarządzanie aktualizacjami oprogramowania”.
- Tryb chroniony programu Internet Explorer daje jedynie znacznie ograniczone uprawnienia procesom wywołanym przez przeglądarkę Internet Explorer, nawet jeśli użytkownik jest zalogowany jako administrator. Każdy proces uruchomiony z poziomu przeglądarki Internet Explorer ma dostęp jedynie do katalogu Temporary Internet Files. Żadnego pliku zapisanego w tym katalogu nie można uruchomić.
- W przypadku administratorów Kontrola konta użytkownika (UAC) prosi użytkownika o potwierdzenie, zanim dokonana zostanie zmiana konfiguracji komputera. W przypadku użytkowników standardowych ograniczone uprawnienia blokują większość trwałych zmian dla komputera, chyba że użytkownik może podać poświadczenia administracyjne.
- Windows Defender powiadamia użytkownika, jeśli szkodliwe oprogramowanie próbuje się zainstalować jako obiekt pomocniczy przeglądarki, uruchomić się automatycznie po ponownym rozruchu systemu lub zmodyfikować inny monitorowany aspekt systemu operacyjnego.

Te poziomy ochrony zilustrowano na rysunku 2-2.

Ochrona przed robakami sieciowymi

Dołączanie do innych programów, socjotechnika i luki w przeglądarkach polegają na zainicjowaniu przez użytkownika połączenia z witryną, na której znajduje się szkodliwe oprogramowanie, natomiast robaki mogą infekować komputer bez żadnej interakcji ze strony użytkownika. Robaki sieciowe rozprzestrzeniają się poprzez przysyłanie komunikatów przez sieć w celu wykorzystania luk w komputerach zdalnych i zainstalowania robaka. Po zainstalowaniu robak nadal wyszukuje nowe komputery do zainfekowania.

Jeśli robak zaatakuje komputer z systemem Windows Vista lub Windows 7, system oferuje cztery poziomy ochrony:

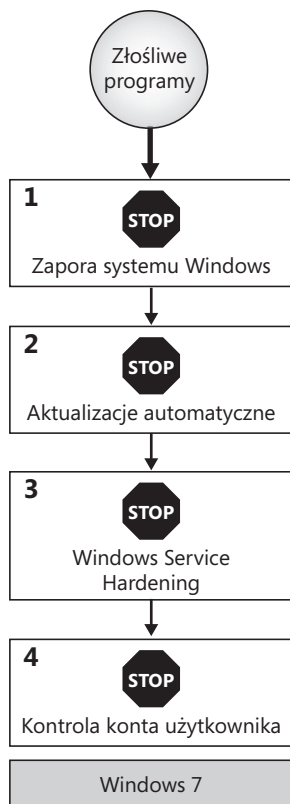


Rysunek 2-2 Windows 7 wykorzystuje dogłębną obronę do ochrony przed instalacjami szkodliwego oprogramowania wykorzystującymi luki w przeglądarce.

- Zapora systemu Windows blokuje cały ruch przychodzący, który nie został wprost dozwolony (plus kilka wyjątków dla podstawowej funkcjonalności sieci w profilach domenowym i prywatnym). Ta funkcja blokuje większość obecnych ataków robaków.
- Jeśli robak zaatakuję lukę w funkcji Microsoft, automatyczne aktualizacje – które są włączone domyślnie – być może już rozwiązały problem z tą luką w zabezpieczeniach.
- Jeśli robak wykorzystuje lukę w usłudze, która stosuje Windows Service Hardening i spróbuje podjąć działanie niedozwolone przez profil tej usługi (na przykład zapis pliku lub dodanie robaka do grupy Autostart), system Windows zablokuje robaka.
- Jeśli robak wykorzystuje lukę w aplikacji użytkownika, ograniczone uprawnienia kontrolowane przez UAC zablokują zmiany w konfiguracji systemu.

Te poziomy ochrony zilustrowano na rysunku 2-3.

Pierwotne wydanie systemu Windows XP nie miało żadnego z tych poziomów ochrony. W Windows XP Service Pack 2 (SP2) Zapora systemu Windows i aktualizacje automatyczne są włączone, ale pozostałe poziomy ochrony oferowane przez Windows Vista i Windows 7 są niedostępne.



Rysunek 2-3 Systemy Windows Vista i Windows 7 wykorzystują dogłębną obronę do ochrony przed robakami sieciowymi.

Kradzież danych

W miarę rozpowszechniania się komputerów mobilnych, łączności sieciowej i nośników wymiennych coraz powszechniejsza staje się też kradzież danych. Wiele firm i organizacji rządowych przechowuje niezwykle cenne dane na swoich komputerach, a koszt trafiaenia tych danych w niepowołane ręce może być ogromny.

Obecnie wiele organizacji ogranicza ryzyko kradzieży danych poprzez ograniczanie dostępu do nich. Na przykład aplikacje mogą nie pozwalać na przechowywanie poufnych plików na komputerach mobilnych. Użytkownicy mogą też po prostu nie mieć pozwolenia na wynoszenie komputerów poza biuro. Te ograniczenia faktycznie skutecznie ograniczają ryzyko, ale również ograniczają wydajność użytkowników, nie pozwalając im korzystać z możliwości mobilnych.

Systemy Windows Vista i Windows 7 zapewniają technologie ochrony danych zaprojektowane tak, aby spełniały surowsze wymagania dotyczące zabezpieczeń, a przy tym pozwalały użytkownikom pracować z poufnymi danymi w różnych lokalizacjach. Rozważmy następujące typowe scenariusze kradzieży danych i sposoby ograniczania ryzyka każdego z nich przez system Windows.

Fizyczna kradzież komputera mobilnego lub dysku twardego albo odzyskiwanie danych z wyrzuconego dysku twardego

Systemy operacyjne mogą zapewniać aktywną ochronę danych przechowywanych na dysku twardym tylko podczas działania systemu operacyjnego. Innymi słowy, listy kontroli dostępu do plików (ACL), takie jak zapewniane przez system plików NTFS, nie mogą chronić danych, jeśli napastnik może fizycznie uzyskać dostęp do komputera lub dysku twardego. W ostatnich latach było wiele przypadków skradzionych komputerów mobilnych, z których poufne dane zostały wyciągnięte z dysku twardego. Dane są często odzyskiwane z komputerów zużytych (przekazanych innemu użytkownikowi) lub wyrzuconych (pod koniec życia danego komputera), nawet jeśli dysk twardy został sformatowany.

Systemy Windows Vista i Windows 7 ograniczają ryzyko tego typu kradzieży danych poprzez zezwalanie administratorom na szyfrowanie plików przechowywanych na dysku. Tak jak w przypadku Windows XP, systemy Windows Vista i Windows 7 obsługują *system szyfrowania plików (EFS)*. EFS umożliwia administratorom i użytkownikom selektywne szyfrowanie plików lub oznaczanie całego foldera, aby szyfrował wszystkie zawarte w sobie pliki. Oprócz możliwości oferowanych przez Windows XP systemy Windows Vista i Windows 7 umożliwiają konfigurowanie EFS przy użyciu ustawień zasad grupy tak, abyśmy mogli centralnie chronić całą domenę bez wymagania zrozumienia szyfrowania od użytkowników.

EFS nie może jednak chronić plików systemu Windows. Ochrona systemu Windows przed atakiem offline (rozruchem z wymiennego nośnika w celu bezpośredniego dostępu do systemu plików lub przeniesieniem dysku twardego do innego komputera) pomaga zapewnić spójność systemu operacyjnego, nawet jeśli komputer zostanie skradziony. Szyfrowanie dysków funkcją BitLocker w systemie Windows Vista zapewnia szyfrowanie całego woluminu systemowego – chroniąc w ten sposób nie tylko system operacyjny, ale również wszelkie dane przechowywane na tym samym woluminie (literze napędu). W systemie Windows 7 administratorzy mogą korzystać z funkcji BitLocker do ochrony zarówno woluminów systemowych, jak i nie-systemowych (a także nośników wymiennych, co zostanie opisane w następnym podrozdziale). Funkcja BitLocker może pracować w sposób przezroczysty wykorzystując obsługiwany sprzęt albo może wymagać wieloczynnikowego uwierzytelniania nakazując użytkownikom podawać hasło przed zezwoleniem na odszyfrowanie woluminu. W zależności od wymagań zabezpieczeń możemy korzystać z funkcji BitLocker na istniejącym sprzęcie komputerowym, zachowując klucze odszyfrowujące na nośniku wymiennym lub nawet nakazując użytkownikom wpisywać kod PIN, lub hasło przed rozruchem systemu Windows. Więcej informacji można znaleźć w rozdziale 16 „Zarządzanie dyskami i systemami plików”.

Kopiowanie poufnych plików na nośnik wymienny

Organizacje z surowymi wymaganiami dotyczącymi zabezpieczeń ograniczają dostęp do poufnych danych tylko dla komputerów w sieci lokalnej i nie pozwalają wynosić tych komputerów poza swoją siedzibę. Dawniej organizacje te usuwały napędy dyskietek z komputerów, aby uniemożliwić użytkownikom zapisywanie poufnych plików. Ostatnio jednak wzrosła znacząco dostępność różnych typów nośników wymiennych. W szczególności telefony komórkowe, urządzenia PDA, przenośne odtwarzacze muzyki i napędy USB często mają kilka gigabajtów pojemności pamięci. Ponieważ są małe i bardzo rozpowszechnione,

mogą zostać przeoczone, nawet jeśli w danej lokalizacji dostępny jest personel ochrony przeszukujący pracowników wchodzących do budynku lub wychodzących z niego.

Systemy Windows Vista i Windows 7 umożliwiają użycie ustawień zasad grupy w celu ograniczania ryzyka ze strony nośników wymiennych. Korzystając z ustawień zasad grupy w folderze Konfiguracja komputera\Zasady\Szablony administracyjne\System\Instalacja urządzenia\Ograniczenia dotyczące instalacji urządzeń, administratorzy mogą:

- Zezwalać na instalowanie całej klasy urządzeń (takich jak drukarki), używając opcji Zezwalaj na instalację urządzeń za pomocą sterowników odpowiadających tym klasom konfiguracji urządzeń.
- Zabraniać użycia wszelkich nieobsługiwanych lub nieautoryzowanych urządzeń, korzystając z opcji Zapobiegaj instalacji urządzeń o identyfikatorach odpowiadających tym identyfikatorom urządzeń.
- Zabraniać użycia wszelkiego rodzaju urządzeń pamięci wymiennej, korzystając z opcji Zapobiegaj instalacji urządzeń wymiennych.
- Uchyłać te zasady, jeśli to konieczne, dla celów rozwiązywania problemów lub zarządzania, korzystając z opcji Zezwalaj administratorom na zastępowanie zasad ograniczających instalację urządzeń.

Podczas gdy system Windows Vista skupiał się na zapewnianiu administratorom kontroli potrzebnej do uniemożliwiania użytkownikom zapisywania plików na nośnikach wymiennych, system Windows 7 zawiera technologię ochrony plików, gdy są one kopiowane na nośnik wymienny: BitLocker To Go. BitLocker To Go zapewnia szyfrowanie na poziomie woluminu dla nośników wymiennych. Aby odszyfrować zawartość nośnika wymiennego, użytkownik musi wpisać hasło lub użyć karty inteligentnej. Bez hasła lub karty inteligentnej zawartość nośnika zaszyfrowanego funkcją BitLocker To Go nie może być dostępna.

Więcej informacji na temat zarządzania nośnikami oraz funkcji BitLocker można znaleźć w rozdziale 16. Więcej informacji na temat korzystania z zasad grupy do zarządzania komputerami z systemem Windows 7 można znaleźć w rozdziale 14 „Zarządzanie środowiskiem pulpitu”.

Przypadkowe drukowanie, kopiowanie lub przekazywanie dalej dokumentów poufnych

Użytkownicy często muszą udostępniać poufne dokumenty, aby efektywnie nad nimi pracować. Na przykład użytkownik może przesłać dokument pocztą elektroniczną do recenzji przez innego użytkownika. Jednakże gdy dokument zostanie skopiowany z chronionego foldera udostępnianego lub intranetu, tracimy kontrolę nad tym dokumentem. Użytkownicy mogą przypadkowo skopiować, przesłać dalej lub wydrukować ten dokument tak, że może on trafić do użytkownika, który nie powinien mieć do niego dostępu.

Nie ma idealnego rozwiązania chroniącego dokumenty elektroniczne przed kopiowaniem. Jednakże klient usług *Rights Management Services (RMS)* wbudowany w Windows Vista i Windows 7 umożliwia komputerom otwieranie dokumentów zaszyfrowanych przez RMS i wymuszanie ograniczeń narzuconych na dany dokument. Dzięki infrastrukturze RMS i aplikacji obsługującej RMS, takiej jak Microsoft Office, możemy:

- Zezwalać użytkownikowi na przeglądanie dokumentu, ale nie na zapisywanie jego kopii, drukowanie go lub przekazywanie go dalej.
- Ograniczać użytkownikom możliwość kopiowania i wklejania tekstu wewnątrz dokumentu.
- Znacznie utrudniać otwieranie dokumentu przy użyciu klienta, który nie wymusza ochrony RMS.

System Windows 7 zapewnia wbudowane wsparcie dla wykorzystania RMS do ochrony dokumentów XPS (XML Paper Specification). Aby korzystać z RMS, potrzebna jest infrastruktura RMS i obsługujące ją aplikacje oprócz samego systemu Windows Vista lub Windows 7. Więcej informacji na temat RMS można znaleźć w części „Rights Management Services” w dalszej części tego rozdziału.

Funkcje zabezpieczeń wprowadzone wcześniej w systemie Windows Vista

Ta część rozdziału opisuje najbardziej widoczne i namacalne usprawnienia zabezpieczeń z systemu Windows Vista, które nie zostały znacząco zmienione w systemie Windows 7. Wymieniono je w tabeli 2-1. Każde z tych usprawnień jest również zawarte w systemie Windows 7. Usprawnienia architektoniczne i wewnętrzne – jak również usprawnienia, które wymagają dodatkowych aplikacji lub infrastruktury – zostały opisane w dalszej części tego rozdziału. Nowe usprawnienia zabezpieczeń w systemie Windows 7 i funkcje systemu Windows Vista, które zostały znacząco poprawione w Windows 7, są również omawiane w dalszej części tego rozdziału.

Tabela 2-1 Usprawnienia zabezpieczeń wcześniej wprowadzone w systemie Windows Vista

Usprawnienie	Opis
Windows Defender	Próbuje wykrywać i blokować niechciane oprogramowanie.
Zapora systemu Windows	Filtruje przychodzący i wychodzący ruch sieciowy. Nowe usprawnienia zapewniają większą elastyczność i możliwości zarządzania.
Encrypting File System	Szyfruje pliki i foldery inne niż pliki systemowe. Usprawnienia zapewniają większą elastyczność i możliwości zarządzania.
Usprawnienia Menedżera poświadczeń	Umożliwia użytkownikom wykonywanie typowych zadań związanych z zarządzaniem poświadczeniami, na przykład ustalanie nowych numerów PIN.

Tabela 2-1 Usprawnienia zabezpieczeń wcześniej wprowadzone w systemie Windows Vista

Usprawnienie	Opis
Windows Defender	Próbuje wykrywać i blokować niechciane oprogramowanie.
Zapora systemu Windows	Filtruje przychodzący i wychodzący ruch sieciowy. Nowe usprawnienia zapewniają większą elastyczność i możliwości zarządzania.
Encrypting File System	Szyfruje pliki i foldery inne niż pliki systemowe. Usprawnienia zapewniają większą elastyczność i możliwości zarządzania.
Usprawnienia Menedżera poświadczeń	Umożliwia użytkownikom wykonywanie typowych zadań związanych z zarządzaniem poświadczeniami, na przykład ustalanie nowych numerów PIN.

Dalsze podrozdziały opisują te funkcje bardziej szczegółowo. Aby uzyskać szczegółowe zalecenia jak konfigurować ustawienia zabezpieczeń systemu Windows Vista, należy zwrócić się do przewodnika *Windows Vista Security Guide*, dostępnego pod adresem <http://www.microsoft.com>. Interesujący opis, jak zmiany zabezpieczeń w systemie Windows Vista doprowadziły do realnej poprawy, można przeczytać w artykule „Windows Vista Security One Year Later” pod adresem <http://blogs.msdn.com/windowsvistasecurity/archive/2008/01/23/windows-vista-security-one-year-later.aspx>.

Windows Defender

Windows Defender jest funkcją systemów Windows Vista i Windows 7, która zapewnia ochronę przed programami szpiegowskimi i innym potencjalnie niechcianym oprogramowaniem. Windows Defender opiera się na sygnaturach, wykorzystując opisy unikalnie identyfikujące programy szpiegowskie i inne potencjalnie niechciane oprogramowanie, żeby wykrywać i usuwać znane aplikacje tego typu. Program Windows Defender regularnie pobiera nowe sygnatury z witryny Microsoft tak, aby mógł identyfikować i usuwać nowoutworzone programy szpiegowskie i inne potencjalnie niechciane oprogramowanie. Microsoft nie pobiera opłat za aktualizacje sygnatur.

Dodatkowo ochrona programu Windows Defender w czasie rzeczywistym monitoruje krytyczne punkty systemu operacyjnego w celu wykrywania zmian zwykle dokonywanych przez programy szpiegowskie. Ochrona w czasie rzeczywistym skanuje każdy plik podczas jego otwierania, a także monitoruje folder Autostart, klucze Run w rejestrze, dodatki do systemu Windows i inne obszary systemu operacyjnego w celu wykrywania zmian. Jeśli aplikacja spróbuje dokonać zmiany w jednym z chronionych obszarów systemu operacyjnego, Windows Defender poprosi użytkownika o podjęcie odpowiedniego działania.

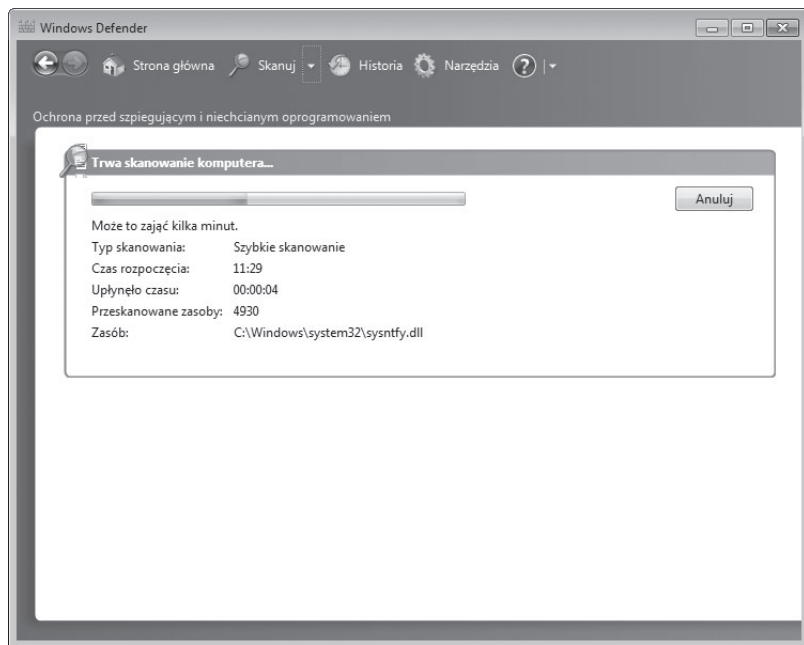
Jak pokazano na rysunku 2-4, Windows Defender może również uruchamiać skanowanie na żądanie, aby wykrywać i usuwać znane programy szpiegowskie. Domyślnie Windows Defender skanuje komputery z systemem Windows Vista codziennie o godzinie 2 w nocy w poszukiwaniu infekcji szkodliwym oprogramowaniem, ale można skonfigurować to zachowanie. Mimo że ochrona Windows Defender w czasie rzeczywistym próbuje zapobiec większości infekcji, nocne skanowanie pozwala temu programowi wykryć i usunąć

ostatnio odkryte szkodliwe oprogramowanie, które mogło obejść mechanizmy ochrony w czasie rzeczywistym.

Spółeczność Microsoft SpyNet umożliwia programowi Windows Defender zgłaszanie odkryć nowych aplikacji i ustalanie, czy użytkownicy określają te aplikacje jako szkodliwe, czy prawowite. W zależności od tego, jak skonfigurujemy program Windows Defender, może on przysyłać informacje zwrotne do społeczności SpyNet dotyczące nowych aplikacji i tego, czy użytkownicy pozwalają tym aplikacjom na instalację. Informacje zwrotne ze społeczności SpyNet pomagają firmie Microsoft i użytkownikom odróżniać szkodliwe oprogramowanie od prawowitego oprogramowania, co pozwala programowi Windows Defender dokładniej rozpoznawać szkodliwe oprogramowanie i ograniczyć liczbę fałszywych alarmów. Zapewnianie prywatnej komunikacji zwrotnej dla społeczności SpyNet jest opcjonalne; jednakże wszyscy użytkownicy mogą czerpać korzyści z informacji zebranych przez społeczność.

Oprócz tych funkcji Windows Defender zawiera Eksploratora oprogramowania. Eksplorator oprogramowania zapewnia użytkownikom kontrolę nad wieloma różnymi typami aplikacji, w tym aplikacjami, które instalują się w przeglądarce i w aplikacjach uruchamianych automatycznie. Eksplorator oprogramowania jest przeznaczony głównie dla użytkowników, którzy zarządzają swoimi komputerami. W środowiskach korporacyjnych zwykle departamenty IT zajmują się usuwaniem oprogramowania.

Windows Defender można również instalować w systemie Windows XP z SP2. Więcej informacji na temat programu Windows Defender można znaleźć w rozdziale 24 „Zarządzanie ochroną klienta”.



Rysunek 2-4 Użytkownicy, którzy podejrzewają, że szkodliwe oprogramowanie zainfekowało ich komputer, mogą uruchamiać skanowanie Windows Defender na żądanie.

Zapora systemu Windows

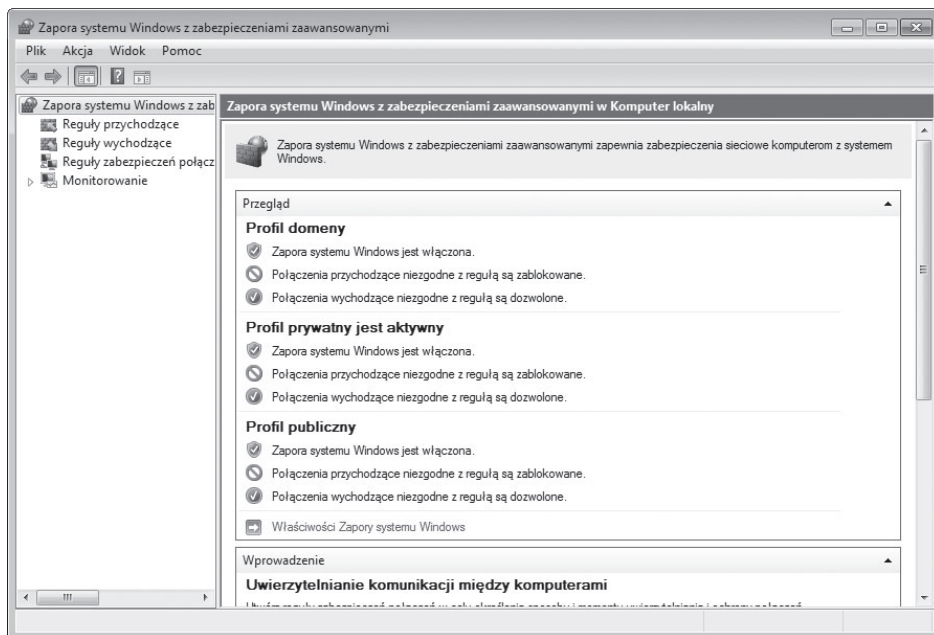
Systemy Windows Vista i Windows 7 mają ulepszoną wersję Zapory systemu Windows, która została po raz pierwszy dołączona do systemu Windows XP SP2. Zapora systemu Windows łączy funkcjonalność dwukierunkowej zapory programowej i protokołu Internet Protocol security (IPsec) w jednym, zunifikowanym narzędziu ze spójnym interfejsem użytkownika. W odróżnieniu od zapory obwodowej Zapora systemu Windows działa na każdym komputerze z systemem Windows Vista lub Windows 7 i zapewnia lokalną ochronę przed atakami sieciowymi, które mogą przedostać się przez sieć obwodową lub pochodzić z wewnątrz organizacji. Zapewnia również zabezpieczanie połączeń pomiędzy komputerami, które pozwala nam wymagać uwierzytelniania i ochrony danych w całej komunikacji.

Zapora systemu Windows jest w pełni stanową zaporą, więc bada i filtruje cały ruch w protokołach TCP/IP version 4 (IPv4) oraz TCP/IP version 6 (IPv6). Nieproszony ruch przychodzący jest odrzucany, o ile nie jest odpowiedzią na zapytanie ze strony komputera (ruch zamówiony) albo nie jest specjalnie dozwolony (to znaczy – został dodany do listy wyjątków lub jest dozwolony przez regułę ruchu przychodzącego). Ruch wychodzący z aplikacji interaktywnych jest domyślnie dozwolony, ale ruch wychodzący z usług jest ograniczony przez zaporę do tego, co jest wymagane zgodnie z profilem każdej usługi w Windows Service Hardening. Można określać ruch, który ma być dodawany do listy wyjątków i tworzyć reguły ruchu przychodzącego i wychodzącego opierające się na nazwie aplikacji, nazwie usługi, numerze portu, sieci docelowej, członkostwie domenowym lub innych kryteriach poprzez konfigurowanie ustawień Zapory systemu Windows z zabezpieczeniami zaawansowanymi.

Dla ruchu, który jest dozwolony, Zapora systemu Windows pozwala również żądać lub wymagać, aby komputery wzajemnie się uwierzytelniały przed nawiązaniem komunikacji i wykorzystywały techniki zachowywania spójności danych i szyfrowania danych podczas wymiany komunikatów.

W systemie Windows Vista Zapora systemu Windows ma wiele nowych funkcji, w tym następujące:

- **Integracja zarządzania z IPsec** Windows XP i wcześniejsze systemy operacyjne stosowały dwa oddzielne interfejsy, chociaż funkcje Zapory systemu Windows i protokołu IPsec w dużym stopniu się pokrywają. Teraz, jak widać na rysunku 2-5, możemy zarządzać obiema tymi funkcjami, korzystając z pojedynczego interfejsu.
- **Filtrowanie ruchu wychodzącego** Możemy filtrować ruch wysyłany z komputera klienckiego, jak również otrzymywany przez dany komputer. Pozwala to ograniczyć, które aplikacje mogą wysyłać dane i dokąd mogą je wysyłać. Na przykład moglibyśmy filtrować alarmy związane z zarządzaniem tak, aby mogły być wysyłane tylko do sieci wewnętrznej. Funkcja filtrowania ruchu wychodzącego w Zaporze systemu Windows nie ma za zadanie uniemożliwiania komunikacji z zainfekowanym komputerem, co jest raczej niemożliwe (szkodliwe oprogramowanie mogłoby po prostu wyłączyć zaporę). Filtrowanie ruchu wychodzącego pozwala raczej administratorom przypisywać zasady do komputerów, żeby zabraniać pewnych zachowań, na przykład uniemożliwiać komunikację nieautoryzowanemu oprogramowaniu peer-to-peer.



Rysunek 2-5 Możemy korzystać z pojedynczego narzędzia do zarządzania zarówno Zaporą systemu Windows, jak i protokołem IPsec.

- **Nowe interfejsy użytkownika i wiersza polecenia** Ulepszone interfejsy upraszczają zarządzanie i umożliwiają zautomatyzowaną kontrolę nad ustawieniami zapory.
- **Pełne wsparcie dla IPv6** Jeśli organizacja wykorzystuje protokół IPv6, możemy teraz korzystać z Zapory systemu Windows.
- **Windows Service Hardening** Ta funkcja ogranicza działania, jakie może podejmować usługa, a także ogranicza, jak dana usługa komunikuje się przez sieć, redukując szkody powodowane w przypadku naruszenia zabezpieczeń.
- **Pełna integracja z zasadami grupy** Ta funkcja pozwala centralnie konfigurować Zaporę systemu Windows na wszystkich komputerach w danej domenie Usług domenowych w usłudze Active Directory (AD DS).
- **Filtrowanie ruchu według nowych właściwości** Zapora systemu Windows może filtrować ruch korzystając z:
 - ❑ Grup AD DS (autoryzowani użytkownicy i autoryzowane komputery)
 - ❑ Rozszerzeń protokołu ICMP (Internet Control Message Protocol)
 - ❑ List adresów IP
 - ❑ List portów
 - ❑ Nazw usług
 - ❑ Uwierzytelniania przez IPsec
 - ❑ Szyfrowania przez IPsec
 - ❑ Typu interfejsu

- **Uwierzytelnianie adresu IP** Zapora systemu Windows obsługuje uwierzytelnianie adresu IP z możliwością dwóch rund uwierzytelniania z różnymi poświadczeniami w każdej, w tym poświadczeniami użytkownika.
- **Zasady IPsec oparte na aplikacjach** Zapora systemu Windows obsługuje teraz zasady IPsec oparte na aplikacjach.
- **Uproszczone zasady IPsec** Ten typ zasad znacznie ułatwia wdrażanie izolacji serwera i domen. W przypadku skonfigurowania z uproszczonymi zasadami komputery klienckie nawiązują dwa połączenia z miejscem docelowym: jedno niechronione połączenie i jedno połączenie z użyciem IPsec. Komputer kliencki odrzuci to połączenie, które nie uzyska odpowiedzi. Dzięki prostej regule komputery klienckie mogą więc przystosowywać się do komunikowania przy pomocy IPsec lub czystym tekstem, w zależności od tego, co jest obsługiwane po stronie docelowej.

Szczegółowe informacje na temat Zapory systemu Windows można znaleźć w rozdziale 26 „Konfigurowanie Zapory systemu Windows oraz IPsec”.

UWAGA Jednym z największych wyzwań związanych z ochroną komputerów jest to, że ustawienia zabezpieczeń mogą z czasem ulegać degradacji. Na przykład personel wsparcia technicznego mógłby zmienić ustawienia zabezpieczeń podczas rozwiązywania jakiegoś problemu, a później zapomnieć je poprawić. Nawet jeśli włączymy aktualizacje automatyczne, komputerowi mobilnemu może nie pójść o pobranie aktualizacji w razie utraty połączenia z siecią. Do pomocy w wykrywaniu luk zabezpieczeń można skorzystać z programu Microsoft Baseline Security Analyzer (MBSA) dostępnego pod adresem <http://www.microsoft.com/mbsa>. MBSA może sprawdzać ustawienia zabezpieczeń na wielu komputerach w sieci. MBSA jest też świetnym sposobem weryfikowania ustawień zabezpieczeń na nowych komputerach przed ich wdrożeniem.

Encrypting File System

Encrypting File System (EFS) jest technologią szyfrowania plików (obsługiwaną jedynie na woluminach NTFS), która chroni pliki przed atakami offline, takimi jak kradzież twardego dysku. EFS jest całkowicie przezroczysty dla użytkowników końcowych, ponieważ zaszyfrowane pliki zachowują się dokładnie, tak jak pliki niezasyfrowane. Jeśli jednak użytkownik nie ma poprawnego klucza odszyfrowującego, plików nie da się otworzyć, nawet jeśli napastnik obejdzie zabezpieczenia systemu operacyjnego.

EFS jest szczególnie przydatny do zabezpieczania poufnych danych na komputerach przenośnych lub na komputerach wykorzystywanych wspólnie przez kilku użytkowników. Oba rodzaje systemów są podatne na ataki technikami, które omijają ograniczenia list ACL. Napastnik może ukraść komputer, wyjąć napędy dysków twardych, umieścić je w innym systemie i uzyskać dostęp do przechowywanych na nich plików. Pliki zaszyfrowane przez EFS pojawiają się jednak jako nieczytelne znaki, gdy napastnik nie ma klucza odszyfrowującego.

Systemy Windows Vista i Windows 7 zawierają następujące nowe funkcje EFS:

- Przechowywanie klucza użytkownika i klucza odzyskiwania na kartach inteligentnych. Jeśli karty inteligentne są używane do logowania, EFS działa w trybie rejestracji jednokrotnej, w którym wykorzystuje kartę inteligentną logowania do szyfrowania plików bez dodatkowego zwracania się o numer PIN. Nowe kreatory kierują użytkowników przez proces tworzenia i wybierania kluczy kart inteligentnych, jak również przez proces migracji kluczy szyfrowania ze starej karty inteligentnej do nowej. Narzędzia wiersza polecenia dla kart inteligentnych zostały również ulepszone tak, aby zawierały te funkcje. Przechowywanie kluczy szyfrujących na kartach inteligentnych zapewnia szczególnie silną ochronę dla scenariuszy z komputerami mobilnymi i wspólnymi.
- Szyfrowanie pliku stronicowania systemu.

Więcej informacji na temat EFS można znaleźć w rozdziale 16.

Usprawnienia Menedżera poświadczeń

Systemy Windows Vista i Windows 7 zawierają nowe narzędzia umożliwiające administratorom lepsze wspieranie zarządzaniem poświadczeń dla przemieszczających się użytkowników, w tym usługi Digital Identity Management Services (DIMS), oraz nowy proces zamawiania certyfikatów. Wśród innych usprawnień użytkownicy mogą teraz zmieniać numery PIN na swoich kartach inteligentnych bez wzywania centrum wsparcia technicznego. Dodatkowo użytkownicy mogą teraz tworzyć i odzyskiwać kopie zapasowe poświadczeń przechowywanych w magazynie Stored User Names And Passwords.

Aby poprawić zabezpieczenia Harmonogramu zadań systemy Windows Vista i Windows 7 mogą wykorzystywać rozszerzenia Service-for-User (S4U) protokołu Kerberos do przechowywania poświadczeń dla zaplanowanych zadań zamiast przechowywania tych poświadczeń lokalnie, gdzie mogłyby zostać skompromitowane. Daje to dodatkową korzyść związaną z brakiem wpływu zasad wygasania haseł na zaplanowane zadania.

Usprawnienia zabezpieczeń architektonicznych i wewnętrznych

Gdzie to możliwe funkcje zabezpieczeń systemów Windows Vista i Windows 7 zostały zaprojektowane tak, aby były przezroczyste dla użytkowników końcowych i nie wymagały poświęcenia czasu przez administratora. Pomimo to administratorzy i programiści mogą czerpać korzyści ze zrozumienia usprawnień architektonicznych. Ta część rozdziału opisuje te usprawnienia architektoniczne i wewnętrzne, jak również usprawnienia, które wymagają dodatkowych aplikacji lub infrastruktury. Tabela 2-2 omawia te funkcje wprowadzone pierwotnie w systemie Windows Vista i zawarte również w systemie Windows 7.

Tabela 2-2 Usprawnienia architektonicznych i wewnętrznych zabezpieczeń w systemach Windows Vista i Windows 7

Usprawnienie	Opis
Integralność kodu	Wykrywa szkodliwe modyfikacje plików jądra podczas startu systemu.
Ochrona zasobów systemu Windows	Zapobiega potencjalnie niebezpiecznym zmianom w zasobach systemowych.

Tabela 2-2 Usprawnienia architektonicznych i wewnętrznych zabezpieczeń w systemach Windows Vista i Windows 7

Usprawnienie	Opis
Ochrona jądra	Blokuje potencjalnie szkodliwe zmiany, które mogłyby skompromitować spójność jądra w systemach 64-bitowych.
Wymagane podpisywanie sterowników	Wymaga, aby sterowniki były podpisane, co poprawia niezawodność i utrudnia dodawanie szkodliwych sterowników. Obowiązkowe w systemach 64-bitowych.
Hartowanie usług systemu Windows	Pozwala usługom systemowym na dostęp tylko do tych zasobów, z których normalnie muszą korzystać, co ogranicza skutki działania skompromitowanej usługi.
Klient NAP	W przypadku używania razem z systemem Windows Server 2008 pomaga chronić daną sieć przed klientami, którzy nie spełniają wymagań dotyczących zabezpieczeń.
Usługi WWW do zarządzania	Ogranicza ryzyka związane z zarządzaniem zdalnym poprzez obsługę szyfrowania i uwierzytelniania.
Usługi kryptograficzne nowej generacji	Pozwala dodawać niestandardowe algorytmy kryptograficzne spełniające wymagania rządowe.
Zapobieganie wykonywaniu danych	Ogranicza ryzyko ataków przepełnienia bufora poprzez oznaczanie obszarów pamięci z danymi jako niemożliwych do wykonywania.
Losowość układu przestrzeni adresowej	Ogranicza ryzyko ataków przepełnienia bufora poprzez przypisywanie kodu wykonywalnego do losowych lokalizacji w pamięci.
Nowa architektura logowania	Upraszcza tworzenie niestandardowych mechanizmów logowania.
Klient usług zarządzania prawami	Zapewnia obsługę otwierania dokumentów chronionych przez usługi zarządzania prawami, gdy odpowiednie aplikacje są zainstalowane i dostępna jest konieczna infrastruktura.
Wiele lokalnych obiektów zasad grupy	Pozwala administratorom stosować wiele lokalnych obiektów zasad grupy na pojedynczym komputerze, co upraszcza zarządzanie konfiguracją zabezpieczeń dla komputerów w grupie roboczej.

Poniższe podrozdziały opisują te funkcje bardziej szczegółowo.

Integralność kodu

Gdy system Windows się uruchamia, integralność kodu (CI) weryfikuje, że pliki systemowe nie zostały w sposób szkodliwy zmodyfikowane i zapewnia, że nie ma żadnych niepodpisanych sterowników działających w trybie jądra. Program rozruchowy sprawdza integralność jądra, warstwy abstrakcji sprzętowej (HAL) i sterowników rozruchowych. Po tym, te pliki zostaną zweryfikowane, integralność kodu sprawdza podpisy cyfrowe wszelkich elementów

binarnych, które są ładowane do obszaru pamięci jądra. Dodatkowo integralność kodu sprawdza elementy binarne ładowane w chronionych procesach oraz dynamicznie dołączane biblioteki kryptograficzne.

Integralność kodu działa automatycznie i nie wymaga zarządzania.

UWAGA Integralność kodu jest przykładem działań wykrywających, ponieważ może stwierdzić po fakcie, że komputer został skompromitowany. Chociaż zawsze lepiej jest zapobiegać atakom, środki wykrywające, takie jak integralność kodu, pozwalają ograniczyć szkody powodowane przez atak dzięki wykrywaniu naruszeń, co pomaga nam naprawić komputer. Powinniśmy mieć zawsze przygotowany plan reakcji umożliwiający szybką naprawę systemu, w którym zostały skompromitowane krytyczne pliki.

Ochrona zasobów systemu Windows

Wszelki kod, który działa w trybie jądra, w tym wiele typów sterowników, może potencjalnie uszkodzić dane jądra w sposób, który ujawni się dopiero później. Diagnostowanie i naprawianie tych błędów może być trudne i czasochłonne. Uszkodzenie rejestru zwykle ma niewspółmierny wpływ na ogólną niezawodność, ponieważ to uszkodzenie może przetrwać ponowny rozruch systemu.

