

Microsoft

MCSA/MCSE

Examin 70-290

Zarządzanie i obsługa
środowiska Microsoft

WINDOWS SERVER 2003

Zestaw szkoleniowy
do samodzielnej nauki

Dan Holme, Orin Thomas

Training Kit

darmowe ebooki
aktualne czasopisma



ebookgigs.com



Oficjalny zestaw szkoleniowy do egzaminu 70-290, obejmujący przygotowanie teoretyczne, zadania kontrolne i pytania.

Niniejszy podręcznik firmy Microsoft ułatwia nabycie odpowiednich umiejętności, koniecznych zarówno podczas zdawania egzaminu MCP 70-290, jak i przy codziennej pracy. Książka pozwala na samodzielne opanowanie materiału egzaminacyjnego poprzez system lekcji i ćwiczeń praktycznych, rozwiązywanie szeregu przykładowych problemów oraz zapoznanie się z zestawem pytań egzaminacyjnych.

Na dysku CD-ROM został zamieszczony zestaw testów przygotowawczych, opracowany przy użyciu zaawansowanych technologii firmy MeasureIt. Zestaw zawiera 425 pytań w języku angielskim, stawiających wysokie wymagania i pozwalających

jeszcze przed przystąpieniem do egzaminu dogłębnie ocenić stopień przygotowania i umiejętności. Student może wybrać różne tryby testowania ograniczone bądź nieograniczone czasowo, generujące losowy zestaw pytań lub dotyczący wybranego zagadnienia. Student może też zapoznać się z uzasadnieniem, dlaczego dana odpowiedź jest prawidłowa lub nieprawidłowa. Pozwala to zorientować się, które tematy wymagają dalszego przestudiowania. Książka zawiera również szereg wartościowych wskazówek egzaminacyjnych i wiadomości podsumowujących, związanych z omawianymi w książce zagadnieniami.

Zdanie egzaminu staje się proste, jeśli wiadomo, w jaki sposób:

- + Utworzyć i zarządzać użytkownikami, grupami i kontami komputerów.
- + Zarządzać uprawnieniami plików i udziałów.
- + ■ Kontrolować dostęp do serwera sieci Web i zarządzać witrynami za pomocą usługi IIS (Internetowe usługi informacyjne).
- + Zarządzać urządzeniami sprzętowymi, pamięciami dyskowymi, oprogramowaniem i usługami drukowania.
- + Wdrażać procedury tworzenia kopii zapasowych oraz przywracać działanie systemu.



Dan Holliie spędził 10 lat jako konsultant i szkoleniowiec opracowując rozwiązania dla dziesiątków tysięcy pracowników działów IT, zatrudnianych w najbardziej prestiżowych organizacjach i przedsiębiorstwach na całym świecie. Do jego klientów zaliczają się firmy AT&T, General Electric, Johnson & Johnson i wiele innych. **Orin Thomas** jest pisarzem, edytorem i administratorem systemu zatrudnionym przy utrzymaniu witryny sieci Web Ccrttutor.net, która poświęcona jest zagadnieniom związanym z certyfikacjami. Uzyskał wiele certyfikatów, w tym MCSE, CCNA, CCDA oraz Linux+, współpracował także z organizacją The Insider's Guide to IT Certification.

Polecamy również następujące publikacje Microsoft Press:

- > Vademecum administratora Windows Server 2003
- > Microsoft Windows Security Resource Kit
- > Microsoft Windows Server 2003 Protokoły i usługi TCP/IP

Aby otrzymać aktualny katalog wydawnictw **Microsoft Press**, napisz: mSPress@promise.com.pl



<http://www.promise.com.pl>

Spis treści

Wstęp	1
Dla kogo przeznaczona jest książka?	1
Wymagania wstępne	1
Informacje o dysku CD-ROM	2
Cechy książki	3
Część 1: Samodzielna nauka	3
Część 2: Przygotowania do egzaminu	3
Uwagi i informacje	4
Konwencje notacji	4
Konwencje znaków klawiatury	5
Rozpoczęcie pracy	5
Wymagania sprzętowe	5
Wymagania oprogramowania	6
Instrukcje dotyczące instalacji	6
Program Microsoft Certified Professional	8
Certyfikaty	8
Warunki uzyskania certyfikatu MCP	9
Wsparcie techniczne	10
Wsparcie testowego wydania oprogramowania	10

Część I Samodzielna nauka

1 Wprowadzenie do Windows Server 2003	13
Cele rozdziału	13
Wymagania	13
Lekcja 1: Rodzina Windows Server 2003	14
Wersje systemu Windows Server 2003	14
Pytania	16
Podsumowanie lekcji	17
Lekcja 2: Instalacja i konfiguracja Windows Server 2003 i usługi Active Directory	18
Instalacja i konfiguracja Windows Server 2003	18
Usługa Active Directory	21
Zadanie praktyczne: Instalacja Windows Server 2003	23
Pytania	29
Podsumowanie lekcji	30
Pytania i odpowiedzi	31

Konfigurowanie dzienników programu Event Viewer	448
Zadanie kontrolne: Monitor zdarzeń	450
Pytania	451
Podsumowanie lekcji	452
Lekcja 2: Wykorzystywanie programu Performance Console (Wydajność)	453
Konfigurowanie programu System Monitor (Monitor systemu)	453
Wybór obiektów i liczników	457
Zadanie kontrolne: Wykorzystanie programu Performance Console	460
Pytania	461
Podsumowanie lekcji	462
Lekcja 3: Wykorzystywanie programu Task Manager (Menedżer zadań)	463
Omówienie programu Task Manager	463
Zakładka Applications (Aplikacje)	463
Zakładka Processes (Procesy)	464
Zakładka Performance (Wydajność)	465
Zakładka Networking (Sieć)	466
Zakładka Users (Użytkownicy)	467
Zadanie kontrolne: program Task Manager (Menedżer zadań)	467
Pytania	468
Podsumowanie lekcji	468
Lekcja 4: Wykorzystywanie usługi WMI Event Logging Provider (dostawcy protokolowania zdarzeń)	469
Działanie usługi WMI	469
Monitorowanie przy użyciu usługi WMIC	472
Zadanie kontrolne: Dane usługi WMI dostępne w programie Event Viewer (Podgląd zdarzeń)	473
Pytania	474
Podsumowanie lekcji	474
Zadanie praktyczne	475
Rozwiązywanie problemów	476
Podsumowanie rozdziału	477
Informacje dla zdających egzamin	478
Najważniejsze fakty	478
Najważniejsze pojęcia	478
Pytania i odpowiedzi	479
Odzyskiwanie systemu po awarii	483
Cele rozdziału	483
Wymagania	483
Lekcja 1: Odzyskiwanie systemu po awarii	484
Przegląd opcji związanych z odzyskiwaniem	484
System State	485
Stan systemu kontrolera domeny	487
Automated System Recovery (Automatyczne odzyskiwanie systemu)	488
Program Recovery Console (Konsola odzyskiwania)	490
Zadanie kontrolne: Przywracanie systemu po awarii	492
Pytania	495
Podsumowanie lekcji	496

' Informacje dla zdających egzamin	496
Najważniejsze fakty	496
Najważniejsze pojęcia	497
Pytania i odpowiedzi	497

Część II Przygotowanie do egzaminu

14 Zarządzanie oraz konserwacja fizycznych i logicznych urządzeń (1.0)	501
Sprawdzanie umiejętności i sugerowane ćwiczenia praktyczne	502
Lektura uzupełniająca	503
Zadanie 1.1	505
Pytania do zadania 1.1	506
Odpowiedzi do zadania 1.1	509
Zadanie 1.2	512
Pytania do zadania 1.2	512
Odpowiedzi do zadania 1.2	515
Zadanie 1.3	518
Pytania do zadania 1.3	518
Odpowiedzi do zadania 1.3	522
Zadanie 1.4	525
Pytania do zadania 1.4	525
Odpowiedzi do zadania 1.4	530
.5 Zarządzanie użytkownikami, komputerami i grupami (2.0)	533
Sprawdzanie umiejętności i sugerowane ćwiczenia praktyczne	533
Lektura uzupełniająca	535
Zadanie 2.1	537
Pytania do zadania 2.1	537
Odpowiedzi do zadania 2.1	539
Zadanie 2.2	541
Pytania do zadania 2.2	541
Odpowiedzi do zadania 2.2	542
Zadanie 2.3	544
Pytania do zadania 2.3	544
Odpowiedzi do zadania 2.3	545
Zadanie 2.4	548
Pytania do zadania 2.4	548
Odpowiedzi do zadania 2.4	549
Zadanie 2.5	551
Pytania do zadania 2.5	551
Odpowiedzi do zadania 2.5	553
Zadanie 2.6	555
Pytania do zadania 2.6	555
Odpowiedzi do zadania 2.6	556
Zadanie 2.7	558
Pytania do zadania 2.7	558
Odpowiedzi do zadania 2.7	559

16 • Zarządzanie i obsługa dostępu do zasobów (3.0)	561
Sprawdzanie umiejętności i sugerowane ćwiczenia praktyczne	562
Lektura uzupełniająca	563
Zadanie 3.1	564
Pytania do zadania 3.1	564
Odpowiedzi do zadania 3.1	566
Zadanie 3.2	569
Pytania do zadania 3.2	569
Odpowiedzi do zadania 3.2	572
Zadanie 3.3	574
Pytania do zadania 3.3	574
Odpowiedzi do zadania 3.3	577
Zadanie 3.4	579
Pytania do zadania 3.4	579
Odpowiedzi do zadania 3.4	581
17 Zarządzanie i obsługa środowiska serwera (4.0)	583
Sprawdzanie umiejętności i sugerowane ćwiczenia praktyczne	584
Lektura uzupełniająca	586
Zadanie 4.1	588
Pytania do zadania 4.1	588
Odpowiedzi do zadania 4.1	591
Zadanie 4.2	593
Pytania do zadania 4.2	593
Odpowiedzi do zadania 4.2	598
Zadanie 4.3	600
Pytania do zadania 4.3	600
Odpowiedzi do zadania 4.3	602
Zadanie 4.4	604
Pytania do zadania 4.4	604
Odpowiedzi do zadania 4.4	606
Zadanie 4.5	608
Pytania do zadania 4.5	608
Odpowiedzi do zadania 4.5	611
Zadanie 4.6	613
Pytania do zadania 4.6	613
Odpowiedzi do zadania 4.6	614
Zadanie 4.7	616
Pytania do zadania 4.7	616
Odpowiedzi do zadania 4.7	617
Zadanie 4.8	619
Pytania do zadania 4.8	619
Odpowiedzi do zadania 4.8	622
Zadanie 4.9	624
Pytania do zadania 4.9	624
Odpowiedzi do zadania 4.9	627

18	Zarządzanie i wprowadzanie metod odzyskiwania danych po awarii (5.0)	629
	Sprawdzanie umiejętności i sugerowane ćwiczenia praktyczne	630
	Lektura uzupełniająca	631
	Zadanie 5.1	632
	Pytania do zadania 5.1	632
	Odpowiedzi do zadania 5.1	637
	Zadanie 5.2	640
	Pytania do zadania 5.2	640
	Odpowiedzi do zadania 5.2	642
	Zadanie 5.3	644
	Pytania do zadania 5.3	644
	Odpowiedzi do zadania 5.3	646
	Zadanie 5.4	648
	Pytania do zadania 5.4	648
	Odpowiedzi do zadania 5.4	653
	Zadanie 5.5	658
	Pytania do zadania 5.5	658
	Odpowiedzi do zadania 5.5	661

Część III Dodatki

Terminal Server	665
Instalowanie i konfigurowanie środowiska programu Terminal Server (Serwer terminali)	666
Komponenty programu Terminal Server	666
Aplikacje	666
Licencjonowanie	668
Zarządzanie i rozwiązywanie problemów dotyczących programu Terminal Server (Serwer terminali)	669
Punkty administracji	669
Konfiguracja połączenia	671
Przekierowanie urządzeń	674
Zarządzanie sesjami i procesami	677
Zarządzanie sesjami użytkownika	677
Równoważenie obciążenia serwerów terminali	678
Sterowanie zdalne	679
Podsumowanie	680
Słownik	681
Indeks	703

Administracja systemu Windows Server 2003	33
Cele rozdziału	33
Wymagania	34
Lekcja 1: Konsola MMC (Microsoft Management Console)	35
Konsola MMC	35
Dostosowywanie konfiguracji konsoli MMC	37
Opcje konsoli	38
Zadanie kontrolne: Tworzenie i zapisywanie konsoli	39
Pytania	40
Podsumowanie lekcji	40
Lekcja 2: Zarządzanie zdalne komputerami za pomocą konsoli MMC	41
Konfigurowanie przystawki do pracy zdalnej	42
Zadanie kontrolne: Wybór komputera zdalnego w celu zarządzania tym komputerem (zadanie opcjonalne)	43
Pytania	43
Podsumowanie lekcji	44
Lekcja 3: Zarządzanie serwerami za pomocą programu Remote Desktop for Administration (Pulpit zdalny dla administracji)	45
Włączanie i konfigurowanie programu Remote Desktop for Administration (Pulpit zdalny dla administracji)	45
Remote Desktop Connection (Podłączanie pulpitu zdalnego)	47
Konfigurowanie klienta programu Remote Desktop	48
Rozwiązywanie problemów programu Terminal Services (Usługi terminalowe)	49
Zadanie kontrolne: Instalowanie programu Terminal Services (Usługi terminalowe) oraz uruchamianie administracji zdalnej	50
Pytania	51
Podsumowanie lekcji	52
Lekcja 4: Korzystanie z programu Remote Assistance (Pomoc zdalna)	53
Realizacja żądań pomocy	53
Korzystanie z programu Remote Assistance (Pomoc zdalna)	54
Zadanie kontrolne: Korzystanie z programu Remote Assistance (Pomoc zdalna) za pomocą aplikacji Windows Messenger	58
Pytania	58
Podsumowanie lekcji	59
Zadanie praktyczne	59
Rozwiązywanie problemów	60
Podsumowanie rozdziału	61
Informacje dla zdających egzamin	61
Najważniejsze fakty	61
Najważniejsze pojęcia	62
Pytania i odpowiedzi	62
Konta użytkowników	65
Cele rozdziału	65
Wymagania	66
Lekcja 1: Tworzenie i zarządzanie obiektami użytkowników	67
Tworzenie obiektów użytkownika za pomocą konsoli Active Directory Users and Computers	67

Zarządzanie obiektami użytkownika za pomocą konsoli Active Directory Users And Computers.....	71
Zadanie kontrolne: Tworzenie i zarządzanie obiektami użytkownika	75
Pytania	77
Podsumowanie lekcji	78
Lekcja 2: Tworzenie wielokrotnie obiektów użytkownika	79
Tworzenie i wykorzystywanie szablonów obiektu użytkownika.....	79
Importowanie obiektów użytkowników za pomocą programu CSVDE	80
Korzystanie z narzędzi wiersza poleceń usługi Active Directory	81
Zadanie kontrolne: Tworzenie wielu obiektów	87
Pytania.....	90
Podsumowanie lekcji.....	91
Lekcja 3: Zarządzanie profilami użytkowników	92
Profile użytkownika	92
Lokalne profile użytkownika	93
Mobilny profil użytkownika	93
Tworzenie wstępnie skonfigurowanych profili użytkowników	95
Tworzenie wstępnie skonfigurowanego profilu grupy	96
Konfigurowanie profilu obowiązkowego.....	96
Zadanie kontrolne: Zarządzanie profilami użytkowników	97
Pytania.....	100
Podsumowanie lekcji.....	101
Lekcja 4: Bezpieczeństwo i rozwiązywanie problemów związanych z uwierzytelnieniem.....	102
Stosowanie zasad dla zabezpieczania uwierzytelnienia	102
Inspekcja uwierzytelnienia	106
Administrowanie uwierzytelnieniem użytkownika	107
Zadanie kontrolne: Zabezpieczenia i rozwiązywanie problemów dotyczących uwierzytelnienia...	109
Pytania.....	110
Podsumowanie lekcji.....	111
Zadanie praktyczne.....	112
Rozwiązywanie problemów.....	114
Podsumowanie rozdziału	115
Informacje dla zdających egzamin	116
Najważniejsze fakty	116
Najważniejsze pojęcia.....	117
Pytania i odpowiedzi	117
Konta grup	121
Cele rozdziału	121
Wymagania	122
Lekcja 1: Omówienie rodzajów grup i ich zakresów	123
Zakresy grupy	124
Konwersja grupy.....	125
Tożsamości specjalne	126
Zadanie kontrolne: Zmiana typu i zakresu grupy	127
Pytania.....	128
Podsumowanie lekcji	128

' Lekcja 2: Zarządzanie kontami grup	129
Tworzenie grupy zabezpieczeń	129
Modyfikowanie członkostwa grup	130
Wyszukiwanie grup domeny, do których należy dany użytkownik	131
Zadanie kontrolne: Modyfikowanie członkostwa grupy	131
Pytania	132
Podsumowanie lekcji	132
Lekcja 3: Automatyzacja zarządzania kontami grup	133
Korzystanie z programu LDIFDE	133
Tworzenie grup za pomocą polecenia DSADD	136
Modyfikowanie grup za pomocą polecenia DSMOD	137
Zadanie kontrolne: Wykorzystanie programu LDIFDE do zarządzania kontami grup	137
Pytania	139
Podsumowanie lekcji	139
Zadanie praktyczne	140
Rozwiązywanie problemów	141
Podsumowanie rozdziału	141
Informacje dla zdających egzamin	142
Najważniejsze fakty	142
Najważniejsze pojęcia	142
Pytania i odpowiedzi	142
Konta komputerów	145
Cele rozdziału	145
Wymagania	146
Lekcja 1: Dołączanie komputera do domeny	147
Tworzenie kont komputerów	148
Porównanie kontenerów i jednostek organizacyjnych komputerów	152
Zadanie kontrolne: Dołączenie komputera do domeny usługi Active Directory	154
Pytania	155
Podsumowanie lekcji	156
Lekcja 2: Zarządzanie kontami komputerów	157
Zarządzanie uprawnieniami obiektu komputera	157
Konfigurowanie właściwości komputera	158
Wyszukiwanie i dołączanie do obiektów usługi Active Directory	158
Zadanie kontrolne: Zarządzanie kontami komputerów	159
Pytania	160
Podsumowanie lekcji	161
Lekcja 3: Rozwiązywanie problemów związanych z kontami komputerów	162
Usuwanie, wyłączanie bądź zerowanie kont komputerów	162
Rozpoznawanie problemów związanych z kontami komputerów	164
Zadanie kontrolne: Rozwiązywanie problemów związanych z kontami komputera	165
Pytania	167
Podsumowanie lekcji	167
Zadanie praktyczne	168
Rozwiązywanie problemów	169
Podsumowanie rozdziału	170

Informacje dla zdających egzamin	171
Najważniejsze fakty	171
Najważniejsze pojęcia	171
Pytania i odpowiedzi	172
6 Pliki i foldery	175
Cele rozdziału	175
Wymagania	176
Lekcja 1: Konfiguracja folderów udostępnionych	177
Udostępnianie foldera	177
Zarządzanie folderem udostępnionym	178
Konfigurowanie uprawnień udziału	180
Zarządzanie sesjami użytkownika i otwartymi plikami	183
Zadanie kontrolne: Konfiguracja folderów udostępnionych	183
Pytania	185
Podsumowanie lekcji	186
Lekcja 2: Konfigurowanie uprawnień systemu plików	187
Dziedziczenie	191
Uprawnienia czynne	194
Właściciel zasobu	197
Zadanie kontrolne: Konfigurowanie uprawnień systemu plików	199
Pytania	203
Podsumowanie lekcji	204
Lekcja 3: Inspekcja dostępu systemu plików	205
Konfigurowanie zdarzeń inspekcji	205
Włączanie inspekcji	207
Analiza dziennika zabezpieczeń	207
Zadanie kontrolne: Inspekcja systemu plików	209
Pytania	210
Podsumowanie lekcji	211
Lekcja 4: Administracja Internet Information Services (Internetowe usługi informacyjne)	212
Instalowanie programu IIS6.0	212
Administracja środowiska sieci Web	212
Konfigurowanie oraz zarządzanie witrynami Web i FTP	214
Ochrona plików w programie IIS	217
Zadanie kontrolne: Administracja programu IIS	219
Pytania	220
Podsumowanie lekcji	221
Zadanie praktyczne	222
Rozwiązywanie problemów	224
Podsumowanie rozdziału	227
Informacje dla zdających egzamin	227
Najważniejsze fakty	227
Najważniejsze pojęcia	228
Pytania i odpowiedzi	229

