helion.pl
KSIĘGARNIA INTERNETOWA · WYDAWNICTWO

IDŹ DO
PRZYKŁADOWY ROZDZIAŁ
SPIS TREŚCI

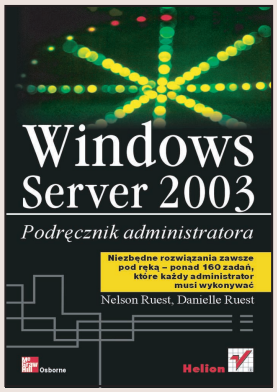
KATALOG KSIĄŻEK
KATALOG ONLINE
ZAMÓW DRUKOWANY KATALOG

TWÓJ KOSZYK
DODAJ DO KOSZYKA

CENNIK I INFORMACJE
ZAMÓW INFORMACJE O NOWOŚCIACH
ZAMÓW CENNIK

CZYTELNIA
FRAGMENTY KSIĄŻEK ONLINE

Windows Server 2003. Podręcznik administratora



Autorzy: Nelson Ruest, Danielle Ruest
Tłumaczenie: Adam Jarczyk
ISBN: 83-7361-421-4
Tytuł oryginału: Windows Server 2003 Pocket Administrator
Format: B5, stron: 264

„Windows Server 2003. Podręcznik administratora" to książka opisująca najważniejsze kwestie związane z zarządzaniem systemem Windows Server 2003 i rozwiązywaniem dotyczących go problemów. Opisuje ona ponad 160 zadań administracyjnych, wraz z zalecaną częstotliwością wykonywania każdego z nich. Rozpoczyna się przedstawieniem ogólnych działań, które należy podjąć w przypadku wszystkich serwerów, niezależnie od roli, jaką pełnią. Omówione zostały również jednorazowe zadania, które musimy wykonać, aby odpowiednio przygotować środowisko administracyjne. Opisano ponadto klastry serwerów, a także serwery zarządzające infrastrukturą sieciową, w skład których wchodzą DHCP (Dynamic Host Configuration Protocol) i WINS (Windows Internet Naming Service). Zostały przedstawione również serwery służące do zdalnej instalacji systemów operacyjnych, takich jak Windows XP lub sam Windows Server 2003. Na koniec omówiono jeszcze czynności administracyjne związane z wydajnością i monitorowaniem sieci.

W książce omówiono między innymi:

- Serwery zarządzania tożsamościami
- Active Directory
- Serwery DNS
- Dedykowane serwery WWW
- Serwery aplikacji
- Serwery terminali
- Serwery DHCP i WINS
- Serwery dostępu zdalnego i VPN

O autorach:

Nelson Ruest głównie zajmuje się przygotowywaniem strategicznych rozwiązań dla dużych firm i specjalizuje się w projektach infrastruktury. W swojej urozmaiconej karierze zawodowej bywał operatorem komputerów, administratorem systemów i sieci oraz menedżerem IT.

Danielle Ruest zajmuje się organizacją pracy oraz doradztwem z zakresu biznesu. Specjalizuje się w problemach związanych z wdrażaniem dużych projektów informatycznych. Wraz z Nelsonem Ruestem jest autorką „Windows Server 2003: Best Practices for Enterprise Deployments". Oboje pisują do MCP Magazine i .NET Magazine oraz pracują dla Resolutions Enterprises.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

O Autorach **11**

Przedmowa **13**

Wstęp **15**

Rozdział 1. Ogólne zarządzanie serwerem **21**

Czynności administracyjne 21
Ogólne zarządzanie serwerem 24
GS-01. Skróty Uruchom jako 24
GS-02. Ogólna weryfikacja stanu usług 28
GS-03. Weryfikacja dziennika zdarzeń System 29
GS-04. Weryfikacja dziennika zdarzeń Zabezpieczenia 30
GS-05. Zarządzanie kontami usług i administracyjnymi 32
GS-06. Utrzymanie dziennika działań 34
GS-07. Zarządzanie raportem o czasie dostępności systemu 35
GS-08. Zarządzanie skryptami 36
GS-09. Zarządzanie certyfikatami skryptów 38
GS-10. Aktualizacje definicji wirusów dla programów antywirusowych 40
GS-11. Restart serwera 40
GS-12. Przegląd i aktualizacja zasad zabezpieczeń 42
GS-13. Weryfikacja aktualizacji zabezpieczeń 43
GS-14. Aktualizacja poprawek i pakietów Service Pack 45
GS-15. Ocena nowego oprogramowania 46
GS-16. Inwentaryzacja 47
GS-17. Tworzenie globalnej konsoli MMC 50
GS-18. Automatyczne pobieranie sygnatur dla oprogramowania antywirusowego 51
GS-19. Tworzenie i weryfikacja zaplanowanych zadań 52

GS-20. Tworzenie i modyfikacja szablonów zabezpieczeń 53
GS-21. Zarządzanie plikami pomocy technicznej 55
GS-22. Przygotowanie serwera 55
GS-23. Konfiguracja narzędzi administracyjnych 56
GS-24. Aktualizacja domyślnego profilu użytkowników 57
GS-25. Przegląd środowiska sprzętowego 59
GS-26. Dokumentacja systemu i sieci 60
GS-27. Zarządzanie umowami o świadczeniu usług 60
GS-28. Zarządzanie priorytetami w rozwiązywaniu problemów ... 61
GS-29. Przegląd nakładów pracy 61
Administrowanie sprzętem 61
HW-01. Kontrola urządzeń sieciowych 62
HW-02. Zarządzanie BIOS-em serwerów 62
HW-03. Zarządzanie aktualizacjami oprogramowania sprzętowego i zarządzającego serwerami 63
HW-04. Zarządzanie urządzeniami 63
Tworzenie i przywracanie kopii zapasowych 64
BR-01. Generowanie kopii zapasowych stanu systemu 65
BR-02. Weryfikacja kopii zapasowych 66
BR-03. Zarządzanie składowaniem taśm poza lokalizacją serwerów 67
BR-04. Testowanie strategii usuwania skutków awarii 67
BR-05. Testowanie procedury przywracania kopii zapasowych 68
BR-06. Przegląd strategii kopii zapasowych 69
BR-07. Odbudowa serwera 69
Administrowanie zdalne 70
RA-01. Zarządzanie RDC w serwerach 70
RA-02. Zarządzanie RDC w komputerach osobistych 72
RA-03. Pomoc dla użytkowników poprzez narzędzie Pomoc zdalna . 73
RA-04. Skróty do Podłączania pulpitu zdalnego i dostęp przez WWW 74

Rozdział 2. Zarządzanie serwerami plików i drukowania 77

Czynności administracyjne 77
Administrowanie usługami plików 79
FS-01. Weryfikacja dostępnego miejsca 80
FS-02. Zarządzanie kopiami zapasowymi danych 81
FS-03. Zarządzanie folderami udostępnionymi 82
FS-04. Weryfikacja dziennika zdarzeń usługi replikacji plików 84
FS-05. Zarządzanie kopiowaniem woluminów w tle 85
FS-06. Zarządzanie rozproszonym systemem plików 87
FS-07. Zarządzanie przydziałami 88
FS-08. Zarządzanie usługą indeksowania 89
FS-09. Weryfikacja integralności dysków danych 89
FS-10. Defragmentacja dysków z danymi 90

FS-11. Weryfikacja dziennika inspekcji dostępu do plików 91
FS-12. Usuwanie plików tymczasowych 92
FS-13. Weryfikacja parametrów zabezpieczeń 93
FS-14. Zarządzanie folderami zaszyfrowanymi 94
FS-15. Archiwizacja danych 94
FS-16. Zarządzanie usługą replikacji plików 95
FS-17. Zarządzanie dyskami i woluminami 97
Usługi drukowania 97
PS-01. Zarządzanie kolejkami drukowania 99
PS-02. Zarządzanie dostępem do drukarek 99
PS-03. Zarządzanie sterownikami drukarek 100
PS-04. Udostępnianie drukarek 101
PS-05. Zarządzanie buforowaniem drukowanych dokumentów .. 102
PS-06. Zarządzanie śledzeniem lokalizacji drukarek 102
PS-07. Masowe zarządzanie drukarkami 104
PS-08. Ocena nowych modeli drukarek 104
Usługi klastrów 105
CS-01. Klastry — weryfikacja ich stanu 105
CS-02. Klastry — weryfikacja stanu kolejek drukowania 106
CS-03. Klastry — zarządzanie serwerem klastrów 106
CS-04. Klastry — weryfikacja stanu kworum 107

Rozdział 3. Zarządzanie serwerami infrastruktury sieciowej 109

Czynności administracyjne 109
Administrowanie serwerami DHCP i WINS 111
DW-01. Weryfikacja stanu serwera DHCP 111
DW-02. Weryfikacja stanu serwera WINS 115
DW-03. Zarządzanie rekordami WINS 117
DW-04. Zarządzanie atrybutami DHCP 117
DW-05. Zarządzanie zakresami DHCP 119
DW-06. Zarządzanie rezerwacjami DHCP 120
DW-07. Zarządzanie superzakresami DHCP 121
DW-08. Zarządzanie zakresami multiemisji DHCP 122
DW-09. Zarządzanie klasami opcji DHCP 123
DW-10. Autoryzacja serwerów DHCP i RIS 126
Serwery wdrażania 127
RI-01. Weryfikacja stanu serwera RIS 128
RI-02. Zarządzanie obrazami RIS 128
Klastry NLB 130
NC-01. Weryfikacja stanu klastrów NLB 130
NC-02. Zarządzanie członkami klastrów NLB 131
Dostęp zdalny i sieci VPN 132
RV-01. Weryfikacja stanu serwerów dostępu zdalnego 133
RV-02. Weryfikacja stanu serwerów RADIUS/IAS 134
RV-03. Monitorowanie sieci bezprzewodowych 134

RV-04. Weryfikacja zasad dostępu zdalnego 135
RV-05. Zarządzanie usługą NAT 135
RV-06. Zarządzanie łączami VPN 136

Rozdział 4. Zarządzanie serweramitożsamości 139

Czynności administracyjne 139
Zarządzanie kontrolerami domen 141
DC-01. Zarządzanie użytkownikami 142
DC-02. Zmiana haseł użytkowników 145
DC-03. Weryfikacja dziennika zdarzeń usługi katalogowej 147
DC-04. Zarządzanie kontami 147
DC-05. Zarządzanie grupami zabezpieczeń 148
DC-06. Kontrola stanu usługi KCC 151
DC-07. Kontrola topologii replikacji AD 152
DC-08. Weryfikacja stanu wykazu globalnego 154
DC-09. Zarządzanie administracyjnymi grupami uniwersalnymi ... 155
DC-10. Weryfikacja zasad kont 156
DC-11. Weryfikacja usługi PKI 158
DC-12. Weryfikacja usługi AD i konta administratora 159
DC-13. Zarządzanie obiektami Lost And Found 159
DC-14. Zarządzanie delegowaniem praw 160
DC-15. Zarządzanie instalowaniem oprogramowania 163
DC-16. Zarządzanie GPO 165
DC-17. Zarządzanie obiektami komputerów 167
DC-18. Zarządzanie grupami dystrybucyjnymi 169
DC-19. Zarządzanie lasem AD 170
DC-20. Zarządzanie informacjami w AD 172
DC-21. Zarządzanie schematem 172
DC-22. Zarządzanie dostępem do schematu 174
DC-23. Modyfikacje zawartości schematu 175
DC-24. Ocena programów modyfikujących schemat 177
DC-25. Zarządzanie rolami wzorców operacji 178
DC-26. Przenoszenie ról wzorców operacji 181
DC-27. Przywracanie wzorców operacji po awarii 182
DC-28. Promocja kontrolerów domen 182
DC-29. Przywracanie kontrolerów domen 185
DC-30. Zarządzanie relacjami zaufania 187
DC-31. Zarządzanie strukturami lasów, domen i OU 189
DC-32. Zarządzanie skryptami Active Directory 191
DC-33. Zarządzanie synchronizacją czasu 193
DC-34. Zarządzanie listami kontroli dostępu 194
DC-35. Zarządzanie zapisanymi kwerendami 197
DC-36. Zarządzanie miejscem w AD 198
DC-37. Zarządzanie zasadami kwerend LDAP 199
DC-38. Zarządzanie bazą danych AD 201

Zarządzanie serwerem przestrzeni nazw (DNS) ... 202
DN-01. Kontrola dziennika zdarzeń DNS ... 202
DN-02. Zarządzanie konfiguracją DNS-u ... 203
DN-03. Zarządzanie rekordami DNS ... 204
DN-04. Zarządzanie partycją aplikacji DNS ... 205

Rozdział 5. Zarządzanie serwerami aplikacji ... 207

Czynności administracyjne ... 207
Zarządzanie dedykowanymi serwerami WWW ... 209
WS-01. Weryfikacja dziennika zdarzeń Aplikacje ... 209
WS-02. Weryfikacja stanu serwera IIS ... 210
WS-03. Generowanie statystyk użycia serwera IIS ... 211
WS-04. Weryfikacja dziennika zdarzeń serwera WWW ... 213
WS-05. Weryfikacja aktualizacji zabezpieczeń IIS ... 214
WS-06. Zarządzanie konfiguracją serwera WWW ... 215
Zarządzanie serwerami aplikacji ... 216
AS-01. Weryfikacja stanu współużytkowanych aplikacji ... 217
AS-02. Administrowanie aplikacjami COM+ ... 218
AS-03. Administrowanie aplikacjami .NET ... 221
AS-04. Administrowanie serwerem baz danych ... 223
AS-05. Dostęp klientów serwera aplikacji ... 223
AS-06. Instalacja oprogramowania użytkowników ... 224
Serwery usług terminalowych ... 226
TS-01. Zarządzanie połączeniami usług terminalowych ... 227
TS-02. Zarządzanie drukarkami w usługach terminalowych ... 228
TS-03. Zarządzanie katalogiem sesji ... 229
TS-04. Administrowanie licencjami usług terminalowych ... 230
TS-05. Administrowanie dostępem użytkowników usług terminalowych ... 230
TS-06. Zarządzanie aplikacjami w usługach terminalowych ... 231
Zarządzanie wydajnością i monitorowaniem ... 232
PM-01. Weryfikacja dzienników ruterów i zapór sieciowych ... 233
PM-02. Ogólne monitorowanie miejsca na dyskach ... 234
PM-03. Zarządzanie zasobami systemów ... 235
PM-04. Monitorowanie ruchu w sieci ... 237
PM-05. Zarządzanie wydajnością serwerów ... 238
PM-06. Diagnostyka systemów ... 240
PM-07. Zarządzanie raportowaniem błędów w przedsiębiorstwie ... 241
PM-08. Przegląd narzędzi do monitorowania ... 242
Uwagi końcowe ... 243

Dodatek A Lista częstotliwości wykonywania zadań ... 245

Skorowidz ... 251

Rozdział 1.

Ogólne zarządzanie serwerem

Wprawdzie większość serwerów odgrywa konkretne role w strukturze naszej organizacji, lecz jest oczywiste, że pewne zadania administracyjne należy wykonywać we wszystkich serwerach, niezależnie od ich ról. Są to ogólne zadania administracyjne. Należą do nich wszelkie czynności — od upewnienia się, że serwer funkcjonuje poprawnie, aż po weryfikację, czy konfiguracja serwera jest zgodna ze standardami organizacji. Wiele z tych zadań ma charakter techniczny i część z nich może być zautomatyzowana, lecz niektóre są czysto administracyjne i ich przeprowadzenie nie wymaga pracy z technologią.

Czynności administracyjne

Ogólne zarządzanie serwerami Windows dzieli się na cztery kategorie administracyjne. Należą do nich ogólna obsługa serwera, sprzęt, tworzenie i przywracanie kopii zapasowych oraz administrowanie zdalne. Tabela 1.1 przedstawia listę czynności administracyjnych, które musimy wykonywać regularnie, aby zapewnić prawidłowe funkcjonowanie usług, świadczonych przez serwery naszej społeczności użytkowników. W tabeli tej została też przedstawiona częstotliwość wykonywania poszczególnych zadań.

Nie każdy musi zgadzać się z częstotliwością zadań zasugerowaną w tabeli 1.1. Co więcej, wykonywanie absolutnie wszystkich czynności może nie być konieczne, jeśli nie stosujemy wszystkich wspomnianych w tabeli usług. Dlatego Czytelnik powinien spersonalizować tę książkę, zaznaczając wszystkie numery procedur, z których faktycznie będzie korzystać. Dzięki temu łatwiej będzie znaleźć najczęściej używane procedury.