Systemy Windows Vista i Windows 7 chronią ustawienia systemowe przed uszkodzeniami lub nieumyślnymi zmianami, które mogą powodować, że system będzie działał nieprawidłowo lub nie będzie działał w ogóle. Ochrona zasobów systemu Windows (WRP), funkcja będąca następcą funkcji ochrony plików systemu Windows (WFP) dostępnej w poprzednich wersjach Windows, ustawia ściśle listy kontroli dostępu (ACL) dla krytycznych ustawień systemowych, plików i folderów, aby chronić je przed zmianami przez dowolne źródła (włączając w to administratorów), z wyjątkiem zaufanych instalatorów. Uniemożliwia to użytkownikom przypadkową zmianę krytycznych ustawień systemowych, które mogą sprawić, że system nie będzie się nadawał do użytku.

Systemy Windows Vista i Windows 7 również uniemożliwiają źle napisanym sterownikom uszkodzenie rejestru. Ta ochrona pozwala na zabezpieczanie funkcji zarządzania pamięcią przez większość czasu przy niskich kosztach. Do chronionych zasobów należą:

- Pliki wykonywalne, biblioteki i inne krytyczne pliki instalowane przez system Windows.
- Krytyczne foldery.
- Podstawowe klucze rejestru instalowane przez system Windows.

Ochrona zasobów systemu Windows nie pozwala modyfikować chronionych zasobów, nawet jeśli podamy poświadczenia administracyjne.

Ochrona jądra

64-bitowe wersje systemów Windows Vista i Windows 7, podobnie jak 64-bitowe wersje systemów Windows XP i Windows Server 2003, obsługują technologię *Ochrony jądra*. Ochrona jądra uniemożliwia nieautoryzowanym programom modyfikowanie jądra systemu

Windows, co daje większą kontrolę nad podstawowymi aspektami systemu, które mogą wpływać na ogólną wydajność, bezpieczeństwo i niezawodność. Ochrona jądra wykrywa zmiany w krytycznych fragmentach pamięci jądra. Jeśli zmiana zostanie dokonana w nieobsługiwany sposób (na przykład aplikacja trybu użytkownika nie wywoła odpowiednich funkcji systemu operacyjnego), ochrona jądra utworzy błąd stopu w celu zatrzymania systemu operacyjnego. Uniemożliwia to sterownikom trybu jądra rozszerzanie lub zastępowanie innych usług jądra i uniemożliwia oprogramowaniu firm trzecich aktualizowanie dowolnych części jądra.

W szczególności, aby ochrona jądra nie generowała błędów stopu, 64-bitowe sterowniki muszą unikać następujących praktyk:

- Modyfikowania tabel usług systemowych
- Modyfikowania tabeli opisów przerwań (IDT)
- Modyfikowania tabeli deskryptorów globalnych (GDT)
- Używania stosów jądra, które nie są alokowane przez jądro
- Aktualizowania dowolnej części jądra w systemach opartych na AMD64

W praktyce czynniki te są głównie istotne dla programistów sterowników. Nie powinien zostać nigdy wydany żaden sterownik 64-bitowy, który mógłby powodować problemy z ochroną jądra, więc administratorzy nigdy nie powinni zarządzać lub rozwiązywać problemów z ochroną jądra. Szczegółowe informacje można znaleźć w artykule „An Introduction to Kernel Patch Protection” pod adresem <http://blogs.msdn.com/windowsvistasecurity/archive/2006/08/11/695993.aspx>.

UWAGA Ochrona jądra, oparte na sprzęcie zapobieganie wykonywaniu danych (DEP) i wymagane podpisywanie sterowników są głównymi powodami, dla których systemy 64-bitowe mogą być bezpieczniejsze niż 32-bitowe.

Wymagane podpisywanie sterowników

Sterowniki zwykle działają jako część jądra, co daje im niemal nieograniczony dostęp do zasobów systemowych. W efekcie sterowniki, które mają błędy lub są źle napisane, albo szkodliwe sterowniki specjalnie napisane w celu nadużywania tych uprawnień mogą znacząco wpływać na niezawodność i bezpieczeństwo komputera.

Aby pomóc ograniczyć wpływ sterowników, firma Microsoft wprowadziła podpisywanie sterowników począwszy od systemu Microsoft Windows 2000. Podpisane sterowniki mają podpis cyfrowy, który wskazuje, że zostały zatwierdzone przez firmę Microsoft i najprawdopodobniej są pozbawione znaczących uchybień, które mogłyby wpłynąć na niezawodność systemu. Administratorzy mogą konfigurować Windows 2000 i późniejsze systemy operacyjne, aby blokować wszystkie niepodpisane sterowniki, co może znacząco obniżyć ryzyko problemów związanych ze sterownikami.

Jednakże duża liczba niepodpisanych sterowników 32-bitowych sprawiała, że blokowanie niepodpisanych sterowników było niepraktyczne dla większości organizacji. W rezultacie większość istniejących komputerów z systemem Windows pozwala na instalowanie niepodpisanych sterowników.

W przypadku 64-bitowych wersji systemów Windows Vista i Windows 7 wszystkie sterowniki poziomu jądra muszą być podpisane cyfrowo. Moduł jądra, który jest uszkodzony lub został poddany manipulacji, nie zostanie załadowany. Wszelkie sterowniki, które nie są prawidłowo podpisane, nie mogą sięgać do obszaru jądra i nie zostaną załadowane. Chociaż podpisany sterownik nie daje gwarancji bezpieczeństwa, pomaga identyfikować i zapobiegać wielu szkodliwym atakom, pozwalając przy tym firmie Microsoft pomagać programistom w poprawieniu ogólnej jakości sterowników i ograniczeniu liczby zawiesznień komputera związanych ze sterownikami.

Wymagane podpisywanie sterowników pomaga również poprawić niezawodność systemów Windows Vista i Windows 7, ponieważ wiele zawiesznień systemu wynika z luk w sterownikach trybu jądra. Wymaganie od autorów tych sterowników, aby się identyfikowali, ułatwia firmie Microsoft określanie przyczyn zawiesznień systemu i współpracę z producentem odpowiedzialnym za dany sterownik w celu rozwiązania problemu. Administratorzy systemowi mogą również czerpać korzyści z cyfrowo podpisanych i identyfikowanych sterowników, ponieważ uzyskują dodatkowy wgląd w stan magazynu oprogramowania i instalacji na komputerach klienckich. Z perspektywy zgodności sterowniki jądra x64 certyfikowane przez laboratoria jakości sprzętowej firmy Microsoft są uważane za prawidłowo podpisane w systemach Windows Vista i Windows 7.

Hartowanie usług systemu Windows

Historycznie wiele sieciowych ataków na system Windows (zwłaszcza robaków) wynikało z wykorzystywania przez napastników luk w usługach systemu. Ponieważ wiele usług systemu Windows nasłuchuje połączeń przychodzących i często ma uprawnienia na poziomie systemu, luka może pozwolić napastnikowi wykonywać zadania administracyjne na komputerze zdalnym.

Hartowanie usług systemu Windows, funkcja systemów Windows Vista i Windows 7, ogranicza wszystkim usługom systemu Windows wykonywanie nietypowych działań w systemie plików, rejestrze, sieci lub innych zasobach, które mogą być wykorzystane do zezwolenia na zainstalowanie szkodliwego oprogramowania lub zaatakowania innych komputerów. Na przykład usługa Zdalne wywoływanie procedur (RPC) jest ograniczona do wykonywania komunikacji sieciowej tylko na określonych portach, co eliminuje możliwość niewłaściwego jej wykorzystania na przykład do zamiany plików systemowych lub zmodyfikowania rejestru (jak robił to robak Blaster). Zasadniczo Hartowanie usług systemu Windows wymusza stosowanie pojęcia najmniejszych uprawnień dla usług, nadając im tylko tyle uprawnień, aby mogły wykonywać swoje wymagane zadania.

UWAGA Hartowanie usług systemu Windows zapewnia dodatkową warstwę ochrony dla usług opierających się na zasadzie dogłębnej obrony. Hartowanie usług systemu Windows nie może zapobiec kompromitacji wadliwej usługi – co jest zadaniem wspieranym przez Zaporę systemu Windows i aktualizacje automatyczne. Zamiast tego Hartowanie usług systemu Windows ogranicza ile zniszczeń może dokonać napastnik w przypadku, gdy będzie w stanie zidentyfikować i wykorzystać podatną usługę.

Hartowanie usług systemu Windows ogranicza potencjał zniszczeń ze strony skompromitowanej usługi poprzez:

- Wprowadzenie identyfikatora zabezpieczeń dla każdej usługi (SID) w celu jednoznacznego identyfikowania usług, co z kolei umożliwia partycjonowanie kontroli dostępu poprzez istniejący model kontroli dostępu w systemie Windows obejmujący wszystkie obiekty i menedżerów zasobów wykorzystując listy ACL. Usługi mogą teraz stosować bezpośrednie listy ACL wobec zasobów, które są prywatne dla usługi, co zapobiega dostępowi do zasobu ze strony innych usług oraz użytkowników.
- Przeniesienie usług z konta LocalSystem do mniej uprzywilejowanego konta, takiego jak LocalService lub NetworkService w celu ograniczenia poziomu uprawnień dla danej usługi.
- Ograniczanie niepotrzebnych uprawnień systemu Windows dla poszczególnych usług – na przykład możliwości debugowania.
- Stosowanie znacznika z ograniczonym zapisem wobec usług, które uzyskują dostęp do ograniczonego zbioru plików i innych zasobów tak, aby ta usługa nie mogła aktualizować innych aspektów systemu.
- Przypisywanie zasad zapory sieciowej do usług w celu uniemożliwiania dostępu sieciowego poza normalnymi granicami programu usługi. Zasady zapory są połączone bezpośrednio z identyfikatorem SID usługi i nie mogą być uchylane ani zwalniane przez wyjątki lub reguły definiowane przez użytkownika lub administratora.

Konkretnym celem hartowania usług systemu Windows jest unikanie wprowadzania złożoności zarządzania dla użytkowników i administratorów systemowych. Każda usługa zawarta w systemie Windows Vista i Windows 7 przeszła wnikliwy proces w celu zdefiniowania jej profilu hartowania usług systemu Windows, który jest automatycznie stosowany podczas instalowania systemu Windows i nie wymaga bieżącej administracji, konserwacji lub interakcji ze strony użytkownika końcowego. Z tych powodów nie ma interfejsu administracyjnego do zarządzania hartowaniem usług systemu Windows. Więcej informacji na temat hartowania usług systemu Windows można znaleźć w rozdziale 26.

UWAGA Twórcy oprogramowania zewnętrznego mogą również korzystać z zabezpieczeń hartowania usług systemu Windows, zapewniając profile dla swoich usług.

Klient NAP

Większość sieci ma zapory zewnętrzne pomagające chronić sieć wewnętrzną przed robakami, wirusami i innymi napastnikami. Jednakże napastnicy mogą spenetrować naszą sieć poprzez połączenia dostępu zdalnego (takie jak VPN) lub zarażając komputer mobilny, a następnie rozprzestrzeniając się na inne komputery wewnętrzne po połączeniu komputera mobilnego z naszą siecią LAN.

Systemy Windows Vista i Windows 7 podczas przyłączania do infrastruktury Windows Server 2008 wykorzystują ochronę Network Access Protection (NAP) w celu ograniczania ryzyka związanego z wejściem napastnika poprzez dostęp zdalny i połączenia LAN, stosując

wbudowane oprogramowanie klienta NAP. Jeśli komputer kliencki Windows nie ma bieżących aktualizacji zabezpieczeń albo sygnatur antywirusowych lub w inny sposób nie spełnia wymagań dla zdrowego komputera, system NAP może zablokować temu komputerowi dostęp do sieci wewnętrznej.

Jeśli jednak komputer nie będzie spełniał wymagań potrzebnych, aby dołączyć się do sieci, użytkownik nie musi czuć się sfrustrowany. Komputery klienckie mogą być kierowane do odizolowanej kwarantanny sieciowej w celu pobrania aktualizacji, sygnatur antywirusowych lub ustawień konfiguracyjnych niezbędnych dla zgodności z zasadami wymaganymi w sieci. W ciągu paru minut potencjalnie podatny na ataki komputer może zostać zabezpieczony i znowu uzyskać zezwolenie na połączenie z siecią.

NAP jest rozszerzalną platformą, która zapewnia infrastrukturę oraz interfejs programowania aplikacji (API) dla wymuszania zasad dotyczących stanu komputerów. Niezależni sprzedawcy sprzętu i oprogramowania mogą dołączać swoje rozwiązania zabezpieczeń do NAP tak, aby administratorzy IT mogli wybierać rozwiązania zabezpieczeń, które spełniają ich potrzeby. NAP pomaga zapewnić, aby każdy komputer w sieci w pełni wykorzystywał te niestandardowe rozwiązania.

Firma Microsoft wyda też obsługę klienta NAP z Windows XP SP3. Więcej informacji na temat NAP można znaleźć pod adresem <http://www.microsoft.com/nap/>.

Usługi WWW do zarządzania

Usługi WWW do zarządzania (WS-Management) ułatwiają zdalne zarządzanie systemem Windows Vista i Windows 7. WS-Management (będący przemysłowym standardem protokołów usług WWW do chronionego zdalnego zarządzania sprzętem i oprogramowaniem) razem z odpowiednimi narzędziami programowymi pozwala administratorom zdalnie uruchamiać skrypty i wykonywać inne zadania zarządcze. W systemach Windows Vista i Windows 7 komunikacja może być zarówno szyfrowana, jak i uwierzytelniana, co ogranicza ryzyko. Narzędzia zarządzające firmy Microsoft, takie jak Systems Center Configuration Manager 2007, wykorzystują WS-Management do zapewniania bezpiecznego zarządzania zarówno sprzętem, jak i oprogramowaniem.

Usługi kryptograficzne nowej generacji

Kryptografia jest krytyczną funkcją usług uwierzytelniania i autoryzacji w systemie Windows, która wykorzystuje kryptografię do szyfrowania, funkcji skrótów i podpisów cyfrowych. Systemy Windows Vista i Windows 7 dostarczają usługi kryptograficzne nowej generacji (CNG), które są wymagane przez wiele rządów i organizacji. Usługi CNG pozwalają na dodawanie nowych algorytmów do systemu Windows w celu wykorzystania w protokołach Secure Sockets Layer/Transport Layer Security (SSL/TLS) i IPsec. Systemy Windows Vista i Windows 7 zawierają również nowy procesor zabezpieczeń pozwalający na zaufane decyzje dotyczące usług, na przykład przy zarządzaniu uprawnieniami.

W przypadku organizacji, które muszą wykorzystywać określone algorytmy kryptograficzne i zatwierdzone biblioteki, usługi CNG są absolutnie wymagane.

Zapobieganie wykonywaniu danych

Jedną z najczęściej stosowanych technik wykorzystywania luk w oprogramowaniu jest atak przepełnienia bufora. Przepełnienie bufora następuje, kiedy aplikacja próbuje zapisać zbyt wiele danych w buforze i zostaje nadpisana pamięć, która nie została zaalokowana dla tego bufora. Napastnik może być w stanie celowo wywołać przepełnienie bufora poprzez wprowadzenie większej ilości danych, niż tego oczekuje aplikacja. Szczególnie przebiegły napastnik może nawet wprowadzić dane, które nakażą systemowi operacyjnemu uruchomienie szkodliwego kodu wprowadzonego przez napastnika z uprawnieniami danej aplikacji.

Jednym z dobrze znanych ataków używających przepełnienia bufora był robak CodeRed, który wykorzystywał lukę w aplikacji Index Server Internet Server Application Programming Interface (ISAPI) dostarczanej jako część wcześniejszej wersji usług Microsoft Internet Information Services (IIS) do uruchamiania szkodliwego oprogramowania. Niszczące działanie robaka CodeRed było ogromne, a można było mu zapobiec dzięki zastosowaniu zapobiegania wykonywaniu danych (DEP).



Rysunek 2-6 Możemy włączać lub wyłączać DEP w oknie dialogowym Opcje wydajności lub z poziomu ustawień zasad grupy.

DEP oznacza fragmenty pamięci jako zawierające albo dane, albo kod aplikacji. System operacyjny nie uruchomi kodu zawartego w pamięci oznaczonej jako dane. Dane wprowadzane przez użytkownika i otrzymywane przez sieć powinny być zawsze zapisywane jako dane i dlatego nie mogą być stosowane do uruchamiania jako aplikacja.

32-bitowe wersje systemów Windows Vista i Windows 7 zawierają programową implementację DEP, która może zapobiegać uruchamianiu kodu z pamięci nieprzeznaczonej do wykonywania. 64-bitowe wersje systemów Windows Vista i Windows 7 współpracują z funkcjami DEP wbudowanymi w procesory 64-bitowe do wymuszania tych zabezpieczeń w warstwie sprzętowej, gdzie bardzo trudno jest je obejść napastnikowi.

UWAGA DEP zapewnia ważną warstwę zabezpieczeń do ochrony przed szkodliwym oprogramowaniem. Jednakże rozwiązanie to musi być stosowane razem z innymi technologiami, takimi jak Windows Defender, aby zapewniać wystarczającą ochronę spełniającą wymagania biznesowe.

Funkcja DEP jest domyślnie włączona zarówno w 32-bitowych, jak i 64-bitowych wersjach systemów Windows Vista i Windows 7. Domyślnie DEP chroni tylko podstawowe programy i usługi systemu Windows, aby zapewniać optymalną zgodność. W celu uzyskania dodatkowych zabezpieczeń możemy chronić wszystkie programy i usługi.

Losowość układu przestrzeni adresowej

Losowość układu przestrzeni adresowej (ASLR) jest kolejną opcją obronną w systemach Windows Vista i Windows 7, która utrudnia szkodliwemu kodowi atak na funkcję systemową. Gdy komputer z systemem Windows Vista lub Windows 7 jest ponownie uruchamiany, funkcja ASLR losowo przypisuje obrazy wykonywalne (pliki .dll i .exe) załączone jako część systemu operacyjnego do jednej z wielu możliwych lokalizacji w pamięci. Utrudnia to szkodliwemu kodowi lokalizowanie i tym samym wykorzystywanie funkcjonalności zawartej wewnątrz tych plików wykonywalnych.

Systemy Windows Vista i Windows 7 zawierają również usprawnienia w funkcji wykrywania przepełnienia bufora sterty, które są jeszcze bardziej rygorystyczne niż wprowadzone w systemie Windows XP SP2. Gdy zostaną wykryte oznaki naruszenia bufora sterty, system operacyjny może natychmiast zakończyć dany program, ograniczając zniszczenia, które mogłyby wynikać z tego naruszenia. Ta technologia ochrony jest włączona dla funkcji systemu operacyjnego, w tym wbudowanych usług systemowych i może też być wykorzystywana przez niezależnych dostawców oprogramowania (ISV) poprzez pojedyncze wywołanie API.

Nowa architektura logowania

Logowanie do systemu Windows zapewnia dostęp do zasobów lokalnych (w tym do plików zaszyfrowanych przez EFS), a w środowiskach AD DS również dostęp do chronionych zasobów sieciowych. Wiele organizacji wymaga więcej niż tylko nazwy użytkownika i hasła do uwierzytelniania użytkowników. Na przykład mogą wymagać wieloczynnikowego uwierzytelniania przy użyciu zarówno hasła, jak i identyfikacji biometrycznej albo klucza haseł jednorazowych.

W systemie Windows XP i wcześniejszych wersjach systemu Windows implementacja niestandardowych metod uwierzytelniania wymagała od programistów pełnego przepisania interfejsu Graphical Identification and Authentication (GINA). Wymagany wysiłek często nie był uzasadniony korzyściami zapewnianymi przez silne uwierzytelnianie i taki projekt porzucano. Ponadto system Windows XP obsługiwał tylko pojedynczy interfejs GINA.

W systemach Windows Vista i Windows 7 programiści mogą teraz zapewniać niestandardowe metody uwierzytelniania poprzez tworzenie nowych dostawców poświadczeń. Wymaga to znacznie mniej wysiłku programistycznego, pozwalając większej liczbie organizacji oferować niestandardowe metody uwierzytelniania.

Ta nowa architektura pozwala również na sterowanie dostawców poświadczeń zdanieniami i integrowanie w środowisku użytkownika. Na przykład ten sam kod używany

do implementowania schematu uwierzytelniania przez odciski palców na ekranie logowania systemu Windows może być też używany do zwracania się do użytkownika o przedstawienie odcisków palców podczas dostępu do określonych zasobów korporacyjnych. Ta sama prośba może być też używana przez aplikacje, które wykorzystują nowy interfejs API dla poświadczeń.

Dodatkowo interfejs logowania użytkownika w Windows może wykorzystywać jednocześnie wielu dostawców poświadczeń, zapewniając większą elastyczność dla środowisk, które mogłyby mieć różne wymagania dotyczące poświadczeń dla różnych użytkowników.

Usługi zarządzania prawami

Usługi zarządzania prawami (RMS) w systemie Windows są technologią ochrony informacji, która współpracuje z aplikacjami obsługującymi RMS, żeby pomagać w ochronie informacji cyfrowej przed nieautoryzowanym wykorzystaniem zarówno wewnątrz jak i poza daną siecią prywatną. Usługi RMS zapewniają trwale zasady użycia (znane również jako prawa i warunki użytkowania), które pozostają obowiązujące dla danego pliku, niezależnie od tego, gdzie ten plik trafi. Usługi RMS trwale chronią wszelkie binarne formaty danych tak, aby prawa użytkownika pozostawały powiązane z daną informacją – nawet podczas transportu – a nie obowiązywały jedynie w sieci danej organizacji.

Usługi RMS działają poprzez szyfrowanie dokumentów, a następnie zapewnianie kluczy odszyfrowujących jedynie autoryzowanym użytkownikom, korzystającym z zatwierdzonego klienta RMS. Aby klient RMS mógł być zatwierdzony, musi wymuszać prawa użytkownika przypisane do dokumentu. Na przykład, jeśli właściciel dokumentu określił, że zawartość dokumentu nie może być kopiowana, przekazywana dalej lub drukowana, klient RMS nie pozwoli użytkownikowi na podjęcie tych działań.

W systemach Windows Vista i Windows 7 usługi RMS są teraz zintegrowane z formatem XPS. XPS jest otwartym, międzyplatformowym formatem dokumentów, który pomaga klientom bez wysiłku tworzyć, udostępniać, drukować, archiwizować i chronić bogate cyfrowe dokumenty. Dzięki sterownikowi drukarki generującemu XPS każda aplikacja może tworzyć dokumenty XPS, które mogą być chronione przez usługi RMS. Podstawowa funkcjonalność znacząco rozszerza zakres informacji, które mogą być chronione przez usługi RMS.

System Microsoft Office 2007 zapewnia jeszcze głębszą integrację z usługami RMS poprzez nowe opcje w Microsoft SharePoint. Administratorzy SharePoint mogą ustawiać zasady dostępu dla bibliotek dokumentów SharePoint dla poszczególnych użytkowników, które będą dziedziczone przez zasady RMS. Oznacza to, że użytkownicy, którzy mają prawa „tylko do przeglądania” podczas dostępu do zawartości, będą mieli te prawa „tylko do przeglądania” (bez drukowania, kopiowania lub wklejania) wymuszone przez RMS, nawet kiedy dokument zostanie pobrany z witryny SharePoint. Klienci korporacyjni mogą ustawiać zasady użytkownika, które są wymuszane nie tylko wtedy, gdy dokument jest na miejscu, ale również wtedy, gdy informacja znajdzie się poza bezpośrednią kontrolą przedsiębiorstwa.

Chociaż funkcje usług RMS są wbudowane w systemy Windows Vista i Windows 7, mogą być używane jedynie z infrastrukturą zarządzania prawami oraz aplikacją, która obsługuje usługi RMS, taką jak Microsoft Office. Klient usług RMS może być też instalowany w systemie Windows 2000 i późniejszych systemach operacyjnych. Więcej informacji na temat korzystania z usług RMS można znaleźć pod adresem <http://www.microsoft.com/rms>.

Wiele lokalnych obiektów zasad grupy

Jako administratorzy możemy teraz stosować wiele lokalnych obiektów zasad grupy na pojedynczym komputerze. Upraszcza to zarządzanie konfiguracją, ponieważ możemy tworzyć osobne obiekty zasad grupy dla różnych ról i stosować je pojedynczo tak samo, jak możemy to robić z obiektami zasad grupy AD DS. Na przykład moglibyśmy mieć obiekt zasad grupy dla komputerów będących członkami grupy Marketing i osobny obiekt zasad grupy dla komputerów mobilnych. Jeśli trzeba by było skonfigurować komputer mobilny dla członka grupy Marketing, moglibyśmy po prostu zastosować oba lokalne obiekty zasad grupy zamiast tworzyć pojedynczy obiekt zasad grupy łączący w sobie wszystkie ustawienia.

Nowe i poprawione funkcje zabezpieczeń Windows 7

Ten podrozdział opisuje najbardziej widoczne i namacalne usprawnienia zabezpieczeń Windows 7, które są wymienione w tabeli 2-3. Usprawnienia architektoniczne i wewnętrzne – jak również usprawnienia, które wymagają dodatkowych aplikacji lub infrastruktury – zostały opisane w dalszej części rozdziału.

Tabela 2-3 Usprawnienia zabezpieczeń Windows 7

Usprawnienie	Opis
BitLocker i BitLocker To Go	Szyfruje całe woluminy w tym woluminy systemowe, niesystemowe i napędy wymienne.
AppLocker	Zapewnia elastyczną kontrolę nad tym, które aplikacje mogą być uruchamiane przez użytkowników.
Wiele aktywnych profili zapory	Zapewnia różne profile zapory dla fizycznych kart sieciowych i wirtualnych kart sieciowych używanych przez sieci VPN.
Kontrola konta użytkownika	Daje standardowym użytkownikom możliwość podawania poświadczeń administracyjnych, gdy są one wymagane przez system operacyjny. W przypadku administratorów domyślnie uruchamia procesy ze standardowymi uprawnieniami i prosi administratora o potwierdzenie przed udzieleniem procesowi uprawnień administracyjnych.
Funkcje zabezpieczeń programu Internet Explorer	Ogranicza ryzyko ataków wyłudzenia informacji (phishing) i szkodliwego oprogramowania podczas przeglądania stron WWW przez użytkowników.
Usprawnienia Inspekcji	Zapewnia dokładniejszą kontrolę nad tym, które zdarzenia są śledzone.
Bezpieczne odłączanie w puli jądra	Ogranicza ryzyko ataków związanych z przekroczeniem bufora.

Tabela 2-3 Usprawnienia zabezpieczeń Windows 7

Usprawnienie	Opis
Windows Biometric Framework	Zapewnia spójny interfejs dla skanerów linii papilarnych.
Karty inteligentne	Zapewnia standardowy interfejs sterownika kart inteligentnych.
Konta usług	Umożliwia administratorom tworzenie kont dla usług bez potrzeby zarządzania hasłami kont usług.

Dalsze części tego rozdziału opisują te funkcje bardziej szczegółowo.

BitLocker i BitLocker To Go

Korzystając z szyfrowania dysków funkcją BitLocker, organizacje mogą ograniczać ryzyko utraty poufnych danych w przypadku kradzieży mobilnego komputera użytkownika. Opcja szyfrowania pełnego woluminu zabezpiecza symetryczny klucz szyfrowania w układzie Trusted Platform Module (TPM) 1.2 (dostępnym w niektórych nowszych komputerach) lub na dysku USB. Funkcja BitLocker ma cztery tryby TPM:

- **Tylko TPM** Jest to tryb przezroczysty dla użytkownika, a funkcjonalność logowania użytkownika pozostaje bez zmian. Jednakże jeśli moduł TPM będzie nieobecny lub zostanie zmieniony, funkcja BitLocker przejdzie do trybu naprawy i będzie potrzebować klucza odzyskiwania lub numeru PIN do ponownego uzyskania dostępu do danych. Zapewnia to ochronę przed kradzieżą twardego dysku, nie wymagając przy tym szkolenia użytkowników.
- **TPM z kluczem startowym** Użytkownik będzie też musiał podać klucz startowy, aby uruchomić system Windows. Klucz startowy może być albo fizyczny (napęd USB z zapisanym na nim kluczem), albo osobisty (hasło ustawiane przez użytkownika). Zapewnia to ochronę zarówno przed kradzieżą twardego dysku, jak i komputera (przy założeniu, że komputer był wyłączony lub zablokowany); jednakże wymaga pewnego wysiłku od użytkownika.
- **TPM z numerem PIN** Użytkownik będzie też musiał wpisać numer PIN, aby uruchomić system Windows. Podobnie jak wymaganie klucza startowego, zapewnia to ochronę zarówno przed kradzieżą twardego dysku, jak i komputera (przy założeniu, że komputer był wyłączony lub zablokowany); jednakże wymaga pewnego wysiłku od użytkownika.
- **TPM z numerem PIN i kluczem startowym** Użytkownik będzie musiał wpisać numer PIN i udostępnić klucz startowy, aby uruchomić system Windows.

UWAGA Na potrzeby zarządzania układami TPM system Windows 7 zawiera przystawkę Zarządzanie TPM.

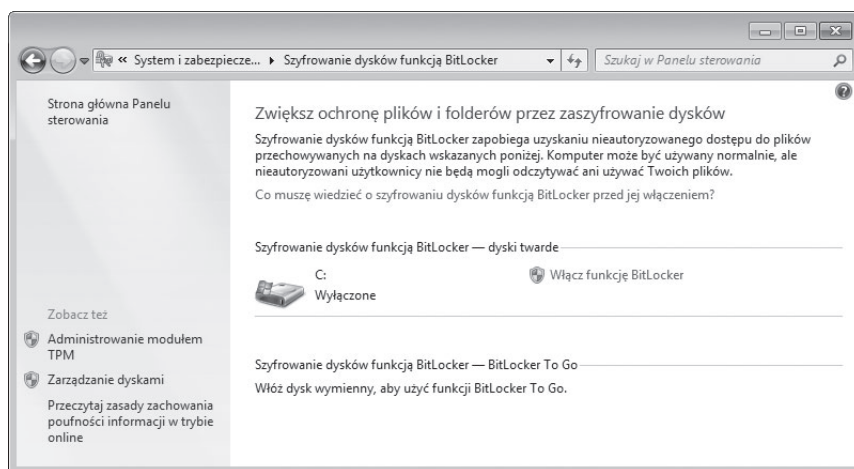
BitLocker działa, zachowując pomiary różnych elementów komputera i systemu operacyjnego w układzie TPM. W konfiguracji domyślnej BitLocker nakazuje funkcji TPM mierzyć główny rekord rozruchowy, aktywną partycję rozruchową, sektor rozruchowy, zarządzanie

rozruchem systemu Windows oraz klucz główny magazynowania danych w funkcji BitLocker. Za każdym razem, gdy komputer jest uruchamiany, TPM oblicza funkcję skrótu SHA-1 dla mierzonego kodu i porównuje ją ze skrótem zapisanym w układzie TPM przy poprzednim uruchamianiu systemu. Jeśli skróty pasują do siebie, proces uruchamiania jest kontynuowany; jeśli skróty nie pasują, proces uruchamiania zostanie wstrzymany. Na końcu udanego procesu uruchamiania TPM zwalnia główny klucz magazynowania danych dla funkcji BitLocker; BitLocker odszyfrowuje dane w trakcie ich odczytywania przez system Windows z chronionego woluminu.

BitLocker chroni system Windows przed atakami offline. Atak offline jest scenariuszem, w którym napastnik uruchamia inny system operacyjny, aby przejąć kontrolę nad komputerem. Moduł TPM zwalnia główny klucz magazynu danych tylko wtedy, gdy nakaze mu to funkcja BitLocker działająca w wystąpieniu systemu Windows, które pierwotnie utworzyło ten klucz. Ponieważ żaden inny system operacyjny nie może tego zrobić (nawet inne wystąpienie systemu Windows), moduł TPM nigdy nie zwolni klucza i dlatego wolumin pozostanie bezużytecznym zaszyfrowanym zbiorem danych. Wszelkie próby modyfikacji chronionego woluminu sprawią, że nie będzie się dało uruchomić z niego systemu.

UWAGA Przed zestawem SP1 szyfrowanie dysków funkcją BitLocker mogło chronić tylko partycję systemu Windows. Przed SP1 do ochrony innych partycji można było korzystać z EFS. Po zainstalowaniu SP1 możemy korzystać z szyfrowania dysków funkcją BitLocker, aby zaszyfrować dowolną partycję. Jednakże nadal możemy korzystać z EFS do ochrony danych, gdy wielu użytkowników korzysta z tego samego komputera.

Jak pokazano na rysunku 2-7, poszczególni użytkownicy mogą włączać funkcję BitLocker z Panelu sterowania. Większość przedsiębiorstw powinna jednak wykorzystywać usługi AD DS do zarządzania kluczami.



Rysunek 2-7 Możemy włączać funkcję BitLocker z Panelu sterowania.

Wymagania związane z zarządzaniem kluczami i odzyskiwaniem danych są głównymi powodami, dla których funkcja BitLocker jest skierowana do przedsiębiorstw. Tak jak w przypadku dowolnego rodzaju szyfrowania, jeśli zgubimy klucz, utracimy też dostęp do danych. Tak jakbyśmy byli napastnikiem, cała partycja Windows będzie niedostępna bez klucza. Najefektywniejszym sposobem zarządzania kluczami jest wykorzystanie istniejącej infrastruktury AD DS przedsiębiorstwa do zdalnego deponowania kluczy odzyskiwania. Funkcja BitLocker ma też konsolę odzyskiwania awaryjnego zintegrowaną z funkcjami rozruchowymi w celu zapewnienia możliwości odzyskania danych. Użytkownicy indywidualni mogą korzystać z narzędzi zarządzających kluczami BitLocker w celu utworzenia klucza odzyskiwania lub dodatkowego klucza startowego i zapisywać te klucze na nośniku wymiennym (lub w dowolnym miejscu poza szyfrowanym woluminem). Administratorzy mogą tworzyć skrypty do automatycznego tworzenia i odzyskiwania kluczy.

BitLocker zapewnia ważną warstwę ochrony, ale jest tylko jedną częścią infrastruktury ochrony danych w systemie Windows. BitLocker:

- **BARDZO** utrudnia napastnikowi uzyskanie dostępu do danych na skradzionym komputerze lub dysku twardym.
- Szyfruje cały wolumin systemu Windows w tym plik uśpienia, plik stronicowania i pliki tymczasowe (o ile nie zostaną przeniesione na jakiś inny wolumin).
- Pozwala łatwo powtórnie wykorzystywać napędy poprzez usunięcie kluczy szyfrujących.
- **NIE** chroni danych przed atakami sieciowymi.
- **NIE** chroni danych podczas działania systemu Windows.

Inne technologie zabezpieczeń, takie jak EFS, zaporę systemu Windows i uprawnienia systemu plików NTFS, zapewniają ochronę danych podczas działania systemu Windows. Więcej informacji na temat funkcji BitLocker można znaleźć w rozdziale 16.

Trzy filary bezpieczeństwa informacji

Trzy filary bezpieczeństwa informacji są znane jako triada CIA:

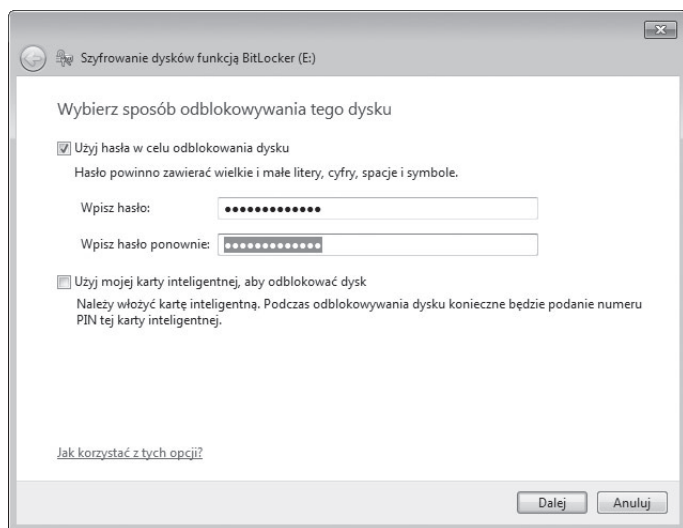
- **Poufność (Confidentiality)** Trzeba pozwalać na dostęp do danych ludziom, którzy mogą je oglądać, ale nikomu innemu.
- **Integralność (Integrity)** Trzeba wiedzieć, kto utworzył, przeglądał i modyfikował dane oraz zapobiegać nieautoryzowanym zmianom oraz podszywaniu się pod uprawnionych użytkowników.
- **Dostępność (Availability)** Należy pozwalać użytkownikom na dostęp do danych, gdy ich potrzebują, nawet jeśli wystąpią ataki i katastrofy naturalne.

BitLocker zapewnia poufność poprzez szyfrowanie danych i utrudnianie napastnikowi, który ma fizyczne dojście do twardego dysku, dostępu do tych danych. BitLocker może też zapewniać integralność, wykrywając zmiany w krytycznych plikach systemowych. Nie zapewnia jednak dostępności. W istocie jeśli nie zaplanujemy szybkiego odzyskiwania systemów ze zgubionymi kluczami, BitLocker może ograniczać dostępność.

W systemie Windows Vista administratorzy mogli włączyć ochronę funkcją BitLocker w celu szyfrowania całego woluminu systemowego, co bardzo utrudniało napastnikowi wyjęcie twardego dysku z komputera i dostęp do zawartości woluminu systemowego.

Windows 7 nadal obsługuje użycie funkcji BitLocker do szyfrowania woluminu systemowego. Dodatkowo administratorzy mogą szyfrować dowolny stały wolumin funkcją BitLocker, co zostało wprowadzone w Windows Vista SP1. Instalator Windows 7 automatycznie dzieli dysk systemowy, zapewniając dodatkową partycję wymaganą przez funkcję BitLocker. W systemie Windows Vista administratorzy musieli na nowo podzielić dysk systemowy na partycje przed włączeniem funkcji BitLocker, co mogło być bardzo trudne – w zależności od zapewnienia istniejących woluminów.

Funkcja BitLocker To Go może szyfrować napędy wymienne, takie jak napędy USB. Ponieważ użytkownicy często przenoszą poufne dokumenty, korzystając z tych napędów, są one narażone na ryzyko utraty i kradzieży. Funkcja BitLocker To Go chroni zawartość dysku wymiennego, nawet jeśli napastnik uzyska do niego dostęp. Podczas gdy BitLocker zazwyczaj chroni wolumin systemowy przy użyciu klucza zapisanego w mikroukładzie TPM, funkcja BitLocker To Go chroni woluminy przenośne, wykorzystując hasło określone przez użytkownika, jak pokazuje rysunek 2-8.



Rysunek 2-8 Funkcja BitLocker To Go chroni woluminy przenośne hasłem.