Tworzenie kopii zapasowych danych	233
Cele rozdziału	233
Wymagania	234
Lekcja 1: Podstawy tworzenia kopii zapasowych	235
Zapoznanie z programem Backup Utility (Kopia zapasowa)	235
Określanie strategii tworzenia kopii zapasowych	238
Łączenie różnych typów kopii zapasowych	240
Zadanie kontrolne: Wykonywanie różnicowej kopii zapasowej	240
Pytania	243
Podsumowanie lekcji	245
Lekcja 2: Odtwarzanie danych	246
Przywracanie danych przy użyciu programu Backup Utility	246
Opcje przywracania	247
Zadanie kontrolne: Przywracanie danych	248
Pytania	249
Podsumowanie lekcji	250
Lekcja 3: Zaawansowane funkcje tworzenia kopii zapasowych i przywracania danych	251
Omówienie usługi VSS	251
Zabezpieczenia dla procesów tworzenia kopii zapasowych	252
Zarządzanie nośnikami	252
Opcje kopii zapasowych	254
Polecenie Ntbackup	256
Harmonogram zadań wykonywania kopii zapasowych	259
Kopiowanie w tle folderów udostępnionych	260
Zadanie kontrolne: Zaawansowane funkcje wykonywania kopii zapasowych i przywracania danych	264
Pytania	266
Podsumowanie lekcji	267
Zadanie praktyczne	268
Rozwiązywanie problemów	270
Podsumowanie rozdziału	271
Informacje dla zdających egzamin	272
Najważniejsze fakty	272
Najważniejsze pojęcia	272
Pytania i odpowiedzi	273
Drukarki	277
Cele rozdziału	277
Wymagania	277
Lekcja 1: Instalowanie i konfigurowanie drukarek	279
Omówienie modelu drukarki systemu Windows Server 2003	279
Instalowanie drukarki w systemie Windows Server 2003	280
Konfigurowanie właściwości drukarki	282
Podłączanie klientów do drukarek	284
Zadanie kontrolne: Instalowanie i konfigurowanie drukarki	285
Pytania	289
Podsumowanie lekcji	290

Lekcja 2: Zaawansowana konfiguracja i zarządzanie drukarkami	291
Zarządzanie właściwościami drukarek	291
Konfigurowanie puli drukarek	295
Konfigurowanie kilku drukarek logicznych dla jednej drukarki fizycznej	296
Integracja drukarki systemu Windows Server 2003 z usługą Active Directory	297
Drukowanie w sieci Internet	299
Zadanie kontrolne: Zaawansowana konfiguracja drukarek i zarządzanie drukarkami	301
Pytania	302
Podsumowanie lekcji	303
Lekcja 3: Konserwacja, monitorowanie i rozwiązywanie problemów związanych z drukarkami	304
Konserwacja drukarek	304
Monitorowanie drukarek	305
Rozwiązywanie problemów związanych z drukarkami	308
Zadanie kontrolne: Rozwiązywanie problemów związanych z drukarkami	310
Pytania	311
Podsumowanie lekcji	312
Zadanie praktyczne	312
Rozwiązywanie problemów	316
Podsumowanie rozdziału	317
Informacje dla zdających egzamin	317
Najważniejsze fakty	318
Najważniejsze pojęcia	318
Pytania i odpowiedzi	318
9 Obsługa systemu operacyjnego	323
Cele rozdziału	323
Wymagania	324
Lekcja 1: Usługi aktualizacji oprogramowania	325
Omówienie usługi SUS	325
Instalowanie usługi SUS w systemie Windows Server 2003	326
Konfigurowanie i zarządzanie usługami SUS	328
Klient aktualizacji automatycznej	334
Konfigurowanie funkcji Automatic Updates za pomocą Zasad grupy	336
Rozwiązywanie problemów usługi SUS	338
Kopia zapasowa i przywracanie usługi SUS	340
Pytania	342
Podsumowanie lekcji	343
Lekcja 2: Pakiety serwisowe	344
Pobieranie i rozpakowywanie pakietów serwisowych	344
Instalowanie pakietów serwisowych za pomocą zasady grupy	345
Pytania	345
Podsumowanie lekcji	346
Lekcja 3: Zarządzanie licencjami oprogramowania	347
Otrzymywanie licencji dostępu klienta CAL	347
Tryb licencjonowania Per-Server (Na serwer)	348
Tryb licencjonowania Per-Device or Per-User (Na urządzenie lub na użytkownika)	348
Administracja licencjonowania lokacji	350

Pytania	354
Podsumowanie lekcji	355
Zadanie praktyczne	355
Podsumowanie rozdziału	360
Informacje dla zdających egzamin	360
Najważniejsze fakty	360
Najważniejsze pojęcia	361
Pytania i odpowiedzi	362
Zarządzanie sprzętem i sterownikami	365
Cele rozdziału	365
Wymagania	366
Lekcja 1: Instalowanie urządzeń sprzętu i sterowników	367
Urządzenia i sterowniki	367
Korzystanie z programu Device Manager (Menedżer urządzeń)	368
Użytkownicy i administratorzy a instalacja urządzeń	370
Opcje podpisywania sterownika	370
Zadanie kontrolne: Instalowanie sterowników urządzenia	371
Pytania	372
Podsumowanie lekcji	373
Lekcja 2: Konfigurowanie urządzeń sprzętu i sterowników	374
Aktualizacja sterowników	374
Przywracanie sterowników	375
Odinstalowywanie sterowników	376
Konfiguracja zasobów	377
Program Control Panel i konfiguracja urządzeń	378
Zadanie kontrolne: Konfigurowanie urządzeń	378
Pytania	378
Podsumowanie lekcji	379
Lekcja 3: Rozwiązywanie problemów związanych z urządzeniami sprzętu i sterownikami	380
Przywracanie po awarii urządzenia	380
Kody statusu w programie Device Manager	381
Pytania	383
Podsumowanie lekcji	383
Zadanie praktyczne	384
Rozwiązywanie problemów	385
Podsumowanie rozdziału	386
Informacje dla zdających egzamin	386
Najważniejsze fakty	386
Najważniejsze pojęcia	387
Pytania i odpowiedzi	388
Zarządzanie pamięcią dyskową w systemie Microsoft Windows Server 2003.391	
Cele rozdziału	391
Wymagania	392
Lekcja1: Omówienie opcji dotyczących pamięci dyskowych	393
Dyski fizyczne	393

Woluminy logiczne	393
Woluminy zainstalowane.....	394
Odporność na uszkodzenia.....	394
Separacja danych	395
Dyski podstawowe i dynamiczne	395
Pytania	399
Podsumowanie lekcji	400
Lekcja 2: Konfigurowanie dysków i woluminów	401
Zarządzanie dyskami	401
Konfigurowanie dysków i woluminów.....	402
Woluminy rozszerzone	405
Przenoszenie dysków pomiędzy serwerami	406
Konwersja pamięci dyskowych	407
Wykonywanie zadań związanych z zarządzaniem dyskami w oknie wiersza poleceń	408
Zadanie kontrolne: Konfigurowanie dysków i woluminów	410
Pytania	412
Podsumowanie lekcji.....	413
Lekcja 3: Konserwacja woluminów pamięci dyskowej.....	414
Program CHKDSK	414
Defragmentator dysku.....	415
Przydziały dysku	417
Zadanie kontrolne: Implementacja przydziałów dysku.....	419
Pytania	421
Podsumowanie lekcji	422
Lekcja 4: Implementacja macierzy dyskowych RAID.....	423
Wprowadzanie odporności na uszkodzenia.....	423
Woluminy rozłożone	424
Woluminy dublowane	425
Woluminy RAID-5.....	427
Porównanie woluminów dublowanych i RAID-5.....	428
Tworzenie woluminu odpornego na uszkodzenia dla woluminu systemowego	429
Zadanie kontrolne: Planowanie konfiguracji macierzy RAID	430
Pytania	431
Podsumowanie lekcji	433
Zadanie praktyczne	433
Rozwiązywanie problemów	435
Podsumowanie rozdziału	438
Informacje dla zdających egzamin	438
Najważniejsze fakty.....	438
Najważniejsze pojęcia	439
Pytania i odpowiedzi	440
Monitorowanie systemu Microsoft Windows Server 2003	445
Cele rozdziału	445
Wymagania	446
Lekcja 1: Wykorzystywanie programu Event Viewer.....	447
Dostępne dzienniki programu Event Viewer (Podgląd zdarzeń).....	447

Wstęp

Zapraszamy do Zestawu szkoleniowego MCSA/MCSE (Egzamin 70-290): *Zarządzanie i obsługa środowiska Windows Server 2003*. Niniejsza książka przygotowana została tak, aby udostępnić czytelnikowi skuteczną metodę przygotowania się do egzaminów MCSE i w ten sposób przekazać mu wiedzę potrzebną do wprowadzenia serwera Windows Server 2003 w środowisku sieci przedsiębiorstwa. Założeniem powstania książki była pomoc w zrozumieniu podstawowych technologii, szeregu opcji związanych z konfigurowaniem zestawów cech oraz złożonych interakcji między poszczególnymi komponentami, dzięki czemu czytelnik będzie lepiej przygotowany, by sprostać wyzwaniom stawianym przez technologie informacyjne (IT). Realizacja takiego założenia oznacza, że każdy certyfikat to bogatsza wiedza i doświadczenia oraz profesjonalizm służący również całej grupie zawodowej, niezależnie od wartości samego certyfikatu MCSE.



Informacja Szczegółowe informacje o wymaganiach związanych z uzyskaniem certyfikatu Microsoft Certified Professional można znaleźć w sekcji zatytułowanej „Program Microsoft Certified Professional”, umieszczonej w dalszej części wstępu.

Dla kogo przeznaczona jest książka?

Książka przeznaczona jest dla fachowców branży IT planujących zdawać egzamin 70-290, *Zarządzanie i obsługa środowiska Windows Server 2003* będący jednym z wymaganych dla certyfikatu MCP, bądź do osób zajmujących się administracją serwera Microsoft Windows Server 2003.



Informacja Zakres wiedzy i umiejętności związanych z egzaminami jest zmieniany bez wcześniejszego powiadomienia i wyłącznie według uznania firmy Microsoft.

Wymagania wstępne

Opracowując niniejszy zestaw szkoleniowy założono, że studenci spełniają następujące wymagania:

- Co najmniej 12—18 miesięcy doświadczeń w administrowaniu technologiami systemu Windows w środowisku sieci.
- Zrozumienie usługi katalogowej Active Directory i związanych z nią technologii, w tym obiektu Group Policy (Zasady grupy).

Informacje o dysku CD-ROM

Do książki dołączony został dysk CD-ROM Supplemental Course Materials (Uzupełniające materiał) kursu), który zawiera szereg dodatkowych informacji stanowiących uzupełnienie zawartości podręcznika:

- Zestaw testów przygotowawczych opracowany przez MeasureUp (Microsoft Press Readiness Suite Powered by MeasureUp) w języku angielskim. Ten zestaw kontrolnych oraz przekrojowych zadań zawiera pytania o zróżnicowanym stopniu złożoności i udostępnia szereg trybów testowania. Czytelnik może sprawdzić swój stopień zrozumienia omawianych w książce pojęć i wykorzystać wyniki do opracowania takiego planu nauki, aby osiągnąć zamierzone rezultaty.
- Elektroniczna wersja książki (eBook) w języku angielskim. Szczegółowe informacje o sposobie korzystania z książki elektronicznej znajdują się w dalszej części tego rozdziału, w sekcji „Książka elektroniczna”.
- Dwie książki elektroniczne *Microsoft Encyclopedia of Networking, Second Edition* oraz *Microsoft Encyclopedia of Security* są pełnym i aktualnym źródłem informacji dotyczących sieci i jej ochrony.
- Fragmenty rozdziałów kilku książek wydanych przez Microsoft Press dostarczają dodatkowe informacje o serwerze Windows Server 2003 i zaznajamiają z innymi zasobami udostępnianymi przez Microsoft Press.

Drugi dysk CD-ROM zawiera 180-dniową, testową wersję serwera Microsoft Windows Server 2003, Enterprise Edition.



Informacja 180-dniowe wydanie testowe, dostarczane wraz z zestawem szkoleniowym jedynie dla oceny produktu i ćwiczeń praktycznych, nie jest pełnym produktem komercyjnym. Wsparcie techniczne firmy Microsoft nie obejmuje tego produktu.

Dodatkowe informacje dotyczące niniejszej książki i dysku CD-ROM (zawierające odpowiedzi na najczęściej zadawane pytania związane z instalacją i używaniem produktu) znaleźć można w witrynie Microsoft Press Technical Support Web pod adresem <http://www.microsoft.com/mspress/support/>. Można również zwracać się z pytaniami wysyłając wiadomość e-mail w języku angielskim na adres tkinput@microsoft.com lub pisać list do Microsoft Press, Attention: Microsoft Press Technical Support, One Microsoft Way, Redmond, WA 98052-6399-

Cechy książki

Książka składa się z dwóch części. Część pierwszą należy wykorzystywać do nauki w odpowiednim dla siebie tempie i do osiągnięcia wprawy wynikającej z przeprowadzania ćwiczeń praktycznych. W części drugiej zamieszczone zostały pytania i odpowiedzi służące do samooceny postępów nauczania.

Część 1: Samodzielna nauka

Każdy rozdział identyfikuje zamieszczone w nim zadania egzaminu, stanowi opis istoty tematów dzięki określeniu, w jaki sposób dana informacja stosowana jest w rzeczywistości oraz przedstawia listę warunków wstępnych, które muszą być spełnione, by zrealizować prezentowaną w rozdziale lekcję.

Rozdziały zawierają zestaw lekcji. Z kolei lekcje zawierają zestawy kontrolne z jednym lub kilkoma ćwiczeniami praktycznymi. Ćwiczenia są okazją opanowania prezentowanych umiejętności lub pogłębienia wiedzy o opisywanym fragmencie aplikacji. W każdej lekcji znajduje się zestaw pytań przekrojowych oceniających wiedzę związaną z prezentowanym materiałem.

Dzięki zamieszczonym po lekcji ćwiczeniom opisującym różne sytuacje, student ma okazję sprawdzić swoją wiedzę. Zadania wykonywane w ćwiczeniach są wieloetapowe i przypominają rzeczywiste sytuacje. Student ma także okazję pracować w „laboratorium” usuwania problemów, które pokazuje trudności spotykane podczas wykorzystywania poznanych zagadnień.

Każdy rozdział kończy się podsumowaniem kluczowych pojęć i krótką sekcją zawierającą listę podstawowych tematów i terminów, których znajomość wymagana jest podczas egzaminu. Podsumowanie jest listą tematów, na których głównie skupiają się pytania egzaminacyjne.



W praktyce **Przydatne informacje**

Tak oznaczona notatka zawiera informacje powiązane z danym tematem, które mogą być przydatne. Oznaczenie „W praktyce” dotyczy specyficznych informacji uzyskanych dzięki doświadczeniom profesjonalistów branży IT.

Część 2: Przygotowania do egzaminu

Część 2 pomaga zapoznać się z rodzajami pytań spotykanych na egzaminie MCP. Przegląd zadań i pytań testowych pozwala skupić się na tych dziedzinach, które przed przystąpieniem do egzaminu wymagają ze strony studenta pogłębienia wiadomości.



Informacja Pełna lista egzaminów MCP i związanych z nimi zadań znajduje się na stronie o adresie <http://www.microsoft.com/traincert/mcp>.

Część 2 jest uporządkowana według zadań egzaminu. W każdym rozdziale umieszczona została jedna z grup zadań nazwana Tematem, a rozdział zawiera listę umiejętności, które trzeba opanować, aby podczas egzaminu udzielać prawidłowych odpowiedzi. W każdym rozdziale znajduje się również lista lektur uzupełniających wiedzę związaną z danym tematem, co pozwala poprawić umiejętności i sposób realizacji prezentowanych zadań.

Każdy temat zawiera powiązane z nim zadania objęte egzaminem. W zadaniach tych znajduje się kilka kontrolnych pytań egzaminacyjnych. Dla każdej prawidłowej i nieprawidłowej odpowiedzi dołączone są wyjaśnienia.

Informacja Pytania te zostały również zamieszczone na dołączonym do książki dysku CD w postaci testów kontrolnych w języku angielskim.

Uwagi i informacje

W niniejszym zestawie ćwiczeń zastosowano szereg elementów ułatwiających percepcję tekstu:

- **Wskazówka** Opisuje metodę szybszego lub nietypowego sposobu wykonania zadania.
- **Ważne** Zawiera informacje, które są istotne dla zakończenia zadania.
- **Informacja** Zawiera informacje uzupełniające.
- **Uwaga** Zawiera ważne informacje o możliwości utraty danych; informacje te należy czytać bardzo uważnie
- **Ostrzeżenie** Zawiera istotne informacje o możliwości uszkodzeń fizycznych; informacje te należy czytać bardzo uważnie.
- **Zobacz także** Zawiera odniesienia do dodatkowych źródeł informacji.
- **Planowanie** Zawiera wskazówki i potrzebne informacje, które powinny pomóc rozplanować implementację.
- **Alert bezpieczeństwa** Wyróżnione informacje, z którymi trzeba się zapoznać, aby maksymalnie zwiększyć ochronę środowiska pracy.
- **Wskazówki egzaminacyjne** Oznaczenie informacji, z którymi należy zapoznać się przed przystąpieniem do egzaminu.
- **Nieoficjalnie** Zawiera praktyczne rady wynikające z rzeczywistych implikacji prezentowanych na lekcji informacji.

Konwencje notacji

W książce stosowane są następujące konwencje:

- Znaki i polecenia, które wprowadza czytelnik, drukowane są za pomocą pogrubionej czcionki (**bold**).
- *Kursywa* stosowana w poleceniach to znaki zastępcze dla informacji zmiennych. Kursywą drukowane są również tytuły książek.
- Nazwy plików i folderów rozpoczynają się dużą literą, za wyjątkiem sytuacji, kiedy student wpisze inaczej. Podczas wpisywania nazw plików w oknach dialogowych lub wierszu poleceń nie trzeba stosować dużych liter, chyba że zostało to inaczej określone.
- Rozszerzenia nazw plików pisane są zawsze małymi literami.
- Akronimy zawsze pisane są wielkimi literami.
- Czysta odstępowa linia używana jest przy przedstawianiu kodu, przykładach tekstów ekranowych lub wpisach w wierszu poleceń bądź plikach startowych.

- Opcje występujące w składni poleceń obejmowane są nawiasami kwadratowymi []- Na przykład, zapis [nazwa_pliku] znajdujący się w poleceniu wskazuje, że w poleceniu należy wprowadzić nazwę pliku. Wpisywać należy jedynie informacje wewnątrz nawiasów, bez samych nawiasów.
- Nawiasy { } są używane w składni poleceń do obejmowania wymaganych elementów. Wpisywać należy jedynie informacje wewnątrz nawiasów, bez samych nawiasów.