Tabela 1.1. *Lista zadań administracyjnych dla serwera*

Nr procedury	Czynność	Harmonogram
	Ogólne zarządzanie serwerem	
GS-01	Skróty Uruchom jako	Codziennie
GS-02	Ogólna weryfikacja stanu usług	Codziennie
GS-03	Weryfikacja dziennika zdarzeń System	Codziennie
GS-04	Weryfikacja dziennika zdarzeń Zabezpieczenia	Codziennie
GS-05	Zarządzanie kontami usług i administracyjnymi	Codziennie
GS-06	Utrzymanie dziennika działań	Codziennie
GS-07	Zarządzanie raportem o czasie dostępności systemu	Co tydzień
GS-08	Zarządzanie skryptami	Co tydzień
GS-09	Zarządzanie certyfikatami skryptów	Co tydzień
GS-10	Aktualizacje definicji wirusów dla programów antywirusowych	Co tydzień
GS-11	Restart serwera	Co tydzień
GS-12	Przegląd i aktualizacja zasad zabezpieczeń	Co miesiąc
GS-13	Weryfikacja aktualizacji zabezpieczeń	Co miesiąc
GS-14	Aktualizacja poprawek i pakietów Service Pack	Co miesiąc
GS-15	Ocena nowego oprogramowania	Co miesiąc
GS-16	Inwentaryzacja	Co miesiąc
GS-17	Tworzenie globalnej konsoli MMC	W miarę potrzeb
GS-18	Automatyczne pobieranie sygnatur dla oprogramowania antywirusowego	W miarę potrzeb
GS-19	Tworzenie i weryfikacja zaplanowanych zadań	W miarę potrzeb
GS-20	Tworzenie i modyfikacja szablonów zabezpieczeń	W miarę potrzeb
GS-21	Zarządzanie plikami pomocy technicznej	W miarę potrzeb
GS-22	Przygotowanie serwera	W miarę potrzeb
GS-23	Konfiguracja narzędzi administracyjnych	W miarę potrzeb
GS-24	Aktualizacja domyślnego profilu użytkowników	W miarę potrzeb
GS-25	Przegląd środowiska sprzętowego	W miarę potrzeb
GS-26	Dokumentacja systemu i sieci	W miarę potrzeb
GS-27	Zarządzanie umowami o świadczeniu usług	W miarę potrzeb
GS-28	Zarządzanie priorytetami w rozwiązywaniu problemów	W miarę potrzeb
GS-29	Przegląd nakładów pracy	W miarę potrzeb

Tabela 1.1. *Lista zadań administracyjnych dla serwera (ciąg dalszy)*

Nr procedury	Czynność	Harmonogram
	Sprzęt	
HW-01	Kontrola urządzeń sieciowych	Co tydzień
HW-02	Zarządzanie BIOS-em serwerów	Co miesiąc
HW-03	Zarządzanie aktualizacjami oprogramowania sprzętowego i zarządzającego serwerami	Co miesiąc
HW-04	Zarządzanie urządzeniami	W miarę potrzeb
	Tworzenie i przywracanie kopii zapasowych	
BR-01	Generowanie kopii zapasowych stanu systemu	Codziennie
BR-02	Weryfikacja kopii zapasowych	Codziennie
BR-03	Zarządzanie składowaniem taśm poza lokalizacją serwerów	Co tydzień
BR-04	Testowanie strategii usuwania skutków awarii	Co miesiąc
BR-05	Testowanie procedury przywracania kopii zapasowych	Co miesiąc
BR-06	Przegląd strategii kopii zapasowych	Co miesiąc
BR-07	Odbudowa serwera	W miarę potrzeb
	Administrowanie zdalne	
RA-01	Zarządzanie RDC w serwerach	Co miesiąc
RA-02	Zarządzanie RDC w komputerach osobistych	Co miesiąc
RA-03	Pomoc dla użytkowników poprzez narzędzie Pomoc zdalna	W miarę potrzeb
RA-04	Skróty do Podłączania pulpitu zdalnego i dostęp przez WWW	W miarę potrzeb

Harmonogram również może różnić się od przedstawionego w tabeli 1.1. Częstotliwość zadań zależy od mnóstwa czynników, na przykład od niezawodności systemu, jego obciążenia, wielkości i szybkości dysków, mocy obliczeniowej procesorów i tak dalej. Jeśli przedstawiony harmonogram nie pasuje do konkretnych potrzeb, można go zmienić.

Jeśli przedstawiony harmonogram nie zaspokaja potrzeb Czytelników, prosimy o uwagi. Chętnie dowiemy się, jaki harmonogram najlepiej pasuje do Waszych wymagań i opublikujemy zaktualizowane arkusze na stronie *www.Reso-Net.com/PocketAdmin*. Oczekujemy na uwagi pod adresem *PocketAdmin@Reso-Net.com*.

Ogólne zarządzanie serwerem

Serwery z założenia projektowane są z myślą o obsługiwaniu wielu użytkowników wykonujących codzienne zadania. Niezależnie od tego, czy organizacja ma 4 użytkowników czy 4000, zadaniem administratora systemów jest zapewnienie, by systemy działały poprawnie, zagwarantowanie ich bezpieczeństwa i wydajności wystarczającej do produktywnego funkcjonowania serwerów teraz i w przyszłości.

Część działań wymaganych, by osiągnąć te cele stosuje się do wszystkich serwerów. Wiele z nich dotyczy po prostu ciągłości działania systemu i sposobów interakcji z nim.

GS-01. Skróty Uruchom jako

✔ **Harmonogram: codziennie**

Praca z serwerami często wymaga dostępu administracyjnego do systemu. Prawa dostępu przyznane administratorom systemów Windows Server 2003 są ogromne, ponieważ pozwalają na całkowitą kontrolę nad komputerem na poziomie lokalnym, nad domeną na poziomie domeny i nad całym lasem na poziomie przedsiębiorstwa. Praw tych musimy używać z rozwagą, szczególnie dlatego, że każdy program działający w kontekście administracyjnym uzyskuje automatycznie wszystkie prawa do komputera.

Ponieważ konta administracyjne mogą stanowić zagrożenie dla przedsiębiorstwa, należy zmienić ich nazwy na inne niż domyślne i zastosować do nich silne, złożone hasła, zwykle dłuższe niż 15 znaków. Aby dodatkowo zwiększyć bezpieczeństwo tych kont, możemy je powiązać z kartami inteligentnymi.

Na przykład, wirus lub robak uruchomiony w kontekście administracyjnym może spowodować o wiele więcej szkód niż wtedy, gdy uruchomi się w kontekście użytkownika. Z tego powodu skróty Uruchom jako są tak ważne. Ponieważ umożliwiają one wykonywanie poleceń i uruchamianie aplikacji w innym kontekście zabezpieczeń, pozwalają na bardziej oszczędne stosowanie dostępu administracyjnego — możemy korzystać z konta zwykłego użytkownika, wykonując działania administracyjne z ograniczeniem dostępu administracyjnego do minimum, jednocześnie chroniąc dobra przedsiębiorstwa.

Poprzez *Uruchom jako* możemy skorzystać z każdego narzędzia. W systemie Windows Server 2003 wystarczy kliknąć prawym przyciskiem myszy narzędzie, wybrać *Uruchom jako*, podać odpowiednią nazwę konta i hasło oraz kliknąć *OK*. Jeśli polecenie *Uruchom jako* nie pojawia się w menu podręcznym, należy przy kliknięciu prawym przyciskiem myszy przytrzymać klawisz *Shift*.

To zadanie zostało określone jako wykonywane codziennie, ponieważ jeśli prawidłowo zaprojektujemy skróty, to będziemy z nich korzystać codziennie przy wykonywaniu czynności administracyjnych w każdym serwerze w obrębie organizacji. Możemy tworzyć tyle skrótów, ile tylko potrzebujemy. Zaletą skrótów Uruchom jako jest możliwość wyboru konta administracyjnego przy każdym uruchomieniu narzędzia. Dzięki temu możemy do każdego skrótu przyznać tylko niezbędne prawa dostępu. I ponieważ skróty nie są uruchamiane automatycznie w nowym kontekście (nie można osadzić w nich nazwy konta i hasła), same z siebie nie stanowią zagrożenia.

Najbezpieczniejszą metodą korzystania z polecenia *Uruchom jako* jest stosowanie skrótów w trybie graficznym.

Za pomocą skrótów Uruchom jako warto uruchamiać następujące narzędzia:

- globalną konsolę MMC, którą utworzymy w procedurze **GS-17**,
- Eksplorator Windows,
- wiersz poleceń,
- narzędzie Kopia zapasowa.
- narzędzia wyspecjalizowane, np. konsole Active Directory i zarządzanie Zasadami grup.

Skróty najłatwiej tworzyć na pulpicie. Po utworzeniu możemy je przenieść do paska narzędzi Szybkie uruchamianie i usunąć z pulpitu. Aby utworzyć skrót Uruchom jako:

1. Przejdź do widoku pulpitu. Najszybciej możesz to zrobić, klikając ikonę *Pokaż pulpit* w obszarze *Szybkie uruchamianie*.
2. Kliknij prawym przyciskiem myszy dowolne miejsce na pulpicie i wybierz *Nowy*/*Skrót*.

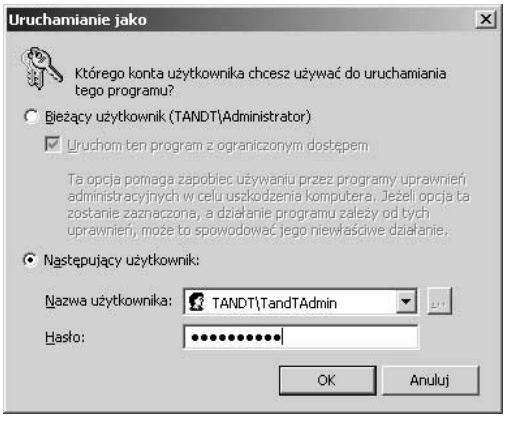
3. Kliknij przycisk *Przeglądaj*, aby znaleźć pożądane polecenie lub konsolę, która ma zostać otwarta, albo wpisz polecenie bezpośrednio. Zaletą bezpośredniego wpisania polecenia jest możliwość użycia zmiennych środowiskowych do zlokalizowania polecenia lub konsoli. Na przykład, dla Eksploratora, wiersza poleceń i konsoli Kopia zapasowa możemy użyć zmiennej `%SystemRoot%`. Kliknij *Dalej*.
4. Kliknij *Zakończ*, aby utworzyć skrót.

Zadanie to możemy sobie ułatwić poprzez utworzenie kopii skrótów z menu *Wszystkie programy*.

5. Po utworzeniu skrótu kliknij go prawym przyciskiem myszy i wybierz *Właściwości*.
6. Na zakładce *Skrót* kliknij przycisk *Zaawansowane*.
7. W oknie dialogowym *Zaawansowane* wybierz *Uruchom z innymi poświadczeniami*. Kliknij *OK*, aby zamknąć okno dialogowe.
8. Kliknij *OK*, aby zamknąć okno dialogowe *Właściwości*.

Skrót jest gotowy. Teraz możemy przenieść go do obszaru szybkiego uruchamiania. Użycie skrótu spowoduje automatyczne wyświetlenie okna dialogowego *Uruchom jako*. Tutaj możemy uruchomić polecenie z bieżącymi poświadczeniami lub wybrać *Następujący użytkownik* i wprowadzić dane konta administracyjnego (patrz rysunek 1.1).

Rysunek 1.1. *Uruchomienie programu poprzez Uruchom jako*



Skróty Uruchom jako można też tworzyć za pomocą wiersza poleceń. Wystarczy umieścić polecenie w pliku z rozszerzeniem *.cmd* i wskazać skrót do tego pliku. Wiersz poleceń daje nam możliwość bardziej precyzyjnego zdefiniowania

polecenia *Uruchom jako* za pomocą opcji, które zmienią domyślne zachowanie polecenia. Oprócz tego wiersz poleceń pozwala utworzyć pojedynczy plik *.cmd* zawierający polecenia uruchamiające wszystkie narzędzia niezbędne do wykonywania standardowych zadań administracyjnych. Do takiego pliku poleceń możemy następnie utworzyć skrót i umieścić go w obszarze szybkiego uruchamiania.

Kolejną zaletą tej metody jest dostępność opcji `/savecred`. Pełni ona dwie funkcje: zapamiętuje poświadczenia dla polecenia i pozwala wykorzystać zapisane poświadczenia. Jeśli więc użyjemy w pliku *.cmd* polecenia o strukturze przedstawionej poniżej, będziemy mogli uruchomić wszystkie niezbędne narzędzia, przydzielając do każdego z nich odpowiednie konto użytkownika:

```
runas /user:nazwaużytkownika@nazwadomeny /savecred polecenie
```

gdzie *nazwaużytkownika@nazwadomeny* to nazwa główna użytkownika dla konta administracyjnego, którego chcemy użyć, a *polecenie* oznacza ścieżkę i nazwę polecenia, które chcemy uruchomić. Polecenia uruchamiające narzędzia wspomniane uprzednio będą wyglądać tak:

```
runas /user:nazwaużytkownika@nazwadomeny /savecred "mmc C:\Toolkit\
globalmmc.msc"
runas /user:nazwaużytkownika@nazwadomeny /savecred %SystemRoot%\explore.exe
runas /user:nazwaużytkownika@nazwadomeny /savecred %SystemRoot%\system32\
cmd.exe
runas /user:nazwaużytkownika@nazwadomeny /savecred %SystemRoot%\system32\
ntbackup.exe
```

Tej samej struktury poleceń możemy użyć dla innych narzędzi, które uznamy za niezbędne do pracy, wymagających uprawnień administracyjnych. Plik poleceń należy zapisać w folderze *C:\Toolkit*, aby udostępnić je wszystkim używanym kontom administracyjnym. Folder ten jest niezbędny, ponieważ folder *Moje dokumenty* domyślnie pozwala na interakcję z własnego konta i wymaga modyfikacji uprawnień, aby inni użytkownicy mieli dostęp do jego zawartości. Folder ten zostanie dokładniej omówiony w procedurze **GS-17**.

Koniecznie skorzystaj z procedury **FS-13**, aby przypisać odpowiednie parametry zabezpieczeń do folderu *C:\Toolkit*, zwłaszcza jeśli mają się w nim znaleźć pliki poleceń zawierające polecenia `runas` z zapisanymi poświadczeniami. Umożliwienie komukolwiek dostępu do tego folderu stanowi poważne zagrożenie bezpieczeństwa. Można rozważyć ograniczenie dostępu do tego folderu jedynie dla kont administracyjnych i stworzenie skrótu Uruchom jako do pliku poleceń zestawu narzędzi. W ten sposób nikt nie będzie mógł nieumyślnie uruchomić tego pliku przez niepoprawny dostęp do naszej stacji roboczej.

Z poleceniem `runas` można jeszcze użyć dwóch przydatnych opcji wiersza poleceń. Opcja `/smartcard` umożliwia użycie do uwierzytelnienia karty inteligentnej (ang. *SmartCard*) i powinna być używana w organizacjach kładących duży

nacisk na bezpieczeństwo. Stosowanie kart inteligentnych w systemie Windows Server 2003 jest tak proste, że użycie ich dla kont administracyjnych jest wysoce zalecane. Opcja `/netonly` ogranicza prawa dostępu jedynie do sieci i nie pozwala nowemu kontekstowi zabezpieczeń na interakcję z komputerem lokalnym.

GS-02. Ogólna weryfikacja stanu usług

✔ **Harmonogram: codziennie**

Przeznaczeniem serwera jest dostarczanie usług. Serwer można uznać za funkcjonujący poprawnie, gdy wszystkie usługi, które ma dostarczać, są uruchomione i w pełni funkcjonalne. Dlatego też tak ważna jest dokładna dokumentacja nie tylko konkretnej roli każdego serwera w infrastrukturze naszej sieci, lecz również zainstalowanych usług i ogólnego stanu każdej usługi.

Szczegółowy arkusz danych serwera jest dostępny pod adresem *www.Reso-Net.com/PocketAdmin*. Arkusz ten może posłużyć jako podstawa dokumentacji serwera i identyfikacji zainstalowanych usług.

Aby zweryfikować stan usług w serwerze:

1. Uruchom konsolę *Zarządzanie komputerem*.
2. Połącz się z odpowiednim serwerem (*Akcja*/*Połącz z innym komputerem*) i albo wpisz nazwę serwera (`\\nazwaserwera`), albo zlokalizuj serwer za pomocą przycisku *Przeglądaj*. Kliknij *OK*.
3. Przejdź do okna *Usługi* (*Usługi i aplikacje*/*Usługi*).
4. Posortuj usługi według stanu, klikając *Stan* na górze okna *Usługi*.
5. Zweryfikuj na podstawie notatek, czy wszystkie usługi są w odpowiednim stanie uruchomienia. Jeśli któreś z usług używają poświadczeń innych niż lokalne konto systemowe, skorzystaj z procedury **GS-05**, aby upewnić się, że wszystkie poświadczenia zostały wprowadzone prawidłowo. Zanotuj i zbadaj wszystkie usługi znajdujące się w innym stanie niż oczekiwany. Zweryfikuj wszystkie serwery.

Alternatywą dla tej procedury może być użycie polecenia Remote Server Information z zestawu narzędzi Resource Kit dla każdego serwera, którym zarządzamy i przekierowanie wyjścia polecenia do pliku tekstowego:

```
srvinfo \\nazwakomputera >nazwapliku.txt
```

gdzie *nazwakomputera* oznacza nazwę serwera, który chcemy zbadać. Jeśli nazwa serwera nie zostanie podana, polecenie wyświetli informacje o serwerze lokalnym. *nazwapliku.txt* oznacza nazwę i ścieżkę do pliku, do którego informacje

mają zostać wysłane. Ponownie możemy umieścić serię takich poleceń w pliku *.cmd* i za pomocą procedury **GS-19** codziennie generować automatycznie pliki wyjściowe. To pomoże szybko zorientować się w stanie wszystkich usług w sieci.

Oprócz tego wszystkie usługi możemy kontrolować za pomocą poleceń `sc` i `net`. Wpisanie `net` w wierszu poleceń powoduje wyświetlenie listy wszystkich obsługiwanych poleceń. Szczegółowe informacje o każdym poleceniu możemy otrzymać, wpisując `net help` *`nazwapolecenia`*. Jedyną wadą tego narzędzia jest niemożliwość wykonywania poleceń zdalnie. Aby skorzystać z tych poleceń, musimy otworzyć sesję lokalną albo zdalną w serwerze, którym chcemy zarządzać.

Z drugiej strony, polecenie `sc` możemy uruchomić w każdym serwerze, do którego mamy dostęp. Jego struktura wygląda następująco:

```
sc \\nazwaserwera polecenie nazwausługi
```

gdzie *`\\nazwaserwera`* oznacza nazwę serwera, z którym chcemy się połączyć, *`polecenie`* jest nazwą polecenia `sc`, które ma zostać wykonane, a *`nazwausługi`* wskazuje na usługę, z którą chcemy pracować. Dodatkowe informacje otrzymamy przez wpisanie `sc /?`.

Microsoft TechNet Script Center zawiera szereg przykładowych skryptów WSH (ang. *Windows Scripting Host*), pomagających przeprowadzać prace administracyjne z usługami. Skrypty te znajdziemy pod adresem *http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/services/default.asp?frame=true*.

GS-03. Weryfikacja dziennika zdarzeń System

✔ **Harmonogram: codziennie**

Kolejnym przydatnym narzędziem diagnostycznym jest systemowy dziennik zdarzeń, który informuje o ogólnym „stanie zdrowia" i funkcjonowaniu serwera. Każde istotne zdarzenie jest rejestrowane wraz z opisem. Zdarzenia mogą należeć do trzech grup:

Informacja: zaszło zdarze nie wystarczająco istotne, by je zarejestrować. Zdarzenia te zwykle związane są z normalną pracą serwera.