Gdy użytkownik podłączy napęd BitLocker To Go do komputera działającego pod kontrolą systemu Windows XP z SP3, Windows Vista z SP1 lub Windows 7, funkcja autoturuchamiania otworzy narzędzie, które poprosi użytkownika o podanie hasła i pozwoli użytkownikowi skopiować niezaszyfrowane pliki. W systemie Windows 7 użytkownicy mogą automatycznie odblokowywać wolumin zaszyfrowany funkcją BitLocker To Go. Jeśli użytkownik nie zna hasła, nie jest w stanie uzyskać dostępu do zawartości wymiennego nośnika. Jeśli użytkownik przyłączy napęd zaszyfrowany funkcją BitLocker To Go do wcześniejszej wersji systemu Windows, napęd będzie wyglądał na niesformatowane urządzenie i użytkownik nie będzie w stanie uzyskać dostępu do danych. Użytkownik chroniący napęd wymienny

funkcją BitLocker To Go musi zapisać lub wydrukować klucz odzyskiwania, który można wykorzystać w celu uzyskania dostępu do zawartości napędu, jeśli hasło zostanie utracone.

Profesjonaliści IT mogą stosować ustawienia zasad grupy, aby wymagać szyfrowania BitLocker To Go na nośnikach wymiennych. Więcej informacji na temat funkcji BitLocker To Go można znaleźć w rozdziale 16.

Wskazówki ekspertów

Administratorzy godni zaufania

Steve Riley, Starszy strateg ds. zabezpieczeń

Microsoft Corporation, Grupa Trustworthy Computing

Czy ufasz swoim administratorom? Jest to poważne pytanie i zasługuje na poważne przemyślenie. Zadałem to pytanie w sali seminaryjnej wypełnionej niemal tysiącem uczestników słuchających mojej prezentacji na temat zasad zabezpieczeń i o dziwo nikt nie podniósł ręki. To mnie przeraziło, a nawet sprawiło, że na parę chwil zaniemówilem – a ci, którzy mnie znają, mogą przyznać, że nie zdarza się to często! Jeśli nie możemy ufać osobom, które zatrudniamy do budowania i zarządzania krytycznymi sieciami, od których zależy powodzenie naszych firm, to równie dobrze możemy je wyłączyć i wrócić do czasów kamiennych noży i niedźwiedziich skór.

Administratorzy mają niemal lub całkowicie nieskrępowany dostęp do wszystkiego w naszej sieci. Jest to ogromna władza skupiona w kilku osobach – władza, która może służyć dobrym celom lub być wykorzystana w złych celach. Co robimy, aby pomóc w zapewnieniu, że osoby, którym powierzamy taką władzę, korzystały z niej tylko w dobrych celach?

Mówiąc bez ogródek: musimy mieć zaufanie do swoich administratorów. Potrzebny jest proces przepytywania, sprawdzania, zatrudniania, monitorowania i zwalniania tych pracowników. Wiem, że wiele osób czytających tę książkę jest administratorami i to, co piszę, mogłoby ich nieco rozsierdzić. Być może myślicie „Kim on jest, żeby zakładać, że mam złe zamiary?” Przypominam sobie jednak swój eksperyment z konferencji TechEd: wśród publiczności złożonej w większości z administratorów zero procent przyznało, że ufa innym administratorom. To musi coś znaczyć. Środki techniczne mogą utrudnić złośliwym administratorom realizację złych zamiarów, ale odpowiednio zmotywowani ludzie zawsze znajdą sposoby na obejście zabezpieczeń. Administratorów, którym nie można ufać, trzeba wymienić; nie ma innej alternatywy.

AppLocker

AppLocker jest nową funkcją w systemach Windows 7 i Windows Server 2008 R2, która zastępuje zasady ograniczeń oprogramowania z wcześniejszych wersji systemu Windows. Podobnie do zasad ograniczeń oprogramowania AppLocker daje administratorom kontrolę nad tym, które aplikacje mogą być uruchamiane przez standardowych użytkowników. Ograniczanie aplikacji, które mogą być uruchamiane przez użytkowników, nie tylko daje większą

kontrolę nad środowiskiem pulpitu, ale jest jednym z najlepszych sposobów ograniczania ryzyka infekcji szkodliwym oprogramowaniem, ogranicza możliwość uruchamiania nielicencjonowanego oprogramowania i uniemożliwia użytkownikom uruchamianie oprogramowania, które nie zostało zweryfikowane przez IT jako spełniające wymagania zgodności.

W porównaniu z zasadami ograniczeń oprogramowania AppLocker zapewnia następujące korzyści:

- Definiuje reguły oparte na atrybutach w podpisie cyfrowym, takich jak wydawca, nazwa pliku i wersja. Jest to niezwykle użyteczna funkcja, ponieważ może pozwalać administratorom na uruchamianie dowolnej wersji podpisanej aplikacji, w tym wersji przyszłych. Na przykład rozważmy departament IT rozwijający i podpisujący niestandardową aplikację, którą użytkownicy powinni być w stanie uruchamiać. We wcześniejszych wersjach systemu Windows administratorzy mogli utworzyć regułę opartą na skrócie pliku, pozwalając użytkownikom uruchamiać tę konkretną wersję aplikacji. Gdyby departament IT wydał aktualizację pliku wykonywalnego, administratorzy musieliby utworzyć nową regułę dla tej aktualizacji. W systemie Windows 7 administratorzy mogą utworzyć regułę, która ma zastosowanie do obecnych i przyszłych wersji, pozwalając na szybkie wdrażanie aktualizacji bez oczekiwania na zmianę reguł.
- Przypisuje reguły do grup lub pojedynczych użytkowników.
- Tworzy wyjątki dla plików .exe. Na przykład administratorzy mogą utworzyć regułę, która pozwala na uruchamianie dowolnej aplikacji z wyjątkiem określonego pliku .exe.
- Importuje i eksportuje reguły, co pozwala administratorom łatwo kopiować i edytować reguły.
- Identyfikuje pliki, których nie można uruchamiać, jeśli zasada zostanie zastosowana przy użyciu trybu śledzenia.

Więcej informacji na temat funkcji AppLocker można znaleźć w rozdziale 24.

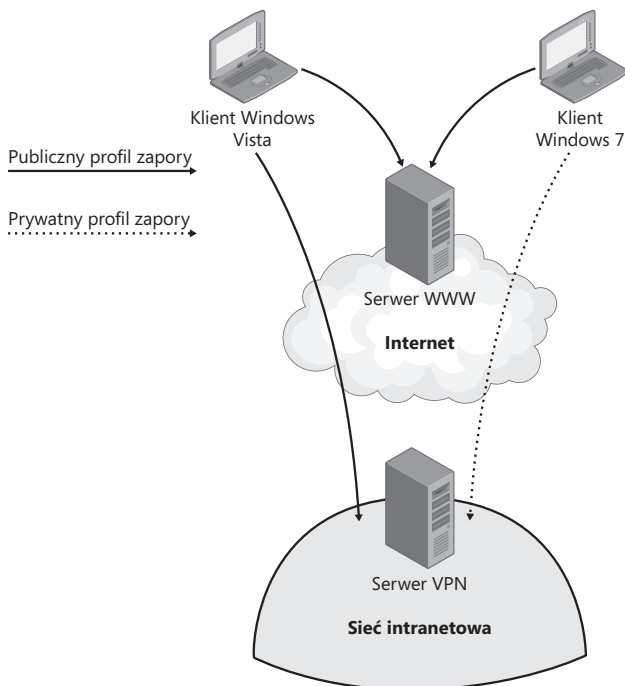
Wiele aktywnych profili zapory

Wiele komputerów, zwłaszcza komputery przenośne, ma kilka kart sieciowych. Na przykład laptop może mieć przewodowe połączenie Ethernet i bezprzewodowe połączenie WiFi. Może to prowadzić do sytuacji, gdy dany komputer jest połączony jednocześnie z siecią prywatną i siecią publiczną – na przykład przenośny komputer może być zadokowany na biurku użytkownika i przyłączony do prywatnej sieci LAN, natomiast karta sieciowa WiFi może utrzymywać połączenie z publiczną siecią WiFi w sąsiedniej kawiarni. Nawet mając tylko jedną kartę sieciową, użytkownik może być połączony z korporacyjną siecią VPN poprzez publiczną sieć bezprzewodową.

W systemie Windows Vista i wcześniejszych wersjach systemu Windows pojedynczy profil zapory był stosowany do wszystkich kart sieciowych. W poprzednim przykładzie prowadziłoby to do sytuacji, gdy komputer przenośny stosowałby publiczny profil zapory do prywatnej sieci LAN lub połączenia VPN, co mogłoby blokować ważny ruch zarządzający siecią. System Windows 7 obsługuje wiele aktywnych profili zapory, co pozwala jej stosować publiczny profil zapory wobec sieci WiFi, a prywatny lub domenowy profil zapory wobec

połączenia VPN. Rysunek 2-9 ilustruje, w jaki sposób klienci Windows Vista wykorzystują pojedynczy profil zapory, a klienci Windows 7 mogą wykorzystywać wiele takich profili.

Więcej informacji na temat tego usprawnienia można znaleźć w rozdziale 26.



Rysunek 2-9 Windows 7 obsługuje wykorzystanie różnych profili zapory dla standardowego połączenia sieciowego i połączenia z siecią VPN korzystających z pojedynczej karty sieciowej.

Kontrola konta użytkownika

Przez lata większość typowych zagrożeń bezpieczeństwa zmieniała się z wirusów na robaki, a całkiem ostatnio na oprogramowanie szpiegowskie i konie trojańskie. Aby pomóc chronić użytkowników przed tymi typami szkodliwego oprogramowania, firma Microsoft zaleca korzystanie z kont z ograniczonymi uprawnieniami (znanymi jako standardowe konta użytkowników w systemie Windows Vista lub konta użytkowników z ograniczeniami w systemie Windows XP). Standardowe konta użytkowników pomagają zapobiegać dokonywaniu zmian przez szkodliwe oprogramowanie w całym systemie, na przykład instalowaniu oprogramowania, które wpływa na wielu użytkowników – jeśli użytkownikowi brakuje uprawnień do zainstalowania nowej aplikacji w udostępnianej lokalizacji, takiej jak %SystemRoot%\Program Files, wszelkie szkodliwe oprogramowanie, które ten użytkownik przypadkowo uruchomi, również nie może dokonać tych zmian. Innymi słowy, szkodliwe oprogramowanie uruchomione w kontekście konta użytkownika ma takie same ograniczenia, jak ten użytkownik.

Co pojawia się użytkownikom, gdy brak jest potrzebnych uprawnień

Steve Hiskey, Lead Program Manager
Windows Security Core

Wiele przedsiębiorstw zaczyna blokować swoich użytkowników nawet w systemie Windows XP, próbując poprawić zabezpieczenia i utrzymać zgodność z różnymi regulacjami. System Windows Vista pozwala blokować tych użytkowników w większym stopniu, wyświetlając użytkownikom okno komunikatu o odmowie dostępu ze względu na ustanowione zasady, gdy próbują oni wykonać działanie wymagające podwyższonych uprawnień. Możemy to skonfigurować, definiując ustawienie zasad grupy „Kontrola konta użytkownika: zachowanie monitu o podniesienie uprawnień dla użytkowników standardowych” jako „Nie monituj”.

Chociaż standardowe konta użytkowników istotnie poprawiają bezpieczeństwo, korzystanie ze standardowych kont użytkowników w systemie Windows XP i wcześniejszych wersjach systemu Windows powoduje dwa główne problemy:

- Użytkownicy nie mogą instalować oprogramowania, zmieniać czasu systemowego lub strefy czasowej, instalować drukarek, zmieniać ustawień zasilania, dodawać kluczy WEP dla ustawień sieci bezprzewodowej albo wykonywać innych typowych zadań, które wymagają podniesionych uprawnień.
- Wiele słabo napisanych aplikacji wymaga uprawnień administracyjnych i nie działa poprawnie z ograniczonymi uprawnieniami.

Chociaż logowanie się na komputerze jako użytkownik standardowy oferuje lepszą ochronę przed szkodliwym oprogramowaniem, praca z tego typu kontem była w przeszłości tak trudna, że wiele organizacji wybierało nadawanie użytkownikom uprawnień administracyjnych do swoich komputerów. Kontrola konta użytkownika (UAC) jest zestawem funkcji wprowadzonych po raz pierwszy w systemie Windows Vista, które oferują zalety standardowych kont użytkowników bez niepotrzebnych ograniczeń. Po pierwsze, wszyscy użytkownicy (włącznie z administratorami) działają domyślnie z ograniczonymi uprawnieniami. Po drugie, system Windows Vista pozwala standardowym kontom użytkowników na zmienianie strefy czasowej (ale nie godziny) i wykonywanie innych typowych zadań bez podawania poświadczeń administracyjnych, co pozwala organizacjom konfigurować więcej użytkowników przy użyciu kont standardowych. Po trzecie, UAC pozwala większości aplikacji – nawet tym, które wymagają uprawnień administracyjnych w systemie Windows XP – działać poprawnie w kontekście standardowych kont użytkowników.

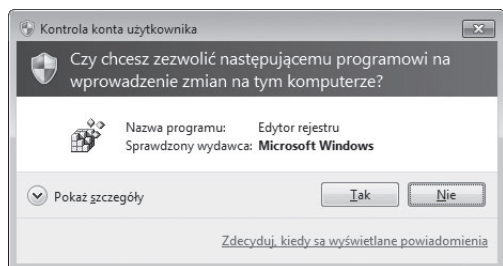
Gdy system Windows Vista pojawił się po raz pierwszy, wielu użytkowników zmagало się ze zgodnością aplikacji i częstotliwością monitów UAC generowanych przez aplikację. Z czasem programiści aplikacji zmodyfikowali swoje aplikacje tak, aby poprawnie działały ze standardowymi uprawnieniami użytkownika i w ten sposób nie wymagały monitu UAC.

Był to jeden z celów UAC – zmotywować programistów aplikacji do zachowania zgodności z najlepszymi praktykami zabezpieczeń.

Tryb zatwierdzania przez administratora

W systemie Windows XP i wcześniejszych wersjach Windows każdy proces uruchomiony przez użytkownika zalogowanego jako administrator działa z uprawnieniami administracyjnymi. Ta sytuacja była kłopotliwa, ponieważ szkodliwe oprogramowanie mogło dokonywać zmian w systemie, na przykład instalować oprogramowanie bez potwierdzenia ze strony użytkownika. W systemach Windows Vista i Windows 7 członkowie grupy Administratorzy działają w *Trybie zatwierdzania przez administratora*, który (domyślnie) monitoruje administratorów o potwierdzenie działań wymagających uprawnień większych niż standardowe. Na przykład, chociaż użytkownik mógłby być zalogowany jako administrator, programy Windows Messenger i Windows Mail będą działać tylko ze standardowymi uprawnieniami użytkownika.

W tym celu tryb zatwierdzania przez administratora tworzy dwa tokeny dostępu, gdy loguje się członek grupy administratorów lokalnych: jeden token z pełnymi uprawnieniami i drugi ograniczony token, który naśladuje token standardowego użytkownika. Token o niższych uprawnieniach jest używany do zadań nieadministracyjnych, a token uprzywilejowany jedynie po bezpośredniej zgodzie użytkownika. Jak pokazano na rysunku 2-10, system Windows Vista monitoruje użytkownika o zgodę przed zezwoleniem aplikacji na wykonanie działania, które wymaga uprawnień administracyjnych.



Rysunek 2-10 UAC monitoruje administratorów o potwierdzenie działań administracyjnych.

Wiele organizacji korzysta z zalet UAC do tworzenia standardowych kont użytkowników zamiast administracyjnych. Tryb zatwierdzania przez administratora oferuje pewną ochronę dla tych użytkowników, którzy potrzebują uprawnień administracyjnych – na przykład programistów – wymagając potwierdzenia, zanim aplikacja dokona jakichś potencjalnie szkodliwych zmian. Podobnie jak większość usprawnień zabezpieczeń w systemie Windows 7 monit wymagający zgody użytkownika jest domyślnie włączony, ale może być wyłączony przy pomocy ustawień zasad grupy. Dodatkowo monit wymagający zgody użytkownika może żądać od użytkowników wpisania hasła administracyjnego lub po prostu poinformować ich, że dostęp nie jest możliwy.

Programiści powinni pracować jako użytkownicy standardowi

Chris Corio, Program Manager

Windows Security

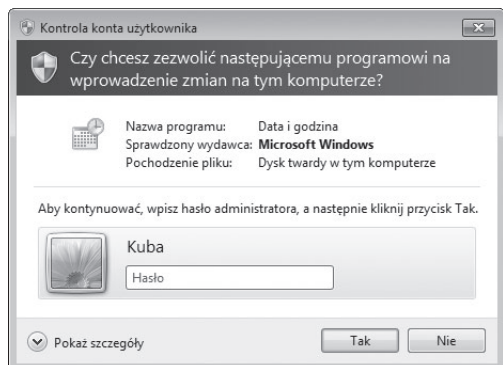
Jednym z moich ulubionych aspektów systemów Windows Vista i Windows 7 jest trend w kierunku ograniczania uprawnień, z którymi aplikacje działają domyślnie. Chroni to użytkowników przed przypadkowymi uszkodzeniami komputerów i jeszcze bardziej pozwala ufać systemowi operacyjnemu. Niestety wielu programistów popełnia typowy błąd, który sprawia, że ich kod nie działa dobrze w środowisku z niższymi uprawnieniami. Pracują na co dzień z uprawnieniami administracyjnymi! Jeśli piszemy nową aplikację dla systemu Windows Vista lub Windows 7, powinniśmy projektować i uruchamiać tę aplikację jako użytkownik standardowy. Jest to najłatwiejszy sposób, aby programista zrozumiał znaczenie kontroli konta użytkownika i innych technologii mających wpływ na kod.

Umożliwianie nieadministratorom dokonywania zmian konfiguracji

Standardowe konta użytkowników w systemie Windows Vista mogą dokonywać zmian konfiguracji, które nie naruszają zabezpieczeń komputera. Na przykład standardowe konta użytkowników w systemie Windows Vista mają prawo zmieniania strefy czasowej na komputerach, co jest ważnym ustawieniem dla użytkowników podróżujących. W systemie Windows XP zwykle konta użytkowników nie miały domyślnie tego uprawnienia, co było niewygodne i powodowało, że wielu profesjonalistów IT wdrażało konta dla użytkowników mobilnych jako konta administracyjne i poświęcało korzyści płynące z zabezpieczeń związanych z wykorzystaniem zwykłych kont użytkowników. Dodatkowo użytkownicy standardowi mogą teraz łączyć się z zaszyfrowanymi sieciami bezprzewodowymi i dodawać połączenia VPN – są to zadania często wymagane przez przedsiębiorstwa.

Jednakże standardowe konta użytkowników w systemie Windows Vista nie mają uprawnień do zmieniania czasu systemowego, ponieważ wiele aplikacji i usług polega na dokładnym czasie systemowym. Jak pokazano na rysunku 2-11, użytkownik, który próbuje zmienić godzinę, jest proszony o podanie poświadczeń administracyjnych.

Niektóre aplikacje nie działają w systemie Windows XP bez uprawnień administracyjnych, ponieważ te aplikacje próbują dokonywać zmian w plikach i lokalizacjach rejestru, które wpływają na cały komputer (na przykład C:\Program Files, C:\Windows, HKEY_LOCAL_MACHINE), a standardowe konta użytkowników nie mają potrzebnych uprawnień. Wirtualizacja rejestru i plików w systemie Windows Vista przekierowuje wiele spośród związanych z całym komputerem operacji zapisu do plików i rejestru do lokalizacji związanych z konkretnym użytkownikiem. Ta funkcja umożliwia uruchamianie aplikacji jako użytkownik standardowy, podczas gdy w poprzednich systemach operacyjnych te aplikacje nie mogły być uruchamiane jako użytkownik standardowy. Wreszcie pozwala to większej liczbie organizacji na korzystanie ze standardowych kont użytkowników, ponieważ aplikacje, które w przeciwnym razie wymagałyby uprawnień administracyjnych, mogą działać z powodzeniem bez dokonywania żadnych zmian w aplikacji.



Rysunek 2-11 UAC monitoruje standardowych użytkowników o poświadczenia administratora.

UWAGA Nie należy mylić wirtualizacji plików i rejestru z produktami do wirtualizacji systemów operacyjnych, takimi jak Microsoft Virtual PC lub Microsoft Virtual Server. Wirtualizacja plików i rejestru wirtualizuje jedynie te funkcje systemu operacyjnego, a nie sprzęt komputerowy.

Więcej informacji na temat UAC można znaleźć w rozdziale 24.

Jak to działa

Wirtualizacja plików

Steve Hiskey, Lead Program Manager
Windows Security Core

Windows Vista zawiera rozszerzenie filtrowania napędów w systemie operacyjnym, które przechwytuje błędy odmowy dostępu, zanim operacja plikowa będzie zwrócona do aplikacji. Jeśli lokalizacja pliku, która wygenerowała błąd odmowy dostępu znajduje się w miejscu, gdzie system operacyjny skonfigurowano na wirtualizację danych, to wygenerowana zostanie nowa ścieżka do pliku i operacja będzie powtórzona bez wiedzy aplikacji, że takie powtórzenie nastąpiło.

Usprawnienia UAC w systemie Windows 7

Systemy Windows 7 i Windows Server 2008 R2 ograniczają liczbę monitów UAC, na które muszą odpowiadać administratorzy lokalni i użytkownicy standardowi:

- Monity związane z operacjami na plikach są scalane.
- Monity programu Internet Explorer związane z uruchamianiem instalatorów aplikacji są scalane.
- Monity programu Internet Explorer związane z instalowaniem formantów ActiveX są scalane.

Domyślne ustawienie UAC pozwala użytkownikowi standardowemu wykonywać następujące zadania bez wyświetlania monitu UAC:

- Instalować aktualizacje z Windows Update.
- Instalować sterowniki pobrane z Windows Update lub zawarte w systemie operacyjnym.
- Przeglądać ustawienia systemu Windows. Zmienianie ustawień nadal wymaga zatwierdzenia monitu UAC.
- Łączyć urządzenia Bluetooth z komputerem.
- Inicjować kartę sieciową i wykonywać inne zadania diagnostyczne i naprawcze związane z siecią.

Dodatkowo domyślne ustawienie UAC pozwala administratorom wykonywać zadania administracyjne przy użyciu funkcji systemu operacyjnego bez monitu UAC. Na przykład administrator może zmieniać czas systemowy lub ponownie uruchamiać usługę bez wyświetlania monitu UAC. Jednakże administratorzy będą nadal otrzymywać monit UAC, jeśli aplikacja wymaga uprawnień administracyjnych.

System Windows Vista oferuje użytkownikowi dwa poziomy ochrony UAC: włączony lub wyłączony. Dodatkowo administrator może zmienić ustawienie zasad grupy, aby zapobiec przyciemnianiu ekranu (funkcja znana jako bezpieczny pulpit), gdy pojawia się monit o zgodę użytkownika.

Systemy Windows 7 i Windows Server 2008 R2 wprowadzają dwa dodatkowe poziomy monitów UAC. Jeśli jesteśmy zalogowani jako administratorzy lokalni, możemy włączać lub wyłączać monity UAC albo wybrać, kiedy mamy być powiadamiani o zmianach w komputerze. Administratorzy mogą wybrać spośród trzech poziomów powiadamiania z dodatkową opcją wyłączającą bezpieczny pulpit:

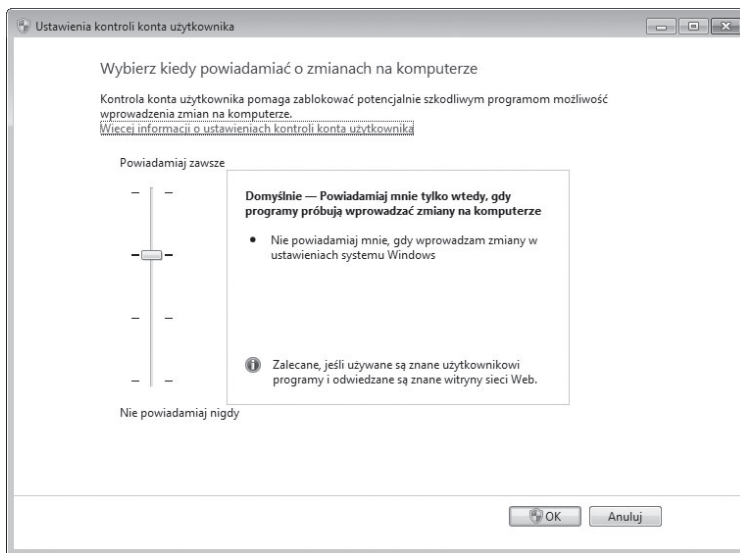
- **Zawsze powiadamiaj mnie** Użytkownicy są powiadamiani, gdy dokonają zmian w ustawieniach systemu Windows i gdy programy próbują dokonać zmian na komputerze. Jest to domyślne ustawienie dla użytkowników standardowych.
- **Powiadamiaj mnie tylko wtedy, gdy programy próbują wprowadzić zmiany na komputerze** Użytkownicy nie są powiadamiani, gdy dokonują zmian ustawień systemu Windows, ale otrzymują powiadomienie, gdy program próbuje dokonać zmian na komputerze. Jest to domyślne ustawienie dla administratorów.
- **Nigdy mnie nie powiadamiaj** Użytkownicy nie są powiadamiani o żadnych zmianach dokonywanych w ustawieniach systemu Windows ani gdy oprogramowanie jest instalowane.

Rysunek 2-12 pokazuje narzędzie Panelu sterowania do ustawień kontroli konta użytkownika. To narzędzie wyświetla czwartą opcję z warunkiem „nie przyciemniaj pulpitu”, które wyłącza bezpieczny pulpit, aby monit UAC był mniej natrączywy.

Tabela 2-4 zawiera porównanie liczby monitów UAC dla działań użytkownika w systemach Windows 7 i Windows Server 2008 R2 z liczbą monitów UAC w systemie Windows Vista SP1.

Tabela 2-4 Domyślne działanie monitów UAC w systemie Windows 7

Działania	Domyślnie w Windows 7
Zmiana ustawień personalizacyjnych	Bez monitów
Zarządzanie pulpitem	Bez monitów
Konfigurowanie i rozwiązywanie problemów z siecią	Bez monitów
Korzystanie z Łatwego transferu w systemie Windows	Mniej monitów
Instalowanie formantów ActiveX przez program Internet Explorer	Mniej monitów
Przylączanie urządzeń	Bez monitów
Korzystanie z Windows Update	Bez monitów
Konfigurowanie kopii zapasowych	Bez monitów
Instalowanie lub usuwanie oprogramowania	Bez monitów



Rysunek 2-12 Ustawianie poziomu monitów UAC

Korzystając z ustawień zasad grupy, administratorzy mogą konfigurować różne zachowania dla administratorów i użytkowników niebędących administratorami. Więcej informacji na temat UAC można znaleźć w rozdziale 24.

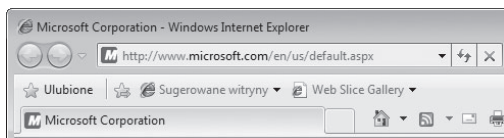
Funkcje zabezpieczeń programu Internet Explorer

Program Windows Internet Explorer 8 zawarty w systemie Windows 7 oferuje więcej usprawnień zabezpieczeń w stosunku do wersji Internet Explorer 7. Usprawnienia te zapewniają dynamiczną ochronę przed kradzieżą danych, oszukańczymi witrynami WWW oraz szkodliwym i ukrytym oprogramowaniem. Firma Microsoft dokonała usprawnień architektonicznych w programie Internet Explorer 7 i przeniosła te usprawnienia do wersji Internet Explorer 8, aby przeglądarka WWW była gorszym celem dla napastników i innych osób o złych zamiarach, co pomaga użytkownikom przeglądać Internet z większym spokojem.

Jednakże w miarę zacieśniania zabezpieczeń następuje tendencja do pogarszania zgodności i rozszerzalności. W wersji Internet Explorer 8 firma Microsoft mocno stara się, żeby skutecznie zapewnić tę równowagę tak, aby użytkownicy mogli mieć najbezpieczniejsze i jak najlepsze środowisko przeglądania Internetu.

Internet Explorer 8 zawiera następujące funkcje zabezpieczeń (z których niektóre są również zawarte w wersji Internet Explorer 7):

- **Filtr SmartScreen** Internet Explorer 8 wykorzystuje usługę internetową do sprawdzania adresów URL, które odwiedza użytkownik i ostrzega użytkowników, gdy próbują odwiedzić witrynę, która może być niebezpieczna. Filtr SmartScreen może też ostrzegać użytkowników, gdy próbują pobrać oprogramowanie, które potencjalnie jest niebezpieczne. Użytkownicy nadal mają możliwość ukończenia danego działania, nawet jeśli filtr SmartScreen ostrzeże ich przed niebezpieczeństwem. W ten sposób SmartScreen ogranicza ryzyko związane z odwiedzeniem przez użytkowników witryn wydłudzających informacje lub pobraniem szkodliwego oprogramowania, nie ograniczając przy tym tego, co użytkownik może zrobić.
- **Filtr skryptów między witrynami (XSS)** Czasami napastnicy wykorzystują luki w witrynie WWW, a następnie wykorzystują witrynę do wydobywania prywatnych informacji od użytkowników odwiedzających witrynę. Może to sprawić, że witryna, która normalnie jest bezpieczna, staje się ryzykowna – bez wiedzy właściciela witryny. Internet Explorer 8 może wykryć szkodliwy kod działający na skompromitowanych witrynach WWW, pomagając chronić użytkowników przed atakami mogącymi prowadzić do ujawnienia informacji, przejęcia plików cookie, kradzieży tożsamości i innych niebezpieczeństw.
- **Wyróżnianie domeny** Napastnicy często stosują odpowiednio przygotowane adresy URL do zmylenia użytkowników tak, aby myśleli, że odwiedzają uprawnioną witrynę WWW. Na przykład właściciel witryny WWW mógłby korzystać z nazwy hosta *www.microsoft.com.contoso.com*, aby sugerować użytkownikowi, że odwiedza on witrynę *www.microsoft.com* – choć w tym wypadku to *contoso.com* kontroluje tę domenę. Wyróżnianie domeny pomaga użytkownikom łatwiej interpretować adresy URL w celu uniknięcia witryn WWW, które próbują oszukać użytkowników za pomocą mylących adresów. Działa to poprzez wyróżnianie nazwy domeny w pasku adresu na czarno, jak pokazano na rysunku 2-13, a wyświetlanie pozostałej części adresu URL na szaro, co ułatwia identyfikację prawdziwej tożsamości witryny.



Rysunek 2-13 Wyróżnianie domeny ułatwia identyfikowanie nazwy domeny w adresie URL.

- **Zapobieganie wykonywaniu danych (DEP)** DEP jest funkcją zabezpieczeń, która może pomagać w zapobieganiu atakom ze strony wirusów i innych zagrożeń poprzez uniemożliwianie zapisu pewnego rodzaju kodu w wykonywalnym obszarze pamięci. Chociaż DEP jest funkcją systemu operacyjnego zawartą w Windows Vista i Windows 7, Internet Explorer

8 wykorzystuje ją do minimalizowania ryzyka ataków ze strony witryn WWW w strefie internetowej. Funkcja DEP nie jest włączona dla witryn WWW w strefie intranetowej.

- **Tryb chroniony programu Internet Explorer** W trybie chronionym Internet Explorer 8 działa z ograniczonymi uprawnieniami, pomagając w zapobieganiu zmianom plików lub ustawień systemowych bez jawnej zgody użytkownika. Nowa architektura przeglądarki wprowadzona w wersji Internet Explorer 7 wykorzystuje proces sterujący, który pozwala istniejącym aplikacjom w bezpieczniejszy sposób zwiększać uprawnienia ponad tryb chroniony. Ta dodatkowa obrona pomaga weryfikować, że akcje ze strony skryptów lub procesów automatycznych nie mogą pobierać danych spoza katalogów wymagających niskich uprawnień, takich jak folder Tymczasowe pliki internetowe. Tryb chroniony jest dostępny tylko przy korzystaniu z przeglądarki Internet Explorer 8 w systemie Windows Vista lub Windows 7, gdy włączona jest funkcja UAC. Tryb chroniony nie jest dostępny w systemie Windows XP.
- **Wybórcze blokowanie formantów ActiveX** Funkcja ta automatycznie wyłącza wszystkie formanty, dla których programista nie określił jawnie użycia w Internecie. Minimalizuje to potencjalne ryzyko niewłaściwego użycia zainstalowanych formantów. W systemach Windows Vista i Windows 7 użytkownicy są monitorowani przez Pasek informacji, zanim będą mogli uzyskać dostęp do wcześniej zainstalowanego formantu ActiveX, który nie był jeszcze używany w Internecie, ale został zaprojektowany do takiego użytku. Ten mechanizm powiadamiania pozwala użytkownikowi zezwalać lub odmawiać dostępu poszczególnym formantom, co jeszcze bardziej ogranicza powierzchnię umożliwiającą przeprowadzanie ataków. Witryny WWW, które próbują dokonywać zautomatyzowanych ataków, nie mogą już w ukryty sposób próbować wykorzystywać formanty ActiveX, które nie są przeznaczone do użycia w Internecie.
- **Popraw ustawienia dla mnie** Większość użytkowników instaluje i wykorzystuje aplikacje korzystając z konfiguracji domyślnej, więc programy Internet Explorer 7 i Internet Explorer 8 są dostarczane z ustawieniami zabezpieczeń, które zapewniają maksymalny poziom wygody przy utrzymywaniu kontroli nad zabezpieczeniami. W rzadkich sytuacjach niestandardowa aplikacja może wymagać od użytkownika obniżenia ustawień zabezpieczeń z domyślnego poziomu, ale ważne jest, aby użytkownik wycofał te zmiany, gdy ustawienia niestandardowe nie będą już dłużej potrzebne. Funkcja Popraw ustawienia dla mnie ostrzega użytkowników poprzez pasek informacji, gdy bieżące ustawienia zabezpieczeń mogą narażać ich na ryzyko. Kliknięcie opcji Popraw dla mnie ustawienia w pasku informacji natychmiast przywraca ustawienia zabezpieczeń programu Internet Explorer do domyślnego poziomu Średnio-wysoki. W środowiskach AD DS możemy konfigurować wymagane uprawnienia dla aplikacji wewnętrznych tak, aby wymagania związane z zabezpieczeniami nie stanowiły problemu.
- **Pasek stanu zabezpieczeń** Pasek stanu zabezpieczeń w programach Internet Explorer 7 i Internet Explorer 8 pomaga użytkownikom szybko odróżniać autentyczne witryny WWW od podejrzanych lub szkodliwych witryn usprawniając dostęp do informacji o certyfikatach cyfrowych, które pomagają potwierdzić zaufanie do witryn komercyjnych. Nowy pasek stanu zabezpieczeń zapewnia też użytkownikom wyraźniejsze wskazówki wizualne, określające poziom bezpieczeństwa i zaufania dla danej witryny, oraz obsługuje

informacje o certyfikatach wysokiej pewności, które mocniej identyfikują bezpieczne witryny (na przykład witryny banków).

- **Ochrona przed manipulacją adresami URL** Programy Internet Explorer 7 i Internet Explorer 8 mają jedną funkcję do przetwarzania danych z adresów URL, co znacznie ogranicza wewnętrzną powierzchnię ataku. Ta nowa procedura obsługi danych daje większą niezawodność, zapewniając przy tym więcej funkcji i zwiększoną elastyczność w związku ze zmienną naturą Internetu, jak również globalizacją adresów URL, międzynarodowymi zestawami znaków i nazwami domen.

Dodatkowo każdą z tych funkcji można konfigurować poprzez korzystanie z zasad grupy, co umożliwia scentralizowaną kontrolę nad zabezpieczeniami programu Internet Explorer. System Windows 7 zawiera program Internet Explorer 8, który ma wszystkie te funkcje. Internet Explorer 8 może być też instalowany w systemie Windows Vista. Więcej informacji na temat programu Internet Explorer można znaleźć w rozdziale 20 „Zarządzanie przeglądarką Windows Internet Explorer”.

Usprawnienia inspekcji

Opcje inspekcji w systemach Windows Vista i Windows 7 są bardzo szczegółowe, pozwalając włączać inspekcję dla bardzo konkretnych zdarzeń. Ogranicza to liczbę nieistotnych zdarzeń, potencjalnie ograniczając „szum” generowany przez fałszywe zdarzenia. To z kolei może pozwolić operatorom łatwiej wykrywać zdarzenia o istotnym znaczeniu. W połączeniu z nową usługą Windows Event Collector możemy budować system do agregowania tylko najważniejszych zdarzeń związanych z zabezpieczeniami w danej organizacji.

Aby przejrzeć nowe kategorie, należy uruchomić następujące polecenie z administracyjnego wiersza poleceń. Wiersze pogrubione pokazują kategorie, które są nowe w systemie Windows 7 i nie są zawarte w Windows Vista.

```
Auditpol /get /category:*
```

Systemowe zasady inspekcji

Kategoria/podkategoria

Ustawienie

System

Security System Extension

Brak inspekcji

System Integrity

Sukces i niepowodzenie

IPsec Driver

Brak inspekcji

Other System Events

Sukces i niepowodzenie

Security State Change

Sukces

Logon/Logoff

Logon

Sukces

Logoff

Sukces

Account Lockout

Sukces

IPsec Main Mode

Brak inspekcji

IPsec Quick Mode

Brak inspekcji

IPsec Extended Mode

Brak inspekcji

Special Logon

Sukces

Other Logon/Logoff Events

Brak inspekcji

Network Policy Server

Sukces i niepowodzenie

Object Access

File System

Brak inspekcji

Registry

Brak inspekcji

Kernel Object	Brak inspekcji
SAM	Brak inspekcji
Certification Services	Brak inspekcji
Application Generated	Brak inspekcji
Handle Manipulation	Brak inspekcji
File Share	Brak inspekcji
Filtering Platform Packet Drop	Brak inspekcji
Filtering Platform Connection	Brak inspekcji
Other Object Access Events	Brak inspekcji
Detailed File Share	Brak inspekcji
Privilege Use	
Sensitive Privilege Use	Brak inspekcji
Non Sensitive Privilege Use	Brak inspekcji
Other Privilege Use Events	Brak inspekcji
Detailed Tracking	
Process Termination	Brak inspekcji
DPAPI Activity	Brak inspekcji
RPC Events	Brak inspekcji
Process Creation	Brak inspekcji
Policy Change	
Audit Policy Change	Sukces
Authentication Policy Change	Sukces
Authorization Policy Change	Brak inspekcji
MPSSVC Rule-Level Policy Change	Brak inspekcji
Filtering Platform Policy Change	Brak inspekcji
Other Policy Change Events	Brak inspekcji
Account Management	
User Account Management	Sukces
Computer Account Management	Brak inspekcji
Security Group Management	Sukces
Distribution Group Management	Brak inspekcji
Application Group Management	Brak inspekcji
Other Account Management Events	Brak inspekcji
DS Access	
Directory Service Changes	Brak inspekcji
Directory Service Replication	Brak inspekcji
Detailed Directory Service Replication	Brak inspekcji
Directory Service Access	Brak inspekcji
Account Logon	
Kerberos Service Ticket Operations	Brak inspekcji
Other Account Logon Events	Brak inspekcji
Kerberos Authentication Service	Brak inspekcji
Credential Validation	Brak inspekcji

Podobnie możemy użyć polecenia *Auditpol /set*, aby włączać opcje inspekcji. Najprostszym sposobem włączania szczegółowych opcji inspekcji jest włączanie lub wyłączanie ustawień zasad grupy znajdujących się w folderze Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Konfiguracja zaawansowanych zasad inspekcji. Zarządzanie szczegółowymi opcjami inspekcji przy użyciu zasad grupy jest nową funkcją w systemach Windows 7 i Windows Server 2008 R2.