Konwencje znaków klawiatury

- Znak plus (+) umieszczony między dwoma nazwami przycisków oznacza, że przyciski te należy nacisnąć jednocześnie. Przykładowo, „naciśnij Alt+Tab” oznacza, że przy wciśniętym przycisku Alt należy nacisnąć przycisk Tab.
- Przecinek (,) umieszczony pomiędzy dwoma lub kilkoma nazwami przycisków klawiatury oznacza, że przyciski te należy naciskać kolejno, a nie jednocześnie. Na przykład, „naciśnij Alt+W, L” oznacza, że najpierw należy jednocześnie nacisnąć przyciski Alt oraz W, a następnie zwolnić je i nacisnąć przycisk L.

Rozpoczęcie pracy

W niniejszym zestawie przygotowawczym zamieszczone zostały ćwiczenia praktyczne pomagające opłacać wiedzę o implementacji, obsłudze i usuwaniu problemów związanych z technologiami serwera Windows Server 2003. Rozdział ten pomaga w przygotowaniu środowiska samodzielnie przeprowadzanych ćwiczeń. Większość ćwiczeń można wykonać na pojedynczym komputerze w środowisku testowym. Kilka ćwiczeń opcjonalnych wymaga drugiego komputera działającego pod kontrolą systemu Microsoft Windows XP, przy czym oba komputery muszą być połączone w jednej sieci.



Uwaga Ćwiczenia, jak również zmiany dokonywane na komputerze testowym mogą dawać niepożądane efekty, jeśli komputer jest połączony z dużą siecią. Przed przystąpieniem do ćwiczeń, należy to skonsultować z administratorem sieci.

Wymagania sprzętowe

Konfiguracja komputera testowego musi spełniać określone wymagania minimalne. Wszystkie urządzenia sprzętowe muszą znajdować się na liście HCL, Hardware Compatible List (Lista kompatybilności urządzeń sprzętu) dla systemu Microsoft Windows Server 2003 oraz powinny spełniać wymagania, których lista znajduje się na stronie: <http://www.microsoft.com/iodowsserver2003/evaluation/requirements/default.aspx>.

- Procesor: minimum 133 MHz dla komputerów zbudowanych w oparciu o rodzinę x86 (zalecane 733 MHz) oraz 733 MHz dla komputerów bazujących na Itanium
- Pamięć RAM: minimum 128 MB (zalecane 256 MB)
- Przestrzeń dyskowa instalacji: 1,5 GB dla komputerów x86 oraz 2,0 GB dla komputerów Itanium
- Rozdzielczość monitora 800x600 lub wyższa
- Napęd dysku CD-ROM lub DVD-ROM
- Mysz Microsoft Mouse lub kompatybilne urządzenie

Wymagania oprogramowania

Wymienione poniżej oprogramowanie jest wymagane, by przeprowadzić procedury zawarte w zestawie szkoleniowym:

- Serwer Windows Server 2003, Enterprise Edition (180-dniowa wersja testowa serwera dołączona została na dysku CD-ROM)
- System Windows XP Professional (system ten nie został dołączony na dysku CD-ROM i wymagany jest jedynie podczas opcjonalnych ćwiczeń praktycznych).



Uwaga 180-dniowe wydanie testowe dostarczane wraz z zestawem przygotowawczym jedynie dla oceny produktu i ćwiczeń praktycznych, nie jest pełnym produktem oferowanym w sprzedaży. Wsparcie techniczne firmy Microsoft nie obsługuje tego produktu. Dodatkowe informacje dotyczące niniejszej książki i dysku CD-ROM (zawierające odpowiedzi na najczęściej zadawane pytania związane z instalacją i używaniem produktu) znaleźć można w witrynie Microsoft Press Technical Support Web pod adresem <http://mspress.microsoft.com/mspress/support/>.

Instrukcje dotyczące instalacji

Komputer należy skonfigurować zgodnie z instrukcjami producenta. Konfiguracja serwera powinna być następująca:

- Windows Server 2003, Enterprise Edition
- Nazwa komputera: Server01
- Kontroler domeny znajduje się w domenie contoso.com
- 1 GB przestrzeni dyskowej bez określonej partycji

Dla uproszczonej instalacji serwera Windows Server 2003 wystarczająca jest konfiguracja podana powyżej, natomiast pełniejszy opis procedury instalacyjnej zamieszczony został w rozdziale 1.

Drugi komputer, z uruchomionym systemem Windows XP, będzie wykorzystywany jako klient podczas przeprowadzania opcjonalnych ćwiczeń praktycznych.



Uwaga Jeśli komputer połączony jest z dużą siecią, należy sprawdzić z administratorem sieci, czy nazwy komputera, nazwa domeny i inne informacje używane do skonfigurowania serwera Windows Server 2003 (opisane powyżej i w rozdziale 1) nie będą w konflikcie z operacjami sieci. Jeśli taki konflikt ma miejsce, należy poprosić administratora o dostarczenie alternatywnych nazw bądź wartości i używać ich podczas wszystkich ćwiczeń zamieszczonych w książce.

Zestaw testów przygotowawczych

Dysk CD-ROM zawiera zadania kontrolne składające się z 300 pytań egzaminacyjnych oraz zadania przygotowawcze z dodatkowymi 125 pytaniami. Narzędzia te można używać do usprawnienia nauczania i określenia, w których obszarach należy zdobyć większe doświadczenie, zanim przystąpi się do egzaminu.

* Instalacja zadań kontrolnych i przeglądu zadań

1. Umieść w napędzie dysków CD-ROM dysk Supplemental Materials (materiały uzupełniające) CD-ROM.



Informacja Jeśli na komputerze zablokowana jest funkcja „AutoRun”, należy przeczytać Informacje zamieszczone w pliku Readme.txt znajdującym się na dysku CD-ROM.

2. Kliknij menu Readiness Review Suite (Zestaw testów przygotowawczych) i postępuj zgodnie z instrukcjami.

Książki elektroniczne (eBooks)

Na dysku CD-ROM zamieszczone zostały' anglojęzyczne wersje elektroniczne niniejszego zestawu szkoleniowego, jak również dwóch innych pozycji *Microsoft Encyclopedia of Security* oraz *Microsoft Encyclopedia of Networking, Second Edition*. Książki elektroniczne są w formacie PDF (Portable Document Format) i mogą być przeglądane za pomocą programu Adobe Acrobat Reader

W celu korzystania z książek elektronicznych

1. Umieść w napędzie dysków CD-ROM dysk Supplemental Materials.



Informacja Jeśli na komputerze zablokowana jest funkcja „AutoRun”, należy przeczytać informacje zamieszczone w pliku Readme.txt znajdującym się na dysku CD-ROM

2. W menu, kliknij opcję Training Kit eBook (Zestaw szkoleniowy eBook). W ten sposób można również przeglądać inne, udostępnione książki elektroniczne.

Program Microsoft Certified Professional

Program MCP (Microsoft Certified Professional) jest najlepszą metodą udokumentowania znajomości aktualnych produktów i technologii firmy Microsoft. Egzaminy i odpowiednie certyfikaty zostały opracowane, aby potwierdzały biegłe opanowanie istotnych umiejętności związanych z projektowaniem, rozwojem, implementacją lub obsługą rozwiązań produktów i technologii firmy Microsoft. Fachowcy branży komputerowej, którzy uzyskali certyfikat firmy Microsoft są postrzegani jako eksperci i poszukiwani we wszystkich dziedzinach przemysłu. Certyfikat przynosi wiele korzyści zarówno indywidualnym osobom, jak i pracodawcom czy organizacjom.



Informacja Pełna lista korzyści certyfikatu MCP zamieszczona została na stronie:

<http://luiwww.microsoft.com/traincert/tartlitpro.asp>.

Certyfikaty

Program Microsoft Certified Professional oferuje różnorodne certyfikaty, które dotyczą określonych technicznych umiejętności specjalistycznych:

- Microsoft Certified Professional (MCP). Dowodzi głębokiej wiedzy o co najmniej jednym systemie operacyjnym Microsoft Windows lub o platformie istotnej z punktu widzenia architektury. Osoba z certyfikatem MCP kwalifikuje się do wprowadzania produktów lub technologii firmy Microsoft jako części rozwiązań biznesowych danej organizacji.
- Microsoft Certified Solution Developer (MCSD). Fachowcy programiści uprawnieni do przeprowadzania analiz, rozwoju i projektowania rozwiązań biznesowych za pomocą narzędzi i technologii projektowych firmy Microsoft, w tym za pomocą Microsoft .NET Framework.
- Microsoft Certified Application Developer (MCAD). Fachowcy programiści uprawnieni do opracowywania, testowania, instalowania i obsługi potężnych aplikacji za pomocą narzędzi i technologii firmy Microsoft, w tym produktów Microsoft Visual Studio .NET oraz usług XML Web.
- Microsoft Certified System Engineer (MCSE). Fachowcy kompetentni do przeprowadzania analiz wymagań biznesu, projektowania oraz wprowadzania infrastruktury rozwiązań biznesowych w oparciu o systemy operacyjne Microsoft Windows oraz Microsoft Windows Server 2003.
- Microsoft Certified Systems Administrator (MCSA). Osoby o tych umiejętnościach zarządzają oraz usuwają problemy istniejących środowisk sieci i systemów w oparciu o systemy operacyjne Microsoft Windows oraz Microsoft Windows Server 2003-
- Microsoft Certified Database Administrator (MCDBA). Osoby, które projektują, wprowadzają i administrują bazami danych serwera Microsoft SQL Server.
- Microsoft Certified Trainer (MCT). Osoba wykwalifikowana pod względem szkoleniowym i technicznym do prowadzenia kursów Microsoft Official Curriculum w ośrodkach CTEC (Microsoft Certified Technical Education Center).

Wymagania uzyskania certyfikatu MCP

Wymagania poszczególnych certyfikatów różnią się między sobą i związane są z konkretnymi produktami i charakterem *pracy* określonej przez certyfikat.

W celu uzyskania certyfikatu MCP wymagane jest zaliczenie rygorystycznych egzaminów, które zapewniają wiarygodną i pewną ocenę biegłości i umiejętności specjalistycznych. Z pomocą doświadczonych fachowców, egzaminy te zostały opracowane, aby sprawdzić umiejętności i możliwości wykonywania ról bądź zadań związanych z danym produktem. Odpowiedzi na pytania egzaminu, wprowadzając odniesienia do rzeczywistości, odzwierciedlają sposób wykorzystywania produktów firmy Microsoft w prawdziwych organizacjach.

- Osoby starające się o uzyskanie certyfikatu Microsoft Certified Product (MCP) muszą zdać jeden z aktualnych egzaminów certyfikujących firmy Microsoft. W celu podniesienia swoich kwalifikacji, kandydaci mogą zdawać dodatkowe egzaminy certyfikujące dotyczące innych produktów firmy Microsoft, narzędzi programistycznych lub aplikacji biurowych.
- Osoby starające się o uzyskanie certyfikatu Microsoft Certified Solution Developer (MCSd) muszą zdać trzy egzaminy obowiązkowe i jeden do wyboru. Chcąc uzyskać certyfikat MCSd dla produktu Microsoft .NET należy zdać cztery egzaminy obowiązkowe i jeden do wyboru.
- Osoby starające się o uzyskanie certyfikatu Microsoft Certified Application Developer (MCAD) muszą zdać trzy egzaminy obowiązkowe i jeden do wyboru, który dotyczy obszaru specjalizacji.
- Osoby starające się o uzyskanie certyfikatu Microsoft Certified System Engineer (MCSE) muszą zdać pięć egzaminów obowiązkowych i dwa do wyboru.
- Osoby starające się o uzyskanie certyfikatu Microsoft Certified System Administrator (MCSA) muszą zdać trzy egzaminy obowiązkowe i jeden do wyboru, które zapewniają wiarygodną i pewną ocenę biegłości i umiejętności specjalistycznych.
- Osoby starające się o uzyskanie certyfikatu Microsoft Certified Database Administrator (MCBDA) muszą zdać trzy egzaminy obowiązkowe i jeden do wyboru, które zapewniają wiarygodną i pewną ocenę biegłości i umiejętności specjalistycznych.
- Osoby starające się o uzyskanie certyfikatu Microsoft Certified Trainer (MCT) muszą spełniać wymagania szkoleniowe i techniczne dotyczące każdego kursu Microsoft Official Curriculum, do przeprowadzania którego uzyskali certyfikat. Program certyfikatu MCT wymaga kontynuowania szkoleń, gdyż konieczne jest coroczne aktualizowanie certyfikatu. Dodatkowe informacje o możliwości uzyskania certyfikatu MCT można znaleźć na stronie <http://www.microsoft.com/traincert/mcp/mct/> lub kontaktując się z najbliższym ośrodkiem regionalnym.

Wsparcie techniczne

Podczas opracowywania niniejszej pozycji szczególny nacisk został położony na zachowanie precyzji sformułowań i zawartości książki oraz dołączonego dysku CD-ROM. Jeśli macie Państwo uwagi, pytania lub pomysły dotyczące tej książki i dysku CD-ROM, prosimy je przysyłać za pomocą poczty elektronicznej lub tradycyjnej na podane poniżej adresy:

Adres e-mail: tkinput@microsoft.com
 Adres pocztowy: Microsoft Press
Attn: MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Editor One
 Microsoft Way Redmond, WA 98052-6399

W celu wyszukania dodatkowych informacji związanych z tą książką i dyskiem CD-ROM (wliczając w to odpowiedzi na najczęściej zadawane pytania o instalacji i wykorzystaniu), można odwiedzić witrynę Microsoft Press Technical Support Web o adresie: <http://www.microsoft.com/mspress/support/>. Aby bezpośrednio skierować pytanie do działu Microsoft Press Knowledge Base, należy odwiedzić witrynę o adresie <http://www.microsoft.com/mspress/support/search.asp>. Z kolei informacje dotyczące oprogramowania firmy Microsoft znaleźć można pod adresem <http://support.microsoft.com/>.

Wsparcie testowego wydania oprogramowania

180-dniowe wydanie testowe, dostarczane wraz z zestawem przygotowawczym jedynie dla oceny produktu i ćwiczeń praktycznych, nie jest pełnym produktem oferowanym w sprzedaży. Wsparcie techniczne firmy Microsoft nie obejmuje tego produktu.

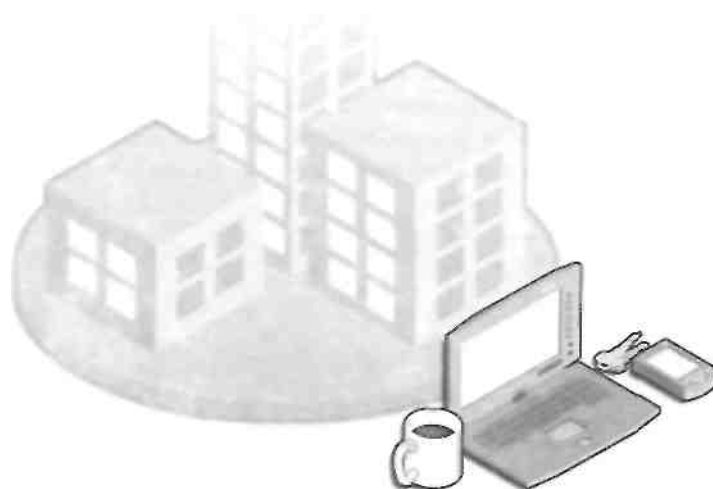


Uwaga Wersja testowa serwera Windows Server 2003 zamieszczona na dysku CD-ROM nie powinna być używana na głównych komputerach produkcyjnych. Wersja ta nie posiada wsparcia technicznego. W sieci Internet można uzyskać informacje o obsłudze pełnej wersji serwera Windows Server 2003 Enterprise Edition, które mogą być również stosowane dla wersji testowej. Informacje te można znaleźć pod adresem <http://support.microsoft.com/>.

Wszystkie informacje dotyczące wykorzystywania w zestawie szkoleniowym wersji testowej systemu kierowane są do działu wsparcia technicznego witryny Microsoft Press Web (<http://www.microsoft.com/mspress/support/>).

Część I

Samodzielna nauka



Wprowadzenie

do Windows Server 2003

Niniejszy rozdział nie zawiera zadań objętych egzaminem. Po części zaznajamiającej z rodziną produktów Windows Server 2003, w rozdziale tym opisane zostały pewne zagadnienia konfiguracji i instalacji wybrane pod kątem wymagań egzaminu certyfikującego 70-290.

Cele rozdziału

Zadaniem książki jest prawidłowe przygotowanie czytelnika do zarządzania i utrzymania środowiska Windows Server 2003 oraz do skutecznego przygotowania do egzaminu certyfikującego 70-290. Pomimo, że student posiada doświadczenie przy korzystaniu z technologii systemów Microsoft Windows, rodzina Windows Server 2003 i usługa katalogowa Microsoft Active Directory może okazać się stosunkowo nowym zagadnieniem. Dlatego celem tego rozdziału jest zapoznanie z różnymi wersjami i wydaniem Windows Server 2003 tak, aby jasne stały się podstawowe różnice między nimi i możliwości łączenia wersji, mające na celu lepsze spełnienie wymagań danej organizacji. W drugiej części czytelnik zostanie zapoznany z procesem instalacji i konfiguracji komputera systemu Windows Server 2003 działającego jako kontroler domeny usługi Active Directory.

Lekcje rozdziału:

- Lekcja 1: Rodzina Windows Server 2003 14
- Lekcja 2: Instalacja i konfiguracja Windows Server 2003 i usługi Active Directory 18

Wymagania

Rozdział ten opisuje kroki wymagane do skonfigurowania komputera działającego pod kontrolą systemu Windows Server 2003. Po skonfigurowaniu, komputer będzie można wykorzystywać do ćwiczeń praktycznych zamieszczonych w tym zestawie szkoleniowym. Komputer powinien być wyposażony w co najmniej jeden dysk twardy, który można wyczyścić i użyć do zainstalowania Windows Server 2003.

Lekcja 1: Rodzina Windows Server 2003

Serwer Windows Server 2003 jest systemem bardziej bezpiecznym, bardziej niezawodnym, bardziej dostępnym i łatwiejszym w administrowaniu niż poprzednie wersje systemu Windows. Przedstawiony zostanie dokładniejszy opis platformy i porównania z systemem Microsoft Windows 2000. Lekcja ta stanowi skrótowy przegląd rodziny Windows Server 2003 skupiający się na przedstawieniu różnic między wersjami produktu: Web Edition, Standard Edition, Enterprise Edition oraz Datacenter Edition.

Materiały omówione podczas lekcji pozwalają na

- Rozpoznawanie podstawowych różnic między wersjami systemu Windows Server 2003

Szacunkowy czas lekcji: 5 minut

Wersje systemu Windows Server 2003

Serwer Windows Server 2003 jest stopniową aktualizacją platformy i technologii wprowadzonych w systemie Windows 2000. Dla osoby znającej serwer Windows 2000 przejście do nowego systemu będzie relatywnie proste, natomiast dla osób mających doświadczenia nabyte podczas pracy z systemem Windows NT 4 będzie to zupełnie nowy świat.

Ta stopniowa aktualizacja może być jednak myląca. Aktualizacje poparte są znaczącymi i długo oczekiwanymi usprawnieniami w zabezpieczeniach oraz niezawodności systemu operacyjnego i zestawu narzędzi administracyjnych. W wielu książkach w tym miejscu przedstawiana jest lista nowych funkcji. I rzeczywiście, lista funkcji Windows Server 2003 jest imponująca i na podstawie tych cech, prawie dla każdego administratora wybór systemu staje się sprawą oczywistą. Jednakże trzeba zdawać sobie sprawę, że poszczególne funkcje nie muszą być tak samo atrakcyjne dla każdego fachowca branży IT.