Ostrzeżenie: wystąpił błąd niekrytyczny, który uzasadnia utworzenie rekordu w Dzienniku zdarzeń. Na zdarzenia tego typu należy zwracać uwagę, ponieważ szybko mogą przejść w błędy.

Błąd: wystąpił błąd krytyczny, który powinien zostać zbadany i naprawiony. Każde takie zdarzenie musi prowadzić do kontroli i naprawy. Windows Server 2003 często dołącza szczegółowe informacje o metodach postępowania w takich przypadkach.

Aby sprawdzić dziennik zdarzeń System w serwerze:

1. Uruchom konsolę *Zarządzanie komputerem*.
2. Połącz się z odpowiednim serwerem (*Akcja*/*Połącz z innym komputerem*) i albo wpisz nazwę serwera (`\\nazwaserwera`), albo zlokalizuj serwer za pomocą przycisku *Przeglądaj*. Kliknij *OK*.
3. Przejdź do dziennika zdarzeń *System* (*Zarządzanie komputerem*/*Podgląd zdarzeń*/*System*).
4. Zidentyfikuj wszelkie błędy i ostrzeżenia oraz podejmij odpowiednie kroki w razie ich pojawienia się.

Zanotuj wszelkie czynności naprawcze, które musisz podjąć. Wykorzystaj procedurę **GS-06** do rejestrowania różnorodnych kontrolowanych codziennie zdarzeń.

Można zmienić wielkość pliku dziennika. W tym celu kliknij prawym przyciskiem myszy nazwę dziennika w lewym panelu MMC i wybierz *Właściwości*. Ustaw *Maksymalny rozmiar dziennika* i związane z nim zdarzenie zgodnie z potrzebami.

Microsoft TechNet Script Center zawiera szereg przykładowych skryptów WSH (ang. *Windows Scripting Host*), pomagających przeprowadzać prace administracyjne z usługami. Skrypty te znajdziemy pod adresem *http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/logs/default.asp?frame=true*.

GS-04. Weryfikacja dziennika zdarzeń Zabezpieczenia

✔ **Harmonogram: codziennie**

Jeśli organizacja zdecydowała się, by prowadzić inspekcje dostępu, to musimy codziennie weryfikować dziennik zdarzeń Zabezpieczenia, aby upewnić się, że w sieci nie zachodzą niestosowne zdarzenia.

Inspekcje dostępu można umożliwić poprzez zmiany w Zasadach grup. Zasady inspekcji mieszczą się w ustawieniach zabezpieczeń zasad grup. Włączenie inspekcji może mieć poważny wpływ na działanie sieci. Kontrola obiektów i zdarzeń spowalnia system, więc powinniśmy prowadzić inspekcje tylko tych zdarzeń i obiektów, które uznamy za krytyczne dla naszej sieci.

W systemie Windows Server 2003 wszystkie inspekcje są domyślnie włączone; wystarczy więc dokładniej zdefiniować i dodać obiekty, które chcemy weryfikować. Poza tym dziennik zdarzeń Zabezpieczenia ma zdefiniowany rozmiar: 132 MB i jest po zapełnieniu nadpisywany.

Aby zdefiniować lub przejrzeć zasady inspekcji:

1. Korzystając z procedury **DC-16**, dokonaj edycji odpowiedniego obiektu zasad grupy (ang. *GPO — Group Policy Object*). Będzie to zazwyczaj GPO stosujący się do wszystkich obiektów w domenie.
2. W Edytorze obiektów zasad grupy wybierz *Konfiguracja komputera*/*Ustawienia systemu Windows*/*Ustawienia zabezpieczeń*/*Zasady inspekcji*.
3. Kliknij dwukrotnie zdarzenie, które chcesz kontrolować i zmodyfikuj zasady. Rejestrowane mogą być sukces lub niepowodzenie zdarzenia, albo jedno i drugie.
4. Udokumentuj każdą dokonaną zmianę ustawień.

Arkusz dokumentacji zasad grup jest dostępny na stronie *www.Reso-Net.com/PocketAdmin*.

Aby dokonać inspekcji dostępu do obiektu, na przykład kontenera w AD lub pliku w serwerze, trzeba włączyć inspekcje dla tego obiektu i zidentyfikować, kto powinien podlegać inspekcji. W tym celu:

1. Znajdź obiekt przeznaczony do inspekcji. Zamiast pojedynczych obiektów warto kontrolować kontenery, na przykład foldery i jednostki organizacyjne.
2. Kliknij obiekt prawym przyciskiem myszy i wybierz *Właściwości*. Przejdź do zakładki *Zabezpieczenia*.
3. Kliknij przycisk *Zaawansowane*. Aby to było możliwe w przypadku AD, należy w konsolach Active Directory włączyć w menu *Widok* opcję *Opcje Zaawansowane*.
4. Zidentyfikuj grupy, które chcesz kontrolować. Zwykle łatwiej jest wybierać grupy o szerokim zasięgu, na przykład Użytkownicy uwierzytelnieni, zamiast grup bardziej konkretnych. Wszystko zależy od tego, kogo i co chcemy kontrolować.
5. Od tej chwili zdarzenia dostępu będą monitorowane w dzienniku zdarzeń Zabezpieczenia.

Zanotuj wszelkie wprowadzone zmiany. Aby przejrzeć wyniki inspekcji:

1. Uruchom konsolę *Zarządzanie komputerem* (pasek *Szybkie uruchamianie*/*Zarządzanie komputerem*).
2. Połącz się z odpowiednim serwerem (*Akcja*/*Połącz z innym komputerem*) i albo wpisz nazwę serwera (`\\nazwaserwera`), albo zlokalizuj serwer za pomocą przycisku *Przeglądaj*. Kliknij *OK*.
3. Przejdź do dziennika zdarzeń *Zabezpieczenia* (*Narzędzia systemowe*/*Podgląd zdarzeń*/*Zabezpieczenia*).
4. Zidentyfikuj wszelkie zdarzenia zakończone powodzeniem lub niepowodzeniem. Podejmij odpowiednie działania w razie odkrycia niepożądanych działań.

Zanotuj wszelkie czynności naprawcze, które trzeba było podjąć. Korzystając z procedury **GS-06**, zarejestruj sprawdzane codziennie zdarzenia.

Rozmiar dziennika zdarzeń Zabezpieczenia można zmienić. W tym celu skorzystaj z ostatniej części procedury **GS-03**.

W przypadku zablokowania pliku dziennika (*Nie zastępuj zdarzeń*) po osiągnięciu przez plik maksymalnej wielkości serwer zostanie automatycznie wyłączony i będzie wymagać wyczyszczenia pliku.

GS-05. Zarządzanie kontami usług i administracyjnymi

✔ Harmonogram: codziennie

Konta administracyjne są cennymi dobrami w każdej sieci. Minęły już czasy, gdy rozdawano je prawie każdemu, kto wystarczająco głośno się ich domagał. W dzisiejszych sieciach Windows Server 2003 możemy i powinniśmy definiować jedynie dostateczny poziom praw dostępu każdemu, kto wchodzi w interakcję z systemem. Wobec tego powinniśmy mieć jak najmniej kont administracyjnych na poziomie domeny lub lasu, za to o wiele więcej wyspecjalizowanych kont administracyjnych, które będą miały prawa dostępu wystarczające jedynie do wykonania określonych zadań. Konta te i ich prawa dostępu powinny być przynajmniej przeglądane codziennie.

Kilka procedur wspomaga przyznawanie odpowiednich praw i uprawnień dla kont administracyjnych. Niektóre z nich są przydzielane przez wykorzystanie wbudowanych grup zabezpieczeń, na przykład Serwer lub Operatorzy kopii zapasowych,

zaś inne przez kojarzenie z zasadami Przypisywanie praw użytkowników dla kont lub grup zawierających te konta. Trzy narzędzia pozwalają przydzielać odpowiednie prawa:

- Użytkownicy i komputery usługi Active Directory — pozwala tworzyć konta i przydzielać je do wbudowanych albo własnych grup administracyjnych.
- Konsola Group Policy Management Console — pozwala znajdować i modyfikować odpowiednie GPO.
- Edytor obiektów zasad grupy — pozwala przypisywać prawa użytkowników.

Oprócz tego konsola Zarządzanie komputerem może przydać się do przydzielania praw lokalnych do grup domeny i kont.

Aby zmodyfikować prawa użytkownika, skorzystaj z procedury **DC-16** w celu edycji odpowiedniego GPO, zwykle tego wpływającego na wszystkie obiekty, które chcesz zmodyfikować. Znajdź ustawienia *User Rights Assignment* (*Computer Policy*/*Security Settings*/*Local Policies*/*User Rights Assignment*) i przypisz odpowiednie ustawienia do kont administracyjnych. Zawsze łatwiej jest przypisywać prawa do grupy niż do indywidualnych obiektów, więc dobrze jest zgromadzić konta administracyjne w grupy administracyjne. Skorzystaj ponownie z procedury **DC-16**, aby zapewnić właściwe wykorzystanie tych kont.

Oprócz tego we współczesnych sieciach przedsiębiorstw trzeba też zarządzać kontami usług — kontami, które posiadają wystarczające przywileje administracyjne, by obsługiwać konkretne usługi w sieci. Na przykład, konta usług mogą służyć do uruchamiania mechanizmów narzędzi antywirusowych i zaplanowanych zadań (patrz procedura **GS-19**). Zaletą korzystania z konta usługi do uruchamiania danej usługi lub zautomatyzowanego zadania jest możliwość kontroli poprawności działania usługi za pomocą dziennika zdarzeń Zabezpieczenia. Zdarzenie sukcesu jest zapisywane w tym dzienniku za każdym razem, gdy usługa wykorzysta swój uprzywilejowany dostęp lub zaloguje się.

Konta usług muszą mieć określone przywileje i ustawienia:

- Konto musi mieć złożoną nazwę.
- Do konta musi być przypisane złożone hasło o długości przynajmniej 15 znaków.
- Hasło nigdy nie wygasa.
- Użytkownik nie może zmienić hasła.
- Prawo Działanie jako element systemu operacyjnego.
- Prawo Logowanie w trybie usługi.

Dwa ostatnie ustawienia nie powinny być stosowane zbyt skwapliwie, zwłaszcza Działanie jako element systemu operacyjnego, ponieważ przyznają usłudze wyjątkowo wysoki poziom dostępu.

Dwa ostatnie ustawienia trzeba skonfigurować w GPO w Przypisywanie praw użytkownika (ang. *User Rights Assignment*). Proszę też pamiętać o przegrupowaniu kont usług w grupy usług.

Konta usług wymagają dodatkowych nakładów pracy, ponieważ wymagają regularnych zmian haseł. Nie jest to ograniczone do prostej zmiany hasła w konsoli Użytkownicy i komputery usługi Active Directory, ponieważ po przypisaniu konta usługi do usługi musimy w usłudze podać hasło konta, aby mogła działać prawidłowo. Oznacza to, że musimy dodatkowo zmienić hasło w oknie dialogowym *Właściwości usługi*. W tym celu można posłużyć się procedurą **GS-02**.

Microsoft TechNet Script Center zawiera przykładowy skrypt WSH, który pozwala zmieniać hasła kont usług. Skrypt ten jest dostępny pod adresem *http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/services/scrsvc01.asp?frame=true*. Pozwala on również zmieniać hasła dla kont użytkowników administracyjnych. Szereg skryptów do pracy z kontami użytkowników znajdziemy pod adresem *http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/user/default.asp?frame=true*.

GS-06. Utrzymanie dziennika działań

✔ **Harmonogram: codziennie**

Jednym z zadań administratora jest rejestrowanie na bieżąco własnych działań i tego, co musi zrobić w celu utrzymania i przeprowadzenia napraw w sieci. Z tego powodu każdy administrator powinien utrzymywać dziennik swoich działań. W idealnej wersji dziennik ten powinien mieć postać elektroniczną i być przenośny, aby można było robić notatki w każdej chwili. Może być przechowywany w komputerze ręcznym Tablet PC lub Pocket PC. Tablet PC jest bardziej przydatny, ponieważ obsługuje w pełni funkcjonalną wersję Windows i pozwala uruchamiać pliki pomocy Windows Server 2003 (patrz procedura **GS-21**) oraz maszyny wirtualne w celu symulowania problematycznych sytuacji. Oprócz tego Microsoft OneNote idealnie nadaje się do rejestrowania codziennych czynności.

Jeśli żadne z tych urządzeń nie jest dostępne, administrator powinien przynajmniej nosić ze sobą cały czas papierowy dziennik. Sposób jego prowadzenia zależy od osobistych preferencji, lecz czasem najlepiej jest rejestrować swoje działania w miarę ich wykonywania zamiast czekać na określoną porę dnia.

Przykładowy dziennik działań dostępny jest pod adresem *www.Reso--Net.com/PocketAdmin*.

GS-07. Zarządzanie raportem o czasie dostępności systemu

✔ **Harmonogram: codziennie**

Raz na tydzień należy generować raporty o czasie dostępności wszystkich serwerów. Pozwoli to śledzić stan poszczególnych serwerów i identyfikować, które konfiguracje najlepiej sprawdzają się w danym środowisku. Do tworzenia tych raportów możemy posłużyć się kilkoma narzędziami.

Ostatni wiersz raportu generowanego przez polecenie `srvinfo`, opisane w procedurze **GS-02**, informuje o tym, od jak dawna serwer jest czynny. Kolejne polecenie, `systeminfo`, podaje informacje o badanym serwerze i od jakiego czasu system funkcjonuje. Trzecie narzędzie, `uptime`, zostało zaprojektowane specjalnie do raportowania czasu pracy serwera. Narzędzie to trzeba pobrać z witryny Microsoftu. Przejdź do *www.microsoft.com/downloads* i wyszukaj „uptime".

Z pomocą tego narzędzia i odrobiny pomysłowości można generować raporty o czasie dostępności automatycznie:

1. Pobierz i zainstaluj *uptime.exe* w folderze *C:\Toolkit*.
2. Utwórz plik poleceń, zawierający dla każdego serwera w sieci polecenie:

   ```
   uptime \\nazwaserwera
   ```

3. Zapisz plik poleceń.
4. Korzystając z procedury **GS-19**, stwórz cotygodniowy harmonogram dla tego pliku poleceń.
5. W zaplanowanym zadaniu przekieruj wynik do pliku tekstowego za pomocą polecenia:

   ```
   nazwaplikupolecen.cmd > nazwapliku.txt
   ```

Polecenie `uptime` będzie teraz tworzyć raport co tydzień. Od tej pory będziemy musieli jedynie znaleźć plik wyjściowy i przejrzeć wyniki.

Microsoft TechNet Script Center zawiera dwa skrypty związane z zarządzaniem czasem dostępności systemu. Pierwszy to Determining System Uptime, a drugi to Monitoring System Uptime. Oba dostępne są pod adresem *http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/monitor/default.asp?frame=true*.

GS-08. Zarządzanie skryptami

✔ **Harmonogram: co tydzień**

Skrypty uruchamiane w środowisku Windows Script Host (host skryptów systemu Windows) są niezbędnym elementem zarządzania siecią Windows. Jak wiemy, skrypty w systemie Windows stanowią własny świat. Język pisania skryptów wyewoluował do poziomu, na którym skrypt stanowi wyrafinowany program, uruchamiany albo w trybie graficznym (przeznaczonym dla użytkowników), albo w trybie tekstowym (skrypty administracyjne). Wybór trybu odbywa się przez wybór polecenia aktywującego skrypt:

```
wscript nazwaskryptu
cscript nazwaskryptu
```

gdzie `wscript` uruchamia skrypt w trybie graficznym, a `cscript` — w znakowym.

Ponieważ pojawiły się już wirusy skryptowe, takie jak *ILOVEYOU.vbs*, musimy upewnić się, że uruchamiane skrypty są bezpieczne. Najlepszym sposobem na to jest podpisywanie skryptów certyfikatami cyfrowymi. Najpierw musimy zdobyć certyfikat. Możemy go albo otrzymać od zewnętrznego wydawcy certyfikatów, albo wydać sobie samemu, jeśli zdecydujemy się zainstalować własny serwer certyfikatów (usługę serwera dostępną w systemie Windows Server 2003). Do tego może posłużyć procedura **DC-11**.

Podpisanie skryptu certyfikatem jest działaniem programistycznym. Przykładowe skrypty do dodawania podpisów i zarządzania nimi są dostępne w Microsoft TechNet Script Center pod adresem *http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/security/default.asp?frame=true*.

Skrypty można również chronić przez zakodowanie. Microsoft Script Encoder jest dostępny pod adresem *http://msdn.microsoft.com/scripting/vbscript/download/x86/sce10en.exe*.

Każdy tworzony i podpisywany skrypt powinien mieć pełną, aktualizowaną co tydzień dokumentację, zawierającą wszystkie istotne informacje o skrypcie.

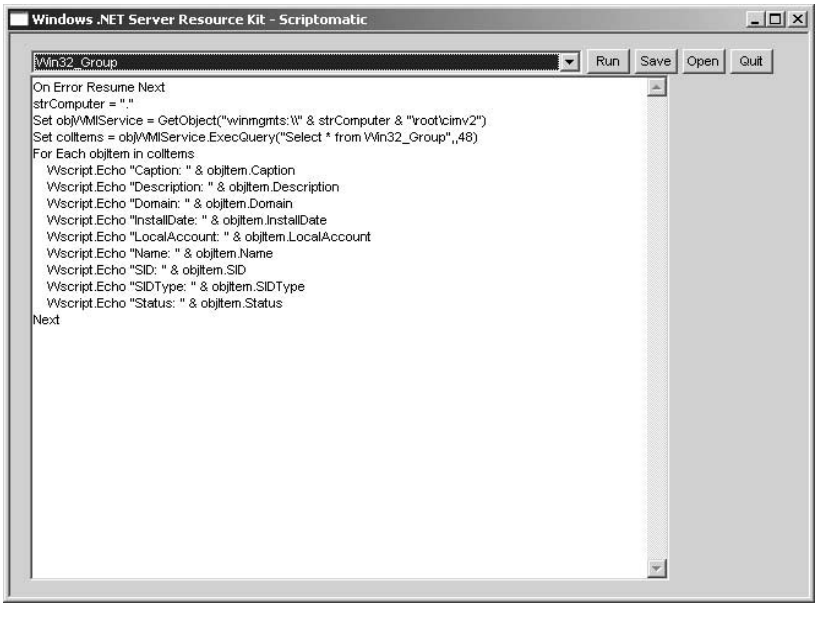
Do dokumentowania zawartości skryptu może posłużyć inny skrypt. Przykładowy kod dostępny jest w Microsoft TechNet Script Center pod adresem *http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/other/ScrOth03.asp?frame=true*.