System Windows 7 obsługuje również Inspekcję globalnego dostępu do obiektów, którą możemy stosować do konfigurowania inspekcji plików lub rejestru na komputerach przy pomocy ustawień zasad grupy. W tym celu należy zdefiniować zasady System plików lub

Rejestr w folderze Konfiguracja komputera\Ustawienia systemu Windows\Ustawienia zabezpieczeń\Konfiguracja zaawansowanych zasad inspekcji\Zasady inspekcji systemu\Inspekcja globalnego dostępu do obiektów. Następnie należy kliknąć przycisk Konfiguruj, aby określić obiekty do inspekcji.

Więcej informacji na temat dziennika zdarzeń systemu Windows i kolekcji zdarzeń można znaleźć w rozdziale 21 „Utrzymywanie kondycji systemu”.

Bezpieczne odłączanie w puli jądra

System Windows 7 zawiera niskopoziomowe sprawdzenia integralności, które nie były zawarte we wcześniejszych wersjach systemu Windows, w celu ograniczenia ryzyka przepełnień. Szkodliwe oprogramowanie często wykorzystuje różne typy przepełnień do uruchamiania podwyższonych uprawnień i kodu bez zgody użytkownika. System Windows 7 podwójnie sprawdza zawartość pamięci w puli – części pamięci, którą aplikacje wykorzystują tymczasowo, ale która jest zarządzana przez system operacyjny. Jeśli pula została zmodyfikowana lub uszkodzona, system Windows 7 inicjuje sprawdzenie błędu uniemożliwiające dalsze działanie kodu.

Zgodnie z wewnętrznymi testami firmy Microsoft dodatkowe sprawdzanie pamięci nie ma mierzalnego wpływu na wydajność. Więcej informacji można znaleźć w artykule „Safe Unlinking in the Kernel Pool” pod adresem <http://blogs.technet.com/srd/archive/2009/05/26/safe-unlinking-in-the-kernel-pool.aspx>.

Windows Biometric Framework

Przed systemem Windows 7 producenci urządzeń biometrycznych sprawdzających odciski palców musieli zapewniać własne technologie obsługi, w tym sterowniki, pakiety do tworzenia oprogramowania (SDK) i aplikacje. Ponieważ jednak różni producenci tworzyli własne rozwiązania, brakowało im spójnego interfejsu użytkownika i platformy zarządzającej.

Windows Biometric Framework (WBF) pozwala producentom urządzeń biometrycznych lepiej integrować skanery linii papilarnych, skanery tęczówek i inne urządzenia biometryczne z systemem Windows. Obecnie urządzenia biometryczne mogą korzystać z tych samych narzędzi panelu sterowania do konfiguracji bez względu na ich producenta. Użytkownicy mogą poszukać możliwości biometrycznych, uruchamiając aplet panelu sterowania Urządzenia biometryczne. Profesjonaliści IT czerpią z tego korzyści, ponieważ nie muszą już zarządzać różnym oprogramowaniem dla każdego typu urządzenia biometrycznego. Dodatkowo czytniki linii papilarnych mogą być teraz używane do odpowiadania na monity poświadczeń UAC i logowania się do domen AD DS.

Aplikacje mogą korzystać z interfejsu API wbudowanego w system Windows 7 do komunikacji z dowolnym typem urządzenia biometrycznego. W przeszłości aplikacje musiały korzystać z interfejsów API specyficznych dla urządzeń, co utrudniało programistom integrację różnych typów urządzeń biometrycznych. Dlatego programiści aplikacji również z tego korzystają, ponieważ mogą użyć dobrze zdefiniowanego interfejsu API i obsługiwać urządzenia biometryczne od dowolnego producenta.

Administratorzy mogą korzystać z ustawień zasad grupy, aby uniemożliwiać wykorzystywanie urządzeń biometrycznych do logowania się na lokalnym komputerze lub w domenie

albo mogą całkiem wyłączyć funkcje biometryczne. W systemie Windows 7 czytniki linii papilarnych są jedynym obsługiwanym typem urządzeń biometrycznych.

Karty inteligentne

Dla wielu organizacji ryzyko, że hasło zostanie skradzione lub odgadnięte, jest nie do zaakceptowania. Aby uzupełnić zabezpieczenia hasłami, organizacje implementują uwierzytelnianie wieloczynnikowe, które wymaga zarówno hasła, jak i drugiej formy identyfikacji. Często tą drugą formą identyfikacji jest karta inteligentna, która zawiera certyfikat cyfrowy jednoznacznie identyfikujący posiadacza karty i klucz prywatny do wykorzystania przy uwierzytelnianiu.

Podobnie jak w przypadku urządzeń biometrycznych, poprzednie wersje systemu Windows nie miały ustandaryzowanej platformy dla kart inteligentnych. W systemie Windows 7 karty inteligentne mogą korzystać z konwencjonalnych sterowników. Oznacza to, że użytkownicy mogą mieć dostęp do kart inteligentnych od producentów, którzy opublikowali swoje sterowniki poprzez Windows Update bez wymagania dodatkowego oprogramowania. Użytkownicy po prostu wkładają kartę inteligentną zgodną z technologią Personal Identity Verification (PIV), a system Windows 7 spróbuje pobrać sterownik z Windows Update lub skorzysta z ministerownika zgodnego z PIV zawartego w systemie Windows 7.

Poniżej wymieniono nowe opcje obsługi kart inteligentnych w systemie Windows 7, z których wszystkie mogą być dostępne bez dodatkowego oprogramowania.

- Odblokowywanie napędów zaszyfrowanych przez BitLocker przy pomocy karty inteligentnej.
- Logowanie się do domeny przy pomocy karty inteligentnej.
- Podpisywanie dokumentów XPS i wiadomości poczty elektronicznej.
- Korzystanie z kart inteligentnych z niestandardowymi aplikacjami, które wykorzystują CNG lub Crypto API w celu umożliwienia aplikacjom korzystania z certyfikatów.

Konta usług

Usługi są procesami działającymi w tle. Na przykład usługa Serwer przyjmuje przychodzące połączenia udostępniania plików, a usługa Stacja robocza zarządza wychodzącymi połączeniami udostępniania plików.

Każda usługa musi działać w kontekście konta usługi. Uprawnienia konta usługi w dużym stopniu definiują, co ta usługa może i nie może zrobić, tak jak konto użytkownika definiuje, co może zrobić użytkownik. We wczesnych wersjach systemu Windows luki zabezpieczeń w usługach były często wykorzystywane w celu dokonywania zmian na komputerze. Aby zminimalizować to ryzyko, konta usług powinny mieć możliwie najbardziej ograniczone uprawnienia.

System Windows Vista zapewniał trzy typy kont usług: Usługę lokalną, Usługę sieciową i System lokalny. Te konta były proste do konfigurowania przez administratorów, ale były często wspólnie wykorzystywane przez wiele usług i nie mogły być zarządzane na poziomie domeny.

Administratorzy mogą też tworzyć konta użytkowników domenowych i konfigurować je, aby działały jako konta usług. Daje to administratorom pełną kontrolę nad uprawnieniami

przypisanymi do usługi, ale wymaga od nich ręcznego zarządzania hasłami i nazwami głównymi usług. Ten koszt zarządzania może stać się bardzo czasochłonny w środowisku korporacyjnym.

System Windows 7 wprowadza dwa nowe typy kont usług:

- Zarządzane konta usług pozwalają usługom na izolację konta domenowego, eliminując przy tym potrzebę zarządzania przez administratorów poświadczeniami konta.
- Wirtualne konta usług działają jak zarządzane konta usług, ale funkcjonują na poziomie komputera lokalnego, a nie na poziomie domeny. Wirtualne konta usług mogą wykorzystywać poświadczenia komputera przy dostępie do zasobów sieciowych.

Oba typy kont mają hasła, które są zerowane automatycznie, więc administratorzy nie muszą tego robić ręcznie. Każdy typ konta może być używany dla wielu usług na pojedynczym komputerze. Jednakże nie mogą być one używane dla usług na różnych komputerach, także komputerach w jednym klastrze.

Więcej informacji na temat tego, jak usługi są implementowane i zarządzane w systemie Windows 7, można znaleźć w rozdziale 17 „Zarządzanie urządzeniami i usługami”.

Podsumowanie

Usprawnienia zabezpieczeń w systemie Windows 7 dotyczą niemal każdego aspektu systemu operacyjnego. Szczegóły funkcji zabezpieczeń są omawiane w całej książce, ale ten rozdział dał przegląd kluczowych usprawnień zabezpieczeń, pozwalając stworzyć wyczerpujący plan zabezpieczeń i lepiej zrozumieć, jak system Windows 7 wpłynie na bezpieczeństwo danej organizacji.

Usprawnienia zabezpieczeń w systemie Windows 7 podlegają kilku różnym zasadom zabezpieczeń:

- **Przypisywanie najmniejszych uprawnień** Użytkownicy, aplikacje i usługi powinny mieć tylko minimalne uprawnienia, których koniecznie potrzebują. Na przykład użytkownicy nie powinni mieć uprawnień administracyjnych na swoim komputerze biurowym, ponieważ wirus lub koń trojański mógłby wykorzystać te uprawnienia. AppLocker, UAC, tryb chroniony programu Internet Explorer i konta usług wymuszają najmniejsze uprawnienia dla użytkowników, programu Internet Explorer i usług.
- **Ochrona danych podczas magazynowania i przesyłania** Chociaż moglibyśmy rozważać bezpieczne pliki komputerowe i komunikację wewnątrz fizycznie zabezpieczonej lokalizacji, wzrost komunikacji mobilnej oznacza, że dane wymagają dodatkowej ochrony. Windows 7 usprawnia funkcję BitLocker, pozwalając na szyfrowanie zarówno woluminów systemowych, jak i niesystemowych. Windows 7 dodaje też funkcję BitLocker To Go, pozwalając użytkownikom szyfrować całą zawartość napędów wymiennych. Nawet jeśli napastnik ukradnie dysk wymienny chroniony przez funkcję BitLocker To Go, nie będzie w stanie uzyskać dostępu do jego zawartości bez hasła.
- **Ograniczanie powierzchni ataku** Każda aplikacja, usługa lub funkcja systemu operacyjnego może zawierać luki. Im więcej usług i aplikacji jest włączonych domyślnie w systemie

operacyjnym, tym większe ryzyko wykorzystania jakiejś luki. System Windows 7 minimalizuje powierzchnię ataku sieciowego bez blokowania ważnego ruchu zarządzającego poprzez przypisywanie różnych profili zapory do różnych wirtualnych kart sieciowych. Na przykład fizyczna karta sieciowa może mieć przypisany publiczny profil zapory, co chroni ją przed wieloma atakami sieciowymi. Karta sieci VPN może mieć przypisany domenowy profil zapory, co pozwala administratorom sieci wewnętrznej łączyć się i zarządzać zdalnym komputerem.

W połączeniu z poprawioną infrastrukturą zabezpieczeń WBF i ustandaryzowanymi sterownikami kart inteligentnych usprawnienia te oferują wiele warstw ochrony, które możemy wykorzystać w celu ograniczania ryzyka zabezpieczeń w danej organizacji.

Dodatkowe zasoby

Dodatkowe informacje i narzędzia związane z tym rozdziałem zawierają następujące zasoby.

Powiązane informacje

- „Windows 7 Security Enhancements” w dziale Windows Client TechCenter na witrynie Microsoft TechNet pod adresem <http://technet.microsoft.com/en-us/library/dd548337.aspx>.
- „An Introduction to Security in Windows 7” w TechNet Magazine pod adresem <http://technet.microsoft.com/en-us/magazine/2009.05.win7.aspx>.
- Webcast na żądanie „Windows 7–The Security Story” pod adresem <http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?culture=en-AU&EventID=1032407883&CountryCode=AU>.
- Najnowszą wersję przewodnika *Windows Vista Security Guide* można pobrać pod adresem <http://www.microsoft.com/downloads/details.aspx?FamilyID=a3d1bbed-7f35-4e72-bfb5-b84a526c1565&DisplayLang=en>. Przewodnik ten zapewnia szczegółowe informacje na temat tego, jak najlepiej skonfigurować zabezpieczenia systemu Windows Vista w danej organizacji.
- „Windows 7 Security Compliance Management Toolkit” pod adresem <http://go.microsoft.com/fwlink/?LinkId=156033>.

Na dołączonym nośniku

- Get-FileAcl.ps1
- Get-LocalAdministrators.ps1
- UnlockLockedOutUsers.ps1
- UserToSid.ps1
- WhoIs.ps1

CZĘŚĆ II

Wdrażanie

A series of thin, light gray wavy lines that flow from the left side of the page, under the title, and curve towards the right side, creating a sense of movement and design.

Platforma wdrożeniowa

- Wprowadzenie do narzędzi 87
- Terminologia wdrażania Windows 7 90
- Składniki platformy 91
- Scenariusze wdrożeń 102
- Zrozumienie programu instalacyjnego 104
- Podstawowy proces wdrożeniowy 108
- Proces Microsoft Deployment Toolkit 110
- Podsumowanie 113
- Dodatkowe zasoby 114

O pierając się na technologii wprowadzonej przez system operacyjny Windows Vista, technologia wdrożeniowa systemu Windows 7 znacząco ewoluowała od czasu systemu Windows XP Professional. Na przykład obsługuje oparte na plikach obrazy dyskowe do szybszego, efektywniejszego i mniej kosztownego wdrażania wielu komputerów. System operacyjny Windows 7 zapewnia też solidniejsze narzędzia wdrożeniowe poprzez Windows Automated Installation Kit 2.0 (Windows AIK 2.0), obejmujące Windows System Image Manager (Windows SIM) i Windows Preinstallation Environment (Windows PE).

Ten rozdział pomoże rozpocząć pracę z platformą wdrożeniową systemu Windows 7. Stanowi wprowadzenie do tych narzędzi, opisując, jak są one ze sobą powiązane i zapewniając podstawowe wyjaśnienia, dlaczego i kiedy używać każdego narzędzia. Pozostałe rozdziały w części II „Wdrażanie” opisują szczegółowo narzędzia wprowadzone w tym rozdziale. Przewodnik *Windows Automated Installation Kit User's Guide* zawarty w pakiecie Windows AIK 2.0 również szczegółowo omawia każde narzędzie opisane w tym rozdziale.

Wprowadzenie do narzędzi

W porównaniu z Windows XP system Windows 7 wprowadza liczne zmiany w technologiach stosowanych do wdrażania. Dodatkowo system Windows 7 poprawia i konsoliduje wiele spośród narzędzi, które były stosowane do wdrażania systemu Windows Vista. Pakiet Windows AIK 2.0 zawiera większość tych narzędzi. Inne są wbudowane w system

operacyjny. Pakiet Windows AIK 2.0 w pełni dokumentuje wszystkie narzędzia opisywane w tym rozdziale, w tym opcje wiersza polecenia stosowane przy korzystaniu z tych narzędzi, opis ich działania na szczegółowym poziomie, itd.

UWAGA Pakiet Windows AIK 2.0 nie jest zawarty na dysku z systemem Windows 7 (dla porównania system Windows XP używał pliku o nazwie Deploy.cab, który zawierał narzędzia wdrożeniowe). Pakiet Windows AIK 2.0 jest natomiast darmowym elementem do pobrania z witryny Microsoft Download Center pod adresem <http://www.microsoft.com/downloads>.

Przy wdrażaniu systemu Windows 7 nowe są następujące funkcje:

- **Windows System Image Manager** Windows System Image Manager (Windows SIM) jest narzędziem do tworzenia udziałów dystrybucyjnych i edytowania plików odpowiedzi (Unattend.xml). Udostępnia wszystkie konfigurowalne ustawienia w systemie Windows 7; korzystamy z niego do zapisywania swoich ustawień w pliku Unattend.xml. Pakiet Windows AIK 2.0 zawiera narzędzie Windows SIM.
- **Windows Setup** Program instalatora systemu Windows 7 instaluje plik obrazu systemu Windows (.wim) i wykorzystuje nowy plik odpowiedzi Unattend.xml do automatyzowania instalacji. Unattend.xml zastępuje zestaw plików odpowiedzi używanych we wcześniejszych wersjach systemu Windows (Unattend.txt, Sysprep.inf, itd.). Ponieważ instalacja na podstawie obrazu jest szybsza, możemy korzystać z niej w dużych wdrożeniach i przy automatyzowaniu utrzymywania obrazów. Firma Microsoft dokonała wielu poprawek w programie Windows Setup (teraz noszącym nazwę Setup.exe zamiast Winnt.exe lub Winnt32.exe), takich jak całkowicie graficzny interfejs użytkownika, zastosowanie pojedynczego pliku odpowiedzi (Unattend.xml) do konfiguracji i obsługa przebiegów (faz) konfiguracji.
- **Sysprep** Narzędzie System Preparation (Sysprep) przygotowuje instalację systemu Windows 7 do tworzenia obrazu, inspekcji i wdrażania. Z tworzenia obrazu korzystamy do przechwycenia niestandardowego obrazu Windows 7, który możemy wdrażać w danej organizacji. Korzystamy z trybu inspekcji, aby dodawać sterowniki urządzeń i aplikacje do instalacji Windows 7 oraz testować integralność instalacji przed przekazaniem komputera użytkownikowi końcowemu. Możemy też używać narzędzia Sysprep do przygotowywania obrazu do wdrożenia. Gdy użytkownik końcowy uruchomi system Windows 7, pojawi się ekran Windows Welcome. W odróżnieniu od wcześniejszych wersji systemu Windows Windows 7 zawiera wbudowany program Sysprep – nie trzeba już pobierać jego bieżącej wersji.
- **Windows Preinstallation Environment** Środowisko Windows Preinstallation Environment 3.0 (Windows PE 3.0) zapewnia funkcje systemu operacyjnego do instalowania, rozwiązywania problemów i odzyskiwania systemu Windows 7. Windows PE 3.0 jest najnowszym wydaniem środowiska Windows PE opartym na Windows 7. Dzięki środowisku Windows PE możemy uruchamiać komputer z sieci lub nośnika wymiennego. Windows PE zapewnia obsługę sieci i innych zasobów potrzebnych do instalowania i rozwiązywania problemów z Windows 7. Windows Setup, Windows Deployment Services,

Microsoft System Center Configuration Manager 2007 R2 oraz Microsoft Deployment Toolkit 2010 (MDT 2010) wszystkie korzystają z środowiska Windows PE do uruchamiania komputerów. Pakiet Windows AIK 2.0 zawiera środowisko Windows PE 3.0.

- **Deployment Image Servicing and Management** Deployment Image Servicing and Management (DISM) jest nowym narzędziem wiersza polecenia, które możemy wykorzystać do obsługi obrazu Windows 7 lub przygotowania obrazu Windows PE. DISM konsoliduje funkcjonalność narzędzi Package Manager (Pkgmgr.exe), PEimg, oraz Intlcfg z systemu Windows Vista. Możemy korzystać z DISM do obsługi pakietów, sterowników urządzeń, funkcji systemu Windows 7 oraz ustawień międzynarodowych w obrazach Windows 7. Dodatkowo narzędzie DISM zapewnia bogate funkcje wyliczeniowe, które możemy wykorzystywać, aby określać zawartość obrazów Windows 7.
- **ImageX** ImageX jest narzędziem wiersza polecenia, które możemy wykorzystywać, aby przechwytywać, modyfikować i stosować obrazy oparte na plikach dla celów wdrożeniowych. Windows Setup, Windows Deployment Services, System Center Configuration Manager 2007 oraz MDT 2010 wszystkie wykorzystują ImageX do przechwytywania, edycji i wdrażania obrazów Windows 7. Windows 7 poprawia narzędzie ImageX w stosunku do Windows Vista poprzez zezwalanie mu na jednoczesne montowanie wielu obrazów i obsługę zapisów pośrednich (nadal musimy obsługiwać każdy zamontowany obraz z osobna przy użyciu DISM). Dodatkowo wersja narzędzia ImageX dla systemu Windows 7 ma nową architekturę do montowania i obsługi obrazów, która jest bardziej sprawna niż w systemie Windows Vista. Pakiet Windows AIK 2.0 zawiera ImageX. Możemy też montować obrazy w środowisku Windows PE, a system Windows 7 zawiera odpowiedni sterownik urządzenia.
- **Windows Imaging** Firma Microsoft dostarcza system Windows 7 na nośniku produktu w postaci mocno skompresowanego pliku Windows Imaging (.wim). Możemy instalować system Windows 7 bezpośrednio z nośnika Windows 7 lub dostosować obraz systemu do wdrożenia. Obrazy Windows 7 są oparte na plikach, co pozwala edytować je w sposób nieniszczący. Możemy też przechowywać wiele obrazów systemu operacyjnego w pojedynczym pliku .wim.
- **DiskPart** Korzystając z narzędzia DiskPart, możemy montować plik wirtualnego dysku twardego (.vhd) offline i obsługiwać go tak samo jak plik obrazu systemu Windows.
- **User State Migration Tool** Możemy korzystać z narzędzia User State Migration Tool 4.0 (USMT 4.0), aby migrować ustawienia użytkownika z wcześniejszego systemu operacyjnego do Windows 7. Zachowywanie ustawień użytkowników pomaga zapewnić, że użytkownicy szybko będą mogli wrócić do pracy po wdrożeniu. Narzędzie USMT 4.0 zapewnia nowe funkcje, które poprawiają jego elastyczność i wydajność w stosunku do USMT 3.0. Migracja łącząca poprawia wydajność w scenariuszach odświeżania systemu, migracja offline pozwala przechwytywać stan użytkownika z Windows PE, a wyszukiwarka dokumentów ogranicza potrzebę tworzenia niestandardowych plików migracji w formacie Extensible Markup Language (XML) podczas przechwytywania wszystkich dokumentów użytkownika. Pakiet Windows AIK 2.0 zawiera USMT 4.0.

Terminologia wdrażania Windows 7

Przy wdrażaniu systemu Windows 7 i MDT 2010 unikalne są następujące terminy. Zrozumienie tej terminologii pomoże lepiej zrozumieć zawartość dotyczącą wdrożenia w tej książce i zasoby, do których się odwołuje.

- **Plik odpowiedzi** Plik XML, który obsługuje w skrypcie operacje i ustawienia instalacji dla systemu Windows 7. Plikiem odpowiedzi dla programu Windows Setup jest zwykle Unattend.xml lub Autounattend.xml. Możemy skorzystać z Windows SIM, aby utworzyć i zmodyfikować ten plik odpowiedzi. MDT 2010 buduje automatycznie pliki odpowiedzi, które można w razie konieczności dostosować.
- **Plik katalogu** Plik binarny, który zawiera stan wszystkich ustawień i pakietów w obrazie Windows 7. Gdy korzystamy z Windows SIM do utworzenia pliku katalogu, wyszczególnia to zawartość obrazu Windows 7 w celu uzyskania listy ustawień w tym obrazie, jak również obecnej listy funkcji i ich stanów bieżących. Ponieważ zawartość obrazu systemu Windows 7 może się zmieniać z czasem, ważne jest, aby ponownie utworzyć plik katalogu, gdy zaktualizujemy obraz.
- **Funkcja** Część systemu operacyjnego Windows 7, która określa pliki, zasoby i ustawienia dla określonej funkcjonalności systemu Windows 7 lub części funkcjonalności systemu Windows 7. Niektóre funkcje zawierają ustawienia instalacji nienadzorowanej, które możemy dostosowywać, korzystając z Windows SIM.
- **Przebieg konfiguracji** Faza instalacji systemu Windows 7. Windows Setup instaluje i konfiguruje różne części systemu operacyjnego w różnych przebiegach konfiguracji. Możemy zastosować ustawienia instalacji nienadzorowanej w jednym lub kilku przebiegach konfiguracji. Więcej informacji na temat tych przebiegów możemy znaleźć w przewodniku *Windows Automated Installation Kit User's Guide* w pakiecie Windows AIK 2.0.
- **Zestaw konfiguracji** Struktura plików i folderów zawierająca pliki, które sterują procesem instalacji wstępnej i definiują niestandardowe ustawienia instalacji systemu Windows 7.
- **Komputer docelowy** Komputer, na którym instalujemy system Windows 7 podczas wdrażania. Możemy albo uruchomić Windows Setup na komputerze docelowym, albo skopiować instalację wzorcową na komputer docelowy.
- **Udział wdrożeniowy** Folder, który zawiera pliki źródłowe dla instalowanych produktów Windows. Może również zawierać dodatkowe sterowniki urządzeń i pliki aplikacji. Możemy utworzyć ten folder ręcznie lub korzystając z Windows SIM. W MDT 2010 udział wdrożeniowy, zwany udziałem dystrybucyjnym w poprzednich wersjach MDT, zawiera pliki systemu operacyjnego, sterowników urządzeń, aplikacji i inne pliki źródłowe, które możemy skonfigurować jako sekwencje zadań.
- **Instalacja oparta na obrazie** Proces instalacji opierający się na zastosowaniu obrazu systemu operacyjnego wobec danego komputera.
- **Komputer wzorcowy** W pełni złożony komputer zawierający instalację wzorcową systemu Windows 7, którą przechwytyjemy do obrazu wzorcowego i wdrażamy

na komputerach docelowych. Termin *komputer źródłowy* jest w tym przypadku też często używany.

- **Obraz wzorcowy** Zbiór plików i folderów (zwykle skompresowanych do jednego pliku) przechwyconych z instalacji wzorcowej. Ten obraz zawiera podstawowy system operacyjny, jak również dodatkowe aplikacje, konfiguracje i pliki.
- **Instalacja wzorcowa** Instalacja systemu Windows 7 na komputerze wzorcowym, którą możemy przechwycić jako obraz wzorcowy. Możemy tworzyć instalację wzorcową, korzystając z automatyzacji, aby zapewniać spójną i powtarzalną konfigurację za każdym razem.
- **Pakiet** Grupa plików, które firma Microsoft zapewnia do modyfikacji funkcji systemu Windows 7. Typy pakietów obejmują pakiety serwisowe, aktualizacje zabezpieczeń, pakiety językowe i zestawy poprawek.
- **Sekwencja zadań** Ciąg zadań wykonywanych na komputerze docelowym w celu zainstalowania systemu Windows 7 i aplikacji, a następnie skonfigurowania komputera docelowego. W MDT 2010 sekwencje zadań sterują procedurą instalacji.
- **Task Sequencer (Sekwencer zadań)** Składnik MDT 2010, który wykonuje sekwencję zadań podczas instalowania systemu.
- **Komputer techniczny** Komputer, na którym instalujemy i wykorzystujemy MDT 2010 lub Windows AIK 2.0. Ten komputer zwykle znajduje się w środowisku laboratoryjnym oddzielnym od sieci produkcyjnej. Może to być komputer klasy stacji roboczej lub klasy serwera.
- **Unattend.xml** Ogólna nazwa pliku odpowiedzi dla systemu Windows 7. Unattend.xml zastępuje wszystkie pliki odpowiedzi we wcześniejszych wersjach systemu Windows, w tym Unattend.txt, Winbom.ini i inne.
- **.wim** Rozszerzenie nazwy pliku identyfikujące pliki obrazów systemu Windows tworzone przez ImageX.
- **Funkcja systemu Windows 7** Opcjonalna funkcjonalność systemu Windows 7, którą możemy włączać lub wyłączać, korzystając z Unattend.xml lub DISM.
- **Plik obrazu systemu Windows** Pojedynczy, skompresowany plik zawierający zbiór plików i folderów duplikujących instalację Windows na woluminie dyskowym. Pliki obrazów systemu Windows mają rozszerzenie .wim.

Składniki platformy

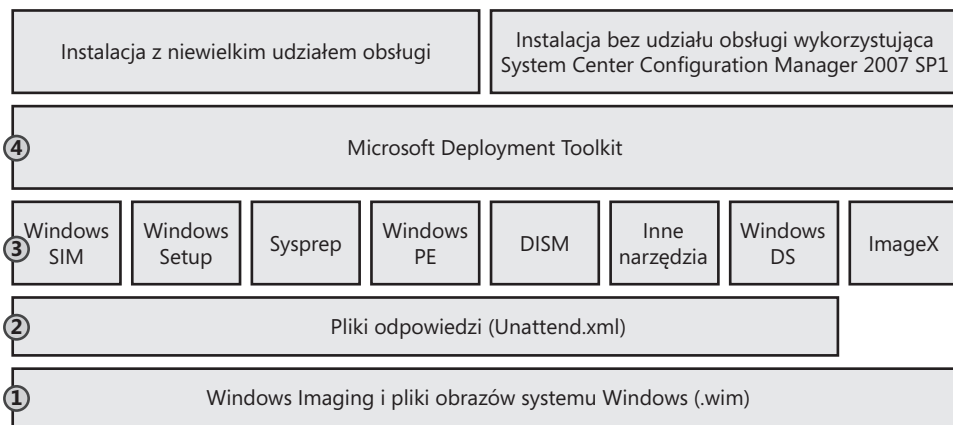
Zrozumienie nowych narzędzi wdrożeniowych i zależności pomiędzy nimi jest pierwszym krokiem do rozpoczęcia projektu wdrażania systemu Windows 7. Rysunek 3-1 ilustruje platformę wdrożeniową systemu Windows 7. W najniższej warstwie znajdują się pliki obrazów systemu Windows (.wim), które są mocno skompresowanymi, opartymi na plikach obrazami systemu operacyjnego.

W drugiej warstwie znajdują się pliki odpowiedzi. Wersje systemu Windows wcześniejsze niż Windows Vista miały liczne pliki odpowiedzi, w tym Unattend.txt i Sysprep.inf, sterujące

procesem wdrażania. Windows 7 wykorzystuje pojedynczy, oparty na formacie XML plik odpowiedzi, Unattend.xml, który steruje wszystkimi *przebiegami konfiguracji* (przebieg konfiguracji jest fazą instalacji). Usprawnienie to powoduje, że konfiguracja jest bardziej spójna i upraszcza zagadnienia techniczne.

Na trzecim poziomie istnieją różne narzędzia wdrożeniowe dla systemu Windows 7. Nośnik dystrybucyjny systemu Windows 7 zawiera kilka z tych narzędzi, w tym Sysprep, DISM i inne narzędzia wiersza polecenia – nie ma ich na nośniku w osobnym pliku, takim jak Deploy.cab. Pakiet Windows AIK 2.0 zawiera większe narzędzia, takie jak Windows SIM, Windows PE oraz ImageX. Są to podstawowe narzędzia potrzebne do tworzenia, dostosowywania i wdrażania obrazów systemu Windows 7. Przy tym są to samodzielne narzędzia, które nie zapewniają platformy wdrożeniowej ani najlepszych praktyk dla procesu wdrażania.

Czwarta warstwa, MDT 2010, zapewnia taką platformę, inteligencję biznesową i najlepsze praktyki. MDT 2010 jest platformą procesową i technologiczną, która wykorzystuje wszystkie narzędzia z trzeciej warstwy, umożliwiając organizacji oszczędność setek godzin poświęconych na planowanie, projektowanie, testowanie i wdrażanie. System MDT 2010 jest oparty na najlepszych praktykach opracowanych przez firmę Microsoft, jej klientów i partnerów. Zawiera sprawdzone wskazówki dotyczące zarządzania i technologii, jak również tysiące wierszy dokładnie przetestowanego kodu skryptowego, z którego możemy korzystać wprost lub dostosowywać tak, aby odpowiadał wymaganiom danej organizacji.



Rysunek 3-1 Składniki platformy wdrożeniowej systemu Windows 7

Korzystając z MDT 2010, możemy dokonywać wdrożeń z niewielkim udziałem obsługi podczas instalacji lub bez żadnego udziału obsługi. Instalacja z niewielkim udziałem obsługi wymaga bardzo niewielkiej infrastruktury i jest odpowiednia dla większości małych i średnich firm. Instalacja bez żadnego udziału obsługi wymaga infrastruktury System Center Configuration Manager 2007 R2 i jest odpowiednia dla organizacji, które już mają tę infrastrukturę dostępną.

Poniższe części tego rozdziału podają więcej informacji na temat składników pokazanych na rysunku 3-1. Więcej informacji na temat procesu wdrażania przy użyciu składników z pierwszych trzech warstw można znaleźć pod nagłówkiem „Podstawowy proces wdrażania” w dalszej części rozdziału. Więcej informacji na temat procesu wdrażania przy użyciu

MDT 2010 można znaleźć pod nagłówkiem „Proces Microsoft Deployment Toolkit” w dalszej części rozdziału.

Windows Imaging

System Windows 7 jest rozprowadzany w plikach .wim, które wykorzystują format plików Windows Imaging. Format ten ma następujące zalety:

- Pliki Windows Imaging są opartym na plikach formatem obrazów, który pozwala nam przechowywać wiele obrazów w jednym pliku. Możemy wykonywać częściowe przechwytywania woluminów, wyłączając pliki, takie jak pliki stronicowania, których nie chcemy wdrażać przy pomocy obrazu.
- Ten format redukuje znacznie rozmiary plików, stosując format pliku skonfigurowanego i techniki przechowywania pojedynczych elementów: Plik obrazu zawiera jedną fizyczną kopię pliku dla każdego jego wystąpienia w pliku obrazu, co znacznie ogranicza rozmiar plików obrazów, które zawierają wiele obrazów.
- Możemy modyfikować obraz zawarty w pliku .wim – dodając i usuwając na przykład pakiety, aktualizacje oprogramowania i sterowniki urządzeń – bez konieczności ponownego tworzenia nowego obrazu przez jego zastosowanie, ponowne dostosowanie i ponowne przechwycenie.
- Możemy montować pliki .wim jako foldery, co ułatwia aktualizowanie plików w obrazach.
- Pliki Windows Imaging pozwalają zastosować dany obraz na twardym dysku komputera docelowego. Możemy też zastosować obraz na napędach docelowych o innych rozmiarach, ponieważ pliki .wim nie wymagają, aby docelowy dysk twardy miał taki sam rozmiar (lub większy) jak źródłowy dysk twardy.
- Pliki Windows Imaging mogą rozciągać się na kilka nośników, więc można stosować płyty CD-ROM do dystrybucji dużych plików .wim.
- Pliki .wim dla Windows PE mogą służyć do rozruchu systemu. Na przykład można uruchomić Windows PE z pliku .wim. W istocie programy Windows Setup i Windows Deployment Services uruchamiają Windows PE z pliku Boot.wim, który możemy dostosować, dodając elementy, takie jak sterowniki urządzeń i skrypty.

UWAGA ImageX jest narzędziem używanym do zarządzania plikami .wim. Więcej informacji na temat ImageX można znaleźć pod nagłówkiem „ImageX” w dalszej części rozdziału i w rozdziale 6 „Przygotowywanie obrazów dysków”.

Pliki odpowiedzi

Plik odpowiedzi jest plikiem opartym na formacie XML, który zawiera ustawienia wykorzystywane podczas instalacji systemu Windows 7. Plik odpowiedzi może w pełni automatyzować całość lub część procesu instalacji. W pliku odpowiedzi zapewniamy ustawienia związane ze sposobem podziału dysków na partycje, lokalizacją obrazu systemu Windows 7

do zainstalowania i kluczem produktu do zastosowania. Możemy też dostosowywać instalację systemu Windows 7, dodając konta użytkowników, zmieniając ustawienia ekranu i aktualizując ulubione w programie Windows Internet Explorer. Pliki odpowiedzi Windows 7 noszą nazwę Unattend.xml.

Narzędzie Windows SIM (opisane dokładnie pod nagłówkiem „Windows SIM” w dalszej części rozdziału) służy do stworzenia pliku odpowiedzi i skojarzenia go z danym obrazem systemu Windows 7. To skojarzenie pozwala sprawdzić poprawność ustawień w pliku odpowiedzi z ustawieniami dostępnymi w obrazie systemu Windows 7. Ponieważ jednak możemy skorzystać z dowolnego pliku odpowiedzi do zainstalowania dowolnego obrazu systemu Windows 7, Windows Setup ignoruje ustawienia w pliku odpowiedzi dla funkcji, które nie istnieją w danym obrazie systemu Windows.

Sekcja features pliku odpowiedzi zawiera wszystkie ustawienia funkcji, które zostaną zastosowane przez Windows Setup. Pliki odpowiedzi organizują funkcje wewnątrz różnych przebiegów konfiguracji: windowsPE, offlineServicing, generalize, specialize, auditSystem, auditUser i oobeSystem (więcej na ten temat można znaleźć w ramce zatytułowanej „Jak to działa: przebiegi konfiguracji” w dalszej części rozdziału). Każdy przebieg konfiguracji reprezentuje inną fazę instalacji, a nie wszystkie przebiegi są wykonywane podczas normalnego procesu instalowania systemu Windows 7. Możemy zastosować ustawienia podczas jednego lub kilku przebiegów. Jeśli ustawienie jest dostępne w więcej niż jednym przebiegu konfiguracji, możemy wybrać przebieg, w którym chcemy zastosować dane ustawienie.

WIĘCEJ INFORMACJI Przewodnik *Windows Automated Installation Kit User's Guide* w pakiecie Windows AIK 2.0 w pełni dokumentuje funkcje, które możemy skonfigurować przy pomocy Windows SIM, oraz ustawienia dostępne dla każdej funkcji.

Firma Microsoft wykorzystuje pakiety w celu rozprowadzania aktualizacji oprogramowania, pakietów serwisowych i pakietów językowych. Pakiety mogą też zawierać funkcje systemu Windows. Korzystając z Windows SIM, możemy dodawać pakiety do obrazu systemu Windows 7, usuwać je z obrazu systemu Windows 7 lub zmieniać ustawienia dla funkcji wewnątrz pakietu.

Pakiet Windows Foundation Package dołączony do wszystkich obrazów systemu Windows 7 zawiera wszystkie podstawowe funkcje systemu Windows 7, takie jak Media Player, Gry i Kopia zapasowa systemu Windows. Funkcje są albo włączone, albo wyłączone w systemie Windows 7. Jeśli funkcja systemu Windows 7 jest włączona, zasoby, pliki wykonywalne i ustawienia dla tej funkcji są dostępne dla użytkowników systemu. Jeśli funkcja systemu Windows 7 jest wyłączona, zasoby pakietu nie są dostępne, ale nie są usuwane z systemu.