W rozdziale objaśnione zostaną istotne cechy i usprawnienia usługi Active Directory, nowe narzędzia obsługi popularnych, a jednocześnie złożonych obiektów GPO, poprawione zabezpieczenia systemu, ulepszone usługi terminalowe oraz szereg innych rozszerzonych bądź poprawionych cech nowego systemu operacyjnego. Jeśli użytkownik rozważa przejście do systemu Windows Server 2003, powinien dobrze zapoznać się z tą platformą odwiedzając witrynę Microsoft Web pod adresem <http://www.microsoft.com/winowdsserver2003> i samemu ocenić, które ulepszenia są najbardziej dla niego istotne.

Niezależnie od długiej listy nowych cech systemu, jego ocenianie staje się jeszcze bardziej atrakcyjne ze względu na to, że system Windows Server 2003 występuje w wersji 32-bitowej, 64-bitowej oraz wbudowanej. Jednak najważniejsze różnice występują między czterema wersjami wymienionymi poniżej w kolejności, która uwzględnia dostępność funkcji i cech, jak również cenę produktu.

- Windows Server 2003, Web Edition
- Windows Server 2003, Standard Edition
- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Datacenter Edition

Web Edition

Dla zapewnienia konkurencyjności systemu Windows Server 2003 w odniesieniu do innych serwerów sieci Web, firma Microsoft opracowała okrojoną, jednakże odpowiednio wyposażoną wersję serwera, specjalnie zaprojektowanego dla usług sieci Web. Zestaw cech i licencjonowanie umożliwia klientom prostą instalację stron, witryn, aplikacji i usług sieci Web.

Wersja Web Edition obsługuje 2 gigabajty (GB) pamięci RAM i dwa procesory w trybie symetrycznego przetwarzania (SMP). Zapewnia nieograniczoną liczbę połączeń anonimowych w sieci Web, przy czym obsługiwanych jest tylko 10 wejściowych połączeń SMB (Serwer Message Block, blok komunikatów serwera), co powinno być w zupełności wystarczające do publikowania danych. Serwer nie może być bramą do Internetu, serwerem DHCP lub serwerem faksów. Pomimo, że serwer może być administrowany zdalnie za pomocą programu Rcmote Desktop (Pulpit zdalny), nie może być serwerem terminali w tradycyjnym znaczeniu. Serwer może należeć do domeny, ale nie może być kontrolerem domeny. Dołączona wersja mechanizmów serwera bazy danych Microsoft SQL Server Databasc Engine może obsługiwać do 25 jednoczesnych połączeń.

Standard Edition

System Windows Server 2003 Standard Edition to mocny, przeznaczony do realizacji różnych zastosowań serwer. W małych i średniej wielkości przedsiębiorstwach może pracować jako serwer katalogów, plików, druku, aplikacji, serwer multimedialny i sieci Web. Jego rozszerzony zestaw funkcji można porównać do systemu Windows 2000 wraz z serwerem MSDE (Microsoft SQL Server Databasc Engine), który obsługuje do 5 jednoczesnych połączeń do bazy danych o rozmiarach do 2 GB, wraz z darmową usługą POP3 (Post Office Protocol wersja 3), która w połączeniu z dołączoną usługą SMTP (Simple Mail Transfer Protocol) umożliwia uruchomienie niedużego, autonomicznego serwera poczty oraz wraz z usługą równoważenia obciążenia sieci (NBL), która jest przydatnym narzędziem dołączanym jedynie w wersji Advanced Server systemu Windows 2000.

Wersja Standard Edition systemu Windows Server 2003 obsługuje do 4 GB pamięci RAM i cztery procesory (SMP).



Informacja W wersji RC 1 (Release Candidate) systemu Windows Server 2003, wersja beta i wersja zapoznawcza kodu programu obsługiwała tylko dwa procesory. Ograniczenie to zostało usunięte w wersji RC2, tak więc wersja Standard Edition obsługuje cztery procesory. Dokumentacja, która powstała przed pojawieniem się tej wersji może zawierać błędne informacje dotyczące obsługi SMP.

Enterprise Edition

Wersja Enterprise Edition systemu Windows Server 2003 zaprojektowana została jako wydajna platforma serwerowa dla średnich i dużych przedsiębiorstw. Ze względu na przeznaczenie (dla przedsiębiorstw), serwer umożliwia obsługę do 8 procesorów, 32 GB pamięci RAM, klastry składające się z ośmiu węzłów (wliczając w to klastry oparte na technologii Storage Area Network — SAN oraz klastry rozproszone geograficznie). Serwer może być uruchamiany na komputerach bazujących na 64-bitowym procesorze Intel Itanium i w takim przypadku serwer obsługuje do 64 GB pamięci RAM i 8 procesorów.

Poniżej wymienione zostały inne cechy odróżniające wersję Enterprise od wersji Standard:

- Usługi MMS (Microsoft Metadirectory Services), które umożliwiają integrację z usługą Active Directory wielu katalogów, baz danych i plików.
- Usługa Hot Add Memory, która pozwala dodawać pamięć do obsługiwanego urządzenia sprzętowego bez wyłączania i ponownego uruchamiania serwera.
- Usługa WRM (Windows System Resource Manager), która obsługuje przydział zasobów procesora i pamięci w odniesieniu do poszczególnych aplikacji.

Datacenter Edition

Wersja Datacenter Edition jest dostępna jedynie jako wersja OEM razem w pakiecie z wysokiej klasy sprzętem (serwerem). Serwer ten zapewnia prawie nieograniczone możliwości skalowania, czyli obsługę 32-bitowych platform z 32 procesorami (SMP) i 64 GB pamięci RAM oraz obsługę 64-bitowych platform z 64 procesorami i 512 GB pamięci RAM. Istnieje także wersja dla 128 procesorów (SMP), która obsługuje dwie 64 kanałowe partycje SMP.

64-Bit Editions

Wersje 64-bitowe Windows Server 2003, uruchamiane na komputerach Intel Itanium, w porównaniu do 32-bitowych wersji Windows opracowane zostały dla szybszych procesorów i szybciej wykonywanych operacji zmiennoprzecinkowych. Ulepszone kodowanie CPU i usprawnione przetwarzanie przyniosło znaczące przyspieszenie operacji obliczeniowych. Zwiększona prędkość dostępu do ogromnej przestrzeni adresowej pamięci pozwala na płynne działanie złożonych i intensywnie wykorzystujących zasoby aplikacji, takich jak masowe aplikacje bazodanowe, aplikacje dotyczące analiz naukowych czy silnie obciążone serwery sieci Web.

Niektóre funkcje wersji 32-bitowych nie są dostępne w wersjach 64-bitowych. W szczególności, wersje 64-bitowe nie obsługują 16-bitowych aplikacji Windows, aplikacji czasu rzeczywistego, aplikacji POSIX i usług drukowania klientów systemu Apple Macintosh.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Planujesz zainstalowanie komputerów systemu Windows Server 2003 w dziale zatrudniającym 250 pracowników. Serwer ma przechowywać katalogi domowe i współużytkowane dla danego działu oraz ma obsługiwać kilka drukarek używanych w dziale. Która wersja Windows Server 2003 stanowi najodpowiedniejsze rozwiązanie dla tego działu?
2. Planujesz zainstalowanie komputerów systemu Windows Server 2003 w nowej domenie usługi Active Directory w dużej korporacji, w której znajduje się wiele oddzielnych usług Active Directory zarządzanych przez filie korporacji. Firma zdecydowała, że Exchange Server 2003 będzie dla

wszystkich filii jednolitą platformą komunikacji oraz że usługa MMS (Microsoft Metadirectory Services) będzie używana do synchronizacji odpowiednich właściwości obiektów w całej organizacji. Która wersja Windows Server 2003 stanowi najodpowiedniejsze rozwiązanie dla takiej instalacji??

3. Planowane jest zainstalowanie serwerów zapewniających dostęp przez sieć Internet do aplikacji typu e-commerce. Przewidywane jest zainstalowanie 4 serwerów dla aplikacji Web oraz jednego dla silnej, aktywnie wykorzystywanej bazy danych. Która wersja Windows Server 2003 stanowi najodpowiedniejsze rozwiązanie?

Podsumowanie lekcji

- System Windows Server 2003 jest dostępny w wersjach 32-bitowych i 64-bitowych.
- Główne różnice między wersjami systemu Windows Server 2003 odzwierciedlają edycje produktu: Web Edition, Standard Edition, Enterprise Edition oraz Datacenter Edition.
- Mówiąc ogólnie, system Windows Server 2003 jest aktualizacją systemu Windows 2000. Jednak wprowadzone ulepszenia cech oraz zabezpieczeń systemu są znaczące i łatwo przekonać się, że poszczególne aktualizacje stanowią istotne usprawnienie środowiska.

Lekeja 2: Instalacja i konfiguracja Windows Server 2003 i usługi Active Directory

Zadania egzaminu 70-290 dotyczą głównie zarządzania i utrzymania środowiska Windows Server 2003, natomiast mniejszy nacisk położony został na samą usługę Active Directory. Co prawda niektóre z zadań odnoszą się do zagadnień administracji obiektami usługi Active Directory, a w szczególności dotyczy to obiektów takich jak użytkownicy, grupy, komputery, drukarki i współużytkowane foldery. W niniejszym rozdziale szczegółowo omówione są zadania egzaminacyjne, a ćwiczenia praktyczne stanowią ważny element w procesie nauki. Ćwiczenia te wymagają, by student skonfigurował kontroler domeny działający pod kontrolą systemu Windows Server 2003. Jeśli konfiguracja kontrolera domeny i tworzenie podstawowych grup, użytkowników czy kont komputera nie sprawia kłopotu, niniejszą lekcję można pominąć. Natomiast przy słabym opanowaniu usługi Active Directory, lekcja ta powinna dostarczyć wystarczających podstaw do zgłębiania systemu Windows Server 2003.

Materiały omówione podczas lekcji pozwalają na

- Zainstalowanie systemu Windows Server 2003
- Zapoznanie się z podstawowymi strukturami i pojęciami usługi Active Directory
- Utworzenie kontrolera domeny
- Utworzenie obiektów usługi Active Directory wliczając w to .. . grupy jednostki organizacyjne (OU)

Szacunkowy czas lekcji: 60 minut

Instalacja i konfiguracja Windows Server 2003

Każdy doświadczony fachowiec branży IT z pewnością spędził wiece godzin podczas instalowania platform systemów Windows. Poniżej wymienione zostały niektóre ważne bądź poprawione kwestie dotyczące instalowania Windows Server 2003:

- **Instalacja z rozruchowego dysku CD-ROM** Większość administratorów przyzwyczaiła się do wprowadzonego w późnych latach 90-tych sposobu instalowania systemu operacyjnego z rozruchowego dysku CD-ROM. W systemie Windows Server 2003 zachowana została ta metoda i serwer może zostać zainstalowany bezpośrednio z dysku CD-ROM. Jednakże zmieniona została jedna cecha: brak możliwości uruchamiania instalacji z dysłdetek.
- **Podczas instalacji ulepszony został graficzny interfejs użytkownika (GUI)** Podczas instalacji system Windows Server 2003 używa interfejsu GUI przypominającego interfejs zastosowany w systemie Windows XE W ten sposób znacznie przejrzystiej prezentowany jest stan instalacji oraz czas potrzebny do jej zakończenia.
- **Aktywacja produktu** Wersje testowe i detaliczne Windows Server 2003 wymagają aktywacji produktu. Programy licencjonowania, takie jak Open License, Select License bądź Enterprise Agreement, nie wymagają aktywacji.

Kolejne kroki instalowania systemu Windows Server 2003 przedstawione zostały w ćwiczeniu 1.

Po zainstalowaniu i aktywacji systemu Windows, można skonfigurować serwer za pomocą dobrze przemyślanej strony Manage Your Server (**Zarządzanie tym serwerem**), której wygląd pokazany został na rysunku 1-1. Strona ta jest automatycznie uruchamiana podczas logowania. Strona ułatwia instalację określonych usług, narzędzi i konfigurację podstawowych ról serwera. Po kliknięciu opcji Add Or Remove A Role (Dodaj lub usuń rolę), pojawia się okno Configure Your Server Wizard (Kreator konfigurowania serwera).



Rysunek 1-1. Strona Manage Your Server (Zarządzanie tym serwerem)

Jeśli użytkownik wybierze opcję Typical Configuration For A First Server (Typowa konfiguracja dla pierwszego serwera), moduł Configure Your Server Wizard (Kreator konfigurowania serwera) skonfiguruje serwer jako kontroler domeny w nowej domenie, zainstaluje usługę Active Directory i jeśli potrzeba zainstaluje usługi DNS (Domain Name System, system nazw domen), DHCP (Dynamic Host Configuration Protocol) i RRAS (Routing And Remote Access).

Jeśli użytkownik wybierze opcję Custom Configuration (Konfiguracja niestandardowa). Za pomocą modułu Configure Your Server Wizard (Kreatora konfiguracji serwera) można skonfigurować następujące role:

- **Serwer plików** Stanowi dogodny, scentralizowany dostęp do plików i katalogów dla poszczególnych użytkowników, departamentów czy całej organizacji. Wybierając te opcje będziemy mieć możliwość zarządzania przestrzenią dyskową użytkownika (poprzez blokowanie i konfigurowanie przydziałów dysku oraz możliwość poprawy wydajności wyszukiwania w systemie plików poprzez aktywowanie usługi indeksowania).
- **Serwer druku** Umożliwia dostęp do centralnego zarządzania urządzeniami drukującymi dzięki udostępnianiu współużytkowanych drukarek i sterowników komputerom klientów. Wybranie tej opcji uruchamia program Add Printer Wizard (Kreator dodawania drukarek) pozwalający zainstalować drukarki i odpowiednie ich sterowniki systemu Windows. W tym samym czasie instalowana jest również usługa Internet Information Services 6.0 (Internetowe usługi informacyjne) konfigurowany protokół IPP (Internet Printing Protocol) oraz instalowane są narzędzia administracyjne bazujące na mechanizmach sieci Web.

- **Serwer aplikacji (IIS, ASP.NET)** Udostępnia komponenty infrastruktury wymagane do obsługi utrzymania aplikacji sieci Web. Rola ta instaluje i konfiguruje również aplikacje IIS, ASP.NET i **COM+**.
- **Serwer poczty (POP3, SMTP)** Instaluje protokoły POP3 i SMTP tak, aby serwer mógł działać jako serwer wiadomości e-mail dla klientów POP3.
- **Serwer terminali** Udostępnia wielu użytkownikom aplikacje i zasoby serwera, takie jak drukarki czy magazyn, tak jakby aplikacje te bądź zasoby zainstalowane były na ich własnych komputerach. Użytkownicy łączą się poprzez klienta programu Terminal Services (Usługi terminalowe) lub Remote Desktop (Pulpit zdalny). W odróżnieniu od systemu Windows 2000, Windows Server 2003 automatycznie udostępnia dla administracji moduł Remote Desktop (Pulpit zdalny). Rola serwera terminali wymagana jest jedynie wtedy, kiedy dla użytkowników utrzymywane są aplikacje na serwerze terminali.
- **Remote Access/VPN Server (Serwer dostępu zdalnego/sieci VPN)** Udostępnia routing wielo-protokołowy i usługi dostępu zdalnego dla połączeń telefonicznych, sieci lokalnych LAN oraz sieci rozległych WAN. Połączenia prywatnych sieci wirtualnych (VPN) umożliwiają użytkownikom i witrynom zdalnym bezpieczne połączenia do sieci przy użyciu standardowych połączeń internetowych.
- **Kontroler domeny (Active Directory)** Udostępnia klientom sieci usługi katalogowe. Opcja ta konfiguruje kontroler domeny w nowej lub istniejącej domenie oraz instaluje DNS. Wybranie tej opcji uruchamia program Active Directory Installation Wizard (Kreator usługi Active Directory).
- **Serwer DNS** Umożliwia rozpoznawanie nazw hostów dzięki translacji nazw hostów na adresy IP (wyszukiwanie w przód) oraz translacji adresów IP na nazwy hostów (wyszukiwanie wsteczne). Wybranie tej opcji instaluje usługi DNS, a następnie uruchamia program Configurat A DNS Server Wizard (Kreator serwera DNS).
- **Serwer DHCP** Udostępnia usługi automatycznej adresacji IP dla klientów, którzy wybrali funkcję dynamicznego przydzielania adresu IP. Wybranie tej opcji instaluje usługi DHCP, a następnie uruchamia program New Scope Wizard (Kreator nowego zakresu), który umożliwia zdefiniowanie w sieci jednego lub kilku zakresów **IP**.
- **Serwer multimediów strumieniowych** Udostępnia usługi WMS (Windows Media Services). Usługi WMS pozwalają serwerowi przysyłać multimedialne dane przez sieć intranet lub Internet. Dane mogą być przechowywane i dostarczane na żądanie lub dostarczane w czasie rzeczywistym. Wybranie tej opcji instaluje usługi WMS.
- **Serwer WINS** Umożliwia rozpoznawanie nazw komputerów dzięki translacji nazw NetBIOS na adresy IP. Instalowanie serwera WINS nie jest konieczne, chyba że obsługiwane mają być starsze systemy operacyjne, takie jak Windows 95 czy Windows NT. Systemy Windows 2000 i Windows XP nie wymagają zainstalowania usługi WINS, chociaż starsze aplikacje zainstalowane na tych platformach mogą do prawidłowego działania potrzebować serwera WINS. Wybranie tej opcji instaluje serwer WINS.

Aby przeprowadzić wszystkie ćwiczenia praktyczne zamieszczone w książce, należy skonfigurować komputer jako SerwerOl, działający jako kontroler domeny w domenie contoso.com. Poszczególne kroki konfigurowania serwera w roli kontrolera domeny za pomocą programu Configure Your Server Wizard (Zarządzanie tym serwerem) zostały przedstawione w Ćwiczeniu 2 na końcu lekcji.

Usługa Active Directory

Wiele książek zostało poświęconych planowaniu, implementacji i obsłudze usługi Active Directory. Osoby zaznajomione z usługą łatwo rozpoznają, że poniższe opisy są uproszczone jedynie dlatego, że omówienie każdego szczegółu tego zagadnienia zajmuje wiele czasu i miejsca. Celem tego rozdziału jest przekazanie tych informacji, które są potrzebne na egzaminie 70-290.

Sieci, usługi katalogowe i kontrolery domen

Sieci powstały w dniu, kiedy pierwszy użytkownik zdecydował, że nie ma ochoty przechodzić przez korytarz, aby pobrać pewne dane od innego użytkownika. W końcu sieci są wszystkim, co związane jest z udostępnianiem zdalnym zasobów. Zasoby te to najczęściej pliki, foldery i drukarki. Z czasem lista zasobów wydłużyła się, a najbardziej znaczące z nich to wiadomości e-mail, bazy danych czy aplikacje. W związku z tym musi istnieć pewien mechanizm śledzenia tych zasobów, ich udostępniania oraz co najmniej katalog użytkowników i grup, aby zasoby mogły być zabezpieczane przed niepożądanym dostępem.

Sieci systemów Microsoft Windows obsługują dwa modele usług katalogowych: grupy robocze i domeny. Model domeny jest z pewnością najbardziej powszechny dla implementacji systemu Windows Server 2003 w przedsiębiorstwach. Model domeny charakteryzuje się pojedynczym katalogiem zasobów przedsiębiorstwa — usługą Active Directory — do której zaufanie mają wszystkie systemy zabezpieczeń należące do domeny. Dzięki temu, systemy te mogą korzystać z katalogu bezpiecznych podmiotów (użytkownik, grupa, konto komputera), aby zabezpieczać ich zasoby. Usługa Active Directory działa jako magazyn identyfikacyjny, udostępniający pojedynczą listę zaufania, opisującą w domenie kto jest kim.