Pisanie skryptów może być sporym wyzwaniem, jeśli nie znamy Windows Management Instrumentation (WMI) lub Active Directory Services Interface (ADSI). Dlatego też doskonałym pomysłem może być wykorzystanie do generowania za nas skryptów narzędzia Microsoft Scriptomatic. Narzędzie to jest dostępne w Microsoft Download Center; wystarczy poszukać Scriptomatic w *www.microsoft.com/downloads*. Oprócz tego dobre wprowadzenie do pisania skryptów jest dostępne pod adresem *http://msdn.microsoft.com/library/en-us/dnclinic/html/scripting06112002.asp*.

Instalacja narzędzia Scriptomatic jest prosta, wystarczy rozpakować pobrane archiwum. Plik *scriptomatic.hta* należy zapisać w folderze *C:\Toolkit*. Możemy też użyć skrótu Uruchom jako (patrz procedura **GS-01**) do uruchamiania Scriptomatic i umieścić go w obszarze szybkiego uruchamiania.

Aby napisać skrypt za pomocą narzędzia Scriptomatic:

1. Uruchom *scriptomatic.hta* lub skrót Uruchom jako.
2. W programie Scriptomatic wybierz klasę WMI, z którą chcesz pracować. Każda klasa ma nazwę w postaci *Win32_nazwa*. Wystarczy zwrócić uwagę na ostatnią część nazwy klasy. Na przykład, aby napisać skrypt pozwalający wyświetlić stan każdej usługi, wybierz klasę `Win32_Service`. Scriptomatic automatycznie generuje właściwy skrypt (patrz rysunek 1.2).



Rysunek 1.2. *Aby wygenerować skrypt wyświetlający grupy lokalne w komputerze, wybierz klasę Win32_Group w narzędziu Scriptomatic*

3. Kliknij *Run*. Scriptomatic uruchomi konsolę poleceń, aby uruchomić skrypt.
4. Kliknij *Save*, aby zapisać skrypt w pliku z rozszerzeniem VBS.

Skrypty te mogą posłużyć do wykonywania zadań administracyjnych i rejestrowania wyników wyjściowych. W tym celu wpisz polecenie:

```
cscript nazwaskryptu.vbs >nazwapliku.txt
```

gdzie `nazwaskryptu.vbs` oznacza nazwę skryptu przeznaczonego do uruchomienia, a `nazwapliku.txt` będzie utworzonym plikiem z danymi wyjściowymi. Za pomocą procedury **GS-19** można umieścić to polecenie w zaplanowanym zadaniu i uruchamiać zgodnie z harmonogramem.

Scriptomatic może pomóc w generowaniu skryptów logowania. Aby utworzyć kompletny skrypt logowania, może okazać się konieczne połączenie fragmentu skryptu WMI z fragmentem skryptu ADSI. Opisuje to procedura **DC-31**.

Oprócz skryptu logowania możemy chcieć wyświetlać komunikat dla użytkowników przed logowaniem. Pomaga to ostrzegać użytkowników przed prawnymi konsekwencjami nadużycia sprzętu komputerowego i informacji. Do tego ponownie posłuży GPO. Aby wyświetlić komunikat przy logowaniu, można posłużyć się procedurą **DC-16** do edycji odpowiedniego GPO i modyfikacji ustawień:

- *User Configuration*/*Windows Settings*/*Security Settings*/*Local Policies*/*Security Options*/*Interactive Logon*/*Message title for users attempting to log on*
- *User Configuration*/*Windows Settings*/*Security Settings*/*Local Policies*/*Security Options*/*Interactive Logon*/ *Message text for users attempting to log on*

GS-09. Zarządzanie certyfikatami skryptów

✔ **Harmonogram: co tydzień**

Najlepszą metodą na zapewnienie, by jedynie podpisane skrypty mogły być uruchamiane w naszej sieci, są Zasady ograniczeń oprogramowania (ang. *SRP — Software Restriction Policies*). SRP umożliwiają weryfikację skryptów i programów poprzez wykorzystanie jednego z czterech sposobów:

- *Reguły mieszania*,
- *Reguły certyfikatów*,

- *Reguły ścieżki*,
- *Reguły strefy internetowej*.

Najprostsze i najbezpieczniejsze w użyciu są reguły mieszania i (lub) certyfikatów. Obie można zastosować do skryptów i programów, takich jak pakiety instalacyjne dla przedsiębiorstwa (zwykle w formacie Instalatora systemu Windows *.msi*). Reguły SRP oparte na certyfikatach można zastosować lub zweryfikować następująco:

1. Zastosuj procedurę **DC-16** do edycji odpowiedniego GPO. Powinna się ona stosować do wszystkich docelowych systemów.
2. Kliknij prawym przyciskiem myszy *Zasady ograniczeń oprogramowania* (*Konfiguracja komputera*/*Ustawienia systemu Windows*/*Ustawienia zabezpieczeń*/*Zasady ograniczeń oprogramowania*) i wybierz *Nowe zasady ograniczeń oprogramowania* z menu podręcznego. Ta czynność spowoduje wygenerowanie środowiska SRP.
3. Upewnij się, że w lewym panelu rozwinięte są *Zasady ograniczeń oprogramowania*, a następnie kliknij prawym przyciskiem myszy *Reguły dodatkowe* i wybierz *Nowa reguła certyfikatu*.
4. W oknie dialogowym *Nowa reguła certyfikatu* kliknij *Przeglądaj*, aby znaleźć certyfikat używany do podpisywania pakietów instalacyjnych i skryptów, wybierz poziom zabezpieczeń *Bez ograniczeń* i wpisz opis. Kliknij *OK*.
5. Przejdź do Zasad ograniczeń oprogramowania i wybierz z prawego panelu *Wyznaczone typy plików*. Pliki *.wsh* i *.msi* będą już wymienione jako wyznaczone. Kliknij *OK*, aby zamknąć okno dialogowe.
6. Wybierz w tej samej lokalizacji *Zaufani wydawcy*. Upewnij się, że *Użytkownicy końcowi* mogą przyjmować certyfikaty, i że zaznaczone są pola wyboru przy *Wydawca* i *Sygnatura czasowa*. Kliknij *OK*.
7. Wybierz *Wymuszanie*, aby sprawdzić, czy pliki *.dll* nie są weryfikowane, i czy to ustawienie stosuje się do wszystkich użytkowników.

Można wyłączyć z tej reguły administratorów lokalnych, lecz z dużą rozwagą.

8. Udokumentuj wszystkie zmiany.

GS-10. Aktualizacje definicji wirusów dla programów antywirusowych

✔ **Harmonogram: co tydzień**

Ochrona przed wirusami jest kluczowym elementem zintegrowanego systemu ochrony. Oznacza to, że musimy na bieżąco kontrolować poprawność jej działania.

To jest pierwsze zadanie typu ogólnego. Zostało tu umieszczone, ponieważ należy je bezwzględnie wykonywać w serwerach, lecz nie dotyczy samego systemu Windows Server 2003.

Zarządzanie zabezpieczeniami antywirusowymi wymaga wykonywania trzech cotygodniowych zadań:

- Kontroli dzienników systemu antywirusowego, aby upewnić się, że w ciągu ostatniego dnia nie zostały znalezione żadne wirusy.
- Kontroli konsoli zarządzania systemem antywirusowym, aby sprawdzić, czy posiadane sygnatury wirusów są aktualne. Harmonogram aktualizacji można zmienić, jeśli jest niewystarczający lub gdy wzrasta zagrożenie wirusami.
- Losowego skanowania udziałów plikowych, aplikacji i dysków systemowych, aby upewnić się, że nie zawierają wirusów.

W niektórych narzędziach antywirusowych większość tych zadań można zautomatyzować, a konsola zarządzająca oprogramowaniem może ostrzegać administratora o znalezieniu nowych wirusów.

Upewnij się, że narzędzie antywirusowe jest zgodne z systemem Windows Server 2003. Najlepiej byłoby, gdyby program był certyfikowany dla tej platformy.

GS-11. Restart serwera

✔ **Harmonogram: co tydzień**

Od chwili pojawienia się Windows NT Microsoftu, zwłaszcza NT 4.0 w roku 1996, większość administratorów systemów doszła do wniosku, że dobrze jest regularnie restartować serwery korzystające z tego systemu operacyjnego, aby

oczyścić pamięć RAM i ogólnie odświeżyć system. Od tamtej pory Microsoft podjął poważne wysiłki, by ograniczyć, a nawet wyeliminować konieczność wykonywania tej procedury.

Przed wprowadzeniem tego zwyczaju w życie zdecydowanie radzimy zorientować się, jak Windows Server 2003 funkcjonuje w danej sieci. Okaże się, że serwery WS03 nie wymagają już regularnych restartów. W istocie Czytelników może zaskoczyć poziom dostępności, jaki można osiągnąć w tym systemie operacyjnym. Dowodem będą raporty czasu dostępności, generowane w procedurze **GS-07**.

Jeśli ktoś uzna, że regularne wykonywanie tej czynności jest niezbędne, to może posłużyć się poleceniem `shutdown`, pozwalającym zdalnie wyłączać i restartować serwery. Poniższe polecenie wykonuje restart zdalnego serwera:

```
shutdown -r -f -m \\nazwaserwera
```

gdzie `-r` żąda restartu, `-f` zmusza uruchomione aplikacje do zamknięcia, a `-m` wskazuje komputer przeznaczony do restartu. Podobnie jak w przypadku każdego polecenia tekstowego, możemy utworzyć plik poleceń zawierający polecenie dla każdego serwera, który chcemy zamknąć. W takim przypadku należy dodatkowo użyć parametru `-c`, aby dodać komunikat do polecenia:

```
shutdown -r -f -m \\nazwaserwera -c "Cotygodniowy restart serwera."
```

Procedura **GS-19** pozwoli przypisać plik poleceń do zaplanowanego zadania.

Polecenie `shutdown` automatycznie omija *Śledzenie zdarzeń zamknięcia systemu* — okno dialogowe, które musimy standardowo wypełnić przy wyłączaniu serwera Windows Server 2003. Wobec tego należy utrzymywać rejestr zdarzeń wyłączenia systemu, aby dokumentować zautomatyzowane restarty.

Śledzenie zdarzeń zamknięcia systemu to narzędzie, którego Windows Server 2003 używa do rejestrowania informacji o wyłączaniu i restartach serwera. Zapisuje ono swoje informacje w folderze *%SystemRoot\System32\LogFiles\Shutdown*. Działanie narzędzia można kontrolować przez dwa ustawienia GPO:

- *Konfiguracja komputera/Szablony administracyjne/System/Wyświetl śledzenie zdarzeń zamknięcia systemu*
- *Konfiguracja komputera/Szablony administracyjne/System/Uaktywnij funkcję Dane o stanie systemu Śledzenie zdarzeń zamknięcia systemu*

Do modyfikacji odpowiedniego GPO może posłużyć procedura **DC-16**. Ten obiekt GPO powinien stosować się do wszystkich serwerów.

Microsoft TechNet Script Center zawiera przykładowy skrypt do restartu komputera pod adresem *http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/comptmgmt/ScrCM38.asp?frame=true*.

GS-12. Przegląd i aktualizacja zasad zabezpieczeń

✔ **Harmonogram: co miesiąc**

Zasady zabezpieczeń są narzędziem, które stanowi podstawę programu bezpieczeństwa sieci. Decydują o wszystkim, między innymi o tym, jak reagować na naruszenia bezpieczeństwa i jak chronić się przed nimi. Identyfikują jednolite standardy bezpieczeństwa, które implementujemy w organizacji, i obejmujące procedury zarówno techniczne, jak i nietechniczne. Przykładem zasad technicznych mogą być parametry zabezpieczeń, definiowane podczas przygotowywania do eksploatacji każdego komputera w organizacji. Zasady nietechniczne to przyzwyczajenie użytkowników do wybierania i chronienia złożonych haseł. Oprócz tego musimy zidentyfikować parametry dla każdej zdefiniowanej zasady.

Przykładowa lista pozycji zawartych w zasadach zabezpieczeń dostępna jest na stronie WWW towarzyszącej książce: *www.Reso-Net.com/PocketAdmin*.

Comiesięczna weryfikacja zasad zabezpieczeń powinna obejmować przegląd wszystkich pozycji zawartych w tych zasadach i odpowiadać na pytania:

- Jak skuteczny jest program komunikacji z użytkownikami? Czy powinien być ulepszony?
- Jak skuteczne są strategie bezpieczeństwa? Czy powinny być wzmocnione?
- Czy administratorzy stosują się do wszystkich zasad bezpieczeństwa?
- Czy nie zostały zidentyfikowane jakieś potencjalne naruszenia bezpieczeństwa?
- Czy nowe technologie są bezpieczne? Jaki jest ich wpływ na globalną strategię bezpieczeństwa firmy?

Wszystkie zmiany dokonane podczas tego przeglądu powinny zostać udokumentowane i przekazane użytkownikom.

GS-13. Weryfikacja aktualizacji zabezpieczeń

✔ **Harmonogram: co miesiąc**

Aktualizacje zabezpieczeń są nieuniknionym elementem środowiska komputerowego każdej organizacji. Lecz jeśli nasze systemy operacyjne są prawidłowo zaprojektowane a w serwerach uruchomione są tylko usługi niezbędne do pełnienia ich ról, to najprawdopodobniej będziemy mogli ograniczyć weryfikacje dostępnych aktualizacji zabezpieczeń do przeglądów raz na miesiąc.

Windows i Microsoft udostępniają kilka narzędzi i technik służących do tego. Microsoft oferuje powiadamianie o biuletynach zabezpieczeń pocztą elektroniczną. Możemy dokonać subskrypcji tego i innych biuletynów Microsoftu w *register.microsoft.com/regsys/pic.asp*. Do tego niezbędny jest Microsoft Passport. Jeśli ktoś go nie ma, to może zdobyć go, postępując zgodnie z instrukcjami umieszczonymi na tej stronie. Kto nie chce korzystać z paszportu, może dokonać subskrypcji pod adresem *http://register.microsoft.com/subscription/subscribeme.asp?ID=135*. Jest jeszcze biuletyn poświęcony bezpieczeństwu i poprawkom, udostępniający przydatne informacje. Można go znaleźć pod adresem *http://www.microsoft.com/technet/security/current.asp*.

Microsoft nie jest jedyną organizacją, która rozsyła biuletyny poświęcone bezpieczeństwu. Doskonałym źródłem informacji tego typu jest SANS Institute. Biuletyny SANS można subskrybować pod adresem *www.sans.org/newsletters*. Kolejnym przydatnym źródłem podobnych informacji o różnych technologiach jest CERT Coordination Center (Cert/CC): *http://www.cert.org*.

Oprócz tego Windows Server 2003 obsługuje aktualizacje automatyczne. Oznacza to, że system może wstępnie pobrać poprawki i aktualizacje oraz powiadomić administratora, że są gotowe do zainstalowania. Funkcję tę można tak zmodyfikować, by wszystkie komputery w sieci przedsiębiorstwa pobierały dane aktualizacji z centralnego serwera intranetowego. Służą do tego ustawienia GPO, mieszczące się w *Konfiguracja komputera*/*Szablony administracyjne*/*Składniki systemu Windows*/*Windows Update* i obejmujące:

- **Konfigurowanie aktualizacji automatycznych** — w środowisku dużego przedsiębiorstwa powinniśmy wybrać ustawienie 4, co oznacza, że aktualizacje będą pobierane i instalowane zgodnie ze stałym harmonogramem co miesiąc.
- **Określ lokalizację intranetową usługi aktualizującej firmy Microsoft** — nazwa serwera, z którego aktualizacje będą pobierane; powinna to być pełna nazwa DNS.

- **Bez automatycznego uruchamiania ponownego dla zaplanowanych instalacji aktualizacji automatycznych** — to ustawienie powstrzymuje serwery przed restartem po instalacji aktualizacji. Serwery możemy uruchamiać ponownie zgodnie z bardziej regularnym harmonogramem, korzystając z procedury **GS-11**.

Do edycji odpowiedniego GPO może posłużyć procedura **DC-16**. Ten obiekt GPO powinien stosować się tylko do serwerów. Kolejny GPO należy skonfigurować podobnie dla stacji roboczych, lecz w miarę możliwości z użyciem innego intranetowego serwera źródłowego. Ustawienia te powinny być stosowane w połączeniu z Microsoft Software Update Services (SUS). Serwer SUS posłuży do sprawdzenia poprawności aktualizacji zabezpieczeń niezbędnych w naszym środowisku sieciowym. Wszystkie zmiany powinny być udokumentowane.

Aby pobrać i zainstalować SUS, poszukaj Microsoft Software Update Services pod adresem *www.microsoft.com/downloads*.