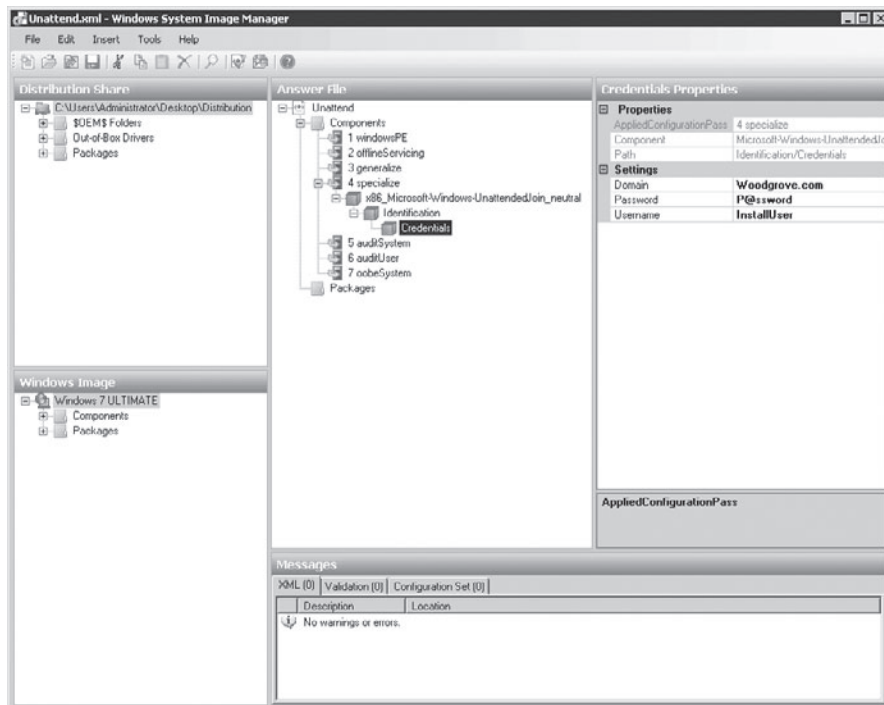
Windows SIM

Windows SIM jest narzędziem używanym do tworzenia i konfigurowania plików odpowiedzi dla systemu Windows 7. Możemy w nim konfigurować ustawienia funkcji, pakietów i plików odpowiedzi. Windows Setup wykorzystuje plik Unattend.xml do konfigurowania i dostosowywania domyślnej instalacji systemu Windows 7 dla wszystkich przebiegów konfiguracji. Na przykład możemy dostosować program Internet Explorer, skonfigurować zaporę

systemu Windows i określić konfigurację dysków twardych. Możemy korzystać z Windows SIM w celu dostosowywania systemu Windows 7 na wiele sposobów, w tym:

- Instalować aplikacje firm trzecich podczas instalacji systemu.
- Dostosowywać Windows 7 poprzez tworzenie plików odpowiedzi (Unattend.xml).
- Stosować pakiety językowe, pakiety serwisowe i aktualizacje wobec obrazu podczas instalacji.
- Dodawać sterowniki urządzeń do obrazu podczas instalacji.

W przypadku wersji systemu Windows wcześniejszych niż Windows Vista musieliśmy edytować ustawienia plików odpowiedzi ręcznie, korzystając z edytora tekstów, nawet jeśli wcześniej utworzyliśmy plik odpowiedzi przy użyciu Windows Setup Manager. Plik odpowiedzi systemu Windows 7 (Unattend.xml) jest jednak oparty na formacie XML i dlatego znacznie bardziej skomplikowany do ręcznej edycji. Musimy więc korzystać z Windows SIM, aby edytować pliki odpowiedzi systemu Windows 7. Rysunek 3-2 pokazuje okno Windows SIM.



Rysunek 3-2 Windows SIM

Windows Setup

Windows Setup (Setup.exe) jest programem, który instaluje system Windows 7. Wykorzystuje instalację opartą na obrazach (IBS), aby zapewniać pojedynczy, zunifikowany proces, w którym wszyscy klienci mogą instalować system Windows. IBS przeprowadza nowe

instalacje oraz aktualizacje systemu Windows. Windows Setup oraz IBS pozwalają łatwo i kosztowo wydajnie wdrażać system Windows 7 w organizacji.

Windows Setup zawiera kilka nowych funkcji ułatwiających instalacje, które są szybsze i spójniejsze niż w przypadku Windows XP:

- **Usprawnione zarządzanie obrazami** Obrazy Windows 7 są przechowywane w pojedynczym pliku .wim. Plik .wim może przechowywać wiele wystąpień systemu operacyjnego w pojedynczym, mocno skompresowanym pliku. Plik instalacyjny Install.wim znajduje się w folderze Sources na nośniku z systemem Windows 7.
- **Usprawniona instalacja** Program Windows Setup został zoptymalizowany, aby pozwalać na scenariusze wdrożeniowe stosowane przez większość organizacji. Instalacja zajmuje mniej czasu i zapewnia bardziej spójny proces konfiguracji i wdrażania, co powoduje mniejsze koszty wdrożenia.
- **Szybsze instalacje i aktualizacje** Ponieważ program Windows Setup jest teraz oparty na obrazach, instalowanie i aktualizowanie systemu Windows 7 jest szybsze i łatwiejsze. Możemy przeprowadzać nowe instalacje systemu Windows 7 poprzez wdrażanie obrazu systemu Windows na komputerach docelowych; możemy przeprowadzać aktualizacje poprzez instalowanie nowego obrazu na istniejącej instalacji systemu Windows. Windows Setup chroni poprzednie ustawienia systemu Windows podczas instalacji.

Windows Setup poprawia komfort procesu instalacji w porównaniu z Windows Vista. Na przykład Windows Setup przenosi wprowadzanie klucza licencyjnego na stronę Windows Welcome, co pozwala użytkownikom wpisać klucz produktu po zakończeniu instalacji. Windows Setup również automatycznie tworzy małą, ukrytą partycję dla opcji szyfrowania dysków funkcją BitLocker. Sprawia to, że późniejsze włączenie szyfrowania dysków funkcją BitLocker jest łatwiejsze, ponieważ użytkownicy nie będą musieli przygotowywać napędu. Dodatkowo ostatnia faza programu Windows Setup – Windows Welcome – jest szybsza i podaje więcej informacji zwrotnych na temat postępów procesu instalacji.

Sysprep

Korzystamy z narzędzia Sysprep, żeby przygotować instalację wzorcową dla tworzenia obrazów i wdrażania systemu. Sysprep wykonuje następujące działania:

- **Usuwa dane instalacyjne specyficzne dla komputera i dla systemu operacyjnego z systemu Windows 7** Sysprep może usunąć wszystkie informacje specyficzne dla komputera z zainstalowanego obrazu systemu Windows 7, w tym także identyfikator zabezpieczeń komputera (SID). Następnie możemy przechwycić i zainstalować instalację systemu Windows w całej organizacji.
- **Konfiguruje system Windows na rozruch w trybie inspekcji** Możemy skorzystać z trybu inspekcji, aby zainstalować aplikacje firm trzecich i sterowniki urządzeń, a także przetestować funkcjonalność komputera przed dostarczeniem go użytkownikowi.
- **Konfiguruje system Windows 7 na rozruch w trybie Windows Welcome** Sysprep konfiguruje instalację Windows 7 tak, aby uruchomiła się w trybie Windows Welcome przy następnym uruchomieniu komputera. Zwykle konfigurujemy system, aby uruchamiał

się w trybie Windows Welcome jako ostatni krok przed dostarczeniem komputera użytkownikowi.

- **Zeruje aktywację produktu Windows** Sysprep może wyzerować aktywację produktu Windows maksymalnie trzy razy.

Sysprep.exe znajduje się w katalogu %WinDir%\System32\Sysprep we wszystkich instalacjach systemu Windows 7 (nie trzeba instalować programu Sysprep oddzielnie, jak we wcześniejszych wersjach systemu Windows, ponieważ program ten jest integralną częścią instalacji). Zawsze musimy uruchamiać narzędzie Sysprep z katalogu %WinDir%\System32\Sysprep w wersji systemu Windows 7, w której zostało ono zainstalowane. Więcej informacji na temat Sysprep można znaleźć w przewodniku *Windows Automated Installation Kit User's Guide* w pakiecie Windows AIK 2.0.

Windows PE

Przed dostępnością Windows PE organizacje często musiały korzystać z dyskietek rozruchowych systemu MS-DOS, aby uruchamiać komputery docelowe, a następnie uruchamiać Windows Setup z udziału sieciowego lub innego nośnika dystrybucyjnego. Dyskietki MS-DOS miały jednak liczne ograniczenia, w tym nie miały wsparcia dla systemu plików NTFS oraz wbudowanej obsługi sieci. Ponadto musiały znajdować 16-bitowe sterowniki urządzeń, które działały w MS-DOS.

Obecnie Windows PE 3.0 zapewnia minimalny system operacyjny Win32 lub Win64 z ograniczonymi usługami – zbudowany na bazie jądra Windows 7 – który służy do przygotowania komputera na instalację systemu Windows 7, kopiowania obrazów do i z sieciowego serwera plików oraz uruchomienia programu Windows Setup. Windows PE 3.0 jest samodzielnym środowiskiem przedinstalacyjnym i integralnym składnikiem innych technologii instalowania i odzyskiwania, takich jak Windows Setup, Windows Deployment Services, System Center Configuration Manager 2007 R2 oraz MDT 2010. W przeciwieństwie do wcześniejszych wersji Windows PE, które były dostępne tylko jako korzyść z licencji Software Assurance (SA), narzędzie Windows PE 3.0 jest teraz dostępne publicznie w pakiecie Windows AIK 2.0.

Windows PE zapewnia następujące funkcje i możliwości:

- Wbudowaną obsługę systemu plików NTFS 5.x, w tym tworzenie woluminów dynamicznych i zarządzania nimi.
- Wbudowaną obsługę sieci Transmission Control Protocol/Internet Protocol (TCP/IP) oraz udostępniania plików (tylko klient)
- Wbudowaną obsługę 32-bitowych (lub 64-bitowych) sterowników urządzeń dla systemu Windows
- Wbudowaną obsługę podzbioru interfejsu API Win32; opcjonalną obsługę Windows Management Instrumentation (WMI) i Windows Script Host (WSH)
- Może być uruchamiane z wielu nośników, w tym płyt CD, DVD, napędów USB oraz usług Windows Deployment Services

Windows PE działa za każdym razem, gdy instalujemy Windows 7, czy instalujemy system operacyjny, uruchamiając komputer z płyty DVD z systemem Windows 7, czy wdrażamy system Windows 7 z Windows Deployment Services. Narzędzia graficzne, które zbierają informacje konfiguracyjne podczas przebiegu konfiguracji Windows PE działają wewnątrz środowiska Windows PE. Ponadto możemy dostosowywać i rozszerzać środowisko Windows PE, aby spełniało określone potrzeby wdrożeniowe. Na przykład MDT 2010 dostosowuje Windows PE na potrzeby instalacji poprzez dodawanie sterowników urządzeń, skryptów wdrożeniowych, itd.

W przypadku systemu Windows 7, Windows PE 3.0 zawiera usprawnienia ułatwiające dostosowywanie go. Po pierwsze, funkcjonalność PEImg jest teraz zawarta w DISM, zapewniając pojedyncze narzędzie, z którego możemy skorzystać do obsługi obrazów niezależnie od tego, czy są to obrazy Windows 7, czy obrazy Windows PE. Po drugie Windows PE 3.0 wykorzystuje nowy model pakietów. Zamiast obrazu podstawowego zawierającego wszystkie pakiety funkcji, z których usuwamy wyłączone funkcje, obraz podstawowy nie zawiera tych pakietów funkcji, a dodajemy funkcje, które chcemy zamieścić w obrazie. Więcej informacji na temat Windows PE można znaleźć w rozdziale 9 „Przygotowywanie środowiska Windows PE”.

UWAGA Ponieważ Windows PE jest tylko podzbiorem systemu Windows 7, ma swoje ograniczenia. Na przykład Windows PE automatycznie zatrzymuje działanie powłoki i ponownie się uruchamia po 72 godzinach ciągłej pracy, aby zapobiegać piractwu. Nie możemy skonfigurować Windows PE jako serwera plików, serwera terminali lub wbudowanego systemu operacyjnego. Co więcej – mapowane litery napędów i zmiany w rejestrze nie są trwałe między sesjami. Więcej informacji na temat ograniczeń Windows PE można znaleźć w przewodniku *Windows Preinstallation Environment User's Guide* w pakiecie Windows AIK 2.0.

Narzędzie Deployment Image Servicing and Management

Deployment Image Servicing and Management (DISM) jest nowym narzędziem wiersza poleceń, które możemy wykorzystać do obsługi obrazów systemu Windows 7 offline przed wdrażaniem. Przy pomocy DISM możemy instalować, usuwać, konfigurować i aktualizować funkcje systemu Windows, pakiety, sterowniki urządzeń i ustawienia międzynarodowe. Niektóre polecenia DISM możemy wykorzystać do obsługi obrazów systemu Windows 7 online.

Możemy użyć DISM, aby:

- Dodawać, usuwać i wyliczać pakiety
- Dodawać, usuwać i wyliczać sterowniki
- Włączać lub wyłączać funkcje systemu Windows
- Zastosować zmiany w oparciu o sekcję offlineServicing pliku odpowiedzi Unattend.xml
- Skonfigurować ustawienia międzynarodowe
- Zaktualizować obraz systemu Windows do innego wydania
- Przygotować obraz Windows PE

- Wykorzystać lepsze rejestrowanie zdarzeń
- Obsługiwać wcześniejsze wersje systemu Windows
- Obsługiwać wszystkie platformy (32-bitowe, 64-bitowe oraz Itanium)
- Obsługiwać 32-bitowy obraz z poziomu maszyny 64-bitowej i vice versa
- Wykorzystać stare skrypty programu Package Manager

DISM konsoliduje funkcjonalność narzędzi Package Manager (Pkgmgr.exe), PEImg, oraz Intlcfg z systemu Windows Vista. Zapewnia jedno narzędzie służące do obsługi obrazów Windows 7 i Windows PE.

Inne narzędzia

Windows 7 i Windows AIK 2.0 zapewniają również różne narzędzia wiersza polecenia, które są przydatne podczas wdrażania:

- **BCDboot** Może szybko konfigurować partycję systemową lub naprawiać środowisko rozruchowe na partycji systemowej. Kopiuje mały zestaw plików środowiska rozruchowego z zainstalowanego obrazu systemu Windows 7 na partycję systemową. Tworzy również magazyn danych konfiguracji rozruchu (BCD) na partycji systemowej zawierający nowy wpis rozruchu umożliwiający uruchomienie systemu z tego obrazu systemu Windows.
- **Bootsect** Bootsect.exe aktualizuje główny kod rozruchowy dla partycji dysku twardego, przełączając go pomiędzy BOOTMGR a NTLDR. Można skorzystać z tego narzędzia, aby przywrócić sektor rozruchowy na komputerze. To narzędzie zastępuje FixFAT i FixNTFS.
- **DiskPart** Jest interpreterem poleceń trybu tekstowego w systemie Windows 7. Możemy użyć narzędzia DiskPart, aby zarządzać dyskami, partycjami lub woluminami, korzystając ze skryptów lub poleceń wprowadzanych bezpośrednio w wierszu polecenia. W systemie Windows 7, DiskPart może też montować pliki .vhd. Montowanie pliku .vhd umożliwia obsłużenie go lub dokonanie innych zmian offline.
- **Drvload** Dodaje sterowniki do rozruchowego obrazu Windows PE. Przyjmuje jeden lub kilka plików .inf ze sterownikami jako dane wejściowe. Aby dodać sterownik do obrazu Windows PE offline, należy użyć narzędzia DISM. Jeśli plik .inf sterownika wymaga powtórnego uruchomienia systemu, Windows PE zignoruje to żądanie. Jeśli plik .sys sterownika wymaga ponownego uruchomienia systemu, nie możemy dodać tego sterownika przy pomocy Drvload.
- **Expand** Rozpakowuje jeden lub kilka skompresowanych plików aktualizacji. Expand.exe pozwala otwierać aktualizacje dla systemu Windows 7, jak również dla poprzednich wersji systemu Windows. Korzystając z Expand, możemy otwierać i badać aktualizacje dla systemu Windows 7 w systemie operacyjnym Windows XP lub Microsoft Windows Server 2003.
- **Lpksetup** Możemy skorzystać z narzędzia Lpksetup, aby wykonywać nienadzorowane lub wykonywane w trybie cichym operacje pakietu językowego. Lpksetup działa tylko w uruchomionym systemie operacyjnym Windows 7.

- **Oscdimg** Jest narzędziem wiersza polecenia do utworzenia pliku obrazu (.iso) z niestandardową 32-bitową lub 64-bitową wersją Windows PE. Możemy następnie wypalić plik .iso na płycie CD-ROM lub DVD-ROM albo skopiować jego zawartość na napęd USB pozwalający na rozruch systemu.
- **Powercfg** Możemy skorzystać z narzędzia Powercfg, aby określić ustawienia zasilania i skonfigurować dla komputerów domyślne tryby uśpienia lub wstrzymania. W systemie Windows 7 narzędzie Powercfg zapewnia pomoc w rozwiązywaniu problemów przy diagnozowaniu kłopotów ze zużyciem energii.
- **Winpeshl** Winpeshl.ini określa, czy niestandardowa powłoka będzie ładowana w środowisku Windows PE zamiast domyślnego okna wiersza polecenia.
- **Wpeinit** Jest narzędziem wiersza polecenia, które inicjuje środowisko Windows PE za każdym razem, gdy jest ono uruchamiane. Gdy środowisko Windows PE jest uruchamiane, Winpeshl.exe wykonuje skrypt Startnet.cmd, który uruchamia Wpeinit.exe. Wpeinit.exe instaluje urządzenia Plug and Play (PnP), przetwarza ustawienia Unattend.xml i łączy zasoby sieciowe. Wpeinit zastępuje funkcję inicjacji obsługiwaną wcześniej przy użyciu polecenia Factory.exe *-winpe*. Wpeinit zapisuje komunikaty dziennika do pliku C:\Windows\System32\Wpeinit.log.
- **Wpeutil** Jest narzędziem wiersza polecenia, które możemy wykorzystać do uruchamiania różnych poleceń w sesji Windows PE. Na przykład możemy zamknąć lub ponownie uruchomić środowisko Windows PE, włączyć lub wyłączyć zaporę systemu Windows, zmienić ustawienia języka i zainicjować sieć.

Usługi Windows Deployment Services

Usługi Windows Deployment Services są zaktualizowaną i przeprojektowaną wersją usług instalacji zdalnej (RIS) z systemu Windows Server 2008. Usługi Windows Deployment Services pomagają organizacjom szybko wdrażać systemy operacyjne Windows, szczególnie system Windows 7. Korzystając z usług Windows Deployment Services, możemy wdrażać systemy operacyjne Windows poprzez sieć bez konieczności fizycznej obecności przy komputerze docelowym i bez korzystania z nośnika.

Usługi Windows Deployment Services zapewniają lepsze rozwiązanie procesu wdrażania niż usługi RIS. Zapewniają składniki platformy, które umożliwiają wykorzystanie rozwiązań niestandardowych, w tym możliwości zdalnego rozruchu; model wtyczek dla rozszerzeń serwera środowiska Pre-Boot Execution Environment (PXE); oraz protokół komunikacji klient-serwer do diagnostyki, rejestracji dziennika i wyliczania obrazów. Usługi Windows Deployment Services unifikują też pojedynczy format obrazów (.wim) i zapewniają znacznie poprawione środowisko zarządzające poprzez konsolę Microsoft Management Console (MMC) i narzędzia wiersza polecenia, z których można korzystać w skryptach.

Usługi Windows Deployment Services wykorzystują protokół Trivial File Transfer Protocol (TFTP) do pobierania sieciowych programów rozruchowych i obrazów. TFTP wykorzystuje konfigurowalny mechanizm okien, który ogranicza liczbę pakietów wysyłanych przez klientów korzystających z rozruchu przez sieć, co poprawia wydajność. Usługi Windows Deployment Services zapisują teraz też szczegółowe informacje o klientach w funkcji rejestrowania

dziennika systemu Windows Server 2008. Możemy eksportować i przetwarzać te dzienniki przy pomocy Microsoft Office InfoPath lub innych narzędzi do przetwarzania danych. Najistotniejszą nową i chyba najbardziej oczekiwaną funkcją jest multiemisja. Wdrażanie multiemisyjne pozwala wdrażać system Windows 7 na wielu komputerach jednocześnie, co pomaga oszczędzić pasmo sieciowe.

W systemach Windows 7 i Windows Server 2008 R2 usługi Windows Deployment Services zawierają następujące nowe funkcje:

- **Multicast Multiple Stream Transfer** Pozwala ustawiać progi wydajnościowe dla klientów multiemisji. Wolniejsi klienci mogą przechodzić do wolniejszych strumieni, tak aby nie spowalniali szybszych klientów, co było ograniczeniem pierwotnej funkcji multiemisji.
- **Dynamic Driver Provisioning** Pozwala programowi Windows Setup dynamicznie wybierać podczas wdrażania sterowniki urządzeń przechowywane na serwerach usług Windows Deployment Services. Sprawia to, że aktualizowanie obrazów systemu Windows poprzez dodawanie nowych sterowników urządzeń staje się mniej ważne, ponieważ można je po prostu dodawać do magazynu sterowników, co ogranicza rozmiar obrazu i koszty konserwacji. Możemy też wstawiać sterowniki urządzeń do obrazów Windows PE bezpośrednio z magazynu sterowników.

Więcej informacji na temat usług Windows Deployment Services można znaleźć w rozdziale 10 „Konfigurowanie Windows Deployment Services”.

ImageX

ImageX jest narzędziem systemu Windows 7, które wykorzystujemy do pracy z plikami obrazów .wim. ImageX jest łatwym w użyciu narzędziem wiersza poleceń. Możemy korzystać z ImageX do tworzenia i zarządzania plikami obrazów wim. Dzięki ImageX możemy przechwytywać obrazy i stosować je wobec twardych dysków komputerów docelowych. Możemy montować pliki obrazów .wim jako foldery i w ten sposób edytować obrazy offline. ImageX odpowiada na wyzwania, przed którymi stawały organizacje, korzystając z formatów obrazowania opartych na sektorach albo z polecenia XCopy systemu MS-DOS do kopiowania instalacji systemu Windows na nowy sprzęt. Na przykład obrazowanie oparte na sektorach:

- Niszczy istniejącą zawartość dysku twardego komputera docelowego, komplikując scenariusze migracji.
- Duplikuje dokładnie dysk twardy; dlatego obraz może być wdrażany tylko na partycjach, które są tego samego typu i mają co najmniej taki sam rozmiar jak partycja źródłowa na komputerze wzorcowym.
- Nie pozwala na bezpośrednie modyfikacje zawartości pliku obrazu.

Ograniczenia obrazowania opartego na sektorach doprowadziły firmę Microsoft do opracowania narzędzia ImageX i towarzyszącego mu formatu plików obrazów .wim. Możemy skorzystać z ImageX do utworzenia obrazu, zmodyfikowania go bez przechodzenia przez proces wyodrębniania plików i ponownego tworzenia oraz wdrażania obrazu w swoim środowisku – wszystko to przy użyciu tego samego narzędzia.

Ponieważ ImageX działa na poziomie plików, zapewnia wiele korzyści. Zapewnia większą elastyczność i kontrolę nad obrazami. Na przykład możemy zamontować obraz do folderu, a następnie dodawać pliki do obrazu, kopiować je z obrazu i usuwać, korzystając z narzędzia zarządzającego plikami, takiego jak Eksplorator Windows. ImageX pozwala na szybsze wdrażanie obrazów i szybsze instalacje. Dzięki formatowi obrazów opartemu na plikach możemy też wdrażać obrazy tak, że ImageX nie wyczyści zawartości dysku twardego komputera docelowego.

ImageX obsługuje też mocno skompresowane obrazy. Po pierwsze, pliki .wim obsługują pojedyncze wystąpienia plików: dane plikowe są przechowywane oddzielnie od informacji o ścieżkach, więc pliki .wim mogą przechowywać zduplikowane pliki, które istnieją w wielu ścieżkach jednocześnie. Po drugie, pliki .wim obsługują dwa algorytmy kompresji – szybki i maksymalny – które dają kontrolę nad rozmiarem obrazów i czasem wymagany do ich przechwycenia i wdrożenia.

Scenariusze wdrożeń

Ogólnie będziemy wykonywać zautomatyzowane wdrożenia systemu Windows 7 w czterech scenariuszach: aktualizacja komputera, nowy komputer, odświeżenie komputera i wymiana komputera. Dalsze części tego rozdziału zawierają przegląd każdego scenariusza.

Aktualizacja komputera

Możemy zaktualizować komputer z systemem Windows Vista Service Pack 1 (SP1) do Windows 7, co oznacza, że zainstalujemy Windows 7 i zachowamy istniejące aplikacje, pliki i ustawienia tak, jak były w poprzedniej wersji systemu Windows Vista. Jeśli chcemy jednak zaktualizować komputer z systemem Windows XP do Windows 7, będziemy musieli użyć scenariusza odświeżenia komputera, który zachowuje pliki i ustawienia, ale nie aplikacje. Więcej informacji można znaleźć pod tytułem „Scenariusz odświeżenia komputera” w dalszej części rozdziału.

Chociaż aktualizacja może być najprostszym sposobem wdrożenia systemu Windows 7, ryzykujemy zachowanie złych konfiguracji i nieautoryzowanego oprogramowania lub ustawień. W wielu przypadkach konfiguracja istniejącego systemu jest trudna do oceny a procesy sterujące zmianami są trudniejsze do zaimplementowania. Aktualizacja komputerów z systemem Windows Vista z Service Pack 1 w nieznanym stanie do systemu Windows 7 nie zmienia stanu komputera – jego stan nadal jest nieznanym. Lepszym scenariuszem dla środowisk zarządzanych jest wykorzystanie scenariusza nowego komputera z migracją stanu użytkownika w celu wybiórczego zachowania ustawień (to znaczy scenariusza odświeżenia komputera).

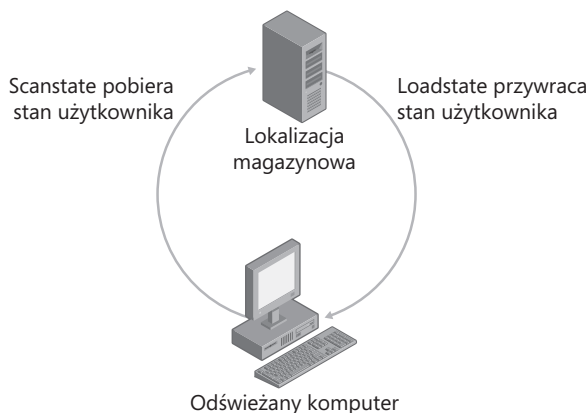
Nowy komputer

W scenariuszu nowego komputera instalujemy czystą kopię systemu Windows 7 na czystym (świeżo podzielonym na partycje i sformatowanym) twardym dysku. Ten scenariusz daje najbardziej spójne wyniki, tworząc konfigurację w znanym stanie. Instalacja znanej konfiguracji

na czystym komputerze jest podstawą dobrego zarządzania konfiguracją. Możemy skorzystać z uznanych procesów sterowania zmianami do ścisłego zarządzania wszelkimi następującymi zmianami.

Odświeżenie komputera

Scenariusz odświeżenia komputera jest podobny do scenariusza nowego komputera. Różnice polegają na tym, że komputer docelowy zawiera system operacyjny Windows, a ten scenariusz zachowuje istniejące pliki i ustawienia użytkownika, jak pokazano na rysunku 3-3.

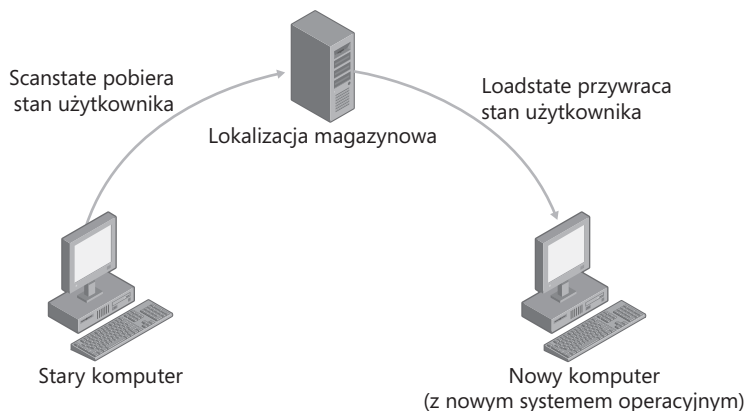


Rysunek 3-3 Zachowywanie stanu użytkownika podczas migracji

Możemy skorzystać z technologii migracji, takich jak USMT 4.0, żeby migrować pliki i ustawienia użytkownika z wcześniejszej wersji systemu Windows do Windows 7. Pomaga to zapewnić, że żadne dane nie zostaną utracone, tworząc przy tym najlepszą możliwą konfigurację systemu. Więcej informacji na temat korzystania z USMT 4.0 można znaleźć w rozdziale 7 „Migrowanie danych stanu użytkowników”. Możemy traktować scenariusz odświeżenia komputera jako połączenie korzyści z nowej instalacji zapewnianej przez scenariusz nowego komputera z korzyściami z zachowania plików i ustawień.

Wymiana komputera

Technologie migracji systemu Windows, takie jak narzędzie Łatwy transfer w systemie Windows i USMT 4.0, pozwalają na migrację danych pomiędzy starym komputerem działającym pod kontrolą systemu Windows XP lub Windows Vista a nowym komputerem działającym pod kontrolą systemu Windows 7. Ten scenariusz zwany scenariuszem wymiany komputera pozwala wykonać czystą instalację na nowym komputerze i po prostu przenieść pliki i ustawienia ze starego komputera. Rysunek 3-4 pokazuje przegląd tego scenariusza.



Rysunek 3-4 Wymiana komputera zaczyna się od nowego, czystego systemu.

Zrozumienie programu instalacyjnego

Aby zautomatyzować program Windows Setup, musimy najpierw zrozumieć proces instalacji. Znajomość wewnętrznego procesu pomoże zrozumieć decyzje, które musimy podjąć, przygotowując system Windows 7 do wdrożenia.

Proces instalacji systemu Windows 7 jest prosty. Wszystkie wydania systemu Windows 7 wykorzystują ten sam obraz instalacji (Install.wim w folderze Sources na nośniku instalacyjnym), ale firma Microsoft dostarcza nośniki specyficzne dla każdego wydania. W rezultacie możemy zainstalować tylko jedno wydanie systemu Windows 7 poprzez interfejs użytkownika, ale możemy też użyć pliku Unattend.xml, aby zainstalować inne wydanie. Proces instalacji jest podzielony na trzy fazy: Windows PE, Konfiguracja online i Windows Welcome.

Windows Setup działa w *fazach*, które są opisane w kolejnych częściach tego rozdziału. Fazy te – faza instalacji wstępnej, faza konfiguracji online i faza Windows Welcome – występują w tej kolejności i po prostu wyznaczają punkt w procesie instalacji. Windows Setup ma również *przebiegi* konfiguracji. Każdy przebieg konfiguracji wykonuje określoną funkcję i wprowadza powiązane ustawienia z pliku odpowiedzi Unattend.xml.

NA DOŁĄCZONYM NOŚNIKU Przewodnik *Windows Automated Installation Kit User's Guide* (Waik.chm), który jest zawarty w pakiecie Windows AIK 2.0, w pełni opisuje opcje wiersza polecenia do uruchamiania programu Windows Setup (Setup.exe).

Możemy dostosować proces instalacji w wielu fazach poprzez użycie plików odpowiedzi. Następująca lista opisuje pliki odpowiedzi używane do dostosowywania procesu instalacji systemu Windows 7:

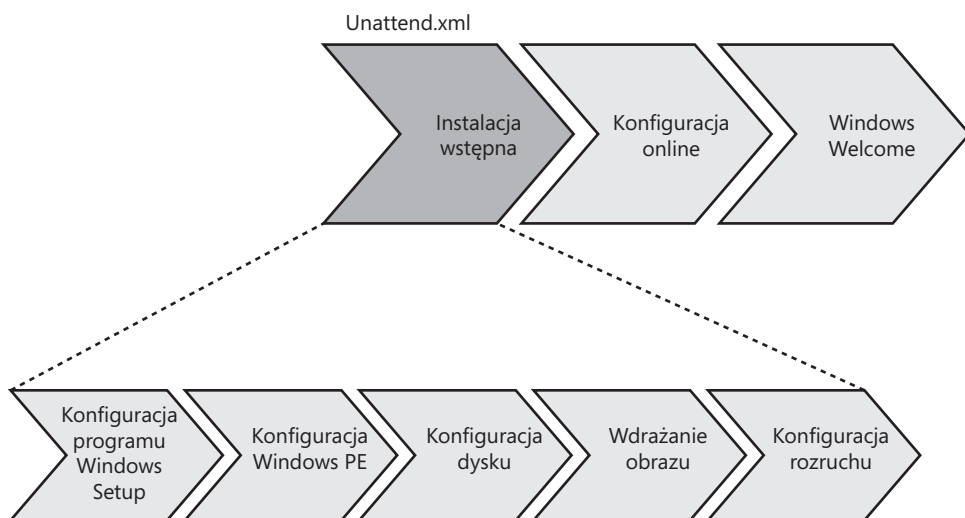
- **Unattend.xml** Ogólna nazwa nadawana plikowi odpowiedzi, który steruje większością działań instalacji nienadzorowanej i ustawieniami dla większości faz. Po nazwaniu go Autounattend.xml i umieszczeniu w odpowiednim folderze, takim jak główny folder

napędu USB, plik ten może w pełni automatyzować instalację z oryginalnego nośnika systemu Windows 7.

- **Oobe.xml** Oobe.xml jest plikiem zawartości używanym do dostosowywania faz: Windows Welcome i Welcome Center.

Faza instalacji wstępnej

Podczas fazy instalacji wstępnej program Windows Setup przygotowuje system docelowy do instalacji. Rysunek 3-5 ilustruje, gdzie ta faza znajduje się w procesie instalacji.



Rysunek 3-5 Faza instalacji wstępnej

Do zadań wykonywanych podczas fazy instalacji wstępnej należą:

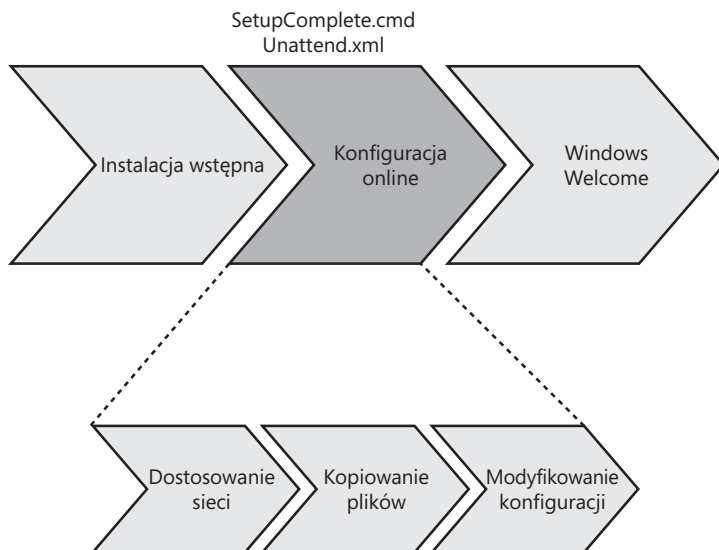
- **Konfiguracja programu Windows Setup** Program Windows Setup jest konfigurowany przy użyciu albo okien dialogowych Windows Setup (interaktywnie), albo pliku odpowiedzi (bez nadzoru). Konfiguracje programu Windows Setup obejmują konfigurowanie dysku lub ustawień językowych.
- **Konfiguracja Windows PE** Ustawienia pliku odpowiedzi są stosowane podczas przebiegu konfiguracji Windows PE.
- **Konfiguracja dysku** Dysk twardy jest przygotowywany do wdrażania obrazu. Może to obejmować partycjonowanie i formatowanie dysku.
- **Kopiowanie pliku obrazu systemu Windows** Obraz systemu Windows 7 jest kopiowany na dysk z nośnika dystrybucyjnego lub udziału sieciowego. Domyślnie obraz ten jest zawarty w pliku Sources\Install.wim na nośniku produktu lub udziale dystrybucyjnym.
- **Przygotowanie informacji rozruchowych** Finalizowana jest konfiguracja rozruchowa systemu Windows 7. Obejmuje to definiowanie ustawień konfiguracji rozruchowej.

- **Przetwarzanie ustawień pliku odpowiedzi w przebiegu konfiguracji offlineServicing**
Aktualizacje i pakiety są stosowane wobec obrazu systemu Windows 7, w tym poprawki oprogramowania, pakiety językowe i inne aktualizacje zabezpieczeń.

WIĘCEJ INFORMACJI Program Windows Setup tworzy wiele plików dziennika, które są przydatne do rozwiązywania problemów z instalacją. Więcej informacji na ten temat można znaleźć w artykule „Windows Setup Log File Locations” pod adresem <http://support.microsoft.com/default.aspx/kb/927521>.

Faza konfiguracji online

Podczas fazy konfiguracji online system Windows 7 wykonuje zadania dostosowawcze związane z tożsamością komputera. Rysunek 3-6 pokazuje, gdzie ta faza znajduje się w całym procesie.



Rysunek 3-6 Faza konfiguracji online

Przebieg Specialize, który jest uruchamiany podczas tej fazy, zajmuje się utworzeniem i zastosowaniem informacji specyficznych dla danego komputera. Na przykład możemy użyć pliku odpowiedzi instalacji nienadzorowanej (Unattend.xml), aby skonfigurować ustawienia sieciowe, ustawienia międzynarodowe i informacje o domenie, jak również uruchamiać programy instalacyjne.

Podczas fazy konfiguracji online możemy korzystać ze skryptów do konfigurowania komputera docelowego. Jednakże sekwencer zadań, który umożliwia filtrowanie zadań w oparciu o warunki, takie jak to, czy określone urządzenie jest zainstalowane, lepiej nadaje się do tego celu. Sekwencer zadań zapewnia też zaawansowane funkcje, takie jak możliwość odczekania, aż pewien warunek nastąpi, zanim przejdzie dalej oraz grupowanie zadań w foldery, a następnie filtrowanie całej grupy.

Instalacji w trybie tekstowym już nie ma

Michael Niehaus, Systems Design Engineer

Microsoft Deployment Toolkit

Podstawowy proces używany do instalowania Windows XP pozostał niezmieniony od najwcześniejszych dni Microsoft Windows NT. Ta czasochłonna procedura obejmowała początkowy krok instalacji w trybie tekstowym, w którym każdy plik systemu operacyjnego był rozpakowywany i instalowany, wszystkie wpisy rejestru tworzone i wszystkie ustawienia zabezpieczeń aplikowane. Począwszy od systemu Windows Vista ta faza instalacji w trybie tekstowym została zupełnie wyeliminowana. Zamiast tego nowy program instalacyjny wykonuje instalację, stosując obraz systemu Windows wobec danego komputera.

Po zastosowaniu tego obrazu musi być on dostosowany do komputera. To dostosowanie zajmuje miejsce tego, co było nazywane mini-instalacją w systemach Windows XP i Microsoft Windows 2000. Cel jest taki sam: system operacyjny zbiera potrzebne ustawienia i konfigurację dla określonego komputera, na którym został wdrożony.