Usługa Active Directory jest jednak czymś więcej niż tylko bazą danych. Jest zbiorem obsługiwanych plików, wliczając w to dzienniki transakcji i wolumen systemu (lub Sysvol), który zawiera skrypty logowania i informacje o zasadach grupy. Jest też serwisem, który obsługuje i korzysta z bazy danych, wliczając w to protokół LDAP (Lightweight Directory Access Protocol), protokół zabezpieczeń Kerberos, procesy replikacji i usługę FRS (File Replication Service). Baza danych i jej usługi instalowane są na jednym lub kilku kontrolerach domen. Kontroler domeny jest serwerem, który został przeznaczony do tej funkcji przez uruchomienie programu Active Directory Installation Wizard (Instalacja usługi Active Directory), przez wprowadzenie w wierszu poleceń rozkazu DCPROMO lub, tak jak jest realizowane w ćwiczeniu 2, przez uruchomienie Configure Your Server Wizard (Kreator konfigurowania serwera). Jeśli dany serwer staje się kontrolerem domeny, przechowuje kopie lub repliki usługi Active Directory oraz zmienia bazę danych, a zmiany te replikowane są do każdego kontrolera domeny.

Domeny, drzewa i lasy

Usługa Active Directory nie może istnieć bez co najmniej jednej domeny i vice versa. Domena jest główną jednostką administracyjną usługi katalogowej Windows Server 2003. W usłudze Active Directory przedsiębiorstwo może mieć kilka domen. Model wielu domen tworzy strukturę logiczną nazwaną drzewami, gdzie zachowana jest ciągłość nazw DNS. Na przykład nazwy contoso.com, us.contoso.com oraz europe.contoso.com współużytkują ciągłą przestrzeń nazw DNS i dlatego mogą być traktowane jako drzewo.

Jeśli domeny usługi Active Directory nie współdzielą jednej domeny głównej, to tworzą wiele drzew. Powstaje w ten sposób największa struktura usługi Active Directory: las. Las usługi Active Directory

zawiera wszystkie domeny tej usługi. Las może zawierać wiele domen w wielu drzewach lub tylko jedną domenę. Jeśli istnieją co najmniej dwie domeny, znaczenia nabiera ciment usługi Active Directory nazwany Global Catalog (Katalog globalny), ponieważ udostępnia on informacje o obiektach znajdujących się w innych domenach lasu.

Obiekty i jednostki organizacyjne (OU)

Zasoby przedsiębiorstwa są przedstawiane w usłudze Active Directory jako obiekty lub rekordy bazy danych. Każdy obiekt ma atrybuty lub właściwości, które go definiują. Przykładowo obiekt użytkownika zawiera nazwę użytkownika i hasło, a obiekt grupy zawiera nazwę grupy i listę jej członków.

W celu utworzenia obiektu usługi Active Directory należy otworzyć konsolę Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) znajdującą się w grupie programów Administrative Tools (Narzędzia administracyjne). Następnie należy rozwinąć domenę, aby wyświetlone zostały jej kontenery i jednostki OU. Wskazany kontener lub jednostkę OU należy kliknąć prawym przyciskiem myszy i wybrać opcję New object_type (Nowy typ obiektu).

Usługa Active Directory może przechowywać miliony obiektów, takich jak użytkownicy, grupy, komputery, drukarki, współużytkowane foldery, witryny, odsyłacze do witryn, obiekty GPO — Group Policy Object (obiekt zasad grupy), a nawet strefy DNS i rekordy hosta. Łatwo można sobie wyobrazić, że bez pewnego rodzaju struktury, dostęp i zarządzanie katalogiem byłoby koszmarem.

Struktura jest funkcją określonego typu obiektu nazwanego jednostką organizacyjną lub w skrócie OU. Wewnątrz domeny jednostki OU są kontenerami, które umożliwiają grupowanie obiektów o wspólnej administracji lub konfiguracji. Jednostki OU mają jednak większe możliwości niż organizowanie obiektów usługi Active Directory. Udostępniają ważne funkcje administracyjne — są punktem, z którego funkcje administracyjne mogą być delegowane oraz do którego odnoszone mogą być zasady grupy.

Delegowanie

Delegowanie administracji dotyczy prostego pomysłu wynikającego z potrzeby, by wybrany administrator mógł zmienić hasło pewnej podgrupy użytkowników. Każdy obiekt usługi Active Directory (w tym przypadku obiektami są użytkownicy) zawiera kontrolną listę dostępu (ACL), która definiuje uprawnienia obiektu, tak samo jak pliki woluminu dyskowego mają listy ACL, które określają dostęp do tych plików. Na przykład, lista ACL obiektu użytkownika będzie definiować, które grupy mogą wyczyścić jego hasło. Przydzielanie uprawnień administratorowi tak, aby mógł zmieniać osobno hasło każdego użytkownika, jest trochę skomplikowane. Zamiast tego można umieścić wszystkich tych użytkowników w pojedynczej jednostce OU i przydzielić temu administratorowi uprawnienia umożliwiające zmianę hasła jednostki OU. Uprawnienia te będą dziedziczone przez wszystkie obiekty użytkownika tej jednostki OU, dzięki czemu administrator będzie mógł modyfikować uprawnienia wszystkich użytkowników.

Usunięcie haseł użytkownika jest tylko jednym przykładem delegowania administracji. Istnieją tysiące kombinacji uprawnień, które mogą być przydzielane do grup administrujących i obsługujących usługę Active Directory. Jednostki organizacyjne OU pozwalają w przedsiębiorstwie aktywnie odzwierciedlać jego model administracji i określać przez kogo i w jaki sposób mogą być modyfikowane obiekty domeny-

Group Policy (Zasady grupy)

Jednostki organizacyjne są również wykorzystywane do gromadzenia obiektów — komputerów i użytkowników, które są w podobny sposób konfigurowane. Dowolna konfiguracja wprowadzona do systemu może być zarządzana centralnie dzięki właściwości usługi Active Directory nazwanej Group Policy (Zasada grupy). Zasada grupy pozwala określić ustawienia zabezpieczeń, instalowane oprogramowanie oraz konfigurować zachowanie systemu operacyjnego i aplikacji bez dotykania komputera. Po prostu wprowadza się daną konfigurację do obiektu GPO.

Obiekty GPO są zbiorem setek możliwych ustawień konfiguracji od uprawnień użytkownika po oprogramowanie, które można uruchamiać na danym systemie. Obiekt GPO jest powiązany do kontenera wewnątrz usługi Active Directory, najczęściej do jednostki OU, chociaż mogą to być także domeny lub nawet witryny. Ustawienia zawarte w obiekcie GPO dotyczą wszystkich użytkowników i komputerów znajdujących się „poniżej” kontenera (powiązanego z obiektem GPO).

Prawdopodobnie podczas egzaminu 70-290 znajdą się odniesienia do obiektu Group Policy (zasady grupy). Należy pamiętać, że obiekt ten jest narzędziem, dzięki któremu konfiguracja może być wprowadzana centralnie, że niektóre ustawienia dotyczą jedynie komputerów, a niektóre jedynie użytkowników oraz że zasada dotyczy tylko tych komputerów i użytkowników, którzy znajdują się „poniżej” jednostki OU, z którą zasadą jest powiązana.

Lektura uzupełniająca

Jak już było wcześniej nadmienione, usługa Active Directory jest dużym i złożonym zagadnieniem, które zasługuje na poważne potraktowanie przed przystąpieniem do wprowadzenia systemu Windows Server 2003 jako kontrolera domeny. Dlatego też rekomendowane jest przeczytanie wymienionych poniżej tytułów wydawnictwa Microsoft Press:

- *Active Directory for Microsoft Windows Server 2003 Technical Reference*
- *MCSE Zestaw szkoleniowy (Exam 70-294): Planowanie, wdrażanie i obsługa infrastruktury Active Directory Windows Server 2003*

Zadanie praktyczne: Instalacja Windows Server 2003

Ćwiczenie praktyczne obejmuje wykonanie konfiguracji komputera niezbędnej do uruchomienia systemu Windows Server 2003 oraz skonfigurowanie serwera tak, aby stał się kontrolerem domeny w domenie contoso.con.

Ćwiczenie 1: Instalacja Windows Server 2003

Ćwiczenie to powinno być wykonywane na komputerze, który jest kompatybilny z systemem Windows Server 2003. Zakłada się, że podstawowy dysk twardy systemu jest pusty. Jeśli dysk ten ma już skonfigurowane partycje, należy zmodyfikować ćwiczenie tak, aby odpowiadało konfiguracji systemu.

1. Skonfiguruj program BIOS komputera lub kontrolera dysku tak, aby system uruchamiał się z dysku CD-ROM. Szczegółowe informacje na ten temat zawiera dokumentacja urządzeń sprzętu.
2. Włóż do napędu instalacyjny dysk CD-ROM systemu Windows Server 2003 i ponownie uruchom komputer.

- , 3. Jeśli podstawowy dysk nie jest pusty, wyświetla się komunikat informujący, że wciśnięcie dowolnego przycisku klawiatury spowoduje uruchomienie komputera z dysku CD-ROM. Jeśli pojawi się taki komunikat, naciśnij dowolny przycisk klawiatury.

Na początku uruchamiania komputera pojawia się informacja o sprawdzaniu konfiguracji systemu, a następnie wyświetlone zostaje okno programu instalacyjnego.

4. Jeśli do pracy komputera potrzebne są specjalne sterowniki pamięci masowej, które nie znajdują się w zestawie sterowników Windows Server 2003, naciśnij przycisk F6 w momencie, kiedy program instalacyjny wyświetla odpowiedni komunikat i udostępnia potrzebne sterowniki.
5. System podpowiada, że wciśnięcie przycisku F2 spowoduje wykonanie procedury automatycznego odzyskiwania systemu *ASR (Automatic System Recovery)*. ASR jest nową funkcją Windows Server 2003. Zastąpiła ona funkcję tworzenia dysku ratunkowego (*Emergency Disk Repair*), która występowała w poprzedniej wersji serwera Windows. Właściwości funkcji ASR zostały opisane w rozdziale 13. Na tym etapie instalacji nie należy naciskać F2, program instalacyjny będzie kontynuował swoje działanie.

Należy zwrócić uwagę, że szary pasek statusu na dole ekranu wskazuje, że komputer jest sprawdzany, a pliki pobierane. Operacje te są wymagane do uruchomienia minimalnej wersji systemu operacyjnego.

6. Jeśli instalowana jest wersja testowa Windows Server 2003, program instalacyjny powiadomi o tym. Przeczytaj odpowiednie komunikaty i aby kontynuować naciśnij **Enter**.

Wyświetlony zostanie ekran zapraszający do instalacji systemu.

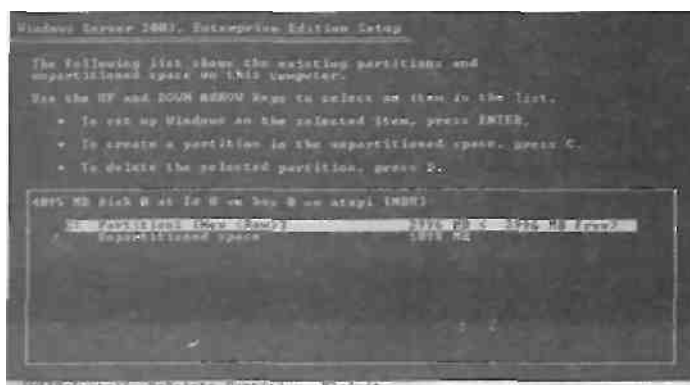
Należy zauważyć, że oprócz wykonania nowej instalacji systemu operacyjnego, użytkownik może użyć programu instalacyjnego do naprawy uszkodzonej instalacji. Program *Recovery Console* (Konsola odzyskiwania) opisany został w rozdziale 13.

7. Po przeczytaniu komunikatów ekranu, naciśnij przycisk **Enter**, aby kontynuować. Program instalacyjny wyświetli ekran akceptacji warunków licencji produktu.
8. Treść umowy licencyjnej można przeczytać przewijając ekran do dołu za pomocą przycisku PAGE DOWN.
9. Naciśnij przycisk F8, aby zaakceptować warunki licencji.

Wyświetlony zostanie ekran instalacji Windows Server 2003 i użytkownik poproszony zostanie o wybranie wolnej przestrzeni dyskowej lub istniejącej partycji, na której zainstalowany zostanie system operacyjny. W tym kroku program instalacyjny umożliwia tworzenie i usuwanie partycji dysku twardego.

Aby wykonać ćwiczenia zamieszczone w książce, należy skonfigurować partycję większą niż przestrzeń potrzebna do zainstalowania samego systemu operacyjnego (zalecana minimalna wielkość to 3 GB) oraz pozostawić co najmniej 1 GB nieprzydzielonej przestrzeni dyskowej. W następnych punktach zakłada się, że dysponujemy pustym dyskiem o pojemności co najmniej 4 GB. Użytkownik może wprowadzić korekty, które odpowiednio przystosują jego system.

10. Naciśnij C, aby utworzyć partycję.
11. Aby utworzyć partycję 3 GB wpisz wartość 3072 w polu Create Partition Of Size (In MB) (Utwórz partycję o rozmiarze (w MB)), a następnie naciśnij **Enter**.
12. Upewnij się, że utworzone partycje są podobne do pokazanych na rysunku 1-2. Powtarzając, w ćwiczeniu zaleca się utworzenie na dysku C partycji o wielkości co najmniej 3 GB oraz pozostawienie 1 GB przestrzeni dysku, dla której nie określono partycji.



Rysunek 1-2. Partycje dysku twardego potrzebne podczas instalacji

13. Wybierz **C: Partycja 1 [New (raw)]** i naciśnij **Enter**, aby ją zainstalować.

Użytkownik **zostanie** poproszony o wybór systemu plików dla partycji.

14. Sprawdź, czy wybrana została opcja **Format partition using NTFS** (Sformatuj partycję używając systemu plików NTFS) i naciśnij **Enter**.

Program instalacyjny sformatuje partycję (NTFS), sprawdzi, czy na dyskach twardych nie występują błędy fizyczne, które mogą powodować, że instalacja nie zakończy się powodzeniem, skopiuje pliki na dysk twardy oraz rozpocznie instalację. Proces ten trwa kilka minut.

Na koniec, program instalacyjny wyświetli czerwony pasek statusu, który odlicza 15 sekund do momentu ponownego uruchomienia komputera i wprowadza tryb graficzny (GUI) do procesu instalacyjnego.

15. Po zakończeniu trybu tekstowego, system jest ponownie uruchamiany. Nie należy naciskać przycisków klawiatury, które powodują rozruch systemu z dysku CD-ROM.

Program instalacyjny Windows wyświetla graficzny interfejs użytkownika. W lewym oknie pokazywane są postępy instalacji. Zaznaczone są opcje **Collecting Information** (Zbieranie informacji), **Dynamic Update** (Aktualizacja dynamiczna) i **Preparing Installation** (Przygotowanie instalacji). Opcja Zbieranie informacji została zakończona przed wprowadzeniem trybu graficznego, a Aktualizacja dynamiczna nie jest używana podczas uruchamiania z dysku CD-ROM. W tym momencie system wykonuje działania związane z opcją Przygotowanie instalacji, czyli kopiuje pliki na dysk lokalny.

16. Na stronie **Regional And Language Options** (Opcje regionalne i językowe) wybierz ustawienia, które są odpowiednie dla języka i wymagań związanych z wprowadzaniem tekstów, a następnie kliknij przycisk **Next** (Dalej).



Wskazówka Ustawienia regionalne mogą być modyfikowane po zainstalowaniu systemu operacyjnego za pomocą modułu Regional And Language Options (Opcje regionalne i językowe) znajdującego się w programie Control Panel (Panel sterowania).

Program instalacyjny wyświetli stronę zatytułowaną *Personalize Your Software* (Spersonalizuj swoje oprogramowanie), w którym należy wprowadzić swoje nazwisko i nazwę organizacji.

MCSE Training Kit: Egzamin 70-290

17. W polu **Name** (Nazwisko) wprowadź swoje nazwisko; w polu **Organization** (Organizacja) wprowadź nazwę organizacji, a następnie kliknij przycisk **Next** (Dalej).
Wyświetlona zostanie strona wprowadzania klucza produktu.
18. Wprowadź klucz produktu, który jest zamieszczony na instalacyjnym dysku CD-ROM dla Windows Server 2003, a następnie kliknij przycisk **Next** (Dalej).
Program instalacyjny wyświetli okno dialogowe **Licensing Modes** (Tryby licencjonowania), za pomocą którego użytkownik wybiera odpowiedni tryb licencjonowania serwera.
19. Sprawdź, czy zaznaczony został tryb **Per Server Number Of Concurrent Connections** (Na serwer Liczba połączeń równoczesnych), a liczba połączeń to 5, a następnie kliknij przycisk **Next** (Dalej).



Ważne Opcja „Na serwer. Liczba połączeń równoczesnych.” i wartość 5 dla liczby równoczesnych połączeń są sugerowanymi ustawieniami, używanymi do zrealizowania tego kursu. Użytkownik powinien używać legalną liczbę równoczesnych połączeń określoną w oparciu o rzeczywiste posiadane licencje. Zamiast opcji Per Server (Na serwer), można wybrać inny tryb licencjonowania - Per Device Or Per User (Na urządzenie lub Na użytkownika).

Program instalacyjny wyświetla stronę **Computer Name And Administrator Password** (Nazwa komputera i hasło administratora).

Należy zwrócić uwagę, że program instalacyjny używa nazwy organizacji do utworzenia sugerowanej nazwy komputera. Jeśli na wcześniejszym etapie instalacji nazwa organizacji nie została określona, program instalacyjny do wygenerowania nazwy komputera użyje nazwiska. 20. W polu tekstowym **Computer Name** (Nazwa komputera) wprowadź **Serrero1**.

Nazwa komputera wyświetlana jest za pomocą dużych liter, bez względu na to jak była wprowadzana. W pozostałej części zestawu szkoleniowego, w zadaniach kontrolnych odniesienia dotyczą nazwy Server01.



Ostrzeżenie Jeśli komputer jest połączony z siecią, przed przydzieleniem nazwy komputera należy skonsultować to z administratorem sieci.

21. W polu tekstowym **Administrator Password** (Hasło administratora) i w polu **Confirm Password** (Potwierdzenie hasła) należy wprowadzić złożone hasło dla konta Administrator (hasło powinno być trudne do odgadnięcia). Hasło należy zapamiętać, ponieważ większość ćwiczeń praktycznych wymaga zalogowania się jako administrator systemu.



Ważne Podczas instalacji ręcznej, program instalacyjny Windows Server 2003 nie pozwala przejść do następnych etapów dopóki dla konta administratora nie zostanie wprowadzone hasło spełniające złożone wymagania. Istnieje możliwość pozostawienia pustych pól określających hasło, ale taka praktyka jest ze wszelkich miar niepożądana.

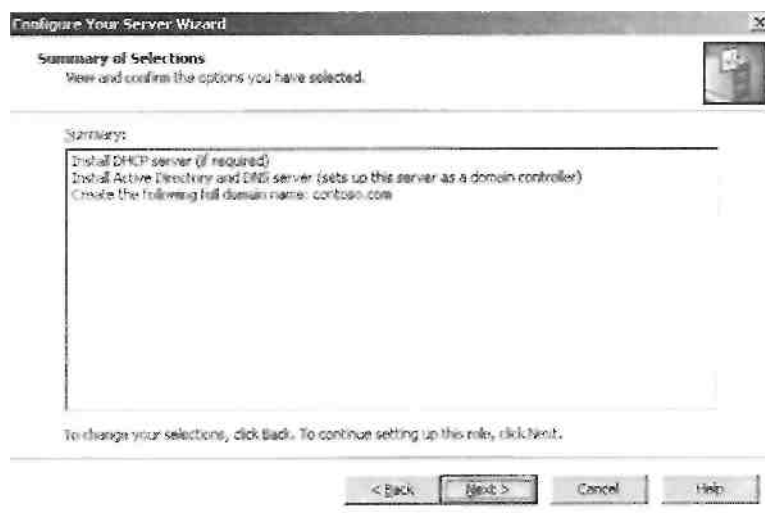
Jeśli w systemie był zainstalowany modem, wyświetlone zostanie okno dialogowe **Modem Dialing Information** (Informacje połączenia modemowego).