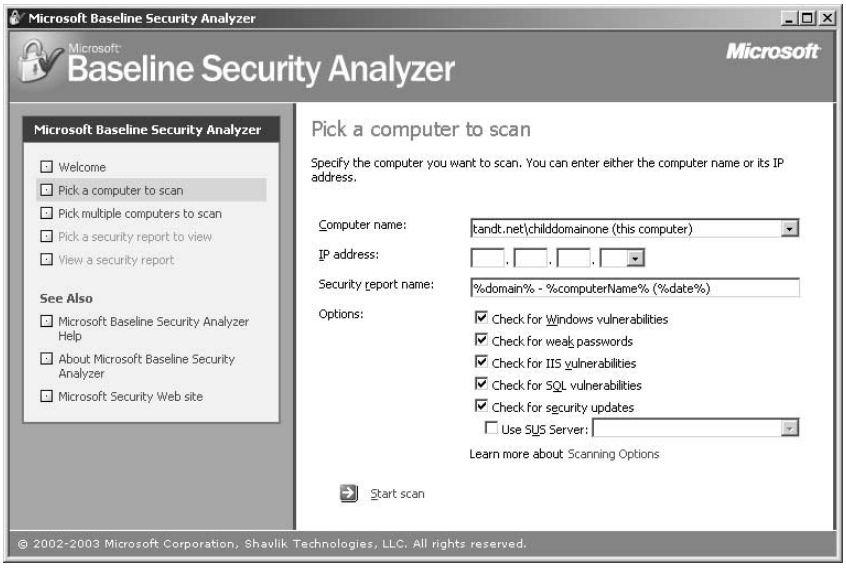
Do analizy stanu poprawek i pakietów Service Pack w naszych systemach może też posłużyć Microsoft Baseline Security Analyzer (MBSA). MBSA jest dostępny w serwisie Microsoft Download: szukaj „MBSA" pod adresem *www.microsoft.com/ downloads*.

Do skanowania systemów Windows Server 2003 potrzebna jest wersja MBSA 1.1.1 lub nowsza.

Ponieważ plik instalacyjny MBSA jest plikiem Instalatora Windows, program można zainstalować interaktywnie lub za pomocą procedury **DC-15** w kilku systemach docelowych. MBSA może posłużyć do skanowania pojedynczego systemu lub całej sieci. Potrafi nawet skanować segmenty sieci na podstawie zakresów adresów IP.

Aby sprawdzić system:

1. Uruchom MBSA (menu *Start*/*Wszystkie programy*/*Microsoft Baseline Security Analyzer*).
2. Wybierz *Scan a computer*.
3. Wpisz nazwę komputera lub adres IP i wybierz opcje skanowania. Kliknij *Start scan* (rysunek 1.3).
4. Po zakończeniu skanowania przejrzyj raport w panelu szczegółów MBSA. Raport jest automatycznie zapisywany wraz z nazwą domeny, nazwą komputera i datą w folderze *\%UserProfile%\Security Scans* bezpośrednio w folderze *Documents and Settings*.



Rysunek 1.3. *Microsoft Baseline Security Analyzer*

Otrzymane raporty zawierają istotne informacje o bezpieczeństwie systemów, więc należy je przechowywać z zachowaniem zasad bezpieczeństwa.

GS-14. Aktualizacja poprawek i pakietów Service Pack

✔ Harmonogram: co miesiąc

Po zaaprobowaniu przez serwer SUS aktualizacje będą automatycznie instalowane we wszystkich wyznaczonych systemach, jeśli odpowiednio skonfigurujemy GPO (patrz procedura **GS-13**). Najlepszym sposobem na użytkowanie SUS jest podział na dwa środowiska: produkcyjne i testowe (laboratorium). Z laboratoryjnym serwerem testowym powinno być połączonych kilka komputerów (PC i serwerów).

Serwer Software Update Services weryfikuje i instaluje jedynie aktualizacje krytyczne i związane z bezpieczeństwem. Aby instalowane były również aktualizacje sterowników i inne, musimy skorzystać z serwisu WWW Windows Update: *http://v4.windowsupdate.microsoft.com/pl/default.asp*.

Do akceptowania aktualizacji powinno posłużyć laboratorium testowe:

1. Uruchom konsolę SUS w serwerze testowym przez przejście do *http://nazwaserwera/SUSAdmin*, gdzie *nazwaserwera* jest adresem DNS serwera testowego.
2. Kliknij *Approve Updates*, aby przejrzeć dostępne aktualizacje. Posortuj aktualizacje według stanu (*Status*). Zaznacz te, które dotyczą posiadanego środowiska.
3. Kliknij przycisk *Approve*, aby wprowadzić wszystkie zaznaczone aktualizacje. Zaczekaj na wprowadzenie ich w komputerach testowych i uruchom komputery ponownie, jeśli to będzie konieczne.
4. Sprawdź, czy systemy testowe działają poprawnie po wprowadzeniu zmian. Jeśli wystąpi problem, usuwaj aktualizacje jedną po drugiej, aby znaleźć tę sprawiającą problemy, dopóki problem nie zostanie rozwiązany. Zastosuj ponownie pozostałe aktualizacje. Zanotuj zaakceptowane poprawki.
5. Przejdź do produkcyjnego serwera SYS i zaaprobuj aktualizacje do rozprowadzenia w systemach produkcyjnych.

Poprawki i aktualizacje są za pomocą SUS instalowane automatycznie, lecz nie dotyczy to pakietów serwisowych (Service Pack). Wymagają one zwykle bardziej dokładnego przygotowania do instalacji. Przygotowanie obejmuje znacznie bardziej szczegółowe testy niż dla poprawek, ponieważ pakiety serwisowe wpływają na wiele elementów serwera. Po sprawdzeniu i zaaprobowaniu pakietu serwisowego można go wdrożyć za pomocą procedury **DC-15** (chyba że w środowisku dostępne jest bardziej solidne narzędzie instalacyjne, na przykład SMS).

Microsoft TechNet Script Center zawiera kilka skryptów związanych z zarządzaniem poprawkami i pakietami serwisowymi (Enumerate Installed Hot Fixes i Identify the Latest Installed Service Pack): *http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/compmgmt/default.asp?frame=true*.

GS-15. Ocena nowego oprogramowania

✔ **Harmonogram: co miesiąc**

Raz na miesiąc musimy znaleźć czas na przegląd nowego oprogramowania administracyjnego. Celem tego zadania jest sprawdzenie, czy możemy zmniejszyć nakłady pracy związane z administrowaniem, wprowadzając nowy produkt. Dobrym przykładem wysoce produktywnego narzędzia eksploatacyjnego jest

Microsoft Operations Management Server (MOM). MOM jest bardzo efektywny, ponieważ monitoruje zdarzenia systemowe w serwerach, automatycznie poprawia zachowania, które mogą być potencjalnie szkodliwe i powiadamia administratora o zmianach.

Jeśli środowisko komputerowe naszej firmy nie jest na tyle duże, by uzasadniało użycie tak wyrafinowanego narzędzia jak MOM, możemy poszukać innego narzędzia o podobnych możliwościach. Wiele powtarzających się zadań administracyjnych można wykonać z pomocą skryptów, jak pokazaliśmy już w szeregu przykładów. Do tego mogą także posłużyć niedrogie lub darmowe narzędzia. Dwoma cennymi źródłami informacji o takich narzędziach są strony *www.MyITForum.com* i *www.TechRepublic.com*.

Warto uważać, aby nie stosować narzędzi różniących się poważnie od siebie sposobem użycia. Dzięki temu ograniczymy liczbę narzędzi lub interfejsów, których administratorzy naszej sieci będą musieli się uczyć. Wszelkie nowe narzędzia w sieci powinny zostać udokumentowane.

Do monitorowania określonych zdarzeń w Dzienniku zdarzeń i generowania alarmów w razie ich wystąpienia może też posłużyć skrypt dostępny w Microsoft TechNet Script Center: *http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/monitor/ScrMon21.asp?frame=true*.

GS-16. Inwentaryzacja

✔ **Harmonogram: co miesiąc**

Jednym z zadań, które należy wykonać przynajmniej raz na miesiąc jest zarządzanie inwentarzem. Dotyczy to zarówno sprzętu, jak i oprogramowania. W sieci może być obecne narzędzie do inwentaryzacji, np. Systems Management Server, lub nie. Jeśli jest, to doskonale — problem z głowy. Jeśli nie, potrzebne będą inne narzędzia.

Microsoft oferuje narzędzie Microsoft Software Inventory Analyser (MSIA). Nie inwentaryzuje ono całości oprogramowania, lecz przynajmniej zarządza wszystkimi programami Microsoftu. Aby pobrać MSIA, wystarczy wyszukać narzędzie w *www.microsoft.com/downloads*.

MSIA jest narzędziem opartym na kreatorach, pozwalającym wykonywać trzy zadania:

- Skanować komputer lokalny w poszukiwaniu produktów Microsoftu.

- Przygotować plik wejściowy dla wiersza poleceń, zawierający wszystkie ustawienia skanowania, których chcemy użyć.
- Przeprowadzić skanowanie z użyciem przygotowanego uprzednio pliku wejściowego wiersza poleceń.

Oprócz tego MSIA pozwala skanować systemy lokalne, zdalne lub całą sieć naraz. Instalacja opiera się na usłudze Instalatora Windows. Narzędzie można instalować interaktywnie lub, za pomocą procedury **DC-15**, w wybranych komputerach docelowych.

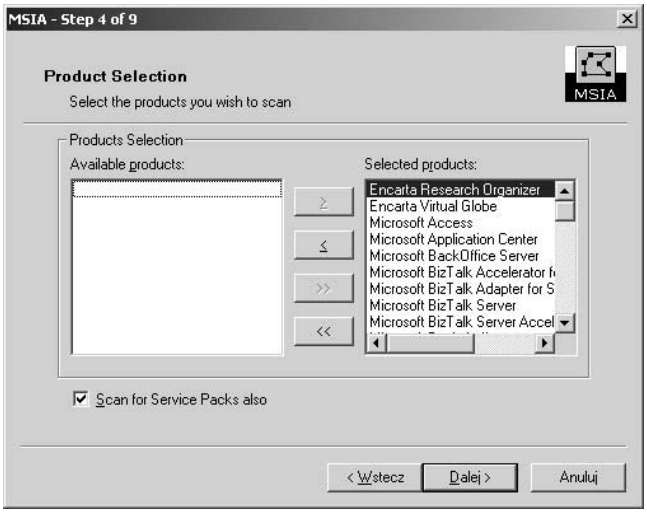
Aby utworzyć plik wejściowy wiersza poleceń:

1. Uruchom MSIA (menu *Start*/*Wszystkie programy*/*Microsoft Software Inventory Analyzer*). Kliknij *Next*.
2. Wybierz *Scan using Custom settings* i *Create Custom settings*. Kliknij *Browse*, aby wybrać folder docelowy i nazwę pliku wyjściowego. Plik wejściowy dla wiersza poleceń otrzyma rozszerzenie *.cli*. Kliknij *Save*, aby utworzyć plik. Kliknij *Next*.
3. Wybierz zakres skanowania: *Local Computer* (komputer lokalny), *Network* (sieć) lub *Report Consolidation* (konsolidacja raportu). Kliknij *Next*.

Wybierając opcję *Network*, musimy podać odpowiednie poświadczenia, aby przeprowadzić skanowanie wszystkich systemów.

4. W oknie dialogowym *Download Database Files* kliknij *Download*. MSIA przejdzie do strony WWW Microsoftu i pobierze najświeższe dane o produktach firmy. Pojawi się zapytanie o akceptację certyfikatu Microsoftu w celu instalacji bazy danych. Kliknij *Yes*. Po zakończeniu pobierania kliknij *OK*, a następnie *Next*.
5. Wybierz produkty, których chcesz szukać i kliknij *Add* (większą liczbę produktów możesz zaznaczyć, przytrzymując klawisz *Ctrl*). Zaznacz *Save these products as the default* (zapisz te produkty jako domyślne) i kliknij *Next*.
6. Wybierz format (formaty) raportu. Kliknij *Browse*, aby wybrać folder dla raportu i nazwę pliku. Kliknij *Save*, aby zapisać plik. Kliknij *Next*.
7. Możesz wybrać opcję konsolidacji raportów zbiorczych, przydatnych w zarządzaniu. Kliknij *Next*.

Rysunek 1.4. *Microsoft Software Inventory Analyser*



8. Możesz wybrać opcję wysłania raportu zbiorczego do kogoś pocztą elektroniczną (lub wysłać go później). Jeśli raport ma być wysłany do grupy, utwórz grupę dystrybucyjną i wpisz tu jej adres e-mail. Nie zaznaczaj opcji *Save settings as default*, ponieważ tworzysz plik wejściowy wiersza poleceń.
9. Kliknij *Finish*, aby zamknąć plik wejściowy.

Aby uruchomić skanowanie MSIA:

1. Uruchom MSIA (menu *Start*/*Wszystkie programy*/*Microsoft Software Inventory Analyzer*). Kliknij *Next*.
2. Wybierz *Scan using Custom settings* i *Load existing Custom settings*. Jeśli wyświetlony plik nie jest tym, którego chcesz użyć, kliknij *Browse*, aby wybrać odpowiedni folder i plik. Kliknij *Open*, aby załadować plik. Kliknij *Next*.
3. MSIA przeprowadzi skanowanie systemów na podstawie ustawień pliku.
4. Zaznacz *View Reports Now* (wyświetl raporty) i kliknij *Finish*.

Jest to doskonałe narzędzie do inwentaryzowania oprogramowania Microsoftu.

Microsoft TechNet Script Center zawiera dwa przydatne skrypty do zarządzania inwentarzem: Enumerate Installed Software (*http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/compmgmt/scrcm16.asp?frame=true*) i Inventory Computer Hardware (*http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/compmgmt/ScrCM30.asp?frame=true*).

GS-17. Tworzenie globalnej konsoli MMC

✔ **Harmonogram: w miarę potrzeb**

W systemie Windows Server 2003 do administracji i zarządzania służą konsole MMC (ang. *Microsoft Management Console*). Najbardziej przydatną z nich jest konsola Zarządzanie komputerem, znajdująca się w folderze *Narzędzia administracyjne*. Można też kliknąć prawym przyciskiem myszy ikonę *Mój komputer* i wybrać *Zarządzaj* z menu kontekstowego.

Lecz chociaż jest to dobra uniwersalna konsola, nie można jej używać do wszystkiego. Wobec tego jednym z doraźnych działań administracyjnych, które warto wykonać jest zbudowanie globalnej konsoli zarządzającej, łączącej wszystkie potrzebne przystawki (ang. *snap-in*) w jedną konsolę MMC. Oprócz wszystkich funkcji narzędzia Zarządzanie komputerem, ta konsola powinna zawierać przystawki:

- .NET Framework 1.1 Configuration.
- Dzienniki wydajności i alerty.
- Group Policy Management (wymaga instalacji GPMC — patrz rozdział 4.).
- Konfiguracja i analiza zabezpieczeń.
- Menedżer autoryzacji.
- Monitor sieci bezprzewodowej.
- Pulpity zdalne.
- Rozproszony system plików (DFS).
- Szablony zabezpieczeń.
- Trzy dostępne przystawki do zarządzania Active Directory.
- Urząd certyfikacji (trzeba wskazać serwer do zarządzania).
- Usługi składowe
- Wynikowy zestaw zasad.

Aby utworzyć tę konsolę:

1. Użyj *Start*/*Uruchom*, aby wydać polecenie:

   ```
   mmc /a %SystemRoot%\system32\compmgmt.msc
   ```

2. Spowoduje to uruchomienie konsoli Zarządzanie komputerem w trybie edycji. Zacznij od *Plik*/*Zapisz jako*, aby zapisać konsolę pod nazwą *globalnaMMC.msc* w folderze *C:\Toolkit*.

3. Użyj *Plik*/*Dodaj*/*Usuń przystawkę*, aby otworzyć okno dialogowe. Upewnij się, że w polu wyboru *Przystawki dodane do* jest wybrana przystawka *Zarządzanie komputerem* i kliknij *Dodaj*.
4. Kliknij dwukrotnie każdą z przystawek wymienionych powyżej. Po dodaniu wszystkich kliknij *Zamknij*.
5. Kliknij *OK*, aby wrócić do konsoli.
6. Kliknij *Plik*/*Opcje*, nazwij konsolę `Globalna konsola MMC`, upewnij się, że jest w trybie *Tryb użytkownika — pełny dostęp* i usuń zaznaczenie przy *Nie zapisuj zmian w tej konsoli*. Kliknij *OK*.
7. Wybierz *Plik*/*Zapisz*, aby zapisać zmiany.

Jak zobaczymy, konsola ta ma kilka zastosowań, lecz zasadniczo będzie naszym najczęściej używanym narzędziem do zarządzania siecią serwerów.

Utwórz skrót do tej konsoli, używając procedury **GS-01**, i zapisz go w pasku Szybkie uruchamianie.

Ten szablon musi być dobrze chroniony, ponieważ ma naprawdę duże możliwości.

GS-18. Automatyczne pobieranie sygnatur dla oprogramowania antywirusowego

✔ **Harmonogram: w miarę potrzeb**

To jest kolejna czynność typu ogólnego, niezbędna w każdej strategii antywirusowej. Jest związana z konfiguracją agenta aktualizacji sygnatur wirusów, który pobiera aktualizacje sygnatur i rozprowadza je do wszystkich PC i serwerów w sieci.

Jest to jednorazowa czynność, której nie możemy pominąć na liście zadań administracyjnych związanych z serwerem.

Powinna być wspierana przez regularne wyrywkowe kontrole w różnych systemach, które pozwolą upewnić się, że serwer aktualizujący sygnatury dla oprogramowania antywirusowego działa poprawnie.

GS-19. Tworzenie i weryfikacja zaplanowanych zadań

✔ **Harmonogram: w miarę potrzeb**

Harmonogram zadań jest jednym z narzędzi, bez których administratorzy nie mogą się obyć, ponieważ pozwala automatyzować powtarzające się zadania w sieci. W systemie Windows Server 2003 mieści się w *Panelu sterowania* w *Eksploratorze Windows*. Można go również znaleźć jako pierwszy udostępniony element każdego serwera w oknie *Moje miejsca sieciowe*.