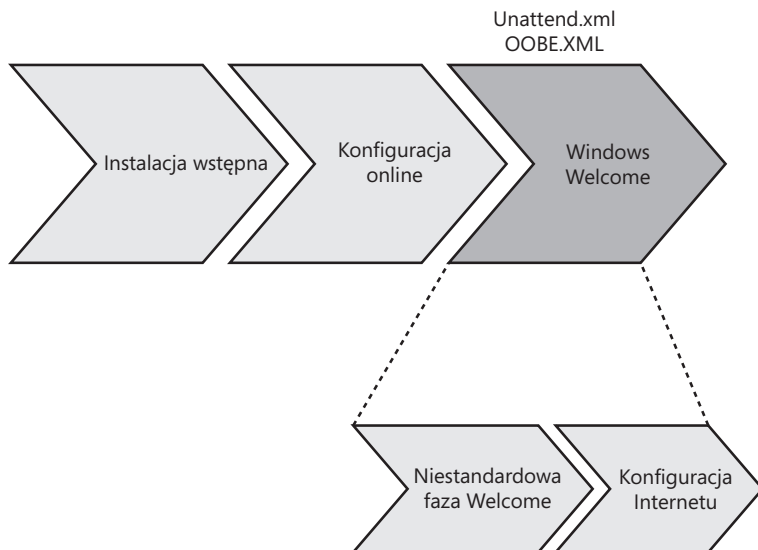
Proces przygotowywania obrazu również się zmienił. W Windows XP używaliśmy Sysprep do przygotowania referencyjnego systemu operacyjnego w celu wdrożenia na komputerze. Począwszy od systemu Windows Vista nadal uruchamiamy narzędzie Sysprep.exe, ale domyślnie jest ono instalowane w folderze C:\Windows\System32\Sysprep.

Począwszy od systemu Windows Vista system operacyjny Windows jest dostarczany na płycie DVD jako już zainstalowany, uogólniony (przez Sysprep) obraz, gotowy do wdrożenia na dowolnym komputerze. Niektórzy klienci mogą decydować się na wdrażanie tego obrazu tak, jak jest (być może wstawiając do niego poprawki lub sterowniki, korzystając z możliwości obsługowych zapewnianych przez narzędzia wdrożeniowe).

NA DOŁĄCZONYM NOŚNIKU Dołączony do książki dysk zawiera sekwencer zadań oparty na skryptach, Taskseq.wsf, który zapewnia między innymi wszystkie te zaawansowane funkcje. Odczytuje sekwencje zadań z plików .xml, a następnie je wykonuje. Plik Sample_Task_Sequences.zip zawiera przykładowe sekwencje zadań, które demonstrują, jak budować pliki .xml dla Taskseq.wsf. Nie należy uruchamiać tych przykładowych sekwencji zadań na komputerach produkcyjnych. Należy przeczytać dokumentację zawartą w kodzie źródłowym, aby uzyskać więcej informacji na temat korzystania z Taskseq.wsf.

Faza Windows Welcome

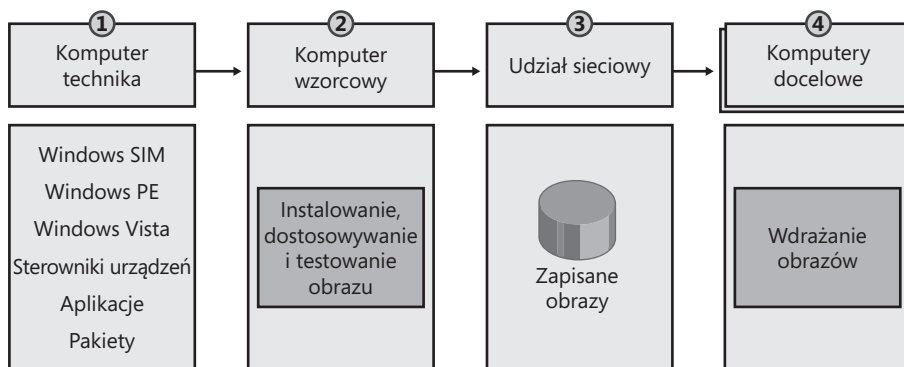
W fazie Windows Welcome, pokazanej na rysunku 3-7, instalacja jest finalizowana i przedstawiane są wszelkie dostosowania związane z pierwszym użyciem systemu, które chcemy zastosować. Dodatkowo system Windows 7 prosi o podanie klucza produktu podczas tej fazy. Możemy dostosować ekrany i komunikaty Windows Welcome i zapisać te ustawienia w pliku Oobe.xml.



Rysunek 3-7 Faza Windows Welcome

Podstawowy proces wdrożeniowy

Rysunek 3-8 ilustruje podstawowy proces wdrożeniowy korzystający jedynie z narzędzi wdrażania systemu Windows 7 do budowy obrazów do wdrażania na wielu komputerach. Chociaż jest to użyteczna informacja, bezpośrednie stosowanie tych narzędzi nie jest zalecane. Użycie platformy, takiej jak MDT 2010, jest najlepszym sposobem wdrażania systemu Windows 7.



Rysunek 3-8 Podstawowy proces wdrożeniowy

Poniższa lista opisuje kroki z rysunku 3-8:

- **Komputer techniczny** Na komputerze technicznym budujemy udział dystrybucyjny. Zawiera on pliki źródłowe systemu Windows 7, aplikacje, sterowniki urządzeń i pakiety. Korzystamy z narzędzia Windows SIM do skonfigurowania udziału dystrybucyjnego,

dodając do niego pliki źródłowe. Stosujemy też narzędzie Windows SIM do utworzenia i dostosowania pliku odpowiedzi Windows 7 do wykorzystania przy instalacji.

- **Komputer wzorcowy** Na komputerze wzorcowym tworzymy instalację wzorcową, uruchamiając Windows Setup z udziału dystrybucyjnego, korzystając z pliku odpowiedzi utworzonego przy pomocy Windows SIM. Instalacja powinna być w pełni zautomatyzowana, aby zapewniać spójny, powtarzalny proces pomiędzy poszczególnymi wdrożeniami. Po utworzeniu instalacji wzorcowej uruchamiamy Sysprep, aby przygotować ją do powielania. W niewielkich wdrożeniach możemy pominąć ten krok i wdrażać system na komputerach biurowych bezpośrednio z nośnika systemu Windows 7 zapewnianego przez firmę Microsoft, a następnie dostosowywać instalację podczas wdrażania.

Jak to działa

Przebiegi konfiguracji

Windows Setup wykorzystuje przebiegi konfiguracji do konfigurowania systemów. Poniższa lista opisuje każdy przebieg konfiguracji, który jest uruchamiany przez Windows Setup:

- **windowsPE** Konfiguruje opcje Windows PE, a także podstawowe opcje Windows Setup. Do opcji tych może należeć konfigurowanie dysku lub ustawień językowych.
- **offlineServicing** Stosuje aktualizacje wobec obrazu Windows 7, jak również pakiety, w tym poprawki oprogramowania, pakiety językowe i inne aktualizacje zabezpieczeń.
- **generalize** Przebieg generalize działa tylko wtedy, gdy uruchomimy sysprep /generalize. W tym przebiegu możemy minimalnie konfigurować system Windows 7, jak również konfigurować inne ustawienia, które muszą być utrwalone w obrazie wzorcowym. Polecenie sysprep /generalize usuwa informacje specyficzne dla danego systemu. Na przykład unikalny identyfikator SID i inne ustawienia specyficzne dla danego sprzętu są usuwane z obrazu.
- **specialize** Tworzy i stosuje informacje specyficzne dla danego systemu. Na przykład możemy skonfigurować ustawienia sieciowe, ustawienia międzynarodowe i informacje o domenie.
- **auditSystem** Przetwarza ustawienia instalacji nienadzorowanej, podczas gdy system Windows 7 działa w kontekście systemowym, zanim użytkownik zaloguje się na komputerze w trybie inspekcji. Przebieg auditSystem działa tylko wtedy, gdy uruchamiamy komputer w trybie inspekcji.
- **auditUser** Przetwarza ustawienia instalacji nienadzorowanej po zalogowaniu się przez użytkownika na komputerze w trybie inspekcji. Przebieg auditUser działa tylko wtedy, gdy uruchamiamy komputer w trybie inspekcji.
- **oobeSystem** Stosuje ustawienia dla systemu Windows 7, zanim uruchomiona zostanie faza Windows Welcome.

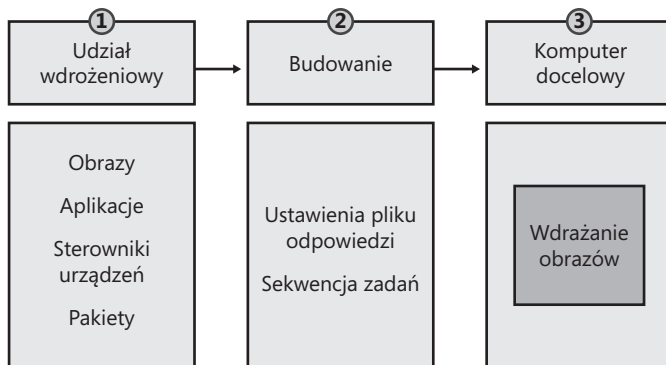
- **Udział sieciowy** Wykorzystujemy ImageX do przechwycenia obrazu instalacji wzorcowej z komputera wzorcowego. Następnie zapisujemy obraz w udziale sieciowym dostępnym dla komputerów docelowych, na których wdrażamy ten obraz. Do alternatyw dla wdrażania z udziału sieciowego należy wdrażanie obrazu z płyty DVD, napędu USB lub usług Windows Deployment Services.
- **Komputery docelowe** Na komputerach docelowych uruchamiamy Windows Setup, aby zainstalować system Windows 7. Windows Setup akceptuje plik obrazu i plik odpowiedzi do wykorzystania jako opcje wiersza polecenia. Korzystanie z Windows Setup w celu zastosowania obrazu na komputerach docelowych jest bardziej zalecane niż użycie ImageX do zastosowania obrazu. Windows Setup zawiera logikę, jakiej brak w ImageX, a która na przykład poprawnie przygotowuje dane konfiguracyjne rozruchu.

Proces Microsoft Deployment Toolkit

Microsoft Deployment Toolkit 2010 (MDT 2010) stanowi holistyczne podejście do wdrażania systemu na komputerach biurkowych, zbierając razem ludzi, procesy i technologie wymagane do przeprowadzenia udanych, powtarzalnych i konsekwentnych projektów wdrożeniowych. Z powodu silnego skupienia się na metodologii i najlepszych praktykach, MDT 2010 jest znacznie cenniejszy niż suma swoich części. Nie tylko przynosi korzyść w postaci zmniejszenia czasu wymaganego do opracowania projektu wdrożenia na komputerach biurkowych, ale też redukuje błędy i pomaga stworzyć wysokiej jakości projekt wdrożeniowy.

Microsoft poleca, aby korzystać z MDT 2010 do wdrażania systemu Windows 7 zamiast bezpośredniego korzystania z podstawowych narzędzi wdrożeniowych. Wszystkie narzędzia wdrożeniowe w Windows 7 i Windows AIK 2.0 są znacznymi usprawnieniami w stosunku do narzędzi wdrożeniowych dla wcześniejszych wersji systemu Windows. Jednakże są one po prostu narzędziami bez platformy, bez żadnej logiki biznesowej. Nie mają „kleju” wiążącego je z końcowym procesem. MDT 2010 zapewnia ten „klej” w postaci kompletnej platformy technologicznej. Wewnętrznie MDT 2010 jest niezwykle skomplikowanym rozwiązaniem. Zapewnia rozwiązywanie problemów, przed jakimi staje większość klientów podczas wdrażania, w tym podczas faz instalacji wstępnej (partycjonowanie dysku, formatowanie, itd.), instalacji (obrazowanie dysku) i faz poinstalacyjnych (migracja stanu użytkownika, instalacja aplikacji, dostosowywanie, itd.). Chociaż MDT 2010 jest wewnętrznie skomplikowany, rozwiązanie to sprawia, że budowanie, dostosowywanie i wdrażanie obrazów systemu Windows 7 jest łatwiejsze dzięki zamaskowaniu szczegółów.

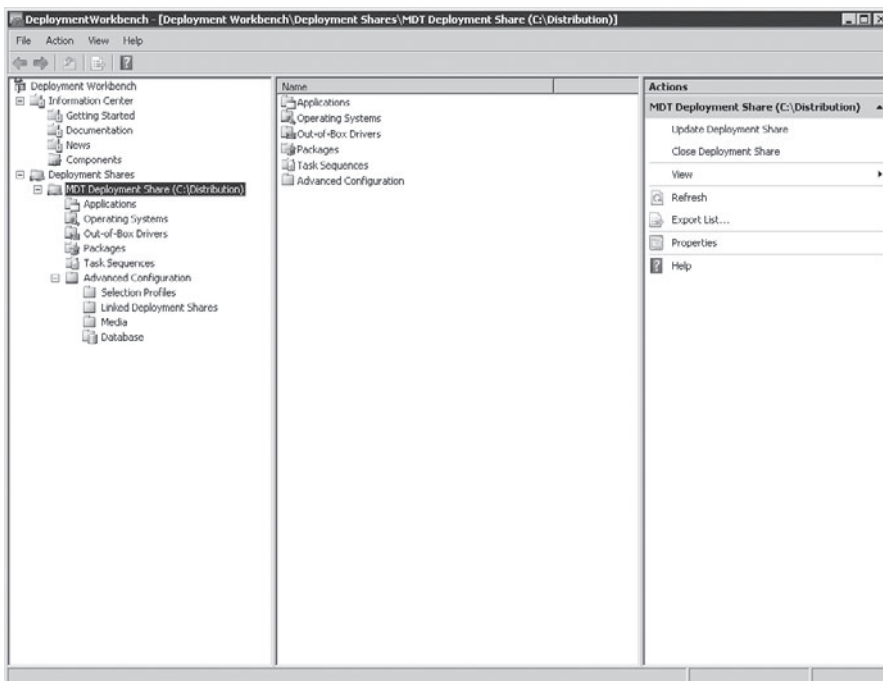
Rysunek 3-9 opisuje typowy proces użycia MDT 2010 do wdrażania systemu Windows 7. Proces ten jest taki sam, czy przechwytujemy obraz w laboratorium, czy wdrażamy obraz w środowisku produkcyjnym. Dodatkowo MDT 2010 zapewnia interfejs użytkownika do konfigurowania wszystkich swoich procesów. Tysiące wierszy kodu działa w tle, aby implementować nasze wybory dokonywane podczas wdrażania.



Rysunek 3-9 Proces Microsoft Deployment Toolkit

Poniższa lista opisuje każdą część procesu MDT 2010 (więcej informacji można znaleźć w rozdziałach 6 i 12).

- Udział wdrożeniowy** Po zainstalowaniu MDT 2010 na serwerze w środowisku laboratoryjnym korzystamy z narzędzia Deployment Workbench, aby wypełnić udział wdrożeniowy plikami źródłowymi. Do plików źródłowych należą obrazy systemu Windows 7, aplikacje, sterowniki urządzeń i pakiety. Deployment Workbench zapewnia interfejs użytkownika do dodawania wszystkich plików źródłowych do udziału wdrożeniowego. Ten interfejs użytkownika zapewnia też inteligencję, taką jak sprawdzanie błędów i budowanie bazy danych sterowników urządzeń do wstawiania odpowiednich sterowników urządzeń podczas wdrażania.



Microsoft Deployment Toolkit

Manu Namboodiri

Windows Product Management

Firma Microsoft zainwestowała dużo w zapewnienie innowacyjnych technologii, które pomagają klientom efektywnie wdrażać komputery biurkowe, zwłaszcza nowe możliwości związane z obrazowaniem opartym na plikach, architekturami opartymi na funkcjach, niezależnością sprzętową, itd. Daje to znaczące korzyści przy ograniczaniu liczby obrazów, kosztów i złożoności.

Jednakże słyszeliśmy wiele komentarzy od naszych klientów i partnerów w związku z najlepszymi praktykami i metodologią wykorzystania tych narzędzi najbardziej efektywnie. Słyszymy też od analityków branżowych, że większość wyzwań migracyjnych, przed którymi stają klienci, skupia się wokół budowy zespołów, harmonogramów, planów projektów, przypadków biznesowych i właściwego zestawu obrazów, jak również procesu i metodologii. Technologia sama w sobie odgrywa mniejszą rolę w udanych wdrożeniach, niż byśmy myśleli.

Wyzwania stojące przed naszymi klientami są następujące:

- Brak standardowego zestawu wskazówek wdrożeniowych, co powoduje bardzo zmienne wyniki i koszty przy wdrożeniach komputerów biurkowych
- Większe skupienie się na technologii, a mniejsze na metodologii, co spowodowało zróżnicowane typy rozwiązań, a przez to zróżnicowane wyniki
- Poczucie wysokich kosztów/skomplikowania ze strony klienta z powodu braku powtarzalnych i spójnych procesów związanych z tą technologią
- Niejasne zalecenia związane z tym, którego z wielu nowych narzędzi używać i kiedy

Ujawnienie się tych problemów spowodowało, że skoncentrowaliśmy się na ulepszeniu zaleceń związanych z wdrożeniami. Wynikiem jest znacznie poprawiona metodologia MDT dla wdrażania komputerów biurkowych. Pracujemy z ekspertami branżowymi, integratorami systemów i dostawcami oprogramowania wdrożeniowego/zarządzającego w celu ulepszenia tych zaleceń tak, aby obejmowały najlepsze praktyki pochodzące z całej branży.

- **Sekwencja zadań** Gdy udział wdrożeniowy zostanie całkiem wypełniony, korzystamy z Deployment Workbench, aby utworzyć sekwencję zadań. Sekwencja zadań kojarzy pliki źródłowe z udziału wdrożeniowego z listą kroków, które mają być podjęte podczas instalacji. Sekwencja zadań określa, kiedy należy podjąć dany krok, a kiedy go pominąć (filtrowanie). Sekwencja zadań obsługuje ponowne uruchamianie systemu podczas instalacji, a dane zebrane podczas sekwencji zadań są zachowywane pomiędzy kolejnymi uruchomieniami systemu. Sekwencja zadań reprezentuje jeden z głównych punktów dostosowywania w MDT 2010.

■ **Komputer docelowy** Mając w pełni wyposażony udział wdrożeniowy i sekwencję zadań, możemy użyć MDT 2010 do wdrażania systemu Windows 7 na komputerach docelowych. Możemy korzystać z instalacji z niewielkim udziałem obsługi do wdrażania systemu Windows 7. Aby skorzystać z tego rodzaju instalacji, uruchamiamy komputer docelowy, korzystając z obrazu rozruchowego Windows PE na udziale wdrożeniowym. Możemy umieścić obraz rozruchowy na nośniku wymiennym (DVD, napęd USB, itd.) albo dodać go do serwera usług Windows Deployment Services. W każdym razie uruchamiamy komputer docelowy, wykorzystując obraz rozruchowy Windows PE zapewniający przez udział wdrożeniowy, żeby rozpocząć działanie kreatora Windows Deployment Wizard. Ten kreator wyświetla kilka stron w celu zebrania informacji (nazwa komputera, członkostwo w domenie, aplikacje do zainstalowania, itd.), a następnie instaluje system operacyjny bez dalszej interakcji z obsługą.

Możemy też skorzystać z instalacji bez udziału użytkownika do wdrażania systemu Windows 7. MDT 2010 integruje się bezpośrednio z System Center Configuration Manager 2007. Więcej informacji na temat korzystania z tego typu instalacji można znaleźć w dokumentacji MDT 2010.

Warto zwrócić uwagę, że rysunek 3-9 nie odwołuje się do tworzenia instalacji wzorcowej i przechwytywania obrazu. W MDT 2010 tworzenie i przechwytywanie obrazu jest procesem instalacji z niewielkim udziałem obsługi. Możemy skonfigurować dowolny udział wdrożeniowy, aby przechwytywał obraz instalacji i automatycznie przechowywać ten obraz w tym udziale wdrożeniowym. Po dokonaniu tego wyboru proces obrazowania jest w pełni zautomatyzowany. Nie musimy uruchamiać Sysprep ani ImageX – kreator Windows Deployment Wizard automatycznie uruchomi Sysprep, a następnie ImageX, aby przechwycić obraz i zapisać go w udziale wdrożeniowym. Następnie możemy po prostu dodać ten obraz do udziału wdrożeniowego, korzystając z Deployment Workbench.

UWAGA MDT 2010 możemy pobrać z <http://technet.microsoft.com/en-us/desktopdeployment/default.aspx>.

Podsumowanie

Platforma wdrożeniowa i narzędzia wdrożeniowe systemu Windows 7 ułatwią wdrażanie tego systemu operacyjnego w organizacji w porównaniu z wdrażaniem wcześniejszych wersji systemu Windows. Format pliku .wim umożliwia wdrażanie mocno skompresowanych plików obrazów. System Windows 7 pomaga ograniczyć liczbę obrazów, usuwając zależności sprzętowe z obrazu. Modularyzacja w systemie Windows 7 ułatwia obsługę obrazów tak, że nie musimy już użyć, dostosować i ponownie przechwycić obrazu, aby go zaktualizować. Format pliku odpowiedzi Unattend.xml zapewnia elastyczniejszą i bardziej spójną konfigurację. Wreszcie narzędzia wdrożeniowe DISM, ImageX i Windows SIM zapewniają solidny sposób tworzenia, dostosowywania i zarządzania obrazami systemu Windows 7.

Chociaż pakiet Windows AIK 2.0 zapewnia podstawowe narzędzia do dostosowywania i wdrażania systemu Windows 7, MDT 2010 zapewnia elastyczniejszą platformę do wdrażania systemu Windows 7 w organizacjach. Dzięki MDT 2010 możemy tworzyć i dostosowywać wiele obrazów. Platforma ta zawiera automatyzację typową dla większości organizacji i można ją rozszerzać tak, aby odpowiadała wszelkim wymaganiom.

Dodatkowe zasoby

Dodatkowe informacje i narzędzia związane z tym rozdziałem zawierają następujące zasoby.

Powiązane informacje

- Przewodnik *Windows Automated Installation Kit User's Guide* zawarty w pakiecie Windows AIK 2.0 zawiera szczegółowe informacje na temat każdego z narzędzi opisanych w tym rozdziale.
- Rozdział 6 „Przygotowywanie obrazów dysków” zawiera więcej informacji na temat korzystania z MDT 2010 do tworzenia udziałów wdrożeniowych oraz tworzenia i przechwytywania obrazów.
- Rozdział 9 „Przygotowywanie środowiska Windows PE” zawiera więcej informacji na temat dostosowywania środowiska Windows PE do wdrażania systemu Windows 7.
- Rozdział 10 „Konfigurowanie Windows Deployment Services” zawiera więcej informacji na temat instalowania, konfigurowania i wykorzystania usług Windows Deployment Services do wdrażania systemu Windows 7.
- Rozdział 12 „Wdrażanie przy użyciu Microsoft Deployment Toolkit” zawiera więcej informacji na temat korzystania z pakietu Microsoft Deployment Toolkit do wdrażania obrazów systemu Windows 7.
- <http://technet.microsoft.com/en-us/desktopdeployment/default.aspx> zawiera najnowsze informacje dotyczące korzystania z Microsoft Deployment Toolkit do wdrażania systemu Windows 7.
- Witryna Deployment Forum pod adresem <http://www.deploymentforum.com/> jest kierowaną przez członków społeczności profesjonalistów IT wdrażających system Windows 7.
- Windows Automated Installation Kit 2.0 (Windows AIK 2.0) i Microsoft Deployment Toolkit 2010 (MDT 2010) można pobrać z witryny Microsoft Download Center pod adresem <http://www.microsoft.com/downloads>.

Na dołączonym nośniku

- Taskseq.wsf
- Sample_Task_Sequences.zip

Planowanie wdrożenia

- Korzystanie z Microsoft Deployment Toolkit 115
- Planowanie wdrożeń na dużą skalę 119
- Planowanie wdrożenia na małą skalę 124
- Wymagania systemu Windows 7 128
- Przygotowanie do wdrożenia 129
- Instalowanie Microsoft Deployment Toolkit 136
- Uruchamianie narzędzia Deployment Workbench 138
- Aktualizowanie składników pakietu Microsoft Deployment Toolkit 138
- Podsumowanie 140
- Dodatkowe zasoby 140

Ten rozdział pomaga nam zaplanować wdrożenie systemu operacyjnego Windows 7 w danej organizacji. Wdrożenie systemu operacyjnego wymaga ostrożnego planowania. Zgodność aplikacji, migracja stanu użytkowników, automatyzacja i inne problemy komplikują ten proces – co sprawia, że wdrażanie jest czymś więcej, niż tylko zainstalowaniem nowego systemu operacyjnego na grupie komputerów biurowych. Ten rozdział pomoże nam skorzystać z najlepszych dostępnych narzędzi do planowania i odkryć problemy, które wymagają planowania tak, abyśmy mogli podjąć świadome decyzje na wczesnym etapie tego procesu.

Korzystanie z Microsoft Deployment Toolkit

Microsoft Deployment Toolkit 2010 (MDT 2010) jest najlepszym rozwiązaniem firmy Microsoft dla projektów wdrażania systemu Windows 7 na dużą skalę. Zmniejsza poziom skomplikowania i zwiększa standaryzację, pozwalając wdrażać podstawowy sprzęt i oprogramowanie dla wszystkich użytkowników i komputerów. Dzięki standardowym punktom odniesienia możemy łatwiej zarządzać środowiskiem obliczeniowym, poświęcać mniej czasu na zarządzanie i wdrażanie komputerów oraz dysponować większą ilością czasu na zadania krytyczne.

MDT 2010 zapewnia narzędzia automatyzujące oraz wskazówki pomagające ograniczyć pracę oraz zwiększyć niezawodność przez tworzenie ustandaryzowanych konfiguracji. Zapewnia w pełni rozwinięte procesy, pomagające wykonywać następujące zadania:

- Określać, które aplikacje mogą być ponownie wdrożone na nowym systemie, i uruchamiać proces opakowania i opatrzenia skryptami tych aplikacji tak, aby można było je szybko i spójnie ponownie zainstalować bez interwencji użytkownika.
- Tworzyć proces obrazowania do utworzenia standardowego, firmowego obrazu systemu Windows 7 do pomocy w zarządzaniu konfiguracją i przyspieszania wdrożeń.
- Ustanawiać proces przechwytywania stanu użytkownika z istniejących komputerów i przywracania stanu użytkownika na nowo wdrożonych komputerach.
- Zapewniać metodę tworzenia kopii zapasowej bieżącego komputera przed wdrożeniem systemu Windows 7.
- Zapewniać pełen proces faktycznego wdrażania nowych komputerów. Wskazówki obejmują instalację z niewielkim udziałem obsługi i bez żadnego udziału obsługi.

Chociaż z pewnością możemy podejmować projekty wdrażania na wielu komputerach bez MDT 2010, takie podejście nie jest zalecane. Wynika to z tego, że bez MDT 2010 musimy opracować własne procesy rozwijania i wdrażania systemu. Musimy też zdefiniować swoje własne najlepsze praktyki i opracować procedury automatyzujące. Korzystając z MDT 2010 jako platformy wdrożeniowej, oszczędzamy potencjalnie setki godzin, które w przeciwnym razie musielibyśmy poświęcić na pisanie skryptów, pisanie plików odpowiedzi, tworzenie obrazów, itd. Pakiet MDT 2010 obsługuje sam w sobie większość scenariuszy i możemy łatwo rozszerzać MDT 2010 w celu obsługi dodatkowych scenariuszy. Możemy nawet wykorzystywać MDT 2010 z większością technologii wdrożeniowych firm trzecich. Ten rozdział zakłada, że będziemy korzystać z MDT 2010.

MDT 2010 ma dwa główne składniki: dokumentację i platformę rozwiązań. Kolejne podrozdziały opisują te składniki bardziej szczegółowo. Wcześniejsze wersje MDT zapewniały szczegółowe wskazówki dotyczące planowania i pomoce dla poszczególnych prac. Jednakże ze względu na ogromny rozmiar dokumentacji w MDT firma Microsoft zredukowała dokumentację w MDT jedynie do podstawowych wskazówek technicznych. Dodatkowo MDT zawiera teraz przewodniki szybkiego startu, które zapewniają pełne instrukcje wdrażania instalacji z niewielkim udziałem obsługi i instalacji bez żadnego udziału obsługi. Fragment zatytułowany „Planowanie wdrożeń na dużą skalę” w dalszej części rozdziału opisuje zamiast dokumentacji MDT, jak planować projekty wdrożeń na dużą skalę.

UWAGA Należy zainstalować pakiet MDT 2010, aby przeglądać jego dokumentację w postaci skompilowanych plików pomocy (.chm). Po zainstalowaniu MDT 2010 kliknij Start, wskaż Wszystkie programy, wybierz Microsoft Deployment Toolkit, a następnie kliknij Microsoft Deployment Help. Aby dowiedzieć się, jak zainstalować MDT 2010, należy zajrzeć do podrozdziału „Instalowanie Microsoft Deployment Toolkit” w dalszej części rozdziału. Można pobrać dokumentację gotową do wydrukowania z witryny Microsoft Download Center pod adresem <http://www.microsoft.com/downloads>.

Dokumentacja

MDT 2010 zawiera trzy typy dokumentacji. Przewodniki techniczne zapewniają szczegółowe informacje na temat określonych obszarów technicznych, takich jak opakowywanie aplikacji albo inżynieria obrazów. Przewodniki referencyjne zawierają treść sformatowaną w postaci list i tabel, aby czytelnicy mogli szybko i łatwo znaleźć potrzebne informacje. Na przykład MDT 2010 zapewnia opisy obsługiwanych właściwości. Na koniec przewodniki szybkiego startu zapewniają kompletne instrukcje dla scenariuszy, takich jak wdrażanie instalacji z niewielkim udziałem obsługi lub instalacji bez żadnego udziału obsługi. Poniższe podrozdziały opisują te przewodniki.

Przewodniki techniczne

Poniższa lista opisuje przewodniki techniczne w MDT 2010:

- **Application Packaging Guide** Zapewnia wskazówki dotyczące przepakowywania aplikacji.
- **Deployment Customization Guide** Opisuje, jak dostosowywać wdrożenia instalacji z niewielkim udziałem obsługi lub instalacji bez żadnego udziału obsługi.
- **Microsoft Deployment Toolkit 2010 Samples Guide** Identyfikuje scenariusze wdrożeniowe i odpowiadające im ustawienia konfiguracji przy wdrażaniu komputerów docelowych przy pomocy instalacji z niewielkim udziałem obsługi lub instalacji bez żadnego udziału obsługi. Możemy skorzystać z przykładowych plików konfiguracyjnych w tym przewodniku jako z punktów wyjścia dla własnego projektu.
- **Microsoft Deployment Toolkit 2010 Management Pack** Opisuje instalację i konfigurację pakietu zarządzającego. MDT 2010 Management Pack może zapewniać szczegółowe informacje dotyczące procesu wdrażania MDT 2010 przeznaczone dla profesjonalistów IT biorących udział w procesach wdrożeniowych i operacyjnych.
- **Image Customization Guide** Opisuje, jak dostosowywać obrazy referencyjne poprzez ustawianie sekwencji zadań, rozwijanie niestandardowych skryptów, przegląd istniejących skryptów MDT 2010 itd. Zawiera informacje na temat zadań dostosowujących, takich jak konfigurowanie dysków, sieci i ról.
- **Preparing for LTI Tools** Opisuje, jak utworzyć domyślną instalację MDT 2010 dla wdrażania instalacji z niewielkim udziałem obsługi.
- **Preparing for Microsoft Systems Center Configuration Manager 2007** Opisuje, jak utworzyć domyślną instalację MDT 2010 dla wdrażania instalacji bez żadnego udziału obsługi przy pomocy Microsoft Systems Center Configuration Manager.
- **Microsoft System Center Configuration Manager 2007 Imaging Guide** Opisuje, jak korzystać z narzędzia Configuration Manager do przygotowywania tworzenia i wdrażania obrazów.
- **User State Migration Guide** Opisuje kluczowe składniki i decyzje dotyczące użycia narzędzia User State Migration Tool (USMT) do migracji danych o stanie użytkowników z poprzedniej do nowej konfiguracji.

- **Workbench Imaging Guide** Opisuje, jak korzystać z narzędzia Deployment Workbench do przygotowania tworzenia i wdrażania obrazów.

Przewodniki referencyjne

Poniższa lista opisuje przewodniki referencyjne w MDT 2010:

- **Toolkit Reference** Opisuje wszystkie kroki sekwencji zadań, które można dostosowywać; właściwości, które można konfigurować, wykorzystywać w skryptach lub stosować w sekwencerze zadań; każdy skrypt zawarty w sekwencji zadań; oraz punkty dostosowywania.
- **Troubleshooting Reference** Opisuje typowe kody błędów i błędy. Zapewnia rozwiązania pewnych problemów, o ile są dostępne.

Przewodniki szybkiego startu

Poniższa lista opisuje przewodniki szybkiego startu w MDT 2010:

- **Quick-Start Guide for Lite Touch Installation** Pomaga szybko ocenić przydatność MDT 2010, zapewniając skondensowane instrukcje krok po kroku, dotyczące wykorzystania MDT 2010 do instalowania systemów operacyjnych Windows przy pomocy instalacji z niewielkim udziałem obsługi
- **Quick-Start Guide for Microsoft Systems Center Configuration Manager 2007** Pomaga szybko ocenić przydatność MDT 2010, zapewniając skondensowane instrukcje krok po kroku, dotyczące wykorzystania MDT 2010 do instalowania systemów operacyjnych Windows przy pomocy narzędzia Configuration Manager

Platforma rozwiązań

Wykorzystujemy platformę rozwiązań (pliki technologiczne) do skonfigurowania serwerów obrazowania i wdrażania. Ta platforma pomaga tworzyć standardowe konfiguracje komputerów biurkowych. Zawiera narzędzia do budowania i wdrażania niestandardowych obrazów systemu Windows 7 o różnych specjalnych potrzebach, na przykład z tworzeniem kopii zapasowej komputera docelowego przed wdrożeniem, przechwytywaniem i przywracaniem stanu użytkownika, włączaniem szyfrowania dysków funkcją BitLocker, itd. Wykorzystując platformę rozwiązań jako punkt początkowy, możemy skorzystać z najlepszych praktyk wdrażania, które firma Microsoft i jej klienci opracowali przez kilka lat, z których większość przejawia się w kodzie skryptów tej platformy.

UWAGA Platforma rozwiązań nie zawiera kopii systemu Windows 7 albo pakietu Microsoft Office 2007. Aby skorzystać z MDT 2010, trzeba uzyskać licencjonowane kopie tego oprogramowania i innych programów związanych ze sprzętem, takich jak oprogramowanie odtwarzacza płyt DVD i oprogramowanie do nagrywania płyt CD. Każdy przewodnik techniczny w MDT 2010 opisuje wymagania związane z użyciem tych wskazówek oraz narzędzi.

Planowanie wdrożeń na dużą skalę

MDT 2008 i wcześniejsze wersje zawierały szczegółowe wskazówki dotyczące planowania i pomoce dla prac, które pomagały przygotowywać zespoły projektowe, synchronizować ich pracę i zarządzać punktami kontrolnymi. Jednakże firma Microsoft skondensowała dokumentację w wersjach MDT 2008 Update 1 i MDT 2010, aby wyeliminować większość wskazówek dotyczących planowania. Ten ruch pomógł ograniczyć ogromną ilość dokumentacji, ułatwiając korzystanie z niej ludziom, którzy potrzebowali tylko wskazówek technicznych.

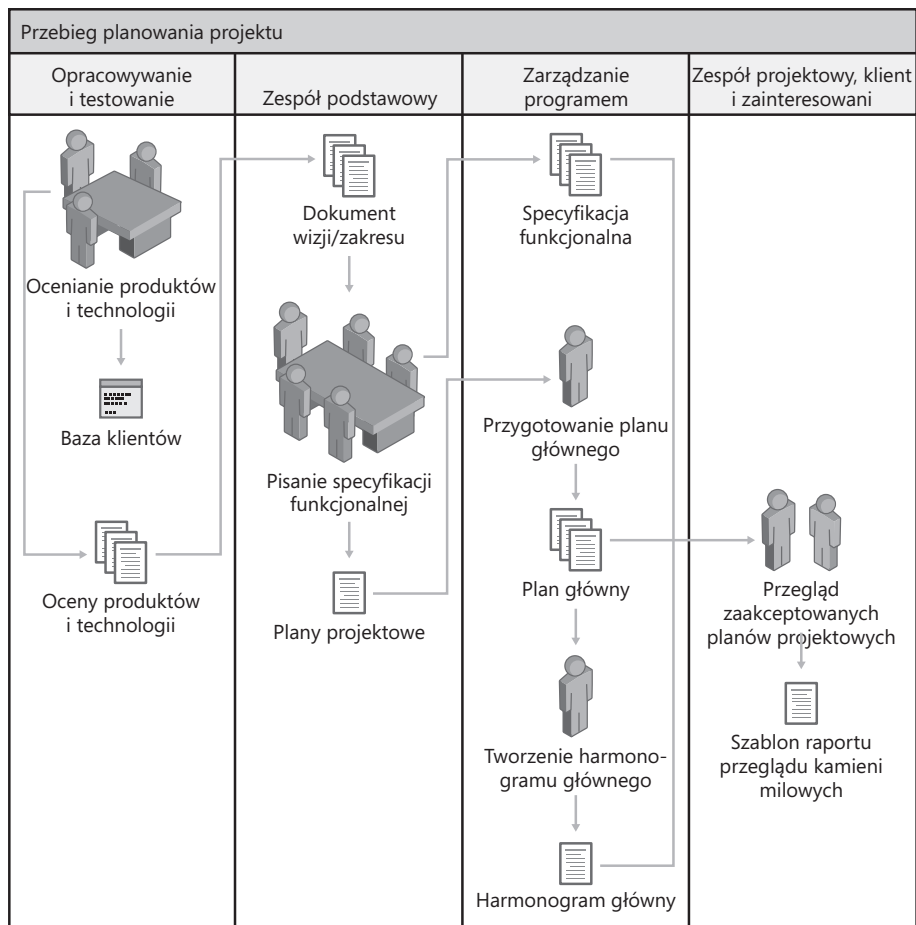
Firma Microsoft nadal jednak zapewnia świetne wskazówki dotyczące planowania i zarządzania projektami wdrożeń na dużą skalę. W istocie jest nawet lepiej: Platforma Microsoft Operations Framework (MOF) 4.0, dostępna pod adresem <http://technet.microsoft.com/en-us/library/cc506049.aspx>, zapewnia wskazówki dotyczące zarządzania projektami i pomoce dla zadań oparte na oryginalnym przewodniku *Planning Guide* z MDT 2008. W MOF 4.0 faza dostarczania wykorzystuje znajomą terminologię: *wizja, planowanie, budowanie, stabilizowanie i wdrażanie* (były to fazy z poprzedniej dokumentacji MDT, a są funkcjami zarządzania usługami (SMF) we wskazówkach MOF 4.0). Te wskazówki opisują przepływ zadań zawierający dane wejściowe, zakresy odpowiedzialności, działania, wyniki i przeglądy dla każdego kroku. Rysunek 4-1 jest przykładem typów przepływu zadań, które MOF 4.0 obsługuje dla wdrożeń na dużą skalę.