22. Wprowadź numer kierunkowy, a następnie kliknij przycisk **Next** (Dalej). Wyświetlona zostanie strona *Date And Time Settings* (Ustawienia daty i godziny).

1. Otwórz moduł **Manage Your Server** (Zarządzanie tym serwerem) w grupie programów Narzędzia administracyjne, o ile nie był wcześniej uruchomiony.
2. Kliknij opcję **Add Or Remove A Role** (Dodaj lub usuń rolę). Wyświetlone zostanie okno programu *Configure Your Server Wizard* (Kreator konfigurowania serwera).
3. Kliknij przycisk **Next** (Dalej), a kreator wykryje ustawienia sieci.
4. Kliknij opcję **Typical Configuration For A First Server** (Ustawienia typowe dla pierwszego serwera), a następnie kliknij przycisk **Next** (Dalej).
5. W polu opisującym nazwę domeny usługi Active Directory wpisz **contoso.com**.
6. Sprawdź, czy nazwa CONTOSO jest wyświetlana w polu *NetBIOS Domain Name*, a następnie kliknij przycisk **Next** (Dalej).
7. Sprawdź, czy okno **Summary Of Selections** (Podsumowanie ustawień) odpowiada rysunkowi 1-3, a następnie kliknij przycisk **Next** (Dalej).

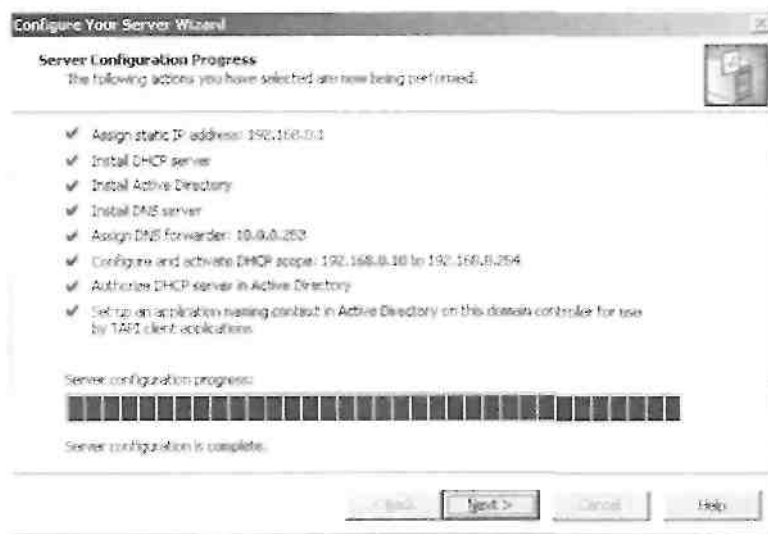
Program *Configure Your Server Wizard* (Kreator konfiguracji tego serwera) wyświetli komunikat informujący o tym, że system zostanie ponownie uruchomiony i poprosi użytkownika o zamknięcie wszystkich otwartych programów.

8. Kliknij przycisk **Yes** (Tak).



Rysunek 1-3. Podsumowanie ustawień

- 9- Po ponownym uruchomieniu komputera zaloguj się w systemie jako administrator.
10. Okno programu *Configure Your Server Wizard* (Konfigurowanie tego serwera) będzie podsumowywać ostatnie etapy tak, jak pokazane to zostało na rysunku 1-4.



Rysunek 1-4. *Kreator Konfigurowanie tego serwera*

11. Kliknij kolejno przyciski **Next** (Dalej) i **Finish** (Zakończ).
12. Uruchom program **Active Directory Users And Computers** (Użytkownicy i komputery usługi Active Directory) w grupie programów Narzędzia administracyjne. Sprawdź, czy w systemie jest domena nazwana **contoso.com** — rozwinięcie domeny i czy w węźle *Domain Controllers* (Kontrolery domeny) znajduje się konto komputera dla serwera **Server01**.

Pytania

1. Które z poniżej wymienionych wersji systemu Windows Server 2003 wymagają aktywacji produktu? (zaznacz wszystkie właściwe)
 - a. Windows Server 2003, Standard Edition, wersja komercyjna
 - b. Windows Server 2003, Enterprise Edition, wersja testowa
 - c. Windows Server 2003, Enterprise Edition, wersja Open License (licencja otwarta)
 - d. Windows Server 2003, Standard Edition, wersja Volume License (licencja pakietowa)
2. Czym różnią się w usłudze Active Directory domena, drzewo i las?
- 3- Które z poniższych stwierdzeń dotyczących Windows Server 2003 jest prawdziwe? (zaznacz wszystkie właściwe)
 - a. Program instalacyjny może być uruchomiony przez rozruch z dysku CD-ROM.
 - b. Program instalacyjny może być uruchomiony przez rozruch z dyskietki.
 - c. Do spełnienia złożonych wymagań dotyczących haseł program instalacyjny wymaga, by hasło nie było puste.

- d. Program instalacyjny pozwala wprowadzać same jedyńki (1) przy wpisywaniu identyfikatora produktu.

Podsumowanie lekcji

- Wersje komercyjne i testowe systemu Windows Server 2003 wymagają aktywacji produktu.
- Strony programów Manage Your Server (Zarządzanie tym serwerem) oraz Configure Your Server Wizard (Konfigurowanie tego serwera) stanowią pomocny przewodnik dla instalacji i konfiguracji dodatkowych usług, zgodnie z wybraną rolą serwera.
- Usługa Active Directory — usługa katalogowa systemu Windows Server 2003 — jest instalowana na serwerze za pomocą programu Active Directory Installation Wizard (Kreator instalacji usługi Active Directory). Kreator jest uruchamiany przy użyciu programu Configure Your Server Wizard (Konfigurowanie tego serwera) lub poprzez wpisanie w wierszu poleceń DCPROMO.

ania i odpowiedzi

Pytania do lekcji 1

1. Planujesz zainstalowanie komputerów systemu Windows Server 2003 w dziale zatrudniającym 250 pracowników. Serwer ma przechowywać katalogi domowe i współużytkowane dla danego działu oraz ma obsługiwać kilka drukarek używanych w tym dziale. Która wersja Windows Server 2003 stanowi najodpowiedniejsze rozwiązanie dla tego działu?

System Windows Server 2003 Standard Edition jest silną platformą usług plikowych i drukowania dla małych i średniej wielkości przedsiębiorstw czy departamentów.

2. Planujesz zainstalowanie komputerów systemu Windows Server 2003 w nowej domenie usługi Active Directory w dużej korporacji, w której znajduje się wiele oddzielnych usług Active Directory zarządzanych przez filie korporacji. Firma zdecydowała, że serwer Exchange Server 2003 będzie dla wszystkich filii jednolitą platformą komunikacji oraz że usługa MMS (Microsoft Mctadirectory Services) będzie używana do synchronizacji odpowiednich właściwości obiektów w całej organizacji. Która wersja Windows Server 2003 stanowi najodpowiedniejsze rozwiązanie dla takiej instalacji?

System Windows Server 2003 Enterprise Edition jest wydajnym rozwiązaniem, które obsługuje usługi MMS. Wersje Standard i Web nie obsługują MMS.

3. Planowane jest zainstalowanie serwerów zapewniających dostęp przez sieć Internet do aplikacji typu e-commerce. Przewidywane jest zainstalowanie 4 serwerów jako czoła aplikacji sieci Web oraz jeden dla silnej, aktywnie wykorzystywanej bazy danych. Która wersja Windows Server 2003 stanowi najodpowiedniejsze rozwiązanie?

System Windows Server 2003 wersja Web Edition to optymalne rozwiązanie dla serwerów aplikacji Web. Jednak wersja ta nie obsługuje aplikacji dla przedsiębiorstw takich jak SQL Server - wersja MSDE dołączona do wersji serwer Web Edition dopuszcza tylko 25 jednoczesnych połączeń. Dlatego w tym przypadku, dla uruchomienia SQL Server najodpowiedniejszą platformą będzie serwer Windows Server 2003 Standard Edition.

Pytania do lekcji 2

1. Które z poniżej wymienionych wersji systemu Windows Server 2003 wymagają aktywacji produktu? (zaznacz wszystkie właściwe)
 - a. Windows Server 2003, Standard Edition, wersja komercyjna
 - b. Windows Server 2003, Enterprise Edition, wersja testowa
 - c. Windows Server 2003, Enterprise Edition, wersja Open License (licencja otwarta)
 - d. Windows Server 2003, Standard Edition, wersja Volume License (licencja pakietowa)

Odpowiedzi: a oraz b

2. Czym różnią się w usłudze Active Directory domena, drzewo i las?

Domena jest podstawową jednostką organizacyjną w usłudze Active Directory. Las jest częścią usługi Active Directory i musi zawierać co najmniej jedną domenę. Jeśli las zawiera kilka domen, a domeny te współużytkują ciągłą przestrzeń nazw DNS, to oznacza, że domeny, które mają

wspólną domenę główną tworzą drzewo. Domeny, które nie współużytkują ciągłej przestrzeni nazw DNS, tworzą odrębne drzewa znajdujące się wewnątrz lasu.

3. Które z poniższych stwierdzeń dotyczących Windows Server 2003 jest prawdziwe? (zaznacz wszystkie właściwe)
- a. Program instalacyjny może być uruchomiony przez rozruch z dysku CD-ROM.
 - b. Program instalacyjny może być uruchomiony przez rozruch z dyskietki.
 - c. Do spełnienia złożonych wymagań dotyczących haseł, program instalacyjny wymaga, by hasło nie było puste.
 - d. Program instalacyjny pozwala wprowadzać same jedynki (1) przy wpisywaniu identyfikatora produktu.

Odpowiedzi: a oraz c

Administracja systemu Windows Server 2003

Zadania egzaminacyjne omawiane w tym rozdziale

- Zarządzanie zdalne serwerami
 - » Zarządzanie serwerem przy użyciu programu Remote Assistance (Pomoc zdalna)
 - » Zarządzanie serwerem przy użyciu trybu zdalnej administracji aplikacji Terminal Services (Usługi terminalowe)
 - » Zarządzanie serwerem przy użyciu dostępnych narzędzi
- Usuwanie problemów programu Terminal Services (Usługi terminalowe)
 - » Diagnoza i rozwiązywanie zagadnień dotyczących zabezpieczeń usługi Terminal Services (Usługi terminalowe)
 - » Diagnoza i rozwiązywanie zagadnień dotyczących dostępu klientów do usług Terminal Services (Usługi terminalowe)

Cele rozdziału

Podczas wykonywania swoich codziennych obowiązków administrator systemu bardzo często używa narzędzi do konfigurowania kont użytkowników, modyfikowania oprogramowania komputera i ustawień usług, instalowania nowego sprzętu, a także wielu innych zadań. Jeśli środowisko komputerowe rozrasta się, zwiększa się zakres prac, które trzeba wykonywać. Konsola MMC (Microsoft Management Console) umożliwia zorganizowanie i konsolidację niektórych, najczęściej używanych narzędzi. Oprócz tego, konsole MMC mogą być dostosowywane i ograniczane tak, aby dokładnie odpowiadały potrzebom i wykonywanym zadaniom. Dzięki temu, wykonywanie zadań może być przy zmniejszonej możliwości pomyłek, przekazywane mniej doświadczonym administratorom.

W sytuacji kiedy zachodzi potrzeba globalnej kontroli komputerów zdalnych, abstrahując od tego, co może być zrealizowane za pomocą konsoli MMC, dwa podstawowe narzędzia umożliwiają administrację zdalną: Remote Desktop for Administration (Pulpit zdalny dla administracji) i Remote Assistance (Pomoc zdalna). Program Remote Desktop for Administration (Pulpit zdalny dla administracji) można rozpatrywać jako aplikację typu klient-serwer, która umożliwia przeglądanie lokalnej konsoli komputera serwera na pulpicie komputera użytkownika. Dzięki tej aplikacji użytkownik może posługiwać się klawiaturą i myszą tak, jak gdyby był zalogowany lokalnie za pomocą konsoli serwera. Moduł Remote Assistance (Pomoc zdalna) działa podobnie, ale przewidziany jest dla pulpitu komputerów działających pod kontrolą systemów operacyjnych z rodziny Microsoft Windows Server 2003 oraz Windows XP. Użytkownik takiego komputera wysyła żądanie pomocy, a połączenie zdalne może być nawiązane od komputera zdalnego do pulpitu komputera żądającego pomocy.

- **Lekcje rozdziału:**

- Lekcja 1: Konsola MMC (Microsoft Management Console)..... 35
- Lekcja 2: Zdalne zarządzanie komputerami za pomocą konsoli MMC..... 41
- Lekcja 3: Zarządzanie serwerem za pomocą programu Remote Desktop for Administration (Pulpit zdalny dla administracji)..... 45
- Lekcja 4: Korzystanie z programu Remote Assistance (Pomoc zdalna) 53

Wymagania

Aby wykonać ćwiczenia praktyczne dotyczące zadań tego rozdziału użytkownik musi spełnić następujące wymagania:

- Komputer, na którym działa system Windows Server 2003. Wykonywanie poleceń identycznych do podanych w przykładach wymaga, aby serwer nazywał się Server01 i był kontrolerem domeny w domenie contoso.com.
- Na serwerze Server01 musi być zainstalowany program Pulpit zdalny dla administracji, a moduły Pulpit zdalny i Pomoc zdalna muszą być włączone.
- Sieć TCP/IP (Transmission Control Protocol/Internet Protocol), do której można przyłączać konsolę i zdalnie administrowane komputery, musi być skonfigurowana i sprawna.

Lekcja 1: Konsola MMC (Microsoft Management Console)

Podstawowym narzędziem zarządzania systemu Windows Server 2003 jest konsola MMC. Umożliwia ona ujednolicony, wspólny interfejs dla kilku aplikacji zwanych przystawkami, używanych do konfigurowania poszczególnych elementów środowiska. Przystawki przeznaczone są do wykonywania określonych zadań, a konsola MMC pozwala na ich porządkowanie bądź grupowanie zgodne z preferencjami użytkownika.

Podstawowymi narzędziami administracji systemu Windows Server 2003 są konsole MMC wraz z zestawem przystawek przeznaczonych do wykonywania określonych zadań. Na przykład, przystawka Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) jest narzędziem specjalnie zaprojektowanym do administrowania zabezpieczeniami głównych elementów domeny (użytkownicy, grupy i komputery). Narzędziem administracji nie jest sama konsola MMC, lecz jej przystawki.



Wskazówka Konsole MMC mogą być uruchamiane pod kontrolą systemów operacyjnych Windows Server 2003, Windows 2000, Windows NT 4, Windows XP oraz Windows 98.

Materiały omówione podczas lekcji pozwalają na

- Konfigurowanie konsoli MMC dla pojedynczej przystawki
- Konfigurowanie konsoli MMC dla wielu przystawek
- Zapisywanie konsoli MMC w trybie użytkownika i w trybie autora

Szacunkowy czas lekcji: 5 minut

Konsola MMC

Wygląd konsoli MMC jest bardzo zbliżony do programu Eksplorator Windows, wyposażonego w mniejszą ilość przycisków. Funkcjonalne składniki konsoli MMC znajdują się wewnątrz elementów nazwanych przystawkami. Menu, paski narzędzi konsoli udostępniają polecenia pozwalające tworzyć nadrzędne i podrzędne okna, a sama konsola (zawierająca przystawki) może być ukształtowana pod kątem funkcjonalności. Oprócz tego, odpowiednio do sytuacji, konsola może być zapisywana dla różnych opcji i w różnych trybach.

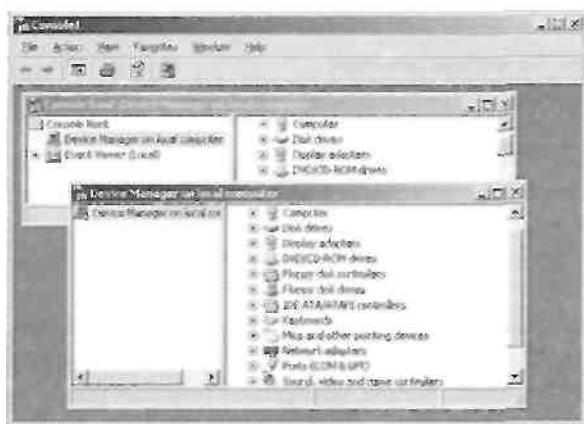
Poruszanie się w konsoli MMC

Rysunek 2-1 przedstawia widok „pustej” konsoli MMC. Należy zwrócić uwagę, że konsola ma nazwę i znajduje się w niej katalog główny. Katalog główny konsoli przechowuje wszystkie przystawki, które użytkownik chce wykorzystywać.



Rysunek 2-1. Wygląd „pustej” konsoli MMC

Na ekranie każdej konsoli umieszczone jest drzewo konsoli, menu i pasek narzędzi oraz okno, w którym wyświetlane są informacje szczegółowe. Wygląd poszczególnych konsol różni się znacznie, w zależności od przeznaczenia i funkcji dołączonych przystawek. Na rysunku 2-2 pokazana została często używana konsola MMC zawierająca dwie przystawki oraz podrzędne okno przystawki Device Manager (Menedżer urządzeń)



Rysunek 2-2. Wygląd typowej konsoli MMC

Korzystanie z menu oraz z paska narzędzi konsoli MMC

Pomimo, że każda przystawka dodaje swoje własne elementy menu i paska narzędzi, istnieje kilka podstawowych menu i poleceń wykorzystywanych w niektórych, wspólnych dla większości przystawek sytuacjach. Polecenia te zostały zebrane w tabeli 2-1.

Tabela 2-1 Wspólne polecenia i menu konsoli MMC

Menu	Polecenia
File (Plik)	Za pomocą tego menu można tworzyć nową i uruchamiać istniejącą konsolę, dodawać lub usuwać przystawki konsoli, określać opcje zapisywania konsoli. Oprócz tego menu wyświetla listę ostatnio utworzonych plików konsoli oraz pozwala zamknąć program. Action (Akcja) Menu różni się w zależności od typu przystawki, ale najczęściej zawiera polecenia eksportu listy, otwarcia nowego okna, konfiguracji oraz pomocy dla specyficznych właściwości danej przystawki.
View (Widok)	Menu różni się w zależności od typu przystawki, ale najczęściej zawiera opcje dostosowujące ogólny wygląd konsoli.
Favorites (Ulubione)	Umożliwia dodawanie i porządkowanie zapisanych konsoli.
Window (Okno)	Polecenia tu zamieszczone otwierają nowe okno, rozmieszczają okna kaskadowo lub sąsiadujące oraz rozmieszczają ikony danej konsoli.
Help (Pomoc)	Moduł pomocy ogólnej wraz z modułami pomocy dołączonych przystawek.

Dostosowywanie konfiguracji konsoli MMC

Każda konsola MMC zawiera jedno narzędzie lub kilka narzędzi nazwanych przystawkami. Przystawka rozbudowuje konsolę MMC dodając do niej specyficzne możliwości zarządzania i dodatkową funkcjonalność. W programie występują dwa rodzaje przystawek: przystawki autonomiczne oraz rozszerzenia.

Przystawki można łączyć dostosowując konsolę MMC, która dzięki temu może być wykorzystywana do scentralizowanych i połączonych zadań administracyjnych. Chociaż do dyspozycji użytkownika jest wiele wstępnie skonfigurowanych konsol, które może używać podczas zarządzania systemami, to niestandardowe konsole umożliwiają indywidualne dostosowanie do konkretnych wymagań, a także umożliwiają standaryzację środowiska.