Dodanie zadania do harmonogramu wymaga posłużenia się Kreatorem zaplanowanych zadań:

1. Kliknij dwukrotnie *Dodaj zaplanowane zadanie* (*Eksplorator Windows*/*Mój komputer*/*Panel sterowania*/*Zaplanowane zadania*). Kliknij *Dalej*.
2. Wybierz zadanie z listy lub kliknij *Przeglądaj*, aby znaleźć je na dysku. Zadaniem może być aplikacja, skrypt lub plik poleceń. Kliknij *Dalej*.
3. Nazwij zadanie i określ jego częstotliwość. Kliknij *Dalej*.
4. Wybierz godzinę i datę rozpoczęcia. Kliknij *Dalej*.
5. Wpisz nazwę odpowiedniego użytkownika i hasło. Kliknij *Dalej*.
6. Zaznacz *Otwórz okno Zaawansowane właściwości dla tego zadania, kiedy kliknę przycisk Zakończ*. Kliknij *Zakończ*.
7. W arkuszu właściwości zadania dokładniej określ harmonogram zadania. Zakładka *Harmonogram* pozwala w razie potrzeby zastosować wiele harmonogramów dla zadania. Zakładka *Ustawienia* pozwoli sprawdzić, czy zadanie jest skonfigurowane zgodnie ze standardami firmy. Kliknij *OK*.

Do weryfikacji stanu zaplanowanych zadań w każdym serwerze może posłużyć polecenie `schtasks`, o następującej składni:

```
schtasks /query /s nazwakomputera
```

gdzie *nazwakomputera* oznacza nazwę DNS lub adres IP serwera. Aby dowiedzieć się więcej o poleceniu, wpisz `schtasks /?`. Tak jak poprzednio, metoda opisana na końcu procedury **GS-07** pozwala wygenerować automatycznie raport dla wszystkich serwerów.

Microsoft TechNet Script Center zawiera cztery różne skrypty do zarządzania zaplanowanymi zadaniami: *http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/schedule/default.asp?frame=true*.

GS-20. Tworzenie i modyfikacja szablonów zabezpieczeń

✔ **Harmonogram: w miarę potrzeb**

Szablony zabezpieczeń służą do definiowania właściwości zabezpieczeń dla serwerów. Ponieważ przypisywane są jako zasady lokalne, powinny zawierać tylko podstawowe ustawienia zabezpieczeń, na przykład zabezpieczenia plików, Rejestru i usług. Możemy tworzyć własne szablony z istniejących. Microsoft udostępnia szereg przyzwoitych szablonów w Windows Server 2003 Security Guide (którego można poszukać w *www.microsoft.com/downloads*), przydatnych na początek.

Szablony zabezpieczeń i konfiguracja zabezpieczeń wraz z GPO to jedne z podstawowych środków zapewnienia bezpieczeństwa serwerów.

Aby utworzyć własne szablony zabezpieczeń:

1. Uruchom globalną konsolę MMC utworzoną w procedurze **GS-17**. Przejdź do *Szablonów administracyjnych*. Szablony mieszczą się w katalogu *%SystemRoot\security\templates*.
2. Aby utworzyć nowy szablon z istniejącego, kliknij go prawym przyciskiem myszy, wybierz *Zapisz jako* i nadaj nową nazwę. Po zmianie nawy będzie można dodawać własne ustawienia.
3. Przejdź do nowego szablonu i zmodyfikuj jego ustawienia. Zacznij od kliknięcia prawym przyciskiem myszy nazwy szablonu i wybrania *Ustaw opis*, aby zmodyfikować opis. Wpisz odpowiednie informacje i kliknij *OK*.
4. Rozwiń szablon, aby wyświetlić jego składniki i zmodyfikuj je zgodnie z potrzebami. Pamiętaj, by kliknąć nazwę szablonu prawym przyciskiem myszy i wybrać *Zapisz przed wyjściem z konsoli*.

Szablony mają szereg różnych zastosowań. Mogą służyć do przypisywania ustawień zabezpieczeń do serwerów lub do analizowania faktycznych ustawień w porównaniu z zapisanymi w szablonie. Jedno i drugie możemy wykonać w trybie graficznym lub tekstowym. Aby przeanalizować serwer lub przywrócić oryginalne ustawienia dla serwera w trybie graficznym:

1. Uruchom globalną konsolę MMC utworzoną w procedurze **GS-17**.
2. Kliknij prawym przyciskiem myszy *Konfiguracja i analiza zabezpieczeń* i wybierz *Otwieranie bazy danych*.

3. W oknie *Otwieranie bazy danych* znajdź odpowiednią bazę danych lub wpisz nazwę nowej i kliknij *OK*. Domyślną ścieżką jest *Moje dokumenty\Security\Database*.
4. Wybierz odpowiedni szablon z listy dostępnych i kliknij *OK*.
5. Aby przeanalizować system, kliknij prawym przyciskiem myszy *Konfiguracja i analiza zabezpieczeń* i wybierz *Analizuj komputer teraz*.
6. Ponieważ każda analiza lub operacja konfiguracji wymaga pliku dziennika, pojawi się okno dialogowe z zapytaniem o położenie tego pliku. Domyślna ścieżka to *Moje dokumenty\Security\Logs*, a domyślna nazwa pliku jest taka sama jak dla bazy danych. Wpisz nazwę nowego pliku dziennika, użyj przycisku *Przeglądaj*, aby zlokalizować istniejący plik albo kliknij *OK*, aby zaakceptować nazwę domyślną. Analiza się rozpocznie.
7. Po zakończeniu analizy widoczne staną się różnice pomiędzy szablonem a komputerem. Przejdź do ustawienia, które chcesz obejrzeć i zaznacz je. Ewentualne różnice zostaną wyświetlone w prawym panelu.
8. Ustawienia w bazie danych możemy modyfikować tak, by były zgodne z wartościami, które chcemy zastosować, przez przejście do odpowiedniej wartości i dwukrotne jej kliknięcie. Zaznacz *Definiuj w bazie danych następujące zasady*, zmodyfikuj ustawienie i kliknij *OK*. Powtórz czynność dla każdego ustawienia, które chcesz zmienić.
9. Używając prawego przycisku myszy, wyświetl menu podręczne konsoli *Konfiguracja i analiza zabezpieczeń* i wybierz *Zapisz*, aby zapisać zmiany wprowadzone w bazie danych.
10. Aby skonfigurować komputer zgodnie z ustawieniami w bazie danych, wybierz *Konfiguruj komputer teraz* z tego samego menu podręcznego. Ponownie trzeba tu podać położenie i nazwę pliku dziennika, aby konfiguracja mogła się rozpocząć.

Te same zadania można wykonać z wiersza poleceń za pomocą polecenia `secedit`. Aby skonfigurować system, wpisz polecenie:

```
secedit /configure /db nazwapliku.db /log /nazwapliku.log /areas REGKEYS
FILESTORE SERVICES /quiet
```

Poniższe polecenie analizuje system:

```
secedit /analyze /db nazwapliku.db /log /nazwapliku.log /quiet
```

Drugie polecenie możesz umieścić w zaplanowanym zadaniu, korzystając z procedury **GS-19**. Aby otrzymać więcej informacji, wpisz `secedit /?`.

GS-21. Zarządzanie plikami pomocy technicznej

✔ **Harmonogram: w miarę potrzeb**

Kolejną czynnością wykonywaną doraźnie jest instalacja plików pomocy serwera we własnym systemie. Zainstalowanie plików pomocy serwera w komputerze lokalnym może być bardzo przydatne, ponieważ daje łatwy dostęp do skarbnicy informacji o serwerze. Posłuży do tego Centrum pomocy i obsługi technicznej Windows XP/Server 2003 i będzie wymagało płyty instalacyjnej Windows Server 2003:

1. Uruchom Centrum pomocy i obsługi technicznej w swoim komputerze i kliknij przycisk *Opcje* na górze okna.
2. Kliknij *Zainstaluj i udostępnij Pomoc systemu Windows* w lewym panelu okna. Kliknij *Zainstaluj zawartość Pomocy dysku CD lub z obrazu dysku*.
3. Wpisz literę napędu CD i kliknij *Znajdź*.
4. Zaznacz pliki pomocy, które chcesz zainstalować i kliknij *Zainstaluj*.
5. Po zainstalowaniu będzie można kliknąć *Przełącz z jednej do drugiej zawartości Pomocy systemu operacyjnego*, wybrać pożądany system operacyjny i kliknąć *Przełącz*.

Teraz w komputerze lokalnym będzie możliwe przeglądanie plików pomocy systemu Windows Server 2003. Można zainstalować pomoc dla każdej wersji i przełączać pomiędzy nimi za pomocą opcji Centrum pomocy i obsługi technicznej.

GS-22. Przygotowanie serwera

✔ **Harmonogram: w miarę potrzeb**

O częstotliwości wykonywania tego zadania decydują skala obsługiwanej sieci komputerowej i liczba znajdujących się w niej serwerów. Niektóre centra komputerowe przygotowują serwery do eksploatacji co tydzień, choćby po to, by odbudować starzejące się serwery i przeprojektować strukturę usług.

Przygotowanie serwera obejmuje szereg różnych czynności. Oprócz tego Windows Server 2003 udostępnia różne metody przygotowywania serwera do eksploatacji:

- **Ręczna lub interaktywna** — ta metoda powinna być oparta przynajmniej na szczegółowej liście kontrolnej.

- **Nienadzorowana z użyciem pliku odpowiedzi** — ta metoda opiera się na drobiazgowym i kompletnym pliku odpowiedzi.
- **Obraz dysku z użyciem SysPrep** — ta metoda wymaga użycia narzędzi do tworzenia obrazu dysku, dostarczanych przez innych producentów.
- **Usługi instalacji zdalnej** (ang. *RIS — Remote Installation Services*) — ta metoda tworzy serwer z modelu zarejestrowanego i zapisanego w serwerze RIS.
- **Automated Deployment Services** — ta metoda łączy RIS i obrazy dysków, zapewniając najszybszy i najdokładniejszy proces konstruowania serwera.

Jeśli to tylko możliwe, powinniśmy korzystać z ADS — ta metoda jest szybka, może posłużyć zarówno do tworzenia, jak i do odtwarzania systemów, i jest łatwa do wdrożenia.

Informacje o różnych metodach instalacji i przygotowaniu serwerów wzorcowych oraz zarządzaniu nimi dostępne są w rozdziale 2. *Windows Server 2003: Best Practices for Enterprise Management* (Ruest & Ruest, McGraw-Hill/Osborne, 2003).

Jeśli trzeba jednocześnie przygotować bardzo dużą liczbę serwerów, to może w tym pomóc skrypt z Microsoft TechNet Script Center, automatycznie przygotowujący konta komputerów wymagane dla każdego serwera (*http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/compmgmt/ScrCM81.asp?frame=true*).

Warto przeprowadzić procedurę **HW-04** po zainstalowaniu każdego nowego serwera. Pozwoli to zidentyfikować ewentualne urządzenia stwarzające problemy.

GS-23. Konfiguracja narzędzi administracyjnych

✔ Harmonogram: w miarę potrzeb

Do zarządzania środowiskiem Windows Server 2003 potrzebnych jest kilka narzędzi. Należą do nich różne zestawy, począwszy od podstawowego zestawu Pakiet narzędzi administracyjnych aż po Windows Server 2003 Support Tools,

w tym narzędzia Windows Server 2003 Resource Kit. Pakiet narzędzi administracyjnych i Support Tools dostępne są na płycie instalacyjnej Windows Server (pierwszy w folderze *\i386*, a drugi w *\Support\Tools*). Wszystkie trzy zestawy można pobrać z witryny WWW Microsoft Download, wystarczy wyszukać nazwę zestawu w *www.microsoft.com/downloads*.

Instalacja każdego z pakietów opiera się na usłudze Instalator Windows. Po pobraniu można je zainstalować interaktywnie lub wykorzystać procedurę **DC-15** do zainstalowania w wyznaczonych komputerach. Wszystkie zestawy narzędzi radzimy zainstalować we wszystkich serwerach i w każdym komputerze służącym do administrowania.

Kilka narzędzi z zestawu Resource Kit daje użytkownikowi wysoki poziom uprzywilejowania. Wszystkie narzędzia powinny być odpowiednio zabezpieczone jako skróty Uruchom jako (patrz procedura **GS-01**).

GS-24. Aktualizacja domyślnego profilu użytkowników

✔ **Harmonogram: w miarę potrzeb**

Nie ma nic lepszego niż zalogowanie do systemu, w którym wszystko, co potrzebne do szybkiego i łatwego zarządzania i administracji jest pod ręką. Jednym z najlepszych sposobów na to jest dostosowanie środowiska do własnych potrzeb i skopiowanie go do profilu domyślnego użytkownika (ang. *Default User*). W ten sposób każdy nowy administrator logujący się do serwera będzie miał pod ręką te same narzędzia służące do zarządzania systemem.

Dostosowanie środowiska powinno objąć:

- Umieszczenie w pasku szybkiego uruchamiania wszystkich skrótów, których używamy najczęściej. Powinny się do nich zaliczać skróty Uruchom jako utworzone w procedurze **GS-01**.
- Konfigurację ustawień Eksploratora Windows (wyświetlanie wszystkich plików, włączenie pasku stanu, szczegółowy widok elementów).
- Zainstalowanie narzędzi administracyjnych, Support Tools i Resource Kit (patrz procedura **GS-23**).
- Na potrzeby bezpieczeństwa możemy nawet utworzyć fałszywe konto „Administrator", mające jedynie przywileje użytkownika Gość.
- Środowisko powinno zdecydowanie zawierać własne ustawienia pulpitu.

Po wybraniu ustawień możemy zaktualizować profil Default User tak, że zawsze będzie generować te same ustawienia przy tworzeniu profilu nowego użytkownika.

Kontrola bezpieczeństwa

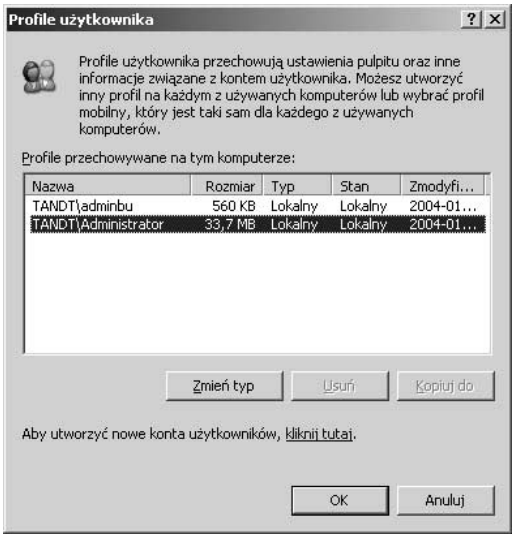
Dostosowanie ustawień pulpitu i innych wymaga uprawnień lokalnego administratora.

Do przeprowadzenia tych działań potrzebne będzie drugie konto administratora (patrz procedura **GS-05**). Windows Server 2003 nie pozwala kopiować otwartego profilu użytkownika do innego, ponieważ wiele otwartych opcji jest nietrwałych. Aby zaktualizować domyślnego użytkownika, trzeba założyć drugie konto administracyjne.

Aby zaktualizować profil Default User:

1. Wyloguj się z konta Administrator (*Start*/*Wyloguj*).
2. Zaloguj się do drugiego konta administracyjnego. Windows Server utworzy nowy profil oparty na starych ustawieniach.
3. Otwórz Eksploratora Windows (menu *Start*/*Wszystkie programy*/*Akcesoria*/*Eksplorator Windows*) i wybierz w opcjach folderów wyświetlanie ukrytych plików (*Narzędzia*/*Opcje folderów*/zakładka *Widok*). Kliknij *OK*.
4. Przejdź do lewego panelu i kliknij prawym przyciskiem myszy *Mój komputer*.
5. Wybierz *Właściwości*/*Zaawansowane*/*Profile użytkownika* (rysunek 1.5).
6. Wybierz profil *Administrator* i kliknij *Kopiuj do*.
7. Przejdź do folderu *Documents and Settings\Default User*. Kliknij *OK*.
8. Kliknij *OK*, aby zastąpić istniejące pliki.
9. Zamknij wszystkie okna dialogowe i **wyloguj się** z drugiego konta administracyjnego.
10. **Zaloguj się** jako Administrator.
11. Uruchom Eksploratora i wróć do okna dialogowego *Profile użytkownika*.
12. **Usuń** profil drugiego konta administracyjnego (jego zadaniem była tylko aktualizacja profilu Default User).
13. Zamknij wszystkie okna dialogowe i **wyloguj się** z konta Administrator.

Rysunek 1.5. *Zarządzanie profilami użytkowników*



14. Zaloguj się do drugiego konta administracyjnego, aby przetestować profil Default User. Powinna to być kopia dostosowanego profilu Administrator.
15. Wróć do profilu administratora.

Z tą operacją należy uważać w serwerach usług terminalowych, ponieważ w nich Default User służy do tworzenia profilu użytkownika, a nie administratora. Oczywiście profile użytkowników wymagają innych ustawień niż administracyjne.

GS-25. Przegląd środowiska sprzętowego

✔ Harmonogram: w miarę potrzeb

Od czasu do czasu należy też poświęcić trochę czasu na przegląd całego środowiska technicznego i sprawdzenie, czy wymaga zmian. Zadanie to zwykle podejmowane jest dwa razy w roku lub podczas przeglądu budżetu. Zgromadzone do tego czasu dzienniki działań i raporty z rozwiązywania problemów pozwolą zidentyfikować obszary sieci, w których przydałyby się ulepszenia i świadczone przez nie usługi. Możemy też znaleźć miejsce na sugestie użytkowników. Najlepszym sposobem na to będzie stworzenie aliasu pocztowego „sugestie” i poinformowanie użytkowników o jego istnieniu.

Każda proponowana zmiana powinna być udokumentowana, aby można było otrzymać finanse i zgodę na zmianę. Każda faktycznie zaimplementowana zmiana również powinna zostać dokładnie opisana.

GS-26. Dokumentacja systemu i sieci

✔ **Harmonogram: w miarę potrzeb**

Trochę czasu trzeba przeznaczyć od czasu do czasu na przegląd dokumentacji systemu i sieci. Czy dokumentacja jest aktualna? Czy precyzyjnie opisuje istniejące środowisko? Nie jest to zadanie zbyt popularne wśród nas, administratorów systemów, lecz niestety jest niezbędne. Do pracy z dokumentacją możemy wykorzystać odpowiednie narzędzia, na przykład Microsoft Office lub Visio.