Te wskazówki pomagają wykonywać następujące zadania:

- Przechwytywać potrzeby biznesowe i wymagania przed planowaniem rozwiązania
- Przygotowywać specyfikację funkcjonalną i projekt rozwiązania
- Opracowywać plany pracy, szacunki kosztów i harmonogramy dla generowanych wyników
- Budować rozwiązanie zgodne ze specyfikacją klienta tak, aby wszystkie funkcje były zrealizowane, a rozwiązanie gotowe do zewnętrznego testowania i stabilizowania.
- Przedstawiać rozwiązanie najwyższej jakości dzięki wykonywaniu dokładnych testów i pilotowaniu wersji próbnych.
- Wdrażać stabilne rozwiązanie w środowisku produkcyjnym i stabilizować rozwiązanie na etapie produkcji.
- Przygotowywać zespoły operacyjne i wspierające do zarządzania oraz zapewniania obsługi klienta dla rozwiązania.

UWAGA MDT 2010 nie zawiera już pomocy do zadań związanych z pisaniem dokumentów wstępnych, specyfikacji funkcjonalnych, itd. Pomoce te są teraz zawarte w MOF 4.0. Można pobrać te pomoce do zadań z witryny Microsoft Download Center pod adresem <http://go.microsoft.com/fwlink/?LinkId=116390>.

Dalsze części tego rozdziału opisują każdą funkcję etapu dostarczania z platformy MOF 4.0. Ponieważ MOF 4.0 jest platformą ogólną, poniżej wiążemy każdą funkcję konkretnie z przeprowadzaniem wdrożenia na dużą skalę przy użyciu MDT 2010.



Rysunek 4-1 Funkcje planowania projektu w MOF 4.0

Wizja

Funkcja wizji obejmuje przedstawienie wizji projektu wdrożenia i określenie celów oraz oczekiwanych wyników. Funkcja wizji jest w dużym stopniu ćwiczeniem zarządczym; nie organizujemy pełnych zespołów projektowych, dopóki ta faza się nie zakończy. Funkcja wizji obejmuje następujące kluczowe kroki:

- **Zorganizowanie głównych zespołów** Początkowym zadaniem jest zdefiniowanie zespołów, które zaplanują, zaprojektują i wykonają wdrożenie.
- **Wykonanie bieżącego szacowania** Krok ten obejmuje zidentyfikowanie istniejących systemów i aplikacji, określenie istniejących systemów operacyjnych i identyfikację braków w bieżącym środowisku, na które odpowie wdrożenie systemu Windows 7.
- **Zdefiniowanie celów biznesowych** Konkretnie, mierzalne cele biznesowe powinny napędzać potrzebę nowego wdrożenia. Zamiast po prostu planować wdrażanie najnowszej technologii dla samej tylko technologii, należy zidentyfikować kluczowe braki

w istniejącym systemie, które zostaną rozwiązane przez system Windows 7, a także korzyści procesowe i wydajnościowe, które będą możliwe do uzyskania dzięki wdrożeniu.

- **Tworzenie opisu wizji i definiowanie zakresu** Należy utworzyć określenie wizji, które definiuje, w jaki sposób zmiany technologii (w tym wdrożenie systemu Windows 7) spełni zdefiniowane cele biznesowe. Zakres określa zasięg wizji, który można osiągnąć poprzez wdrożenie systemu Windows 7.
- **Tworzenie profili użytkowników** Należy opracować dokładny i pełny obraz funkcji, potrzeb i pragnień użytkowników. Trzeba go przetworzyć na profile użytkowników, które precyzyjnie identyfikują typy użytkowników w organizacji. Zrozumienie użytkowników i ich potrzeb jest pierwszym krokiem do określenia, jaką strukturę powinno mieć wdrożenie, aby skorzystała z niego większość użytkowników.
- **Opracowanie koncepcji rozwiązania** Należy utworzyć dokument wysokiego poziomu, aby zdefiniować, w jaki sposób zespół spełni wymagania projektu.
- **Tworzenie dokumentów szacujących ryzyko** W tym kroku oceniamy całkowite wdrożenie pod kątem oczekiwania, przeciwdziałania i reagowania na ryzyka związane z wdrożeniem. Dokumentacja oceny ryzyka jest ciągłym zadaniem podczas całego projektu.
- **Opisanie struktury projektu** Ten dokument opisuje, w jaki sposób zespół zarządza i wspiera projekt oraz omawia strukturę administracyjną zespołu projektowego. Ten dokument powinien definiować standardy, z których zespół będzie korzystał – w tym metody komunikacji, standardy dokumentacji i standardy kontroli zmian.
- **Akceptacja punktów kontrolnych** Gdy zakończymy początkowe planowanie i dokumentowanie, identyfikujemy kluczowe punkty kontrolne procesu wdrożenia i tworzymy ich harmonogram.

UWAGA MOF 4.0 zapewnia pomoce do zadań pomagające ukończyć wiele spośród tych kroków związanych z opracowaniem wizji.

Planowanie projektu

Funkcja wizji tworzy platformę dla wdrożenia systemu Windows 7. Funkcja planowania projektu służy jako przejście od wizji do implementacji, kładąc podwaliny pod faktyczne wdrożenie. Funkcja planowania projektu wykorzystuje dokumenty i procesy utworzone w funkcji wizji, aby dodawać strukturę i zawartość do planu wdrożenia. Kluczowe kroki w tej fazie obejmują następujące zadania:

- **Tworzenie środowiska projektowego i testowego** Budowa laboratorium testowego, które obejmuje środowisko wdrażania, przy użyciu wirtualizacji w celu zredukowania kosztów utworzenia laboratorium. Oprócz zasobów, takich jak serwery i przykładowe systemy docelowe wykorzystywane do opracowania i przetestowania wdrożenia, laboratoria powinny również zawierać zasoby, które zespół projektowy będzie wykorzystywał do przygotowania i osiągnięcia finalnego wdrożenia.
- **Opracowanie projektu rozwiązania** Projekt rozwiązania bazuje na koncepcji rozwiązania, strukturze projektu i innych dokumentach utworzonych w fazie wizji do zdefiniowania

konceptyjnego, logicznego i fizycznego projektu rozwiązania dla planowanego wdrożenia. Ten dokument służy jako mapa drogowa dla zespołu projektowego przy rozpoczynaniu budowania wdrożenia.

- **Utworzenie specyfikacji funkcjonalnej** Specyfikacja funkcjonalna definiuje wymagania wszystkich uczestników, do których kierowane jest wdrożenie i służy jako kontrakt pomiędzy klientem a zespołem projektowym. Powinna jasno definiować cele, zakres i wyniki wdrożenia.
- **Opracowanie planu projektu** Plan projektu jest w istocie zbiorem planów odpowiadających na zadania, które zespół projektowy będzie realizował w celu przeprowadzenia projektu zgodnie z definicjami w specyfikacji funkcjonalnej. Każdy plan w tym dokumencie obejmuje określony obszar, taki jak infrastrukturę i sprzęt, testowanie, szkolenie i komunikację.
- **Utworzenie harmonogramu projektu** Harmonogram projektu łączy pojedyncze harmonogramy tworzone przez członków zespołu do celów planowania działań wdrożeniowych.
- **Wykonanie inwentaryzacji komputerów** W funkcji planowania projektu należy wykonać pełną inwentaryzację komputerów, aby zidentyfikować istniejące systemy i aplikacje, na które wdrożenie będzie miało wpływ. Ponadto zasoby serwerowe, które mają być wykorzystane do wdrożenia, również muszą zostać zidentyfikowane i powinna być oceniona ich przydatność.
- **Przeprowadzenie analizy sieci** Należy wykonać diagram topologii sieci oraz zidentyfikować i zinwentaryzować urządzenia sieciowe.

UWAGA MOF 4.0 zawiera pomoce do zadań dla wielu spośród tych zadań planowania.

Budowanie

Funkcja budowania jest okresem, w którym zespół buduje i testuje rozwiązanie. Faza budowania obejmuje sześć kluczowych zadań:

- **Rozpoczęcie cyklu realizacyjnego** W tym początkowym kroku zespół tworzy serwer laboratoryjny dla prac realizacyjnych i zaczyna proces tworzenia obrazów, skryptów instalacyjnych i pakietów aplikacji. Zespół powinien również utworzyć system śledzenia problemów tak, aby członkowie zespołu mogli zgłaszać problemy i koordynować rozwiązania tych problemów.
- **Przygotowanie środowiska komputerowego** W tym kluczowym zadaniu zespoły budują środowisko wdrożeniowe, obejmujące taką infrastrukturę jak serwery, sieci, kopie zapasowe i repozytoria danych (takie jak Microsoft Visual SourceSafe) z osobnymi przestrzeniami roboczymi (to znaczy komputerami i udziałami sieciowymi) dla każdej roli w zespole. To środowisko zapewnia zespołom infrastrukturę do pracy niezależnej i wspólnej w celu ukończenia swoich zadań.
- **Opracowywanie skryptów dla rozwiązania** W tym kroku zespoły rozpoczynają proces pakowania aplikacji, tworzenia obrazów komputerów i opracowywania kroków

zaradczych dla problemów ze zgodnością aplikacji. Zespoły planują również, jak i jakie dane użytkowników będą zachowywane i migrowane podczas wdrożenia oraz sprawdzają poprawność konfiguracji i działania infrastruktury sieciowej (to znaczy udziały, poświadczenia i inne składniki) przed wdrożeniem.

- **Opracowywanie procedur wdrożeniowych** Przy wykorzystaniu dokumentów, procesów i innych zasobów utworzonych do tej pory rozpoczyna się tworzenie dokumentów, których zespoły będą używać do przeprowadzenia wdrożenia i zadań powdrożeniowych. Do dokumentów tych należą materiały dla użytkowników, administratorów i innych osób, które będą utrzymywać systemy i aplikacje po wdrożeniu; plan komunikacji z użytkownikami w związku z nadchodzącymi zmianami; oraz miejscowe procedury wdrożeniowe upraszczające i standaryzujące wdrażanie rozwiązań w różnych lokalizacjach.
- **Opracowywanie procedur operacyjnych** Tworzenie dokumentu, który opisuje procedury operacyjne dotyczące wspierania, konserwacji i przeprowadzania rozwiązania po wdrożeniu. Do kluczowych procesów, które trzeba opisać, należą konserwacja, odzyskiwanie po awariach, instalacja w nowych lokalizacjach, monitorowanie wydajności i błędów oraz wsparcie i rozwiązywanie problemów.
- **Testowanie rozwiązania** Przeprowadzanie testowych wdrożeń i przygotowywanie rozwiązań dla problemów, które się pojawiają, przy pomocy platformy śledzenia utworzonej w fazie planowania projektu do monitorowania i rozwiązywania tych problemów.

Stabilizacja

Funkcja stabilizacji zajmuje się testowaniem kompletnego rozwiązania. Ta faza zwykle występuje, gdy przeprowadzane są wdrożenia pilotażowe i kładzie nacisk na testowanie w świecie rzeczywistym w celu identyfikowania, szeregowania i naprawiania błędów. Do kluczowych zadań w tej fazie należą:

- **Przeprowadzanie pilotażu** Na tym etapie zespoły wykorzystują małe wdrożenie pilotażowe do przetestowania wdrożenia i zidentyfikowania wszelkich pozostałych problemów. Procedury, zasoby i personel powinny być przygotowane do pomocy w rozwiązywaniu wszelkich problemów użytkowników, które powstaną podczas wdrożenia pilotażowego. To kluczowe zadanie powinno też obejmować uzyskiwanie informacji zwrotnej od użytkowników, jak również przegląd i łagodzenie problemów identyfikowanych podczas pilotażu.
- **Przegląd gotowości operacyjnej** Wszystkie zespoły na tym etapie przeprowadzają pełny przegląd gotowości operacyjnej, aby stwierdzić, że plan wdrożeniowy jest gotowy do przejścia do wdrożenia na pełną skalę. Rozwiązanie jest zamrożone na tym etapie, a wszelkie pozostałe problemy rozwiązywane.
- **Ostateczne wydanie** To zadanie wciela wszystkie poprawki i rozwiązania problemów w celu utworzenia ostatecznego wydania rozwiązania, które powinno być teraz gotowe do pełnego wdrożenia.

Wdrażanie

W fazie wdrażania zespół implementuje rozwiązanie oraz sprawia, że jest ono stabilne i gotowe do użycia. Do kluczowych zadań związanych z fazą wdrażania należą:

- **Wdrażanie technologii podstawowych** W oparciu o plany i procedury opracowane w fazie planowania projektu należy zainstalować, skonfigurować i przetestować serwery wdrożeniowe w każdej lokalizacji. Trzeba też przeszkolić personel administracyjny w celu przygotowania do wdrożenia.
- **Wdrażanie lokalizacji** Zespoły przeprowadzają wdrażanie systemu Windows 7 w każdej lokalizacji, korzystając z procedur i zasobów opracowanych przez fazy planowania projektu i budowy. Członkowie zespołów pozostają na miejscu w lokalizacjach, żeby stabilizować wdrożenie w każdej lokalizacji, zapewniając, że użytkownicy mogą zacząć pracę z solidnymi systemami i aplikacjami i potwierdzając, że cele planu wdrożeniowego dla danej lokalizacji zostały spełnione.
- **Stabilizowanie wdrożenia** W tym kluczowym kroku zespół projektowy zapewnia stabilizację we wszystkich lokalizacjach i reaguje na pozostałe problemy wdrożeniowe.
- **Kończenie wdrożenia** Ten krok oznacza przejście od wdrażania do działań operacyjnych i wsparcia. Bieżące operacje są przekazywane przez zespół projektowy stałemu personelowi. Aktywowane są systemy raportowania, a procesy wsparcia działają w pełni.

Planowanie wdrożenia na małą skalę

W małoskalowych projektach wdrożeniowych, na przykład w małej lub średniej firmie, wskazówki planowania w platformie MOF 4.0 mogą być przytłaczające. Mimo wszystko platforma technologiczna MDT 2010 dobrze się nadaje do projektów wdrożeń na małą skalę. W istocie mała firma może przygotować MDT 2010 do wdrażania systemu Windows 7 w ciągu kilku godzin, a średnia firma może to osiągnąć w kilka dni. Ta część rozdziału opisuje niektóre kroki planowania, które powinniśmy podjąć w tym scenariuszu wdrażania na małą skalę (choć możemy użyć platformy technologicznej MDT 2010 bez korzystania ze wskazówek planowania dostępnych w MOF 4.0, nadal powinniśmy poświęcić nieco wysiłku na zaplanowanie wdrożenia zgodnie z tym, co zostało tutaj zarysowane).

Pierwszym krokiem w procesie wdrażania jest oszacowanie konkretnych potrzeb biznesowych tak, abyśmy mogli zdefiniować zakres i cele projektu. Następnie trzeba zdecydować, jak najlepiej wykorzystać system Windows 7 do spełnienia tych potrzeb. Następnie oceniamy bieżącą konfigurację sieci i komputerów, określamy, czy musimy zaktualizować sprzęt lub oprogramowanie i wybieramy narzędzia do przeprowadzenia wdrożenia. Po podjęciu tych decyzji jesteśmy gotowi na zaplanowanie wdrożenia. Skuteczny plan zwykle obejmuje następujące elementy:

- **Harmonogram wdrożenia** Należy zbudować prosty harmonogram, korzystając z programu Microsoft Office Excel 2007 lub wykorzystując bardziej formalne narzędzie jak Microsoft Office Project 2007.

- **Wszystkie szczegóły potrzebne do dostosowania systemu Windows 7 do naszych wymagań** Należy udokumentować aplikacje, sterowniki urządzeń, aktualizacje i ustawienia, które chcemy dostosować.
- **Ocena bieżącej konfiguracji, w tym informacje o użytkownikach, strukturze organizacyjnej, infrastrukturze sieciowej oraz sprzęcie i oprogramowaniu** Należy utworzyć środowisko testowe, w którym możemy wdrażać system Windows 7, wykorzystując funkcje i opcje danego planu. Środowisko testowe powinno odzwierciedlać sieć produkcyjną jak najlepiej, w tym sprzęt, architekturę sieci i aplikacje biznesowe.
- **Plany testowe i pilotażowe** Gdy będziemy zadowoleni z wyników uzyskiwanych w danym środowisku testowym, możemy przeprowadzić wdrożenie na określonej grupie użytkowników, żeby przetestować wyniki w kontrolowanym środowisku produkcyjnym. Jest to test pilotażowy.
- **Plan finalnego wdrożenia** Na koniec należy wdrożyć system Windows 7 w całej organizacji.

Tworzenie planu wdrożeniowego jest procesem cyklicznym. Podczas przechodzenia przez każdą fazę, można modyfikować plan w oparciu o doświadczenia.

UWAGA Nawet jeśli wybierzemy, że nie będziemy korzystać ze wskazówek wdrożeniowych w MOF 4.0, nadal możemy korzystać z zawartych tam pomocy do zadań, które zapewniają szablony do szybszego i dokładniejszego planowania projektu wdrożeniowego.

Zakres i cele

Zakres jest podstawą do utworzenia specyfikacji dla projektu wdrożeniowego. Zakres konkretnego projektu wdrożeniowego jest w dużym stopniu definiowany przez odpowiedzi na następujące pytania:

- Jakie potrzeby biznesowe chcemy spełnić przy pomocy Windows 7?
- Jakie są długoterminowe cele dla projektu wdrożeniowego?
- Jak klienckie komputery z Windows 7 będą komunikować się z infrastrukturą IT?
- Z jakimi częściami infrastruktury IT projekt będzie się stykał i jak się to będzie odbywać?

Zakres jest po prostu stwierdzeniem, co staramy się osiągnąć i jak planujemy to osiągnąć. Nasze określenie zakresu powinno mieć tylko kilka akapitów i nie być dłuższe niż strona.

Bieżące środowisko

Należy udokumentować istniejące środowisko komputerowe, przyglądając się strukturze danej organizacji i sposobowi wspierania przez nią użytkowników. Należy wykorzystać tę ocenę do określenia gotowości do wdrożenia systemu Windows 7 na komputerach biurowych. Do trzech głównych obszarów środowiska komputerowego, które należy ocenić, należą sprzęt, oprogramowanie i sieć.

- **Sprzęt** Czy komputery biurowe i laptopy spełniają minimalne wymagania sprzętowe dla systemu Windows 7? Oprócz spełniania tych wymagań cały sprzęt musi być zgodny z systemem Windows 7. Więcej informacji można znaleźć w rozdziale 1 „Przegląd usprawnień w systemie Windows 7”.
- **Oprogramowanie** Czy aplikacje są zgodne z systemem Windows 7? Trzeba się upewnić, że wszystkie używane aplikacje działają na komputerach z systemem Windows 7. Więcej informacji na temat zgodności aplikacji można znaleźć w rozdziale 8 „Rozpowszechnianie aplikacji”.
- **Sieć** Należy udokumentować architekturę sieci, w tym topologię, rozmiar i wzorce ruchu. Trzeba również określić, którzy użytkownicy muszą mieć dostęp do różnych aplikacji i danych oraz opisać, jak uzyskują ten dostęp.

UWAGA Tam, gdzie to konieczne, należy tworzyć diagramy w celu dołączenia do planu projektu. Diagramy przekazują więcej informacji niż same słowa. Dobrym narzędziem do tworzenia takich diagramów jest program Microsoft Office Visio 2007. Więcej informacji można znaleźć pod adresem <http://www.microsoft.com/office>.

Plan konfiguracji

Musimy ustalić, które funkcje zawrzeć w konfiguracji i jak zaimplementować te funkcje, aby uprościć zarządzanie użytkownikami i komputerami w danej organizacji. Ważnym środkiem upraszczającym jest standaryzacja. Standaryzowanie konfiguracji komputerów biurowych ułatwia instalowanie, aktualizowanie, zarządzanie, wspieranie i zastępowanie komputerów działających pod kontrolą systemu Windows 7. Standaryzacja ustawień konfiguracyjnych, oprogramowania, sprzętu i preferencji użytkowników upraszcza wdrażanie systemu operacyjnego i aktualizacje aplikacji; można też zagwarantować działanie zmian konfiguracyjnych na wszystkich komputerach.

Gdy użytkownicy instalują sami aktualizacje systemu operacyjnego, aplikacje, sterowniki urządzeń, ustawienia, preferencje i urządzenia sprzętowe, prosty problem może stać się skomplikowany. Ustalenie standardów dla konfiguracji komputerów biurowych zapobiega wielu problemom i ułatwia identyfikowanie oraz rozwiązywanie problemów. Posiadanie standardowej konfiguracji, którą możemy zainstalować na dowolnym komputerze, minimalizuje czas wyłączenia komputera z użytkowania dzięki sprawieniu, że ustawienia użytkowników, aplikacje, sterowniki i preferencje będą takie same, jak przed wystąpieniem problemu. Poniższa lista zapewnia przegląd kilku funkcji, których użycie musimy zaplanować:

- **Zarządzanie** Funkcje zarządzania komputerami biurowymi pozwalają ograniczyć całkowity koszt posiadania w naszej organizacji, ułatwiając instalowanie, konfigurowanie i zarządzanie klientami. Więcej informacji na temat funkcji zarządzania w systemie Windows 7 można znaleźć w części III tej książki „Zarządzanie komputerami biurowymi”.
- **Sieć** Możemy konfigurować komputery działające pod kontrolą systemu Windows 7 tak, aby uczestniczyły w różnych środowiskach sieciowych. Więcej informacji na temat funkcji sieciowych systemu Windows 7 można znaleźć w części V „Sieć”.

- **Zabezpieczenia** Windows 7 zawiera funkcje pomagające zabezpieczać sieć i komputery poprzez kontrolę uwierzytelniania i dostępu do zasobów oraz szyfrowanie danych przechowywanych na komputerach. Do funkcji tych należą szyfrowanie dysków funkcją BitLocker, zapora systemu Windows z zabezpieczeniami zaawansowanymi, itd. Więcej informacji na temat funkcji zabezpieczeń w systemie Windows 7 można znaleźć w rozdziale 2 „Bezpieczeństwo w systemie Windows 7”.

Testowanie i pilotaż

Przed uruchomieniem projektu wdrożeniowego musimy przetestować go pod względem funkcjonalności w kontrolowanym środowisku. Zanim zaczniemy testować projekt wdrożeniowy, tworzymy plan testów opisujący testy, które uruchomimy, kto będzie uruchamiał każdy test, harmonogram przeprowadzania testów i spodziewane wyniki. Plan testów musi określać kryteria i priorytet dla każdego testu. Określanie priorytetów testów może pomóc uniknąć spowolnienia wdrożenia z powodu drobnych błędów, które łatwo możemy poprawić później; może też pomóc identyfikować większe problemy, które mogą wymagać przeprojektowania planu.

Faza testowania jest istotna, ponieważ pojedynczy błąd może zostać powielony na wszystkich komputerach w środowisku, jeśli nie zostanie poprawiony przed wdrożeniem obrazu. Musimy utworzyć laboratorium testowe, które nie jest połączone z siecią, ale odzwierciedla sieć i konfigurację sprzętowe organizacji jak najbliżej. Należy skonfigurować sprzęt, oprogramowanie i usługi sieciowe w taki sposób, jak w środowisku produkcyjnym. Należy przeprowadzić wyczerpujące testy na każdej platformie sprzętowej, testując zarówno instalację, jak i działanie aplikacji. Te kroki mogą znacznie zwiększyć pewność siebie zespołów projektowych i osób podejmujących decyzje biznesowe, dając w efekcie wdrożenie o wyższej jakości.

Firma Microsoft zaleca, aby przeprowadzić projekt pilotażowy (tzn. wykonać wdrożenie) dla małej grupy użytkowników po przetestowaniu projektu. Instalacja pilotażowa pozwala ocenić sukces projektu wdrożeniowego w środowisku produkcyjnym przed przeprowadzeniem go dla wszystkich użytkowników. Głównym celem projektów pilotażowych nie jest testowanie systemu Windows 7, ale uzyskanie informacji zwrotnych od użytkowników. Te informacje zwrotne pomogą określić funkcje, które musimy włączyć lub wyłączyć w systemie Windows 7. Do programu pilotażowego możemy wybrać populację użytkowników, którzy reprezentują przekrój danej firmy, jeśli chodzi o pełnione funkcje i biegłość komputerową. Należy zainstalować systemy pilotażowe, korzystając z tej samej metody, którą planujemy wykorzystać w finalnym wdrożeniu.

Proces pilotażowy zapewnia na małą skalę test wdrożenia na pełną skalę: możemy wykorzystać wyniki pilotażu, w tym wszelkie napotkane problemy, do utworzenia planu finalnego wdrożenia. Należy zebrać wyniki pilotażu i wykorzystać te dane do oszacowania czasów aktualizacji, liczby jednoczesnych aktualizacji, które możemy obsłużyć i szczytowego obciążenia funkcji wsparcia użytkowników.

Przeprowadzanie wdrożenia

Po gruntownym przetestowaniu planu wdrożeniowego, przeprowadzeniu pilotażu wdrożenia dla mniejszych grup użytkowników i zadowoleniu z uzyskanych wyników, przystępujemy do przeprowadzenia wdrożenia systemu Windows 7 dla pozostałej części organizacji.

Aby utworzyć plan finalnego wdrożenia, musimy określić następujące elementy:

- Liczbę komputerów zawartych w każdej fazie wdrożenia
- Czas potrzebny do zaktualizowania lub wykonania czystej instalacji dla każdego komputera
- Personel i inne zasoby potrzebne do wykonania wdrożenia
- Ramy czasowe, w których planujemy wdrożyć instalacje dla różnych grup
- Szkolenia potrzebne użytkownikom w naszej organizacji

Podczas całego tego procesu będziemy zbierać informacje zwrotne od użytkowników i modyfikować plan wdrożenia w razie konieczności.

Wymagania systemu Windows 7

Aby zaplanować wdrożenie, musimy zrozumieć wymagania wdrożeniowe dla systemu Windows 7. Poniższe części tego rozdziału opisują minimalne wymagania sprzętowe i ścieżki migracji dla systemu Windows 7. Więcej informacji na temat wymagań sprzętowych i różnych wydań systemu Windows 7 można znaleźć w rozdziale 1.

Wymagania sprzętowe

Tabela 4-1 opisuje minimalne wymagania sprzętowe do zainstalowania systemu Windows 7. Częścią fazy planowania projektu jest przeprowadzenie inwentaryzacji sprzętu. Należy porównać wymagania sprzętowe z tabeli 4-1 z wykazem sprzętu, aby zidentyfikować wszelkie komputery, które wymagają aktualizacji lub wymiany.

Tabela 4-1 Minimalne wymagania sprzętowe dla komputerów z systemem Windows 7

Sprzęt	Minimalne wymagania
Procesor	1 GHz lub szybszy procesor 32-bitowy lub 64-bitowy
Pamięć	1 GB dla komputerów 32-bitowych lub 2 GB dla komputerów 64-bitowych
Karta graficzna	Karta graficzna zgodna z DirectX 9 ze sterownikiem Windows Display Driver Model (WDDM) 1.0 lub nowszym
Wolne miejsce na dysku	16 GB

UWAGA Minimalne wymagania dla systemu Windows 7 są takie same dla wszystkich wydań.

Ścieżki aktualizacji

Tabela 4-2 opisuje aktualizację systemu Windows 7 i ścieżki migracji. Jak pokazano w tej tabeli, obsługiwane jest przeprowadzenie aktualizacji w miejscu z systemu Windows Vista z Service Pack 1 (SP1) lub nowszego do systemu Windows 7. To oznacza, że możemy zainstalować system Windows 7 na komputerze działającym pod kontrolą systemu Windows

Vista z SP1 i zachować istniejące aplikacje, pliki i ustawienia. Obsługiwane jest też użycie funkcji Łatwy transfer w systemie Windows lub USMT do migracji stanów użytkowników z systemu Windows XP do Windows 7.

Tabela 4-2 Ścieżki migracji do systemu Windows 7

System źródłowy	Aktualizacja do systemu Windows 7?	Migracja do systemu Windows 7 przy użyciu funkcji Łatwy transfer w systemie Windows?	Migracja do systemu Windows 7 przy użyciu USMT?
Windows XP z SP2 lub późniejszy	Nie	Tak	Tak
Windows Vista z SP1 lub późniejszy	Tak	Tak	Tak
Windows 7	Tak (wyższe wydanie)	Tak	Tak

UWAGA Aby ocenić gotowość komputerów klienckich do przejścia na system Windows 7, możemy skorzystać z Microsoft Assessment and Planning Solution Accelerator, scentralizowanego i nie wykorzystującego agentów narzędzia, które może zdalnie przeprowadzić inwentaryzację komputerów, zidentyfikować wspieraną przez nie funkcjonalność Windows 7 i zalecić określone aktualizacje sprzętu, gdzie to konieczne. Więcej informacji na temat tego narzędzia można znaleźć w artykule „Microsoft Assessment and Planning (MAP) Toolkit” dostępnym pod adresem <http://technet.microsoft.com/en-us/solutionaccelerators/dd537566.aspx>.

Przygotowanie do wdrożenia

Czy organizacja wykorzystuje MDT 2010, czy nie, przygotowanie projektów wdrożeniowych na dużą skalę będzie prawdopodobnie wymagać wielu zespołów. Większość zespołów potrzebuje środowiska laboratoryjnego. Chociaż każdy zespół może konstruować oddzielne laboratorium, większość organizacji tworzy pojedyncze laboratorium, które udostępnia infrastrukturę, taką jak serwery, sieci, systemowe kopie zapasowe i kontrolę kodu źródłowego oddzielnym obszarom roboczym (komputerom i udziałom sieciowym) dla każdego zespołu. W tym środowisku zespoły mogą pracować oddzielnie, gdy to konieczne, i wspólnie, gdy to możliwe. Pomaga to też minimalizować liczbę wymaganych komputerów i serwerów.

Pozostałe rozdziały w części II tej książki „Wdrażanie” opisują określone wymagania laboratoryjne dla każdego zespołu pracującego nad projektem wdrożeniowym na dużą skalę. Faza planowania projektu jest jednak najlepszym momentem na rozpoczęcie przygotowywania środowiska projektowego. Proces ten obejmuje zainstalowanie MDT 2010, wyposażenie środowiska laboratoryjnego w pliki konieczne do wykonania zadania każdego z zespołów, lokalizację nośnika aplikacji, itd. Poniższe podrozdziały opisują kroki, które trzeba wykonać podczas fazy planowania projektu, aby usprawnić proces projektowy.

Zarządzanie aplikacjami

Zarządzanie aplikacjami jest procesem przepakowywania aplikacji lub automatyzowania ich instalacji i konfiguracji. Organizacje mogą mieć setki lub nawet tysiące aplikacji. Często użytkownicy instalują każdą aplikację inaczej na każdym komputerze, co prowadzi do braku spójności pomiędzy komputerami i powoduje problemy we wsparciu i zarządzaniu.

Przepakowywanie lub automatyzowanie instalacji aplikacji ma wiele korzyści. Co najbardziej oczywiste, pozwala instalować aplikacje bez interwencji użytkownika, co jest szczególnie pożądane przy wdrażaniu aplikacji jako części obrazu dysku lub podczas wdrażania obrazu dysku. Ponadto przepakowywanie lub automatyzowanie prowadzi do spójności, która obniża koszty wdrażania i posiadania aplikacji, ograniczając problemy związane ze wsparciem i usprawniając zarządzanie. Rozdział 8 opisuje proces przepakowywania i automatyzowania instalacji aplikacji.

Przed migracją z aktualnej wersji systemu Windows do Windows 7 zespół projektowy musi też przetestować aplikacje, aby zapewnić, że są one zgodne z systemem Windows 7. Możemy mieć kilka tysięcy aplikacji zainstalowanych w sieciach rozproszonych. Problemy ze zgodnością dla jednej lub wielu spośród tych aplikacji mogą zakłócić wydajność i pogorszyć odczucia i satysfakcję użytkowników z tego projektu. Testowanie aplikacji i rozwiązywanie problemów ze zgodnością oszczędza czas i pieniądze organizacji. Zapobiega też blokadom przyszłych projektów wdrożeniowych.

Chociaż większość aplikacji opracowanych dla wcześniejszych wersji systemu Windows będzie prawdopodobnie dobrze działać w systemie Windows 7, niektóre aplikacje mogą zachowywać się inaczej z powodu dostępnych w nim nowych technologii. Należy przetestować następujące aplikacje, aby zapewnić ich zgodność:

- Niestandardowe narzędzia, takie jak skrypty logowania
- Podstawowe aplikacje, które są częścią standardowych konfiguracji komputerów biurowych, takie jak pakiety biurowe
- Aplikacje biznesowe, takie jak pakiety do planowania zasobów przedsiębiorstwa
- Narzędzia administracyjne, takie jak aplikacje antywirusowe, do kompresji danych, do tworzenia kopii zapasowych i do zdalnego sterowania

Rozdział 5 „Testowanie zgodności aplikacji” opisuje, jak zbudować laboratorium do testowania zgodności aplikacji i jak zgodność aplikacji integruje się z całym procesem wdrożenia. Poniższa lista opisuje kroki, które możemy podjąć w fazie planowania projektu, aby rozpocząć budowanie środowiska laboratoryjnego do przepakowywania aplikacji i testowania zgodności:

- **Nośniki instalacyjne** Dla każdej aplikacji, którą testujemy, przepakowujemy lub automatyzujemy, musimy mieć kopię nośnika instalacyjnego aplikacji, wszelką dokumentację dotyczącą konfiguracji i klucze produktowe. Jeśli departament IT nie ma nośnika lub innych informacji, należy sprawdzić to u eksperta dziedzinowego dla każdej aplikacji.
- **Komputery docelowe** W laboratorium zespół projektowy wymaga komputerów docelowych, które przypominają komputery znajdujące się w środowisku produkcyjnym. Każdy komputer docelowy powinien mieć zainstalowany system Windows 7 w celu

testowania zgodności aplikacji z tym systemem operacyjnym oraz procesu instalowania aplikacji.

- **Application Compatibility Toolkit** Więcej informacji na temat pakietu Application Compatibility Toolkit (ACT) można znaleźć w rozdziale 5.
- **SQL Server** Należy zainstalować Microsoft SQL Server w środowisku laboratoryjnym. Pakiet ACT przechowuje spis aplikacji, korzystając z programu SQL Server, który jest dostępny na nośnikach licencji grupowych.
- **Komputer główny z udziałami sieciowymi** Potrzebny będzie komputer, na którym umieścimy instalacje aplikacji. Udziały na tym komputerze zawierają oryginalne źródła instalacji i gotowe pakiety. Możemy zainstalować ACT i SQL Server na tym samym komputerze.
- **Oprogramowanie do opakowywania aplikacji** Zespół projektowy potrzebuje oprogramowania, przy pomocy którego będzie mógł przepakowywać aplikacje. Rozdział 8 opisuje to oprogramowanie. Oprogramowanie do pakowania aplikacji będzie instalowane na komputerze każdego członka zespołu.
- **Mechanizm wdrażania** Zespół projektowy wymaga mechanizmu do wdrażania pakietu ACT i pakietów aplikacji. Może to być dokonywane przez skrypty logowania, lokalną witrynę WWW lub inne mechanizmy wdrożeniowe.

Inżynieria obrazów

Prawdopodobnie wszyscy Czytelnicy są już zaznajomieni z narzędziami do obrazowania dysków, takimi jak Symantec Ghost lub ImageX (wprowadzony w systemie Windows Vista). Efektywne korzystanie z narzędzi do obrazowania jest jednak znaczącym wyzwaniem, a to wyzwanie jest powodem, dla którego firma Microsoft opracowała MDT 2010. Dzięki MDT 2010 nie musimy opracowywać całego procesu obrazowania; platforma ta zapewnia większość potrzebnego kodu. Wystarczy go dostosować tak, aby odpowiadał wymaganiom danej organizacji. Użycie MDT 2010 do budowy obrazów systemu Windows 7 wymaga następujących kroków:

- **Utworzenie serwera budowania** Serwer budowania jest komputerem głównym dla MDT 2010 i udziału dystrybucyjnego.
- **Skonfigurowanie udziału wdrożeniowego** Udział wdrożeniowy zawiera pliki źródłowe (system Windows 7, aplikacje, sterowniki urządzeń, itd.), z których budujemy obrazy systemu operacyjnego.
- **Tworzenie i dostosowywanie sekwencji zadań** Po wypełnieniu udziału wdrożeniowego tworzymy sekwencje zadań. Sekwencje zadań kojarzą pliki źródłowe z udziału wdrożeniowego z krokami niezbędnymi do ich zainstalowania i skonfigurowania. Więcej informacji na temat plików odpowiedzi i sekwencji zadań można znaleźć w rozdziale 3 „Platforma wdrożeniowa”.
- **Budowanie początkowych obrazów systemu operacyjnego** Zbudowanie niestandardowego obrazu systemu Windows 7 przy pomocy MDT 2010 jest tak proste jak zainstalowanie systemu operacyjnego z udziału wdrożeniowego przy pomocy kreatora Windows

Deployment Wizard. Jest to proces instalacji z niewielkim udziałem obsługi, który wymaga minimalnej interakcji z użytkownikiem; automatycznie przechwytuje obraz systemu Windows 7 i zapisuje go z powrotem w udziale wdrożeniowym.

Rozdział 6 „Przygotowywanie obrazów dysków” opisuje użycie MDT 2010 do budowania niestandardowych obrazów systemu Windows 7. We wstępie do procesu przygotowywania obrazów możemy zacząć budowanie laboratorium podczas fazy planowania projektu, korzystając z elementów na następującej liście:

- **Nośnik systemu Windows 7** Będzie potrzebny nośnik i klucze licencji grupowej dla systemu Windows 7.
- **Komputery docelowe** Będą potrzebne komputery, na których będziemy tworzyć instalacje i testować obrazy systemu Windows 7.
- **Komputer budowania dla MDT 2010** Musimy mieć komputer, na którym chcemy utrzymywać MDT 2010 i udział wdrożeniowy. Komputer budowania powinien mieć napęd DVD-RW i powinien być połączony siecią z komputerami docelowymi. Możemy instalować MDT 2010 na komputerze biurowym lub na serwerze.
- **Windows Deployment Services** Środowisko laboratoryjne powinno zawierać serwer z uruchomionymi usługami Windows Deployment Services. Korzystanie z usług Windows Deployment Services do rozruchu komputerów docelowych jest znacznie szybsze niż wypalanie płyt DVD i uruchamianie z nich komputerów.
- **Dodatkowe pliki źródłowe** Wcześniej, w fazie planowania projektu zespół projektowy może zacząć zbieranie plików źródłowych wymaganych do wypełnienia udziału dystrybucyjnego. Do plików źródłowych należą sterowniki urządzeń i aplikacje specyficzne dla sprzętu dla każdego komputera w środowisku produkcyjnym. Dodatkowo zespół powinien zacząć zbierać wszelkie aktualizacje zabezpieczeń i pakiety systemu operacyjnego, które muszą zostać dodane do udziału dystrybucyjnego.

UWAGA Faza planowania projektu jest najlepszym momentem, aby zainstalować MDT 2010 w środowisku laboratoryjnym i rozpocząć zaznajamianie się z nim. Pod nagłówkiem „Instalowanie Microsoft Deployment Toolkit” w dalszej części rozdziału opisano wymagania dla zainstalowania MDT 2010 i instrukcje, jak zainstalować MDT 2010 w środowisku laboratoryjnym.