Wskazówka Tworząc niestandardową konsolę MMC, użytkownik nie musi stale przełączać okien różnych programów czy poszczególnych konsol.

Przystawka autonomiczna

Przystawki autonomiczne są udostępniane przez projektantów aplikacji. Na przykład, wszystkie narzędzia w grupie Administrative Tools (Narzędzia administracyjne) systemu Windows Server 2003 są albo pojedynczymi konsolami typu przystawka albo są połączeniem wstępnie skonfigurowanych przystawek przydatnych dla poszczególnych kategorii zadań. Przystawka Computer Management (Zarządzanie komputerem) na przykład jest zbiorem pojedynczych przystawek użytecznych jako całość.

Rozszerzenia

Przystawki nazwane *rozszerzeniami* zostały zaprojektowane, tak aby współpracowały z jedną lub kilkoma przystawkami autonomicznymi. Podczas dodawania rozszerzenia, system Windows Server 2003 umieszcza je w odpowiedniej lokalizacji wewnątrz przystawki autonomicznej.

Wiele przystawek udostępnia funkcjonalność autonomiczną i rozszerza funkcjonalność innych przystawek. Na przykład, przystawka Event Viewer (Podgląd zdarzeń) rejestruje zdarzenia zachodzące w komputerze. Jeśli w konsoli istnieje obiekt Computer Management (Zarządzanie komputerem), przystawka Event Viewer (Podgląd zdarzeń) automatycznie rozszerza każdą instancję obiektu Computer Management (Zarządzanie komputerem) i udostępnia im dzienniki zdarzeń komputera. Przystawka Event Viewer (Zarządzanie komputerem) może również pracować w trybie autonomicznym i w takim przypadku nie będzie pojawiać się jako węzeł umieszczony poniżej węzła Computer Management (Zarządzanie komputerem).



Nieoficjalnie Warto poświęcić trochę czasu analizując codzienne zadania i grupując je według typu funkcji i częstości używania. Na podstawie tej analizy należy zbudować dwie lub trzy niestandardowe konsole zawierające najczęściej używane narzędzia. Łatwo się następnie przekonać, że w ten sposób można zaoszczędzić sporo czasu związanego z częstym otwieraniem, zamykaniem bądź przełączaniem różnych programów.

Opcje konsoli

Opcje konsoli określają sposób działania konsoli MMC definiując, które węzły drzewa konsoli mogą być otwierane, które przystawki mogą być dodawane oraz jakie okna mogą być utworzone.

Tryb autorski

Podczas zapisywania konsoli w trybie Author (tryb autorski), który jest trybem domyślnym, udostępniony zostaje pełny dostęp do funkcji konsoli MMC, wliczając w to:

- Dodawanie i usuwanie przystawek
- Tworzenie okien
- Tworzenie widoków i zadań dla bloku zadań
- Wyświetlanie wszystkich części drzewa konsoli
- Zmianę opcji konsoli
- Zapisywanie konsoli

Tryby użytkownika

Jeśli zachodzi potrzeba rozdzielania konsol MMC posiadających specyficzne funkcje, można określić potrzebny tryb użytkownika, a następnie zapisać konsolę. Ustawienia domyślne określają, że konsole są zapisywane w folderze Administrative Tools (Narzędzia administracyjne), w profilu użytkownika. W tabeli 2-2 przedstawione zostały tryby użytkownika, za pomocą których możliwe jest zapisywanie konsoli MMC.

Tabela 2-2 Tryby użytkownika konsoli MMC**Typ trybu użytkownika Opis**

Fuli Access (pełny dostęp)	Umożliwia użytkownikom swobodne poruszanie się pomiędzy przystawkami czy otwartymi oknami oraz dostęp do wszystkich części drzewa konsoli.
Limited Access, Multiple Windows (ograniczony dostęp, wiele okien)	Uniemożliwia użytkownikom otwieranie nowych okien lub zabrania dostępu do fragmentu drzewa konsoli, ale zezwala na przeglądanie kilku okien konsoli.
Limited Access, Single Window (ograniczony dostęp, jedno okno)	Uniemożliwia użytkownikom otwieranie nowych okien lub zabrania dostępu do fragmentu drzewa konsoli oraz zezwala na przeglądanie tylko jednego okna konsoli.



Informacja Konsole MMC podczas zapisywania otrzymują rozszerzenie *.msc. Przykładowo konsola Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) zostaje nazwana Dsa.msc (Directory Services Administrator.Microsoft Saved Console).

Zadanie kontrolne: Tworzenie i zapisywanie konsoli

W zadaniu tym zostanie utworzona, skonfigurowana i zapisana konsola MMC.

Ćwiczenie 1: Konsola Event Viewer (Podgląd zdarzeń)

1. Kliknij menu **Start**, a następnie kliknij opcję **Run** (Uruchom).
2. W polu tekstowym **Open** (Otwórz) wpisz polecenie **mmc** i kliknij przycisk OK.
3. Maksymalizuj rozmiar okien **Console1** (Konsola 1) oraz **Console Root** (Katalog główny konsoli).
4. W menu **File** (Plik) wybierz polecenie **Options** (Opcje), aby sprawdzić tryb konfiguracji konsoli. W jakim trybie pracuje konsola?
5. Sprawdź, czy w oknie rozwijanej listy **Console Mode** (Tryb konsoli) wybrany jest tryb **Author** (autorski), a następnie kliknij przycisk OK.
6. W menu **File** (plik) kliknij opcję **Add/Remove Snap-In** (Dodaj/Usuń przystawkę)
Wyświetlone zostanie okno dialogowe *Add/Remove Snap-In* (Dodawanie/Usuwanie przystawki), przy czym aktywna jest zakładka *Standalone* (Autonomiczna). Należy zwrócić uwagę, że żadna przystawka nie jest dodana.
7. W oknie dialogowym *Add/Remove Snap-In* (Dodawanie/Usuwanie przystawki) kliknij przycisk **Add** (Dodaj), aby wyświetlić okno *Add Standalone Snap-In* (Dodawanie przystawki autonomicznej).
8. Znajdź przystawkę **Event Viewer** (Podgląd zdarzeń), a następnie kliknij przycisk **Add** (Dodaj).
Wyświetlone zostanie okno *Select Computer* (Wybieranie komputera) umożliwiające wybór komputera, który ma być administrowany. Dla przystawki *Event Viewer* (Podgląd zdarzeń), można wybrać komputer lokalny lub zdalny, jeśli komputer lokalny jest częścią sieci.
9. W oknie *Select Computer* (Wybieranie komputera) wybierz opcję **Local Computer** (Komputer lokalny), a następnie kliknij przycisk **Finish** (Zakończ).

- * 10. W oknie dialogowym *AddStandalone Snap-In* (Dodawanie przysławki autonomicznej) kliknij przycisk **Close** (Zamknij), a następnie w oknie *Add/Remove Snap-In* (Dodaj/Usuń przysławki), kliknij przycisk **OK**.

W drzewie konsoli wyświetlony zostanie obiekt *Event Viewer (Local)* [Podgląd zdarzeń (lokalnie)]. Rozmiary okna drzewa konsoli mogą być zmieniane, a poszczególne węzły rozwijane tak, aby użytkownik dostosował widok drzewa do swoich potrzeb.

- 11. Samodzielnie dodaj przysławkę **Device Manager (local)** (Menedżer urządzeń (lokalny)).
- 12. Zapisz konsolę MMC jako **MyEvents**.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania znaleźć można w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

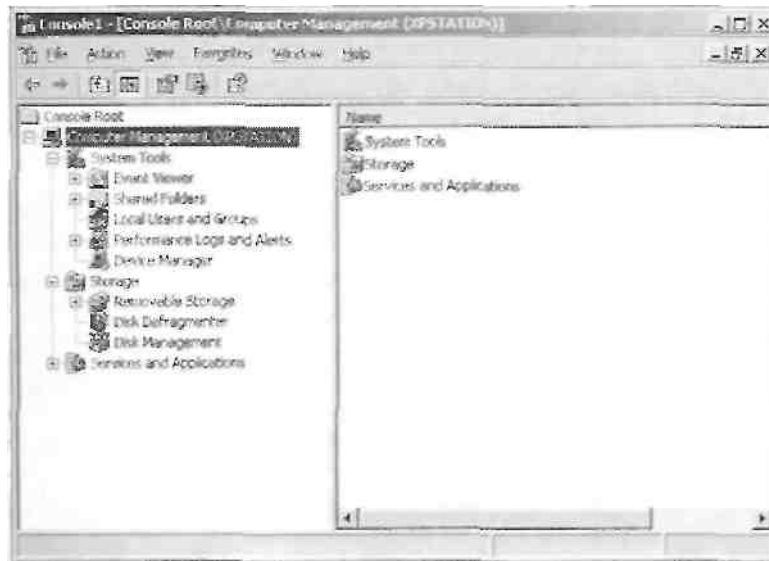
- 1. Który tryb jest domyślnym trybem tworzenia konsoli MMC?
- 2. Czy przysławka może jednocześnie śledzić komputer lokalny i komputer zdalny?
- 3. Jeśli zachodzi potrzeba ograniczenia dostępu do danej przysławki, w jaki sposób należy zbudować konsolę MMC zawierającą tę przysławkę?

Podsumowanie lekcji

Konsola MMC jest przydatnym narzędziem porządkowania i łączenia przysławek lub niewielkich programów, które są używane do wykonywania zadań administracyjnych w sieci czy systemie komputerowym. Hierarchia widoku programu jest podobna do zastosowanej w programie Windows Explorer (Eksplorator Windows) — udostępnia podobny widok właściwości przysławek oparty na analogii do folderów. Istnieją dwa typy przysławek — przysławki autonomiczne i rozszerzenia. Rozszerzenia występują wewnątrz konsoli MMC, a ich działanie zależy od kontekstu, w jakim się znajdują. Każda konsola może być skonfigurowana tak, by działała w jednym z dwóch trybów — trybie autorskim lub użytkownika. Podczas zapisywania w trybie użytkownika istnieje możliwość ograniczania niektórych funkcji konsoli.

Lekcja 2: Zarządzanie zdalnymi komputerami za pomocą konsoli MMC

W sieci niejednokrotnie zachodzi potrzeba pomocy innym użytkownikom podczas tworzenia kont użytkowników czy grup, które mogą współużytkować foldery lokalne. Dzięki możliwości przyłączenia komputera użytkownika zdalnego za pomocą konsoli Computer Management (Zarządzanie komputerem), tak jak zostało to pokazane na rysunku 2-3, można uniknąć konieczności bezpośredniej pracy na komputerze zdalnym. Na komputerze zdalnym użytkownik może wykonać większość tych zadań, które wykonuje na komputerze lokalnym, na przykład formatowanie napędów dyskowych.



Rysunek 2-3. Przyłączanie komputera użytkownika zdalnego za pomocą konsoli Computer Management (Zarządzanie komputerem)

Materiały omówione podczas lekcji pozwalają na

- Utworzenie konsoli MMC w celu zarządzania komputerem zdalnym

Szacunkowy czas lekcji: 10 minut

Konfigurowanie przystawki do pracy zdalnej

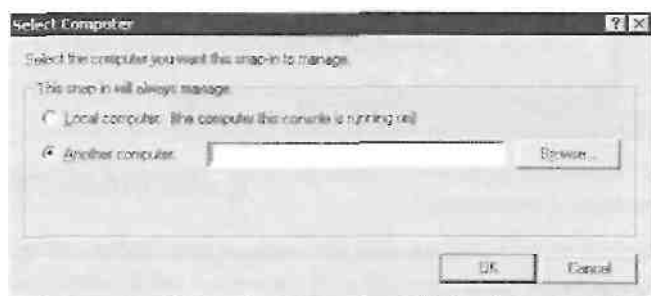
Aby przyłączyć się i zarządzać innym komputerem za pomocą konsoli Computer Management (Zarządzanie komputerem), należy uruchomić konsolę rejestrując się w systemie za pomocą konta, które posiada uprawnienia administracji komputera zdalnego. Jeśli uprawnienia te nie będą wystarczające, będzie można uruchomić przystawkę, ale nie będzie można przeczytać informacji znajdujących się na komputerze zdalnym.



Wskazówka Można użyć polecenia RunAs lub zalogować się za pomocą innego konta, aby uruchomić konsolę jako użytkownik, który ma inne uprawnienia niż przypisane do bieżącego konta.

W celu zarządzania systemem zdalnym, można otworzyć istniejącą konsolę MMC z dodanymi przystawkami lub skonfigurować nową, która podczas tworzenia będzie miała dodawane przystawki skonfigurowane dla połączeń zdalnych. Jeśli natomiast, dla przykładu, chcemy skonfigurować istniejącą konsolę Computer Management (Zarządzanie komputerem), należy postępować zgodnie z poniższą procedurą:

1. Otwórz konsolę *Computer Management* (Zarządzanie komputerem) klikając prawym przyciskiem myszy ikonę **My Computer** (Mój komputer) i wybierając z menu opcję **Manage** (Zarządzaj).
2. Prawym przyciskiem myszy kliknij węzeł **Computer Management** (Zarządzanie komputerem) i wybierz polecenie **ConnectTo Another Computer** (Podłącz do innego komputera).
3. W oknie dialogowym pokazanym na rysunku 2-4 wpisz nazwę lub adres IP komputera bądź kliknij przycisk **Browse** (Przeglądaj) w celu przeszukania sieci, a następnie kliknij przycisk OK.



Rysunek 2-4. Określanie dla przystawki lokalnego lub zdalnego kontekstu

Po połączeniu, użytkownik może wykonywać zadania administracyjne na komputerze zdalnym.

Zadanie kontrolne: Wybór komputera zdalnego w celu zarządzania nim (zadanie opcjonalne)



Informacja Do realizacji tego zadania potrzebny jest komputer dostępny dla połączenia zdalnego, a także do tego komputera wymagane są uprawnienia administracyjne.

Ćwiczenie 1: Połączenie zdalne za pomocą konsoli MMC

W ćwiczeniu tym będzie modyfikowana istniejąca konsola MMC tak, aby możliwe było połączenie do komputera zdalnego.

1. Otwórz zapisaną w ćwiczeniu 1 konsolę MMC MyEvents.
2. W menu **File** (Plik) kliknij polecenie **Add/Remove Snap-In** (Dodaj/Usuń przystawkę)
3. W oknie dialogowym *Add/Remove Snap-In* (Dodawanie/Usuwanie przystawek) kliknij przycisk **Add** (Dodaj), aby wyświetlić okno dialogowe *Add Standalone Snap-In* (Dodawanie przystawki autonomicznej).
4. Znajdź przystawkę **Computer Management** (Zarządzanie komputerem), a następnie kliknij przycisk **Add** (Dodaj).
5. W oknie dialogowym *Computer Management* (Zarządzanie komputerem) zaznacz opcję **Another Computer** (Inny komputer).
6. Wpisz adres IP komputera zdalnego lub przeszukaj sieć, a następnie kliknij przycisk **Finish** (Zakończ), aby przyłączyć komputer.
7. W oknie dialogowym *Add Standalone Snap-In* (Dodawanie przystawki autonomicznej) kliknij przycisk **Close** (Zamknij), a następnie kliknij OK, aby dodać przystawkę *Computer Management* (Zarządzanie komputerem) do konsoli MyEvents.

Po wykonaniu tej procedury można administrować komputerem zdalnym korzystając z odpowiednich narzędzi.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Jakie uprawnienia są wymagane do administrowania komputerem zdalnym za pomocą konsoli MMC?
2. Czy można dla istniejącej przystawki konsoli MMC zmienić kontekst z lokalnego na zdalny lub też konieczne jest załadowanie przystawki takiego samego typu przy skonfigurowaniu jej dla połączenia zdalnego?

3. Czy wszystkie funkcje przystawki dla komputera lokalnego mogą być używane na komputerze zdalnym?

Podsumowanie lekcji

Konsola MMC umożliwia uruchomienie wielu różnych narzędzi w postaci przystawek. Niektóre z przystawek mogą być używane zarówno w połączeniu z komputerem lokalnym, jak i komputerem zdalnym. Połączenie z komputerem zdalnym może być nawiązywane podczas uruchamiania przystawki lub po jej uruchomieniu, poprzez kliknięcie prawym przyciskiem myszy danej przystawki i wybranie polecenia **Connect** (Podłącz do innego komputera). Używanie narzędzi do konfigurowania komputera zdalnego wymaga posiadania uprawnień administracyjnych tego komputera.

Lekcja 3: Zarządzanie serwerami za pomocą programu Remote Desktop for Administration (Pulpit zdalny dla administracji)

Rodzina produktów systemu Windows 2000 Server wprowadziła ściśle zintegrowany zestaw narzędzi i technologii, który umożliwiał dwa tryby pracy modułu Terminal Services (Usługi terminalowe) dla administracji zdalnej oraz współużytkowania aplikacji. Obecnie nastąpił dalszy rozwój tej technologii: program Terminal Services (Usługi terminalowe) jest obecnie integralnym, domyślnym elementem produktów rodziny Windows Server 2003, a program Remote Desktop (Pulpit zdalny) został ulepszony i określony jako rozwiązanie nowatorskie, w którym za pomocą jednego kliknięcia komputer systemu Windows Server 2003 udostępni dla administracji zdalnej dwa jednocześnie połączenia. Dodanie produktu Terminal Server (Usługi terminalowe) i odpowiednie skonfigurowanie licencjonowania jest dalszym rozwinięciem tej technologii, umożliwiającym uruchamianie aplikacji na serwerze przez wielu użytkowników. Niniejsza lekcja omawia sposoby włączania modułu Remote Desktop for Administration (Pulpit zdalny dla administracji).

Materiały omówione podczas lekcji pozwalają na

- Skonfigurowanie serwera umożliwiające włączenie programu Remote Desktop for Administration (Pulpit zdalny dla administracji)
- Przypisanie użytkowników do odpowiednich grup w celu umożliwienia im zdalnej administracji serwera
- Połączenie z serwerem za pomocą programu Remote Desktop for Administration Connection (Podłączenie pulpitu zdalnego dla administracji).

Szacunkowy czas lekcji: 15 minut

Włączanie i konfigurowanie programu Remote Desktop for Administration (Pulpit zdalny dla administracji)

Moduł Terminal Services (Usługi terminalowe) umożliwia współużytkowanie aplikacji dla programów Remote Desktop (Pulpity zdalne), Remote Assistance (Pomoc zdalna) oraz Terminal Server (Serwer terminali). Domyślne ustawienia określają, że usługa ta jest zawsze instalowana w systemie Windows Server 2003, a jej konfigurację określa tryb Remote Desktop for remote administration (Pulpit zdalny dla administracji zdalnej). Moduł Remote Desktop (Pulpity zdalne) zezwala na dwa jednocześnie połączenia zdalne, a współużytkowanie aplikacji komponentów modułu Terminal Server (Serwer terminali) nie jest możliwe. Dzięki temu, program Remote Desktop (Pulpity zdalne) jest niewielkim obciążeniem dla systemu i nie wymaga dodatkowego licencjonowania.



Informacja Ponieważ program Terminal Services (Usługi terminalowe) i zależny od niego moduł Remote Desktop (Pulpity zdalne) są elementami domyślnymi systemu Windows Server 2003, to każdy serwer tego systemu udostępnia funkcje połączeń zdalnych do swojej konsoli. Przyczyna, dla której termin "serwer terminali" odnosi się obecnie specjalnie do komputera systemu Windows Server 2003 wynika z tego, że system udostępnia funkcję współużytkowania aplikacji przez wielu użytkowników dzięki dodatkowym komponentom programu Terminal Server (Serwer terminali).