Oprócz nich Microsoft udostępnia szereg narzędzi, które automatycznie dokumentują niektóre aspekty sieci. Są to Customer Configuration Capture Tools z Microsoft Product Support, które możemy znaleźć na stronie *www.microsoft.com/downloads*. Dostępnych jest pięć narzędzi do dokumentowania Alliance (specjalny program wspomagający), usług katalogowych, sieci, klastrów, SUS i podstawowej konfiguracji (w tym usług plików i drukowania oraz wydajności).

Dokumentacja powinna być regularnie aktualizowana.

GS-27. Zarządzanie umowami o świadczeniu usług

✔ **Harmonogram: w miarę potrzeb**

Kolejną czynnością wykonywaną doraźnie jest przegląd umów o świadczeniu usług (ang. *SLA — Service level agreement*). Należy przeprowadzać go przynajmniej dwa razy w roku. SLA są umowami o dostarczaniu usług, które podpisujemy ze społecznością użytkowników. Usługi powinny być podzielone na kategorie według priorytetów, a dla każdego priorytetu powinien zostać zdefiniowany czas przywracania usługi. Na przykład, usługa niekrytyczna może być przywrócona w ciągu czterech godzin lub szybciej, zaś usługę krytyczną należy przywrócić w ciągu godziny.

Raporty z rozwiązywania problemów będą przy tym przeglądzie bardzo przydatne. Uwagi użytkowników również są tu cenne, ponieważ potrzeby mogą ulegać zmianom, gdy użytkownicy lepiej poznają możliwości systemów.

GS-28. Zarządzanie priorytetami w rozwiązywaniu problemów

✔ **Harmonogram: w miarę potrzeb**

Podobnie jak procedura **GS-27**, priorytety rozwiązywania problemów powinny być przeglądane dwa razy do roku. Ten przegląd pozwala określić, jakie priorytety powinniśmy nadać naszym działaniom, gdy wystąpi jednocześnie kilka różnych problemów. Zależy to od dotychczasowego doświadczenia z działaniem sieci i rozwiązywaniem problemów. Priorytety są mocno zależne od umów SLA z użytkownikami.

Opracowane podejście powinno opierać się na zasadzie maksymalnych korzyści kosztem minimalnych nakładów pracy. Na przykład, jeśli ulegną awarii jednocześnie kontroler domeny (DC) i dysk w macierzy RAID 5 serwera plików, to lepiej najpierw wymienić dysk, a następnie zacząć odbudowywać DC. W ten sposób czas zostanie wykorzystany najskuteczniej. Przydzielając priorytety należy kierować się zdrowym rozsądkiem.

GS-29. Przegląd nakładów pracy

✔ **Harmonogram: w miarę potrzeb**

Ostatni przegląd, który musimy wykonywać co pół roku, dotyczy nakładów pracy. Niniejsza książka pomaga uporządkować pracę Czytelnika-administratora z podziałem na dni i tygodnie. Pomaga też zautomatyzować ogromną liczbę zadań za pomocą skryptów i innych narzędzi.

Nadal jednak nakłady pracy powinny być analizowane, aby upewnić się, że mamy pod dostatkiem czasu, by wykonać wszystkie niezbędne zadania. Jeśli niektórych z zadań nie damy rady wykonać z częstotliwością zaproponowaną w tym przewodniku, może okazać się niezbędna dodatkowa pomoc. W takim przypadku radzimy z rozwagą przygotować uzasadnienie propozycji i przedstawić je kierownictwu. Gdy takie sugestie są dobrze przygotowane i odpowiednio uzasadnione, to rzadko zostają odrzucone.

Administrowanie sprzętem

Wszystkie zadania zawarte w tym podrozdziale są przedstawione ogólnikowo, ponieważ mimo że ich regularne wykonywanie jest niezbędne, trudno opisać dokładnie, jak wykonywać poszczególne prace, gdy na rynku istnieje tak wiele modeli sprzętu i podejść do zarządzania sprzętem.

Wobec tego każdy z Czytelników będzie musiał dostosować wymienione poniżej zadania do swoich potrzeb, dodając własne czynności.

HW-01. Kontrola urządzeń sieciowych

✔ **Harmonogram: co tydzień**

Sieć zwykle zbudowana jest z przełączników, koncentratorów, ruterów, zapór sieciowych i tak dalej. Ich dobry stan zapewnia poprawne działanie systemów Windows Server 2003. Warto więc regularnie zwiedzać pomieszczenia komputerowe i sprawdzać, czy sprzęt sieciowy działa prawidłowo. Do tego przeglądu należą następujące czynności:

- Obejrzenie każdego urządzenia sieciowego i sprawdzenie, czy świecą się właściwe kontrolki.
- Przegląd dzienników urządzeń i ustawień konfiguracji w celu upewnienia się, że konfiguracja jest stabilna i nie zdarzają się próby ataków.
- Sprawdzenie stanu kabli i połączeń.

To zadanie powinno być dostosowane do korzystania z narzędzi dostępnych w konkretnym środowisku.

HW-02. Zarządzanie BIOS-em serwerów

✔ **Harmonogram: co miesiąc**

Podobnie jak systemy operacyjne, wersje BIOS-u ulegają ciągłym zmianom — ich producenci wciąż dodają nowe możliwości i funkcje. Na szczęście większość producentów serwerów stosuje się do zaleceń Desktop Management Task Force (*www.dmtf.org*), więc nie musimy już aktualizować BIOS-u, siedząc przy serwerze. Narzędzie do tego stosowane będzie zależeć od platformy, z którą pracujemy, lecz wszyscy liczący się producenci serwerów udostępniają narzędzia zdalnego zarządzania DMTF. Intel oferował nawet kiedyś ogólne narzędzie DMTF do zarządzania zdalnego, LANDesk, które współpracowało z większością sprzętu opartego na układach Intela. LANDesk jest obecnie dostępny jako produkt LANDesk Software (*www.landesksoftware.com*). Niezależnie od używanego narzędzia, BIOS i inne oprogramowanie producentów sprzętu będziemy musieli często aktualizować, aby w pełni kwalifikować się do ciągłego wsparcia technicznego.

Raz na miesiąc powinniśmy sprawdzić dostępność nowych wersji BIOS-u dla naszego sprzętu i skontrolować, czy w naszym środowisku nowy BIOS będzie potrzebny. Jeśli tak, powinniśmy pobrać nowy BIOS i za pomocą narzędzi DMTF dokonać aktualizacji we wszystkich wybranych serwerach.

Do uzyskania informacji o BIOS-ie systemu może posłużyć skrypt Microsoft TechNet Center, dostępny pod adresem *http://www.microsoft.com/technet/treeview/default.asp?url=/technet/scriptcenter/compmgmt/ScrCM39.asp?frame=true*.

HW-03. Zarządzanie aktualizacjami oprogramowania sprzętowego i zarządzającego serwerami

✔ **Harmonogram: co miesiąc**

Oprócz BIOS-u producenci sprzętu udostępniają oprogramowanie sprzętowe (ang. *firmware*) i oprogramowanie do zarządzania serwerami. Narzędzia te mają różnorodne możliwości, od informowania o stanie komponentów w szafkach serwerów aż po obsługę konkretnych komponentów sprzętowych. W większości przypadków narzędzia te obejmują dużą liczbę różnorodnych komponentów, więc zwykle są regularnie aktualizowane. Jeśli więc chcemy dysponować wsparciem producenta, musimy aktualizować i to oprogramowanie.

Raz na miesiąc powinniśmy sprawdzić dostępność nowego oprogramowania sprzętowego i nowych wersji oprogramowania do zarządzania serwerami dla naszego sprzętu i sprawdzić, czy będą one w naszym środowisku potrzebne. Jeśli tak, to powinniśmy pobrać je i za pomocą narzędzi DMTF lub przeznaczonych do zarządzania serwerami dokonać aktualizacji wszystkich serwerów, których to dotyczy.

HW-04. Zarządzanie urządzeniami

✔ **Harmonogram: w miarę potrzeb**

Windows Server 2003 współpracuje ze sprzętem poprzez sterowniki urządzeń. Interfejsem dla tych sterowników jest Menedżer urządzeń — składnik konsoli MMC Zarządzanie komputerem, a teraz również globalnej konsoli MMC, którą utworzyliśmy w procedurze **GS-17**.

Sterowniki czasem trzeba zaktualizować lub zmodyfikować. W niektórych przypadkach pewne sterowniki mogą w ogóle nie działać, zwłaszcza jeśli używamy serwerów niemarkowych (klonów). Wobec tego warto przynajmniej sprawdzić w Menedżerze urządzeń, czy nie występują jakieś błędy urządzeń.

Aby zweryfikować status sterowników urządzeń:

1. Uruchom globalną konsolę MMC (*pasek szybkiego uruchomienia*/*globalna MMC*).
2. Połącz się z odpowiednim serwerem (*Akcja*/*Podłącz do innego komputera*) i wpisz nazwę komputera (`\\nazwaserwera`) albo zlokalizuj serwer za pomocą przycisku *Przeglądaj*. Kliknij *OK*.
3. Wybierz *Menedżera urządzeń* (*Zarządzanie komputerem*/*Narzędzia systemowe*/*Menedżer urządzeń*).
4. Przejrzyj stan urządzeń w panelu szczegółów. Dla wszystkich urządzeń drzewa powinny być zwinięte. Każde urządzenie sprawiające problemy pojawi się w rozwiniętym drzewie z żółtym znakiem zapytania.
5. Kliknij prawym przyciskiem myszy takie urządzenie i przejrzyj *Właściwości*. Z menu podręcznego można też zaktualizować sterownik. Zidentyfikuj producenta urządzenia i poszukaj nowego lub zaktualizowanego sterownika. Jeśli żaden sterownik nie jest dostępny, wyłącz urządzenie.

Sterowniki urządzeń powinny być certyfikowane dla systemu Windows Server 2003, ponieważ w przeciwnym razie ich stabilność nie będzie gwarantowana. Windows Server domyślnie ostrzega użytkownika przy próbie zainstalowania sterownika, który nie jest certyfikowany.

Tworzenie i przywracanie kopii zapasowych

Chociaż serwery są projektowane z wykorzystaniem redundantnych systemów do ochrony serwera i danych, żadna organizacja nie może funkcjonować bez strategii przywracania systemu po katastrofie. Strategia taka powinna obejmować zarówno efektywną strategię wykonywania regularnych kopii zapasowych, jak i dobry system przywracania. Procedury opisane poniżej opierają się na *NTBackup.exe* — domyślnym narzędziu kopii zapasowych zawartym w systemie Windows Server 2003. Ta wersja NTBackup jest o wiele pełniejsza od poprzednich i zawiera zarówno usługę kopiowania woluminów w tle, jak i usługę automatycznego odzyskiwania systemu. Pierwsza opcja pozwala stworzyć obraz danych przed wykonaniem kopii, co rozwiązuje wiele problemów z kopiowaniem otwartych plików. Druga pozwala odbudować serwer bez konieczności ponownej instalacji oprogramowania.

Lecz jeśli firma poważnie traktuje swoje dane, to najprawdopodobniej Czytelnik będzie miał do czynienia z bardziej wszechstronnym narzędziem kopii zapasowych. Najlepszym z nich jest QiNetix firmy Commvault Systems Inc. (*www.commvault.com*). Jest to jedyne narzędzie kopii zapasowej, które w pełni obsługuje Active Directory, pozwalając przywracać obiekty i atrybuty katalogu bez konieczności wykonania przywracania autorytatywnego — operacji raczej złożonej. Oprócz tego, jeśli mamy do czynienia z naprawdę dużą objętością danych, to QiNetix potrafi zaoszczędzić sporo czasu, zwłaszcza dla pełnych kopii zapasowych, ponieważ dla nich tworzy pełny obraz kopii zapasowej z poprzednich kopii przyrostowych, wykorzystując unikatową technologię pojedynczego magazynu. Oznacza to, że nigdy nie braknie czasu na wykonanie kopii zapasowej, ponieważ nie jest ona pobierana z systemów, lecz z poprzednich kopii zapasowych.

BR-01. Generowanie kopii zapasowych stanu systemu

✔ **Harmonogram: codziennie**

Kopie zapasowe stanu systemu dla każdego serwera są krytyczne, ponieważ stanowią narzędzie chroniące sam system operacyjny. Kopia zapasowa stanu systemu zawiera dziewięć potencjalnych składników. Niektóre są kopiowane zawsze, a pozostałe zależnie od typu serwera. Są to:

- Rejestr systemowy.
- Baza danych rejestru klas COM+.
- Pliki startowe i systemowe.
- Pliki ochrony plików systemu Windows.
- Baza danych Active Directory (w kontrolerach domen).
- Katalog SYSVOL (w kontrolerach domen).
- Baza danych usług certyfikatów (w serwerach certyfikatów).
- Dane konfiguracyjne usługi klastrów (w klastrach serwerów).
- Metakatalog IIS (w serwerach aplikacji WWW).

Dane stanu systemu są zawsze zapisywane w kopii zapasowej jako całość, której nie można podzielić. Jest to zadanie codzienne, które powinno być zautomatyzowane. Aby zaplanować wykonywanie kopii zapasowej stanu systemu:

1. W globalnej konsoli MMC otwórz podłączanie pulpitu zdalnego (patrz procedura **RA-01**) z serwerem, który chcesz zweryfikować. Uruchom NTBackup (*obszar szybkiego uruchamiania*/*Kopia zapasowa*). Upewnij się, że narzędzie jest uruchomione w trybie zaawansowanym.

2. Przejdź do zakładki *Planowanie zadań* i kliknij *Dodaj zadanie*.
3. Otworzy się Kreator kopii zapasowej, który pozwoli zdefiniować parametry zadania. Kliknij *Dalej*.
4. Wybierz *Wykonaj jedynie kopię zapasową danych o stanie systemu* i kliknij *Dalej*.
5. Określ położenie kopii zapasowej, która powinna mieścić się na nośniku wymiennym. Kliknij *Dalej*.
6. Zaznacz *Weryfikuj dane po wykonaniu kopii zapasowej* i *Użyj kompresji sprzętowej, jeśli jest dostępna*. Nie wyłączaj kopiowania woluminów w tle.
7. Wybierz, czy dołączyć dane, czy zamienić istniejące kopie zapasowe, i kliknij *Dalej*.
8. Nadaj nazwę zadaniu i kliknij *Ustaw harmonogram*, aby wybrać *Cotygodniowo* (od poniedziałku do piątku). Kliknij *OK* po wybraniu dni. Wybierz konto, z którego kopia zapasowa będzie wykonywana i kliknij *OK*. Kliknij *Dalej* i *Finish*, aby zakończyć.

Powtórz procedurę, tworząc kopie zapasowe danych w tym samym harmonogramie i dodaj pełne kopie zapasowe w weekendy.

BR-02. Weryfikacja kopii zapasowych

✔ **Harmonogram: codziennie**

Chociaż tworzenie kopii zapasowych jest o wiele łatwiejsze i bardziej niezawodne w systemie Windows Server 2003, i tak powinniśmy poświęcić trochę czasu na upewnienie się, że kopie są wykonywane poprawnie. W tym celu powinniśmy przejrzeć dzienniki kopii zapasowych we wszystkich serwerach plików. Aby przejrzeć te dzienniki:

1. Otwórz w globalnej konsoli MMC podłączanie pulpitu zdalnego do serwera, który chcesz zweryfikować.
2. Uruchom narzędzie *Kopia zapasowa* w widoku zaawansowanym (*obszar szybkiego uruchamiania*/*Kopia zapasowa*).
3. Wybierz *Narzędzia*/*Raport*, aby przejrzeć raporty.
4. Wybierz odpowiedni raport z okna dialogowego *Raporty kopii zapasowych* i kliknij *Widok*.
5. Poszukaj słowa `Error` w dzienniku.

Jeśli znajdą się jakieś błędy, sprawdź, czy są typu krytycznego i skontroluj za pomocą Eksploratora Windows, dlaczego dany plik nie został skopiowany lub czy wymaga przywrócenia. Zanotuj wyniki kontroli w dzienniku swoich prac (patrz procedura **GS-06**).

BR-03. Zarządzanie składowaniem taśm poza lokalizacją serwerów

✔ **Harmonogram: co tydzień**

Jednym z kluczowych elementów strategii usuwania skutków katastrof jest ochrona taśm z kopiami zapasowymi. W końcu jeśli centrum komputerowe spali się do gruntu, a wszystkie taśmy spalą się razem z nim, to rekonstrukcja systemów może okazać się dość trudna. Wobec tego musimy składować taśmy z cotygodniowymi kopiami zapasowymi w innym miejscu, chronionym przed katastrofami. Może to być jakiekolwiek bezpieczne miejsce, od depozytu w banku aż po wyspecjalizowaną firmę chroniącą dane.

Oznacza to, że raz w tygodniu powinniśmy wysłać taśmy z weekendową kopią zapasową na zewnątrz centrum komputerowego do chronionej lokalizacji i pobrać starsze kopie, aby odzyskać taśmy. Należy rozważyć przechowywanie na zewnątrz pełnej miesięcznej kopii zapasowej i przynajmniej jednej rocznej (to może być ostatnia miesięczna kopia zapasowa w danym roku fiskalnym).

BR-04. Testowanie strategii usuwania skutków awarii

✔ **Harmonogram: co miesiąc**

Strategia usuwania skutków katastrof jest tylko tak dobra, jak jej udowodniona zdolność do przywracania i rekonstrukcji systemów. Wobec tego powinniśmy co miesiąc znaleźć czas na sprawdzenie poprawności tej strategii. Inaczej mówiąc, powinniśmy upewnić się, że wszystko, co składa się na strategię usuwania skutków katastrof, jest na miejscu i może w każdej chwili posłużyć do rekonstrukcji systemów. Zaliczają się do tego części zapasowe, serwery zapasowe, zapasowe urządzenia sieciowe, taśmy z kopiami zapasowymi przechowywane poza daną lokalizacją, rozsądny system rotacji taśm z kopiami zapasowymi, regularne czyszczenie napędów taśmowych, udokumentowane procedury rekonstrukcji systemu (zwłaszcza rekonstrukcji AD) i tak dalej. Przegląd powinien opierać się na liście kontrolnej, której użyjemy do kontroli poprawności każdego z elementów składających się na przywracanie systemu. Po ukończeniu przeglądu należy udokumentować wszelkie zmiany wprowadzone w strategii.