Wdrażanie

Wdrażanie jest intensywnym, czasochłonnym procesem podczas każdego wdrożenia na dużą skalę. MDT 2010 zapewnia wskazówki techniczne i narzędzia, które pomogą usprawnić następujące procesy:

- Wybór umieszczenia serwera
- Ocena serwera i pojemności sieci
- Instalacja udziałów dystrybucyjnych i narzędzi
- Wdrożenie komputerów klienckich

Rozdział 12 „Wdrażanie przy użyciu Microsoft Deployment Toolkit” opisuje, jak korzystać z MDT 2010 do wdrażania systemu Windows 7 przy zastosowaniu procesu instalacji z niewielkim udziałem obsługi. Podczas fazy planowania projektu zespół projektowy powinien zacząć przygotowywanie środowiska laboratoryjnego, korzystając z poniższej listy:

- **Replika produkcyjna** Zespół projektowy potrzebuje repliki środowiska produkcyjnego, aby testować połączone wysiłki wszystkich pozostałych zespołów. Komputery docelowe powinny działać pod kontrolą wersji systemu Windows obecnych w środowisku produkcyjnym z załadowanymi danymi użytkowników. Komputery te są używane do wdrażania testowego, w tym migracji stanu użytkownika.
- **Udziały sieciowe na komputerze głównym** Wymagane są dwa typy udziałów sieciowych: jeden dla udziału wdrożeniowego MDT 2010 a drugi dla udziału serwera danych. Te udziały mogą być wszystkie na tym samym serwerze fizycznym lub na oddzielnych serwerach. Przydatne jest również przechowywanie obrazów komputerów produkcyjnych na komputerze głównym w celu szybkiego i łatwego ich przywracania po każdym przebiegu testu.
- **Windows Deployment Services** Środowisko laboratoryjne powinno zawierać serwer z uruchomionymi usługami Windows Deployment Services. Korzystanie z usług Windows Deployment Services do rozruchu komputerów docelowych jest znacznie szybsze niż wypalanie płyt DVD i uruchamianie z nich komputerów. Członkowie zespołu mogą wykorzystywać ten sam serwer usług Windows Deployment Services do przetwarzania obrazów i testowania wdrożenia.

Naprawianie infrastruktury

Zrozumienie środowiska sieciowego jest krytyczne dla dowolnego projektu, który wprowadza zmiany. Aby zaplanować i przygotować się do wcielenia tych zmian, po pierwsze – trzeba zrozumieć aktualny status środowiska organizacji, zdefiniować inne źródła zmian, które mogą wpłynąć na ten projekt, zastosować wobec zmian podejście łagodzenia ryzyka, po drugie – wcielić zaproponowane zmiany. Organizacje mogą rozwiązywać i prawdopodobnie unikać większości problemów sieciowych poprzez tworzenie i utrzymywanie odpowiedniej dokumentacji sieciowej. Korzystając z narzędzia sieciowego, zespół może wykonać następujące operacje:

- Zebrać informacje potrzebne do zrozumienia sieci w obecnie istniejącym stanie
- Zaplanować wzrost
- Diagnozować problemy, gdy się pojawiają
- Aktualizować informacje o zmiany sieciowe
- Pracować z informacjami do zarządzania aktywami sieciowymi. (często na pozór prosta zmiana konfiguracji może spowodować nieoczekiwany błąd)
- Przedstawiać informacje wizualnie tak, aby struktura sieciowa była widoczna dla każdego zadania tak szczegółowo, jak to potrzebne

Zespół projektowy musi mieć dostęp do programu SQL Server. Zespół wykorzystuje SQL Server do tworzenia raportów z inwentaryzacji sprzętu na podstawie bazy danych zgodności

aplikacji. Może być to ta sama instalacja, którą zespół wykorzystuje do zarządzania aplikacjami. Zespół musi też mieć dostęp do aktualnych diagramów topologii sieci i informacji inwentaryzujących urządzenia sieciowe.

Gotowość operacyjna

Zespół projektowy jest odpowiedzialny za gładkie i udane przekazanie wdrożonego rozwiązania personelowi operacyjnemu. Ten aspekt całego projektu jest ważny, ponieważ sukces przekazania rozwiązania bezpośrednio odzwierciedla sukces projektu wdrożeniowego. Aby zapewnić sukces, działania zespołu muszą być zintegrowane z bieżącymi funkcjami zarządzającymi i operacyjnymi personelu operacyjnego. Zespół projektowy może ułatwić wdrożenie wykonując następujące zadania:

- Potwierdzenie, że role stacji roboczych zidentyfikowane w specyfikacji funkcjonalnej są prawidłowe
- Analiza i ocena narzędzi zarządzających będących aktualnie w użyciu
- Ocena dojrzałości środowiska operacyjnego w kluczowych obszarach operacyjnych
- Ustanowienie efektywnych procesów i narzędzi zarządzających w kluczowych obszarach, w których występują braki
- Rozwój programu szkoleniowego dla personelu operacyjnego i wsparcia
- Przygotowanie personelu operacyjnego do pilotażu

Zespół projektowy początkowo nie ma żadnych dodatkowych wymagań dotyczących laboratorium dla gotowości operacyjnej.

Zabezpieczenia

Zabezpieczenia są ważne dla ogólnego sukcesu projektu wdrożeniowego. Bezpieczeństwo jest przedmiotem podstawowej troski we wszystkich organizacjach, a celem zespołu projektowego jest zabezpieczenie danych organizacji. Nieodpowiednie zabezpieczenia w organizacji mogą spowodować utratę lub uszkodzenie danych, przerwy w działaniu sieci, obniżoną wydajność, frustrację pracowników, przepracowanie pracowników IT i być może kradzież informacji, która przyczyni się do utraty przychodów. Dodatkowo wiele organizacji jest poddanych regulacjom zewnętrznym, które niosą za sobą znaczne kary za luki w zabezpieczeniach, na przykład narażające dane klientów. Aby zapewnić odpowiednie środki bezpieczeństwa, zespół projektowy powinien wykonać następujące zadania:

- Zanalizować i określić istniejący poziom zabezpieczeń organizacji
- Zidentyfikować zagrożenia powodowane przez aktualizacje oprogramowania i odpowiednio zaktualizować specyfikacje zabezpieczeń sieciowych
- Zapewnić, żeby środki bezpieczeństwa były aktualne

Zespół projektowy początkowo nie ma żadnych dodatkowych wymagań dotyczących laboratorium dla zabezpieczeń. Więcej informacji na temat funkcji zabezpieczeń w systemie Windows 7 można znaleźć w rozdziale 2.

Migracja

Jednym z najbardziej uciążliwych i czasochłonnych zadań podczas wdrożenia jest zidentyfikowanie plików danych i ustawień na aktualnych komputerach użytkowników (co zwane jest *stanem użytkownika*), zapisanie ich, a następnie przywrócenie. Użytkownicy poświęcają znaczącą ilość czasu na przywracanie elementów, takich jak tapeta, wygaszacze ekranu i inne funkcje, które mogą dostosowywać w systemie. Większość użytkowników nie pamięta, jak przywrócić te ustawienia. Migracja stanu użytkowników może zwiększyć wydajność i zadowolenie użytkowników. Zespół projektowy może wykonać następujące kroki, aby zaplanować migrację stanu użytkowników:

- Przeprowadzić inwentaryzację istniejących aplikacji na klienckich komputerach produkcyjnych
- Zidentyfikować aplikacje wymagające migracji danych lub ustawień
- Określić priorytety dla listy aplikacji
- Zidentyfikować osoby odpowiedzialne od strony merytorycznej za każdą aplikację
- Zidentyfikować wymagania dla każdej aplikacji odnośnie plików danych

Poniższa lista opisuje działania, które możemy podjąć w fazie planowania projektu, aby rozpocząć budowanie środowiska laboratoryjnego dla migracji. Członkowie zespołu pracujący nad migracją mogą dzielić zasoby z członkami zespołu pracującymi nad zarządzaniem aplikacjami.

- **Nośniki instalacyjne** Dla każdej aplikacji zawierającej ustawienia do migracji musimy mieć kopię nośnika instalacyjnego aplikacji, wszelką dokumentację dotyczącą konfiguracji i klucze produktowe. Jeśli nasz departament IT nie ma nośnika lub innych informacji, należy sprawdzić u eksperta dziedzinnego dla każdej aplikacji.
- **Komputery docelowe** Zespół projektowy potrzebuje w laboratorium komputerów, na których mógłby testować rozwiązania migracji stanu użytkowników. Komputery docelowe powinny działać pod kontrolą wersji systemu Windows obecnych w środowisku produkcyjnym z załadowanymi aplikacjami i danymi użytkowników. Komputery te są używane do testowania migracji stanu użytkownika.
- **Komputer główny** Musimy mieć komputer, na którym będziemy utrzymywać pliki źródłowe aplikacji i rozwiązania migracyjne. Przydatne jest również przechowywanie obrazów komputerów docelowych na komputerze głównym w celu szybkiego i łatwego ich przywracania po każdym przebiegu testu.
- **Magazyn danych** Magazyn danych jest udziałem sieciowym, na którym umieszczamy dane stanu użytkowników podczas testowania. Możemy tworzyć magazyn danych na komputerze głównym albo możemy opcjonalnie tworzyć magazyn danych na każdym komputerze docelowym.
- **USMT** MDT 2010 wykorzystuje USMT do migracji stanu użytkowników. Funkcjonalność ta jest już wbudowana w platformę MDT 2010. Zespół musi jednak pobrać i przygotować udział dystrybucyjny z plikami wykonywalnymi USMT. Rozdział 7 „Migrowanie danych stanu użytkowników” opisuje, gdzie umieścić te pliki.

Instalowanie Microsoft Deployment Toolkit

MDT 2010 wymaga oprogramowania Windows PowerShell 2.0. Jeśli instalujemy MDT 2010 w systemie Windows Server 2008 lub Windows Server 2008 R2, musimy też dodać funkcję Windows PowerShell, korzystając z kreatora dodawania funkcji.

Jeśli instalujemy MDT 2010 w systemie Microsoft Windows Server 2003 SP1, musimy zainstalować dodatkowe wymagane oprogramowanie. Systemy Windows Server 2008, Windows Server 2008 R2 i Windows 7 zawierają już to oprogramowanie. Poniższa lista opisuje oprogramowanie, które musimy zainstalować przed zainstalowaniem i wykorzystaniem MDT 2010 w systemie Windows Server 2003 SP1 (Windows Server 2003 SP2 wymaga tylko Microsoft .NET Framework 2.0):

- **Windows PowerShell** Program Windows PowerShell można pobrać z witryny Microsoft Download Center pod adresem <http://www.microsoft.com/downloads>.
- **Microsoft .NET Framework 2.0** Nośnik dystrybucyjny pakietu Windows AIK zawiera plik instalacyjny platformy .NET Framework 2.0. Alternatywnie można pobrać .NET Framework 2.0 z następujących adresów:
 - ❑ **x86** <http://www.microsoft.com/downloads/details.aspx?FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5&DisplayLang=en>
 - ❑ **x64** <http://www.microsoft.com/downloads/details.aspx?FamilyID=b44a0000-acf8-4fa1-affb-40e78d788b00&DisplayLang=en>
- **Microsoft Management Console (MMC) 3.0** Konsolę MMC 3.0 można pobrać z następujących adresów:
 - ❑ **x86** <http://www.microsoft.com/downloads/details.aspx?FamilyID=4c84f80b-908d-4b5d-8aa8-27b962566d9f&DisplayLang=en>
 - ❑ **x64** <http://www.microsoft.com/downloads/details.aspx?FamilyID=b65b9b17-5c6d-427c-90aa-7f814e48373b&DisplayLang=en>

UWAGA Jeśli wybierzemy tylko instalację dokumentacji MDT 2010, jedynym wymaganym oprogramowaniem dodatkowym jest .NET Framework 2.0 i MMC 3.0. Pozostałe oprogramowanie z powyższej listy nie jest wymagane do przeglądania dokumentacji.

Aby zainstalować pakiet MDT 2010, wykonaj następujące kroki:

1. Kliknij prawym przyciskiem myszy plik `MicrosoftDeploymentToolkit_platforma.msi`, gdzie *platforma* oznacza albo x86, albo x64, a następnie kliknij Zainstaluj.
2. Kliknij Next, aby pominąć stronę powitalną.
3. Na stronie End-User License Agreement przejrzyj umowę licencyjną, kliknij I Accept The Terms In The License Agreement, a następnie kliknij Next.
4. Na stronie Custom Setup wybierz funkcje do zainstalowania, a następnie kliknij Next. Aby zmienić stan jakiejś funkcji, kliknij tę funkcję, a następnie wybierz stan: Will Be Installed On Local Hard Drive (zostanie zainstalowane na lokalnym dysku twardym)

albo Entire Feature Will Be Unavailable (cała funkcja będzie niedostępna). Poniższa lista opisuje każdą z funkcji.

- ❑ **Documents** Instaluje wskazówki dla rozwiązania i pomoce robocze. Domyślnie funkcja ta jest instalowana w folderze C:\Program Files\Microsoft Deployment Toolkit\Documentation.
- ❑ **Tools and templates** Instaluje kreatory rozwiązania i pliki szablonów wdrażania, takie jak Unattend.xml. Domyślnie funkcja ta jest instalowana w folderze C:\Program Files\Microsoft Deployment Toolkit.

5. Kliknij Install, aby zainstalować ten pakiet.

6. Kliknij Finish, aby zakończyć instalację i zamknąć instalator.

UWAGA Wersje pakietu MDT wcześniejsze niż 2008, w tym Microsoft Solution Accelerator for Business Desktop Deployment 2007, zawierały funkcję do tworzenia udziału dystrybucyjnego. MDT 2010 nie tworzy jednak udziału dystrybucyjnego podczas instalacji. Zamiast tego możemy utworzyć udział dystrybucyjny lub zaktualizować istniejący udział dystrybucyjny, wykorzystując narzędzie Deployment Workbench.

Poniższa lista opisuje podfoldery w folderze programu MDT 2010 (C:\Program Files\Microsoft Deployment Toolkit) po zainstalowaniu tego pakietu:

- **Bin** Zawiera przystawkę Deployment Workbench do konsoli MMC oraz wykorzystywane przez nią pliki
- **Documentation** Zawiera dokumentację pakietu MDT 2010
- **Downloads** Zapewnia miejsce do przechowywania składników pobieranych przez pakiet MDT 2010
- **ManagementPack** Zawiera pliki pakietu zarządzania z MDT 2010
- **Samples** Zawiera przykładowe skrypty sekwencji zadań
- **SCCM** Zawiera pliki, które obsługują integrację z Microsoft System Center Configuration Manager (SCCM) 2007
- **Templates** Zawiera pliki szablonów wykorzystywane przez narzędzie Deployment Workbench

UWAGA Dysk twardy zawierający foldery programu musi mieć dostępny co najmniej 1 gigabajt (GB) wolnej przestrzeni. MDT 2010 pobiera składniki, w tym pakiet Windows AIK do folderu Downloads.

Uruchamianie narzędzia Deployment Workbench

Deployment Workbench jest narzędziem pakietu MDT 2010, które wykorzystujemy do wypełniania udziałów wdrożeniowych, tworzenia sekwencji zadań, itd. Więcej informacji na temat korzystania z Deployment Workbench do wypełniania udziału dystrybucyjnego i tworzenia niestandardowych obrazów systemu Windows 7 można znaleźć w rozdziale 6. Aby uruchomić Deployment Workbench, należy kliknąć Start, wskazać Wszystkie programy, wybrać Microsoft Deployment Toolkit, a następnie kliknąć Deployment Workbench. Drzewo konsoli wyświetli następujące elementy:

- **Information Center** Zapewnia dostęp do dokumentacji, najnowszych wiadomości na temat MDT 2010 oraz składników wymaganych do korzystania z Deployment Workbench. Element Documentation pomaga szybko nawigować po przewodniku na temat pakietu. Należy kliknąć łącze, aby otworzyć dany przewodnik jako skompilowany plik pomocy (.chm).
- **Deployment Shares** W grupie Deployment Shares możemy zobaczyć element dla każdego utworzonego udziału wdrożeniowego. Każdy udział wdrożeniowy zawiera aplikacje, systemy operacyjne, sterowniki urządzeń, pakiety i sekwencje zadań. Dodatkowo możemy tworzyć nośniki rozruchowe, przyłączać udziały wdrożeniowe i łączyć udział wdrożeniowy z bazą danych wdrożenia.

UWAGA Domyślny widok przystawki MMC Deployment Workbench zawiera okienko Akcje. Aby usunąć okienko Akcje, należy otworzyć konsolę zarządzającą w trybie autorskim. Aby otworzyć tę konsolę w trybie autorskim, należy uruchomić `C:\Program Files\Microsoft Deployment Toolkit\Bin\DeploymentWorkbench.msc /a`. Trzeba kliknąć Widok, kliknąć Dostosuj, wyczyścić pole opcji Okienko akcji, a następnie kliknąć OK. Aby zapisać zmiany, z menu Plik, należy wybrać Zapisz. Gdy pojawi się monit o wybór, czy wyświetlać interfejs pojedynczego okna, klikamy Tak.

Aktualizowanie składników pakietu Microsoft Deployment Toolkit

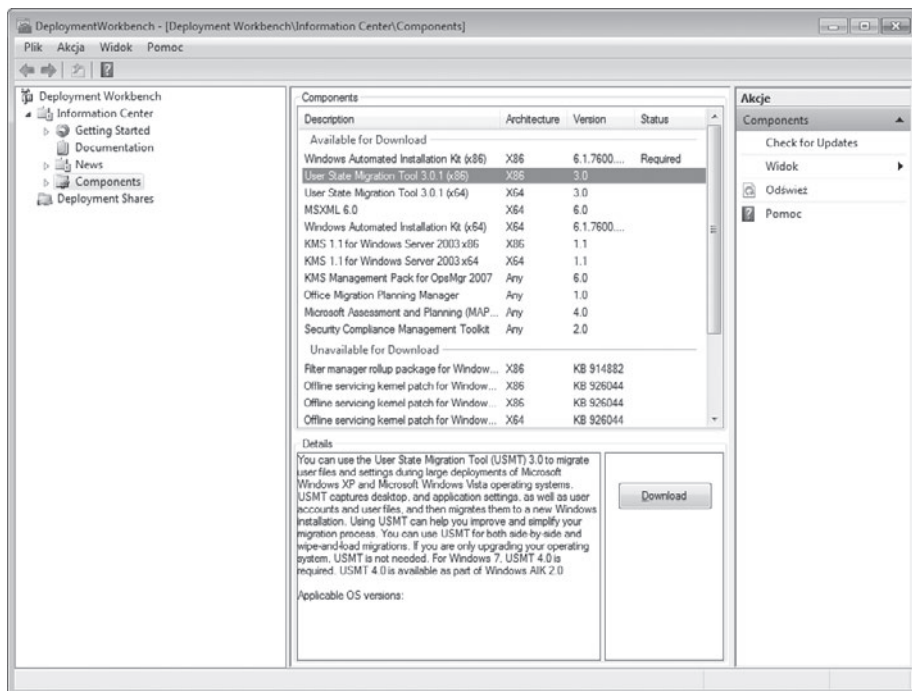
Po zainstalowaniu pakietu MDT 2010 i zapoznaniu się z konsolą Deployment Workbench należy pobrać i zainstalować dodatkowe składniki wymagane przez MDT 2010. Obowiązkowe w MDT 2010 są następujące składniki:

- **Windows AIK 2.0** Pakiet Windows AIK 2.0 możemy zainstalować ręcznie, pobierając go z witryny Microsoft Download Center pod adresem <http://www.microsoft.com/downloads>, albo możemy wykorzystać konsolę Deployment Workbench do pobrania i zainstalowania go automatycznie.
- **MSXML Services 6.0** Możemy wcześniej zainstalować usługi MSXML Services 6.0 albo skorzystać z konsoli Deployment Workbench, żeby je pobrać i zainstalować. Nośnik dystrybucyjny pakietu Windows AIK zawiera plik instalacyjny MSXML Services 6.0 SP1.

Możemy też pobrać usługi MSXML Services 6.0 SP1 z <http://www.microsoft.com/downloads/details.aspx?FamilyID=d21c292c-368b-4ce1-9dab-3e9827b70604&displaylang=en>. Możemy pobrać pod tym adresem zarówno wersję x86, jak i x64. Systemy Windows Vista z SP1, Windows 7, Windows Server 2008 i Windows Server 2008 R2 już zawierają tę funkcję.

Aby pobrać składniki, wykonaj następujące kroki:

1. W konsoli Deployment Workbench, w części Information Center kliknij Components.



2. W sekcji Available For Download listy Components kliknij jakiś składnik. W dolnym okienku kliknij Download. Konsola Deployment Workbench wyświetli status pobierania na liście Components. Po zakończeniu pobierania przeniesie go do sekcji Downloaded w prawym okienku.
3. W sekcji Downloaded listy Components kliknij pobrany składnik. W dolnym okienku kliknij Install, aby go zainstalować lub Browse, aby otworzyć folder zawierający ten składnik w Eksploratorze Windows. Pakiet MDT 2010 nie może instalować niektórych składników automatycznie. Aby je zainstalować, trzeba kliknąć Browse, żeby otworzyć folder zawierający dany składnik, a następnie należy ręcznie zainstalować ten składnik.

UWAGA Należy często sprawdzać w Internecie, czy nie ma zaktualizowanych składników. W głównym menu konsoli Deployment Workbench, w menu Akcja kliknij opcję Check For Updates. Na stronie Check For Updates kreatora Check For Updates Wizard zaznacz pole opcji Check The Internet, a następnie kliknij Check.

Podsumowanie

Wczesne planowanie jest ważne dla udanego projektu wdrożeniowego systemu Windows 7. Chociaż MDT 2010 zapewnia platformę technologiczną do wdrażania systemu Windows 7, MOF 4.0 zawiera najbardziej wyczerpujące wskazówki dotyczące planowania wdrażania opracowane przez Microsoft. Zawiera sprawdzone, najlepsze praktyki z doświadczenia firmy Microsoft oraz jej partnerów i klientów.

Planowanie wdrożenia systemu Windows 7 jest dużo większym przedsięwzięciem niż tylko ustalenie, jak zainstalować system operacyjny. Do kluczowych zagadnień planowania należą testowanie zgodności, pakowanie aplikacji, przetwarzanie obrazów, migracja stanu użytkowników, zabezpieczenia i wdrażanie. Ta książka, MDT 2010 oraz MOF 4.0 pomogą zaplanować i opracować rozwiązania dla każdego z tych zagadnień.

Dodatkowe zasoby

Dodatkowe informacje i narzędzia związane z tym rozdziałem zawierają następujące zasoby.

- Przewodnik *Getting Started Guide* w pakiecie MDT 2010 zawiera podstawowe informacje dotyczące instalowania i konfigurowania MDT 2010, jak również przygotowania infrastruktury do korzystania z tego pakietu.
- Rozdział 6 „Przygotowywanie obrazów dysków” wyjaśnia, jak planować i opracowywać obrazy dyskowe systemu Windows 7 przy pomocy MDT 2010.
- Rozdział 7 „Migrowanie danych stanu użytkowników” wyjaśnia, jak planować i projektować rozwiązania migracji stanu użytkowników przy użyciu USMT.
- Rozdział 8 „Rozpowszechnianie aplikacji” zawiera więcej informacji na temat opakowywania i automatyzacji instalowania aplikacji. Ten rozdział omawia też sprawy związane ze zgodnością aplikacji.
- Rozdział 11 „Korzystanie z mechanizmu Volume Activation” wyjaśnia, jak stosować grupową aktywację systemu Windows 7 w projektach wdrażania na dużą skalę.
- Rozdział 12 „Wdrażanie przy użyciu Microsoft Deployment Toolkit” wyjaśnia, jak korzystać z MDT 2010 do wdrażania systemu Windows 7 przy zastosowaniu procesu instalacji z niewielkim udziałem obsługi.
- Platforma MOF 4.0, dostępna pod adresem <http://technet.microsoft.com/en-us/library/cc506049.aspx>, zapewnia wskazówki dotyczące zarządzania projektami i pomoce do zadań.

Testowanie zgodności aplikacji

- Zrozumienie zgodności 142
- Wybieranie najlepszego narzędzia 144
- Zrozumienie pakietu ACT 148
- Planowanie użycia ACT 151
- Przygotowanie do użycia ACT 156
- Zbieranie danych na temat zgodności 159
- Analizowanie danych na temat zgodności 161
- Racjonalizowanie zestawu aplikacji 170
- Testowanie i rozwiązywanie problemów 171
- Podsumowanie 180
- Dodatkowe zasoby 180

Zgodność aplikacji jest często problemem blokującym wdrożenie. Jest też problemem, na którym większość projektów wdrożeniowych najmniej się skupia – dopóki sprawy nie zaczynają się rozlatywać. Wcześniej skupiając się na zgodności aplikacji, możemy lepiej zadbać o skuteczność projektu wdrożeniowego.

Trzema typowymi powodami, dla których zgodność aplikacji blokuje wdrażanie systemów operacyjnych, są strach, niepewność i wątpliwość. Firmy po prostu nie wiedzą, jakie aplikacje są używane w ich środowiskach, czy te aplikacje są zgodne z systemem operacyjnym Windows 7 i jakie ryzyka niesie z sobą każda aplikacja, jeśli przestanie działać po wdrożeniu.

Aby pomóc w przezwyciężeniu tych problemów, ten rozdział opisuje dostępne narzędzia firmy Microsoft służące do wykrywania aplikacji w danym środowisku, oceny ich zgodności z systemem Windows 7, a następnie opracowywania poprawek dla wszelkich problemów. Głównym takim narzędziem w systemie Windows 7 jest Microsoft Application Compatibility Toolkit (ACT) 5.5.

Zrozumienie zgodności

Od czasu pojawienia się systemu Microsoft Windows jako wszechobecnej platformy aplikacyjnej, niezależni dostawcy oprogramowania i wewnętrzni programiści stworzyli tysiące aplikacji dla tego systemu. Wiele z nich to krytyczne dla przedsiębiorstwa aplikacje, z których część nie jest zgodna z najnowszą wersją systemu Windows. Do typów aplikacji, które mogą nie być zgodne, należą następujące:

- Aplikacje biznesowe, takie jak pakiety planowania zasobów przedsiębiorstwa
- Podstawowe aplikacje, które są częścią standardowych konfiguracji komputerów biurkowych
- Narzędzia administracyjne, takie jak aplikacje antywirusowe, do kompresji danych i do zdalnego sterowania
- Niestandardowe narzędzia, takie jak skrypty logowania

Co oznacza zgodność

Aplikacje zaprojektowane dla wcześniejszych wersji systemu Windows zostają przenoszone do nowego systemu z wielu powodów. Być może dana aplikacja jest koniecznym narzędziem, używanym codziennie w celu wykonywania jakiegoś zadania, które w innym przypadku byłoby bardzo uciążliwe. Być może użytkownicy dobrze poznali daną aplikację i nie chcą przejść na inną, podobną aplikację. Być może aplikacja nie ma zastępnika, ponieważ pierwotny twórca już nie prowadzi tej działalności albo opuścił firmę. Wszystkie te sprawy powodują, że zgodność aplikacji jest istotnym problemem, który musimy rozważyć przy wdrażaniu nowego systemu operacyjnego, takiego jak Windows 7. W tym rozdziale poznamy wiele spraw wpływających na zgodność aplikacji, dowiemy się, jak wykryć aplikacje, od których zależy nasza organizacja i co możemy zrobić, aby zapewnić, że krytyczne aplikacje będą działać w systemie Windows 7.

Aplikacja jest zgodna z systemem Windows 7, jeśli działa zgodnie ze swoim projektem w systemie Windows 7 – to znaczy aplikacja powinna się poprawnie instalować i odinstalowywać. Użytkownicy powinni być w stanie tworzyć, usuwać, otwierać i zapisywać wszelkie pliki danych naturalne dla danej aplikacji. Typowe operacje, takie jak drukowanie, powinny działać zgodnie z oczekiwaniami. Kompatybilna aplikacja działa w systemie Windows 7 bezpośrednio po zainstalowaniu, bez żadnej specjalnej pomocy. Jeśli aplikacja nie jest kompatybilna, możemy odkryć, że dostępna jest nowsza, zgodna wersja tej aplikacji albo że wystarczy użycie jednego z narzędzi zapewnianych przez firmę Microsoft w celu przeciwdziałania problemom zgodności. Możemy też odkryć, że aplikacja będzie wymagać połączenia kilku poprawek, żeby zadziałała poprawnie. Ten rozdział omawia wszystkie te scenariusze.

Dlaczego aplikacje przestają działać

Poniższa lista opisuje typowe problemy zgodności dla systemu Windows 7, zwłaszcza w przypadku korzystania z aplikacji pierwotnie zaprojektowanych dla systemu Windows XP:

- **Kontrola konta użytkownika** W systemie Windows 7 domyślnie wszyscy użytkownicy interaktywni, włącznie z członkami grupy Administratorzy, funkcjonują jako użytkownicy standardowi. Kontrola konta użytkownika (UAC) jest mechanizmem, poprzez który użytkownicy mogą awansować aplikacje do pełnych uprawnień administracyjnych. Z powodu UAC aplikacje, które wymagają uprawnień administracyjnych lub sprawdzają, czy użytkownik ma uprawnienia administracyjne, zachowują się inaczej w systemie Windows 7, nawet jeśli są uruchamiane przez użytkownika będącego administratorem.
- **Ochrona zasobów systemu Windows** Ochrona zasobów systemu Windows (WRP) jest zaprojektowana w celu chronienia systemu w stanie tylko do odczytu, aby zwiększyć stabilność, przewidywalność i niezawodność systemu. Będzie to wpływać na określone pliki, foldery i klucze rejestru. Aktualizacje chronionych zasobów są ograniczone do zaufanych instalatorów systemu operacyjnego (grupy TrustedInstaller), takich jak Windows Servicing. Pomaga to chronić funkcje i aplikacje dostarczane razem z systemem operacyjnym przed wszelkim wpływem innych aplikacji i administratorów. Ten wpływ może być problemem dla niestandardowych instalacji niewykrytych przez system Windows 7 jako programy instalacyjne, gdy aplikacje próbują zastąpić pliki WRP i ustawienia rejestru oraz sprawdzają określone wersje i wartości.
- **Tryb chroniony programu Internet Explorer** W systemie Windows 7 procesy przeglądarki Windows Internet Explorer 8 działają w trybie chronionym ze znacznie ograniczonymi uprawnieniami, aby pomóc chronić użytkowników przed atakiem. Tryb chroniony programu Internet Explorer znacząco ogranicza możliwość zapisu, zmiany lub uszkodzenia danych na komputerze użytkownika albo zainstalowania szkodliwego kodu przez napastnika. Może to wpływać na formanty ActiveX i inny kod skryptowy, który próbuje modyfikować obiekty wyższego poziomu.
- **Sprawdzanie wersji systemu operacyjnego i programu Internet Explorer** Wiele aplikacji sprawdza wersję systemu operacyjnego i zachowuje się inaczej lub przestaje działać, gdy wykryty zostanie nieoczekiwany numer wersji. Możemy rozwiązać ten problem, ustawiając odpowiednie tryby zgodności lub stosując poprawki do określania wersji.
- **Nowe lokalizacje folderów** Foldery Użytkownicy, Moje dokumenty i foldery z określoną lokalizacją zmieniły się od czasu Windows XP. Aplikacje z zakodowanymi trwale ścieżkami do folderów mogą przestać działać. Możemy zapobiegać temu, wykorzystując węzły katalogowe lub zastępując trwale zakodowane ścieżki odpowiednimi wywołaniami API w celu uzyskania lokalizacji folderów.
- **Izolacja sesji 0** Uruchamianie usług i aplikacji użytkownika w sesji 0 powoduje ryzyko dla zabezpieczeń, ponieważ usługi te działają z podwyższonymi uprawnieniami i dlatego są celami ataków agentów szkodliwego oprogramowania szukających sposobów na podwyższenie swojego własnego poziomu uprawnień. We wcześniejszych wersjach systemu operacyjnego Windows usługi i aplikacje działały w tej samej sesji, co pierwszy

użytkownik, który zalogował się do konsoli (Sesja 0). Aby pomóc w ochronie przed agentami szkodliwego oprogramowania w systemie Windows 7, sesja 0 została odizolowana od innych sesji. Może to wpływać na usługi, które komunikują się z aplikacjami, korzystając z komunikatów okienkowych.

Wybieranie najlepszego narzędzia

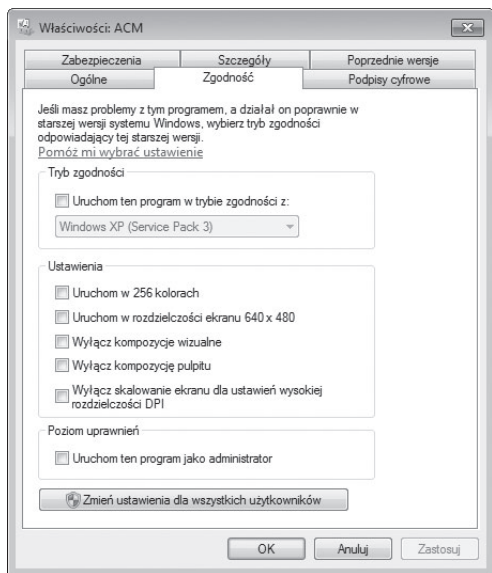
Możemy korzystać z pięciu głównych narzędzi do rozwiązywania problemów ze zgodnością aplikacji: asystenta zgodności programów, kreatora zgodności programów, narzędzia ACT, trybu Windows XP oraz wirtualizacji aplikacji. Poniższe części tego rozdziału opisują każde z tych narzędzi i kiedy odpowiednie jest użycie każdego narzędzia wobec użycia innych narzędzi i technologii.

Pierwsze dwa narzędzia zapewniają opcje dla użytkowników i jednorazowego wsparcia, ale nie nadają się do używania we wdrożeniach na dużą skalę. Pozostała część rozdziału skupia się na wykorzystaniu programu ACT do inwentaryzacji, analizowania i przeciwdziałania problemom z kompatybilnością, ponieważ jest to narzędzie, które organizacje wykorzystują przede wszystkim we wdrożeniach na dużą skalę.

UWAGA Zestaw Microsoft Assessment and Planning (MAP) Toolkit 4.0 jest darmowym narzędziem firmy Microsoft, które możemy wykorzystać do planowania projektu migracji do systemu Windows 7. Może pomóc oszacować gotowość danego środowiska na system Windows 7. Więcej informacji na temat MAP można znaleźć pod adresem <http://technet.microsoft.com/en-us/solutionaccelerators/dd537566.aspx>.

Asystent zgodności programów

Jeśli mamy indywidualną aplikację, która wymaga poprawienia zgodności z systemem Windows 7, jednym z narzędzi, które może w tym pomóc, jest wbudowany Asystent zgodności programów. Aby uruchomić Asystenta zgodności programów, należy kliknąć prawym przyciskiem myszy plik .exe aplikacji, kliknąć Właściwości, a następnie kliknąć kartę Zgodność, żeby zobaczyć ustawienia zgodności dla tej aplikacji, jak pokazano na rysunku 5-1. Jeśli program jest wykorzystywany przez wielu użytkowników na tym samym komputerze, należy kliknąć opcję Zmień ustawienia dla wszystkich użytkowników, aby wybrane tutaj zmiany ustawień wpływały na wszystkich użytkowników.

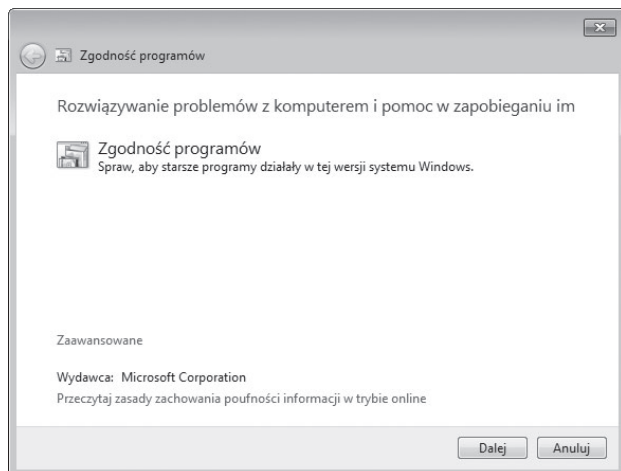


Rysunek 5-1 Ustawienia zgodności

Narzędzie do rozwiązywania problemów ze zgodnością programów

Narzędzie do rozwiązywania problemów ze zgodnością programów może pomóc rozwiązać wiele problemów z aplikacjami. Korzystając z tego narzędzia, możemy testować różne opcje zgodności dla różnych programów, aby znaleźć ustawienia, które pozwolą tym programom działać pod kontrolą systemu Windows 7. Aby uruchomić narzędzie do rozwiązywania problemów ze zgodnością programów, kliknij Start, Panel sterowania, Programy, a następnie Uruchom programy napisane dla starszych wersji systemu Windows. Uruchomione zostanie narzędzie Zgodność programów, jak pokazano na rysunku 5-2. Aby rozpocząć proces diagnozowania zgodności aplikacji, kliknij Dalej.

UWAGA Aby uzyskać najdokładniejsze wyniki przy użyciu tego narzędzia, należy zalogować się na komputerze na koncie użytkownika, który ma standardowe uprawnienia użytkownika, a nie administratora.



Rysunek 5-2 Narzędzie do rozwiązywania problemów ze zgodnością programów

Application Compatibility Toolkit

Można korzystać z pakietu ACT do przeprowadzania prostych zadań związanych z łagodzeniem problemów ze zgodnością. Pomaga on stworzyć spis aplikacji w danej organizacji. Pomaga też zidentyfikować, które aplikacje są zgodne z systemem Windows 7, a które wymagają dalszych testów. Poniżej przedstawiono kilka głównych składników rozwiązania ACT:

- **Application Compatibility Manager** Narzędzie, które pozwala zbierać i analizować dane tak, abyśmy mogli identyfikować wszelkie problemy przed wdrożeniem nowego systemu operacyjnego lub aktualizacji systemu Windows w organizacji. Intensywnie korzystamy z tego programu podczas początkowych faz projektu migracji aplikacji. Powinniśmy rozważyć to narzędzie jako główny interfejs użytkownika dla pakietu ACT.
- **Application Compatibility Toolkit Data Collector** Narzędzie to jest rozprowadzane na wszystkie komputery i skanuje je przy użyciu funkcji oceniających zgodność. Dane są zbierane i zapisywane w centralnej bazie danych zgodności.
- **Setup Analysis Tool (SAT)** Automatyzuje uruchamianie instalacji aplikacji podczas monitorowania działań podejmowanych przez instalatora każdej z aplikacji.
- **Standard User Analyzer (SUA)** Określa możliwe problemy z aplikacjami działającymi w kontekście użytkownika standardowego w systemie Windows 7.

Pakiet ACT jest niezastąpiony przy testowaniu szerokiej palety aplikacji na różnych komputerach i systemach operacyjnych w organizacji, wykorzystując rozwiązania oparte na wspólnej puli poprawek do aplikacji zapewnianych przez producentów i użytkowników. Możemy korzystać z narzędzi ACT osobno lub razem w zależności od potrzeb danej organizacji. Niektóre narzędzia, takie jak SAT i SUA są przeznaczone dla programistów do odpowiedniego przygotowania aplikacji i niekoniecznie są używane w procesie skanowania i łagodzenia problemów.