Dla każdego serwera powinniśmy też wykonywać kopie zapasowe do automatycznego odzyskiwania systemu (ang. *ASR — Automated System Recovery*). Kopię zapasową ASR musimy wykonać ręcznie, ponieważ tworzona jest jednocześnie dyskietka do przywracania systemu. Należy wykonywać kopię zapasową co miesiąc, aby dyskietka ASR była aktualna, oraz po każdej znaczącej zmianie w dowolnym serwerze. ASR rejestruje stan systemu, zainstalowane usługi, wszystkie informacje o dyskach zainstalowanych w systemie i o sposobie przywracania serwera. Aby wykonać kopię zapasową ASR:

1. W globalnej konsoli MMC otwórz *podłączanie pulpitu zdalnego* z odpowiednim serwerem. Uruchom NTBackup (*obszar szybkiego uruchamiania*/*Kopia zapasowa*). Upewnij się, że narzędzie jest uruchomione w trybie zaawansowanym.
2. Na ekranie powitalnym kliknij *Kreator automatycznego odzyskiwania systemu*. Uruchomi to Kreatora ASR. Kliknij *Dalej*.
3. Wybierz typ i nazwę kopii zapasowej i kliknij *Dalej*.
4. Kliknij *Zakończ*, aby rozpocząć tworzenie kopii zapasowej ASR. Upewnij się, że masz pod ręką dyskietkę do utworzenia dyskietki startowej ASR.

Dyskietkę ASR przechowuj w bezpiecznym miejscu.

Kopia zapasowa ASR nie jest pełną kopią zapasową systemu. Służy jedynie do odbudowania systemu operacyjnego. Sam system musi być dodatkowo chroniony pełną kopią zapasową.

BR-05. Testowanie procedury przywracania kopii zapasowych

✔ **Harmonogram: co miesiąc**

Kopie zapasowe są tylko tak dobre, jak ich zdolność do przywracania informacji w systemie. Wobec tego raz na miesiąc powinniśmy przeprowadzić test przywracania z losowo wybranej kopii zapasowej na nośniku, aby upewnić się, że faktycznie działa. Zbyt wielu administratorów pozostało z pustymi rękami, gdy próbowali przywrócić krytyczne pliki z nigdy nie przetestowanych taśm z kopiami zapasowymi, które nie działały. Aby przetestować procedurę przywracania:

1. Wybierz losowo nośnik z kopią zapasową i włóż do napędu w serwerze.
2. W globalnej konsoli MMC otwórz *podłączanie pulpitu zdalnego* z odpowiednim serwerem. Uruchom NTBackup (obszar szybkiego uruchamiania/*Kopia zapasowa*). Upewnij się, że narzędzie jest uruchomione w trybie zaawansowanym.

3. Na ekranie powitalnym kliknij *Kreator przywracania*. Uruchomi to Kreatora przywracania. Kliknij *Dalej*.
4. Wybierz kopię zapasową do przywrócenia lub kliknij *Przeglądaj*, by ją zlokalizować.
5. Rozwiń listing kopii zapasowej i wybierz losowy plik do przywrócenia. Kliknij *Dalej*.
6. Kliknij przycisk *Zaawansowane*, by przywrócić plik do nowej, testowej lokalizacji.
7. Kliknij *Zakończ*, by rozpocząć przywracanie.

Zweryfikuj integralność przywróconych plików, po czym usuń je.

BR-06. Przegląd strategii kopii zapasowych

✔ Harmonogram: co miesiąc

Raz na miesiąc powinniśmy też przejrzeć strategię wykonywania kopii zapasowych. Czy objętość kopii uległa zmianie? Czy do kopii należy dołączyć jakieś nowe informacje? Czy harmonogram kopii zapasowych jest zadowalający? Te i podobne pytania powinny pomóc w stworzeniu listy kontrolnej, która później posłuży do przeglądu strategii.

Udokumentuj wszelkie wprowadzone zmiany.

BR-07. Odbudowa serwera

✔ Harmonogram: w miarę potrzeb

Raz na jakiś czas powinniśmy znaleźć czas na przetestowanie procesu odbudowy serwera. Oznacza to wzięcie serwera testowego, zniszczenie systemu przez „zaoranie" macierzy RAID i wykonanie pełnej odbudowy z wykorzystaniem kopii zapasowej ASR i dyskietki ASR. Taki test powinniśmy przeprowadzać przynajmniej dwa razy do roku.

Aby odbudować serwer z pomocą ASR:

1. Uruchom Instalatora systemu z płyty instalacyjnej Windows Server 2003. Naciśnij *F2*, gdy program o to poprosi i włóż dyskietkę ASR. Upewnij się, że nośnik z kopią zapasową jest również dostępny i online.

2. Narzędzie przywracania ASR odtworzy sygnatury dysków, zainstaluje minimalną wersję Windows i przywróci wszystkie pliki systemowe.
3. Po zakończeniu przywracania ASR przywróć pliki danych z kopii zapasowych.
4. Skontroluj dokładnie serwer, upewniając się, że jest w pełni funkcjonalny.

Udokumentuj wszelkie zmiany wprowadzone w procedurze ASR.

Administrowanie zdalne

W systemie Windows 2000 wprowadzona została koncepcja zdalnego zarządzania serwerem przez Usługi terminalowe w trybie administracji zdalnej. Tryb ten pozwala na maksymalnie dwa jednoczesne zdalne połączenia z serwerem bez dodatkowych licencji klienckich usług terminalowych. W systemie Windows Server 2003 ta funkcja otrzymała nową nazwę, taką jak w Windows XP, Podłączanie pulpitu zdalnego (ang. *RDC — Remote Desktop Connections*).

RDC to cenne narzędzie dla administratorów, ponieważ daje pełny dostęp do pulpitu serwera bez konieczności fizycznego dostępu do komputera.

RDC jest narzędziem bezpiecznym, ponieważ ogranicza konieczność dostępu do pomieszczeń z serwerami. Administratorzy mogą pracować przy własnych biurkach, konfigurując serwery i zarządzając nimi zdalnie.

RA-01. Zarządzanie RDC w serwerach

✔ **Harmonogram: co miesiąc**

Raz na miesiąc powinniśmy dokonać przeglądu metod zdalnego zarządzania serwerami. Przegląd taki powinien odpowiedzieć na pytania typu: Czy nasze zdalne połączenia są bezpieczne? Ilu administratorów ma zdalny dostęp do serwerów? Czy hasła administratorów są zmieniane wystarczająco często? Czy konsole, dające dostęp zdalny do serwerów, są wystarczająco chronione?

Proszę pamiętać, że Podłączanie pulpitu zdalnego jest wymagane tylko wtedy, gdy musimy zmodyfikować ustawienia w serwerze. Radzimy zamiast tego przyzwyczaić się do pracy z globalną konsolą MMC.

Podłączanie pulpitu zdalnego może odbywać się tylko wtedy, gdy ustawienie Pulpit zdalny zostanie w serwerze włączone. W tym celu:

1. Uruchom okno dialogowe *Właściwości systemu* (menu *Start*/*Panel sterowania*/*System*).
2. Przejdź do zakładki *Zdalny* i zaznacz *Zezwalaj użytkownikom na zdalne łączenie się z tym komputerem*.
3. Jeśli wszyscy administratorzy są członkami lokalnej grupy Administratorzy, to nie trzeba już robić nic więcej, ponieważ uzyskają automatycznie dostęp do serwera. Zamiast tego możesz dodać operatorów serwerów zdalnych do wbudowanej grupy Użytkownicy pulpitu zdalnego (*Użytkownicy i komputery usługi Active Directory*/*Builtin*). Da im to dostęp do lokalnego pulpitu za pomocą zdalnych sesji. Jeśli użytkownicy nie należą do żadnej z tych grup, trzeba ich wpisać po kolei. W tym celu kliknij *Wybierz użytkowników zdalnych*.
4. Kliknij *OK* w każdym oknie dialogowym po zakończeniu wprowadzania zmian.

Opcję tę można też ustawić zdalnie za pomocą Zasad grup. Do edycji odpowiedniego GPO posłuży procedura **DC-16**, przy czym GPO powinien obowiązywać tylko dla serwerów. Włącz ustawienie *Zezwalaj użytkownikom na zdalne łączenie się przy użyciu usług terminalowych* (*Konfiguracja komputera*/*Szablony administracyjne*/*Składniki systemu Windows*/*Usługi terminalowe*). To ustawienie GPO zapewnia tę samą funkcjonalność, co pole wyboru w oknie *Właściwości systemu*.

Teraz, gdy serwery już pozwalają na zdalne połączenia, musimy dokonać faktycznego połączenia z każdym serwerem. Posłuży do tego globalna konsola MMC utworzona w procedurze **GS-17**.

1. Przejdź do *Pulpity zdalne*.
2. Kliknij prawym przyciskiem myszy *Pulpity zdalne* i wybierz *Dodaj nowe połączenie*.
3. Wpisz nazwę DNS serwera, nazwę połączenia i upewnij się, że zaznaczone jest pole *Podłącz do konsoli* i wpisz poświadczenia użytkownika (*Nazwa użytkownika*, *Hasło*, *Domena*). Zaznacz *Zapisz hasło*, aby utworzyć połączenie z automatycznym logowaniem. Kliknij *OK* po wpisaniu danych. Powtórz dla każdego serwera.

Upewnij się, że globalna konsola MMC jest zabezpieczona poprzez skrót Uruchom jako (patrz procedura **GS-01**), jeśli wybierzesz połączenie z automatycznym logowaniem, ponieważ może to być poważne zagrożenie bezpieczeństwa.

Od tej pory, gdy trzeba będzie połączyć się z serwerem, wystarczy raz kliknąć nazwę połączenia. Po zakończeniu pracy kliknij nazwę połączenia prawym przyciskiem i wybierz *Rozłącz*.

RDC w trybie administracyjnym pozwala na dwa połączenia na raz. Najlepiej zaraz po połączeniu sprawdzić, czy w danej chwili ktoś inny pracuje z serwerem. Najlepszym sposobem jest otwarcie konsoli wiersza poleceń i wpisanie `query user`. Jeśli zalogowany jest inny administrator, powinniśmy skontaktować się z nim i upewnić, że nasze działania w jednym serwerze nie są konfliktowe.

RA-02. Zarządzanie RDC w komputerach osobistych

✔ **Harmonogram: co miesiąc**

Zarządzanie RDC w komputerach osobistych wygląda tak samo jak w serwerach i wymaga takiego samego podejścia (patrz procedura **RA-01**). Jednak w związku z tym, że komputerów biurkowych mamy zwykle w organizacji o wiele więcej niż serwerów, warto utworzyć wspólną konsolę do zarządzania PC. W tym celu:

1. Utwórz nową konsolę jak w procedurze **GS-17**, lecz tym razem wydając polecenie `mmc /a`.
2. Otworzy się nowa konsola MMC. Dodaj przystawkę Pulpity zdalne do najwyższego poziomu konsoli.
3. Zapisz konsolę jako *Zarządzanie PC* w folderze *C:\Toolkit*. Upewnij się, że tę konsolę można modyfikować podczas korzystania z niej. Zamknij konsolę.
4. Uruchom konsolę ponownie, klikając jej nazwę. Dodaj nowe połączenie dla każdego zarządzanego przez siebie PC.
5. Zapisz konsolę (*Plik*/*Zapisz*).

Upewnij się, że wszystkie komputery PC są zarządzane przez GPO zezwalający na podłączanie pulpitu zdalnego. Zabezpiecz konsolę przez skrót Uruchom jako (procedura **GS-01**).

Komputery osobiste pozwalają na tylko jedno zalogowanie jednocześnie. Jeśli zalogujemy się zdalnie do PC, do którego zalogowany jest już użytkownik, to użytkownik ten zostanie automatycznie wylogowany. Aby udzielić pomocy użytkownikowi, należy skorzystać zamiast tego z procedury **RA-03**.

RA-03. Pomoc dla użytkowników poprzez narzędzie Pomoc zdalna

✔ **Harmonogram: w miarę potrzeb**

Gdy musimy udzielić zdalnej pomocy użytkownikowi, który jest nadal zalogowany, nie możemy skorzystać z Podłączania pulpitu zdalnego, ponieważ w ten sposób wylogowalibyśmy użytkownika automatycznie. Zamiast tego skorzystamy z Pomocy zdalnej.

Pomoc zdalna działa w dwojaki sposób. Może pozwolić użytkownikowi zażądać pomocy od działu pomocy technicznej lub pozwolić pracownikowi tego działu oferować pomoc użytkownikom. Użytkownik musi wyraźnie wyrazić zgodę na pomoc, aby była możliwa. Pomoc zdalną kontrolują dwa ustawienia GPO: *Pomoc zdalna na żądanie* i *Oferuj Pomoc zdalną* (*Konfiguracja komputera*/*Szablony administracyjne*/*System*/*Pomoc zdalna*). Oba ustawienia pozwalają identyfikować **Pomocników** w organizacji. Pomoc na żądanie pozwala ustalić godziny, w których użytkownicy mogą żądać pomocy i mechanizm żądania (mailto lub Simple MAPI). Oprócz tego każda opcja pozwala ustalić typy oferowanej pomocy: czy pomocnik może ingerować w pulpit czy jedynie obserwować. Ingerencja zapewnia najpełniejszą pomoc, lecz również stanowi zagrożenie bezpieczeństwa.

Pamiętajmy, że aby Pomocnik mógł wspomagać użytkownika lub ingerować w jego pulpit, użytkownik musi najpierw zaakceptować ofertę zdalnej pomocy. Musimy ostrzec użytkowników, aby nigdy nie pozostawiali komputerów bez nadzoru, gdy ktoś inny wchodzi w interakcje z pulpitem.

Obie opcje wymagają listy pomocników. Pomocnicy stanowią grupę użytkowników, wpisanych w postaci *nazwadomeny\nazwagrupy*.

Te ustawienia GPO nie pozwalają wybierać nazw grup z AD; musimy wpisać je ręcznie. Przed zastosowaniem GPO do komputerów PC powinniśmy sprawdzić, czy te informacje zostały wpisane poprawnie.

Po zastosowaniu tych ustawień do wszystkich PC możemy oferować pomoc następująco:

1. Uruchom *Centrum pomocy i obsługi technicznej* (menu *Start*/*Pomoc i obsługa techniczna*).
2. Kliknij *Narzędzia* (*Zadania pomocy technicznej*/*Narzędzia*).

3. Rozwiń *Narzędzia centrum pomocy i obsługi technicznej* w lewym panelu i kliknij *Oferuj Pomoc zdalną*.
4. Wpisz nazwę DNS komputera, z którym chcesz się połączyć i kliknij *Połącz*.
5. Zaczekaj na zaakceptowanie połączenia przez użytkownika zanim zaczniesz pomagać.

Zadanie to określiliśmy jako „W miarę potrzeb", ponieważ mamy nadzieję, że Czytelnik nie będzie musiał wykonywać go regularnie.

RA-04. Skróty do Podłączania pulpitu zdalnego i dostęp przez WWW

✔ **Harmonogram: w miarę potrzeb**

Ponieważ utworzyliśmy globalną konsolę MMC (patrz procedura **GS-17**), zawierającą przystawkę Pulpity zdalne, nie będziemy zbyt często potrzebować skrótów RDC. Konsola zapewnia łączność o wiele prostszą niż indywidualne skróty. Jednak może się okazać, że będziemy musieli połączyć się zdalnie z serwerem z innego komputera niż stojący na naszym biurku. Najlepszym sposobem na to jest opublikowanie strony WWW Podłączanie pulpitu zdalnego i stosowanie jej do łączenia z serwerami z dowolnego komputera.

Nigdy nie zapominaj zamknąć połączenia z pulpitem zdalnym serwera po zakończeniu pracy z komputera innego niż własny.

Klient podłączania pulpitu zdalnego (RDWC) nie jest domyślnie instalowany. Operację tę trzeba wykonać w serwerze mieszczącym Internetowe usługi informacyjne (IIS). Jeśli ich nie ma, trzeba będzie zainstalować IIS w serwerze za pomocą następującej procedury (do tej operacji niezbędna jest instalacyjna płyta CD Windows Server 2003):

1. Uruchom *Dodaj lub usuń programy* (menu *Start*/*Panel sterowania*) i wybierz *Dodaj/Usuń składniki systemu Windows*.
2. Przejdź do *Serwer aplikacji* i kliknij *Szczegóły*.
3. Przejdź do *Internetowe usługi informacyjne (IIS)* i kliknij *Szczegóły*.
4. Przejdź do *Usługa World Wide Web* i kliknij *Szczegóły*.

5. Zaznacz *Podłączanie pulpitu zdalnego w sieci Web* i kliknij *OK*. Kliknij *OK* jeszcze trzy razy, aby wrócić do okna dialogowego *Składniki systemu Windows*. Kliknij *Dalej*.
6. Po zainstalowaniu klienta będzie można przejść do folderu *%SystemRoot%\Web\TSWeb* i otworzyć plik *Default.htm*, aby wyświetlić domyślną stronę RDWC.
7. Tę stronę można zmodyfikować tak, by pasowała do standardów przedsiębiorstwa i umieścić w intranecie, aby dać administratorom zdalny dostęp do serwerów przez interfejs WWW.

Domyślne ustawienia zabezpieczeń Internet Explorera w serwerze muszą zostać zmienione; w przeciwnym razie użytkownicy nie będą mogli zobaczyć tej strony. Wybierz w Internet Explorerze *Narzędzia/Opcje internetowe/Zabezpieczenia* i ustaw *Poziom domyślny* dla strefy Lokalny intranet. To powinno pozwolić użytkownikom automatycznie pobierać formant ActiveX Usług terminalowych mieszczący się na tej stronie.

Po zakończeniu instalacji strona ta będzie mogła służyć do łączenia z wszystkimi serwerami z dowolnego PC.