Inne elementy — usługi Terminal Server (Serwer terminali) oraz Terminal Server Licensing (Licencjonowanie serwera terminali) — muszą być dodawane za pomocą modułu Add Or Remove Programs (Dodaj/Usuń programy). Wszystkie narzędzia administracyjne wymagane do konfigurowania i obsługi połączeń klienta oraz do zarządzania programem Terminal Server (Serwer terminali) są w sposób domyślny instalowane na każdym komputerze systemu Windows Server 2003. Narzędzia i ich funkcje opisane zostały w tabeli 2-3.

Tabela 2-3 Komponenty domyślne programów Terminal Server (Serwer terminali) oraz Remote Desktop (Pulpit zdalny)

Zainstalowane oprogramowanie	Przeznaczenie
Terminal Services Configuration (Konfiguracja usług terminalowych)	Określanie właściwości usługi Terminal Server (Serwer terminali), wliczając w to ustawienia dotyczące sesji, sieci, pulpitu klienta oraz zdalnej kontroli klienta.
Terminal Services Manager (Menedżer usług terminalowych)	Wysyłanie wiadomości do przyłączonych klientów programu Terminal Server (Serwer terminali), rozłączanie lub wyrejestrowywanie się z sesji oraz ustanawianie kontroli zdalnej lub śledzenie sesji.
Remote Desktop Client Installation Files (Pliki instalacyjne klienta pulpitu zdalnego)	Instalacja aplikacji Remote Desktop Client (Klient pulpitu zdalnego) dla systemów Windows Server 2003 lub Windows XP. 32-bitowe oprogramowanie klienta programu Remote Desktop (Pulpit zdalny) jest instalowane w katalogu %Systemroot%\System32\Clients\Tsclient\Win32 serwera terminali.
Terminal Services Licensing (Licencjonowanie usług terminalowych)	Konfiguracja licencji połączeń klientów do serwera terminali. Narzędzie to nie jest dostępne dla środowisk, które wykorzystują jedynie program Remote Desktop for Administration (Pulpit zdalny dla administracji).

Aby w systemie Windows Server 2003 włączyć połączenia programu **Remote Desktop** (Pulpit zdalny), należy otworzyć właściwości modułu **System** umieszczonego w programie **Control Panel** (Panel sterowania). Na zakładce *Remote* (Zdalny), należy wybrać opcję **Allow Users To Connect Remotely To This Computer** (Zezwalaj użytkownikom na zdalne łączenie się z tym komputerem).



Informacja Jeśli serwer jest i kontrolerem domeny i serwerem terminali, na kontrolerze domeny dodatkowo musi być skonfigurowany obiekt Group Policy (Zasady grupy) tak, aby poprzez program Terminal Services (Usługi terminalowe) możliwe były połączenia do grupy Remote Desktop Users (Użytkownicy pulpitu zdalnego). Domyślne ustawienia określają, że serwer będący kontrolerem domeny nie zezwala na połączenia do tej grupy za pomocą programu Terminal Services (Usługi terminalowe).

Remote Desktop Connection (Podłączanie pulpitu zdalnego)

Program Remote Desktop Connection (Podłączanie pulpitu zdalnego) jest oprogramowaniem używanym po stronie klienta do połączenia z serwerem za pomocą jednego z dwóch trybów Remote Desktop (Pulpity zdalne) lub Terminal Server (Serwer terminali). Z punktu widzenia klienta, obie konfiguracje serwera funkcjonalnie są identyczne.

Na komputerach systemów Windows XP i Windows Server 2003 program Remote Desktop Connection jest instalowany domyślnie, ale nie jest łatwo wyszukać jego domyślną lokalizację w grupie programów menu Stan — Ali Programs\Accessories\Communications (Wszystkie programy\Akcesoria\Komunikacja).

Na innych platformach, program Remote Desktop Connection może być instalowany z dysku CD-ROM systemu Windows Server 2003 lub z katalogu instalacyjnego klienta (%Systemroot%\System32\Clients\Tsclicnt\Win32) dowolnego systemu Windows Server 2003- Pakiet instalacyjny .msi programu Remote Desktop Connection może być rozprowadzany do systemów Windows 2000 za pomocą obiektu Group Policy (Zasady grupy) lub SMS.



Wskazówka Zaleca się przeprowadzenie aktualizacji poprzedniej wersji programu klienta Terminal Services (Usługi terminalowe), aby w miarę możliwości udostępnić najbardziej wydajne, bezpieczne i stabilne środowisko, dzięki ulepszeniom takim jak 128-bitowe szyfrowanie, wybór alternatywnego portu czy poprawiony interfejs użytkownika.

Na rysunku 2-5 przedstawiona została konfiguracja klienta programu Remote Desktop pozwalająca na połączenie z serwerem Servcr01 znajdującym się w domenie contoso.com.



Rysunek 2-5. Klient programu Remote Desktop (Pulpity zdalne)

Konfigurowanie klienta programu Remote Desktop

Wiele aspektów połączenia programu Remote Desktop (Pulpity zdalne) może być kontrolowanych zarówno po stronie klienta, jak i po stronie serwera.

Tabela 2-4 Ustawienia programu Remote Desktop (Pulpity zdalne)

Ustawienia Funkcja

Ustawienia klienta

General (Ogólne)	Opcje tej zakładki służą do wybrania komputera połączenia zdalnego, do określenia ustawień dotyczących logowania się w systemie zdalnym oraz do zapisywania ustawień połączenia.
Display (Ekran)	Za pomocą tej zakładki można kontrolować rozmiar okna klienta programu Remote Desktop (Pulpit zdalny), ilość kolorów oraz czy pasek kontrolny połączenia będzie wyświetlany w trybie pełnoekranowym.
Experience (Wrażenia)	Kategorie funkcji wyświetlania mogą być włączane lub wyłączane w zależności od szerokości pasma dostępnego w połączeniu między komputerem zdalnym a lokalnym. Poszczególne elementy dotyczą wyświetlania tła pulpitu, pokazywania zawartości okna podczas jego przeciągania, animacji okien i menu, kompozycji oraz możliwości buforowania map bitowych (opcja ta powoduje, że transmitowane są tylko zmiany ekranu, zamiast „przerysowywania” całego ekranu dla każdego okresu jego odświeżania).

Ustawienia serwera

Logon Settings (Ustawienia logowania)	Statyczne informacje umożliwiające zalogowanie się używane zamiast informacji udostępnianych przez klienta.
Local Resources (Zasoby lokalne)	Są to opcje określające efekty dźwiękowe komputera lokalnego dotyczące typowej myszy, klawiatury i wyświetlania. Określają, w jaki sposób kombinacje przycisków klawiatury będą interpretowane przez komputer zdalny (na przykład ALT+TAB) oraz czy połączenia z dyskiem lokalnym, drukarką bądź portem szeregowym powinny być dostępne podczas sesji zdalnej.
Sessions (Sesje)	Ustawienia te określają rozłączanie lub wyrejestrowanie się z sesji, limity czasu trwania i okresów bezczynności sesji oraz czy określone tu właściwości będą wprowadzone przy ponownym połączeniu.
Environment (Środowisko)	Opcje te zastępują ustawienia profilu użytkownika podczas uruchamiania programu poprzez połączenie. Zdefiniowane tutaj ścieżka i docelowe ustawienia zastępują ustawienia zdefiniowane przez program Remote Desktop Connection (Podłączanie pulpitu zdalnego).
Permissions (Uprawnienia)	Umożliwiają dla tego połączenia określanie dodatkowych uprawnień.

ciąg dalszy ze strony pop rzedniej

Ustawienia	Funkcja
Remote Control (Kontrola zdalna)	Ustawienia określają, czy jest możliwa kontrola zdalna sesji programu Remote Desktop Connection (Podłączanie pulpitu zdalnego) i jeśli tak, czy użytkownik musi przydzielać uprawnienia na początku sesji kontroli zdalnej. Dodatkowe ustawienia mogą ograniczać sesję kontroli zdalnej jedynie do funkcji przeglądania lub mogą zezwalać na pełną interaktywność w trakcie sesji klienta programu Remote Desktop (Pulpiot zdalny).
Client Settings (Ustawienia klienta)	Zastępują ustawienia konfiguracji klienta, kontrolują ilość kolorów oraz blokują szereg portów komunikacyjnych (I/O).
NetworkAdapters (Karty sieciowe)	Określają, która karta sieciowa serwera będzie akceptować połączenia programu Remote Desktop for Administration (Pulpit zdalny dla administracji).
General (Ogólne)	Ustawienia te definiują poziom szyfrowania i mechanizmy uwierzytelnienia dla połączeń z serwerem.

Rozwiązywanie problemów programu Terminal Services (Usługi terminalowe)

Podczas używania programu Remote Desktop for Administration (Pulpit zdalny dla administracji), tworzone są połączenia z konsolą serwera. Istnieje kilka potencjalnych przyczyn nieudanych połączeń lub występowania problemów w trakcie sesji:

- **Awary sieci** Błędy typowej sieci TCP/IP mogą spowodować, że połączenie programu Remote Desktop (Pulpit zdalny) nie będzie działać lub będzie przerywane. Jeśli nie działa usługa DNS, klient nie będzie mógł znaleźć serwera wyszukując go według nazwy. Połączenie nie zostanie nawiązane, jeśli nie działa routing lub port programu Terminal Services (Usługi terminalowe) jest źle skonfigurowany zarówno po stronie klienta, jak i po stronie serwera (port domyślny ma wartość 3389).
- **Uprawnienia** Użytkownicy muszą należeć do grupy Administrators (Administratorzy) lub Remote Desktop Users (Użytkownicy pulpitu zdalnego), aby połączyć się z serwerem za pomocą programu Remote Desktop for Administration (Pulpit zdalny dla administracji).



Wskazówka egzaminacyjna Należy sprawdzić członkostwo w grupie, jeśli podczas nawiązywania połączenia programu Remote Desktop for Administration (Pulpit zdalny dla administracji) następuje odmowa dostępu. We wcześniejszych wersjach programu Terminal Server (Serwer terminali) użytkownik, aby połączyć się z serwerem, musiał być członkiem grupy Administratorzy (specjalne uprawnienia mogły być nadawane ręcznie). Maksymalnie można mieć dwa połączenia zdalne do programu Terminal Server (Serwer terminali).

Zasady Kontrolery domen dopuszczają połączenia poprzez program Remote Desktop (Pulpit zdalny) jedynie dla administratorów. Należy skonfigurować zasadę zabezpieczeń kontrolera domeny, tak aby zezwalała na wszystkie inne połączenia użytkowników zdalnych.

- **Za mało połączeń bieżących** Jeśli sesje zostały przerwane bez wykonania procedury wyrejestrowania się, serwer może traktować połączenie tej sesji jako aktywne, chociaż w rzeczywistości dwie osoby nie są połączone z serwerem. Przykładowo, administrator może zamknąć sesję zdalną bez wylogowania się. Jeśli w tym momencie dwaj inni administratorzy próbują połączyć się z serwerem, tylko jeden z nich nawiąże takie połączenie.



Zobacz także Więcej informacji o programie Terminal Services (Usługi terminalowe) i o ostatnich opracowaniach dotyczących funkcji klienta programu Remote Desktop (Pulpit zdalny) można znaleźć pod adresem http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_Server_Trouble_Topnode.asp.

Zadanie kontrolne: Instalowanie programu Terminal Services (Usługi terminalowe) oraz uruchamianie administracji zdalnej

W zestawie tym należy skonfigurować serwer Server01, aby umożliwiał połączenia programu Remote Desktop for Administration (Pulpit zdalny dla administracji). Następne kroki to optymalizacja serwera Server01, aby zapewniał połączenie wtedy, kiedy nie jest ono używane oraz aby serwer zezwalał tylko na jedno połączenie. Następnie należy uruchomić sesję administracji zdalnej z serwera Server02 (lub innego komputera zdalnego).

Jeśli w tym zadaniu kontrolnym możliwe jest tylko jedno połączenie, klient programu Remote Desktop (Pulpit zdalny) może być używany do połączenia z programem Terminal Services (Usługi terminalowe) na tym samym komputerze. Należy dostosować odniesienia do komputera zdalnego tak, aby wskazywały na komputer lokalny.

Ćwiczenie 1 Konfiguracja serwera umożliwiająca korzystanie z programu Remote Desktop (Pulpit zdalny)

W ćwiczeniu tym należy włączyć połączenia programu Remote Desktop (Pulpit zdalny), zmienić dopuszczalną liczbę jednoczesnych połączeń do serwera oraz zdefiniować ustawienia związane z zamykaniem połączenia.

1. Na serwerze Server01 zaloguj się jako administrator. - 2. Otwórz właściwości modułu *System* znajdującego się w programie **Control Panel** (Panel sterowania)
3. Na zakładce *Remote* (Zdalny), włącz program **Remote Desktop** (Pulpit zdalny). Zamknij okno właściwości modułu *System*.
4. Otwórz konsolę *Terminal Services Configuration* (Konfiguracja usług terminalowych) znajdującą się w folderze *Administrative Tools* (Narzędzia administracyjne).
5. W oknie konsoli MMC — *Terminal Services Configuration\Connections* (Konfiguracja usług terminalowych\Połączenia) prawym przyciskiem myszy kliknij połączenie **RDP-tcp** (w oknie szczegółów), a następnie kliknij polecenie **Properties** (Właściwości).
6. Na zakładce *Network Adapter* (Karta sieciowa) zmień maksymalną liczbę połączeń na 1.
7. Na zakładce *Sessions* (Sesje) zaznacz oba pola wyboru **Override User Settings** (Zastąp ustawienia użytkownika) i zmień ustawienia tak, aby każda rozłączona sesja była zamykana po 15 minutach

bez względu na przyczynę rozłączenia, co oznacza że nie będzie określony limit czasu sesji aktywnej, a sesja będzie rozłączana po 15 minutach braku aktywności.

- » **End a disconnected session** (Zakończ sesję odłączoną): 15 minut
- » **Active session limit** (Limit sesji aktywnych): **never** (nigdy)
- » **Idle session limit** (Limit czasu bezczynności sesji): 15 minut
- » **When session limit is reached or connection is broken** (Po osiągnięciu limitu sesji lub zerwaniu połączenia): **Disconnect from session** (Odłącz od sesji) Powyższa konfiguracja zapewnia, że w danym momencie do programu Terminal Server (Serwer terminali) może przyłączyć się tylko jedna osoba, że odłączone sesje będą zamykane po 15 minutach oraz że również po 15 minutach będą rozłączane sesje nieaktywne. Ustawienia te są przydatne w sytuacji, kiedy brak odłączonych sesji lub ich nieaktywność uniemożliwia połączenia do programu Remote Desktop for Administration (Pulpit zdalny dla administracji).

Ćwiczenie 2: Podłączenie do serwera za pomocą klienta programu Remote Desktop (Pulpit zdalny)

1. Na serwerze Server02 (lub na innym komputerze zdalnym lub też na tym samym serwerze Server01, jeśli komputer zdalny nie jest dostępny), otwórz program **Remote Desktop Connection** (Podłączanie pulpitu zdalnego), znajdujący się w grupie programów **Accessories, Communications** (Akcesoria, Komunikacja) - i przyłącz się do serwera Server01, a następnie zarejestruj się w nim.
2. Na serwerze Server01 otwórz konsolę *MMC Terminal Services Configuration\Connections* (Konfiguracja usług terminalowych\Połączenia). Powinna być widoczna sesja zdalna podłączona do serwera Server02.
3. Pozostaw sesję bezczynną przez 15 minut lub zamknij klienta programu **Remote Desktop** bez wylogowania się z sesji programu *Terminal Services* — sesja powinna automatycznie zostać odłączona po 15 minutach.

Po zdalnym zalogowaniu się na serwerze Server01, użytkownik może na tym serwerze wykonywać wszystkie zadania tak, jakby był zalogowany na jego konsoli w trybie interaktywnym.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Jaka jest maksymalna liczba jednoczesnych połączeń do programu Terminal Server (Serwer terminali) uruchomionego w trybie administracji zdalnej? Dlaczego?
2. Jaki jest najlepszy sposób udostępnienia administratorom możliwości zarządzania zdalnego serwerem za pomocą programu Terminal Services (Usługi terminalowe)?
 - a. Nie trzeba wykonywać żadnych czynności, administratorzy mają już taki dostęp.

- b. Usunięcie administratorów z listy uprawnień połączenia programu Terminal Server (Serwer terminali) i przesunięcia tych kont do grupy Remote Desktop for Administration (Pulpit zdalny dla administracji).
 - c. Utworzenie oddzielnego, o niższym niż administratorzy poziomie uwierzytelnienia konta użytkownika, które będzie używane codziennie i umieszczenie tego konta w grupie Remote Desktop for Administration (Pulpit zdalny dla administracji).
3. Które narzędzie jest używane do włączenia na serwerze programu Remote Desktop (Pulpit zdalny)?
- a. Terminal Services Manager (Menedżer usług terminalowych)
 - b. Terminal Services Configuration (Konfiguracja usług terminalowych)
 - c. Właściwości modułu System w programie Control Panel (Panel sterowania)
 - d. Terminal Services Licensing (Licencjonowanie usług terminalowych)

Podsumowanie lekcji

Administratorzy i członkowie grupy Remote Desktop Users (Użytkownicy pulpitu zdalnego) mogą łączyć się z serwerem za pomocą programu Remote Desktop Connection (Podłączanie pulpitu zdalnego). Program Terminal Services (Usługi terminalowe) jest w systemie Windows Server 2003 instalowany domyślnie i udostępnia dwa jednocześnie połączenia programu Remote Desktop for Administration (Pulpit zdalny dla administracji). Klient programu Remote Desktop Connection (Podłączanie pulpitu zdalnego) jest domyślnym komponentem systemów Windows XP oraz Windows Server 2003 i może być zainstalowany na dowolnej 32-bitowej platformie Windows z instalacyjnego dysku CD systemu Windows Server 2003 lub z dowolnego komputera systemu Windows Server 2003 (po udostępnieniu katalogu). Konfiguracja połączeń programu Remote Desktop for Administration (Pulpit zdalny dla administracji) jest określana ustawieniami klienta programu Remote Desktop Connection (Podłączanie pulpitu zdalnego) oraz serwera za pomocą programu Terminal Server Configuration (Konfiguracja serwera terminali). Podstawowe ustawienia połączeń mogą być zmienione przez serwer.

Lekcja 4: Korzystanie z programu Remote Assistance (Pomoc zdalna)

Użytkownicy komputerów, w szczególności mniej doświadczeni, mają często problemy bądź pytania dotyczące konfiguracji czy wykorzystania systemu, które są trudne do diagnozy i usunięcia dla pracowników wsparcia technicznego, a nawet dla przyjaciół lub członków rodziny. Program Remote Assistance (Pomoc zdalna) udziela użytkownikom potrzebnego wsparcia, a także ułatwia i zmniejsza koszty działom pomocy technicznej przedsiębiorstw.

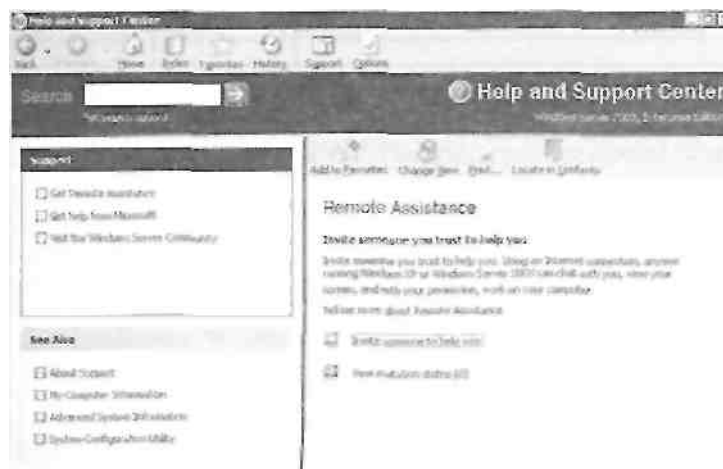
Materiały omówione podczas lekcji pozwalają na

- Skonfigurowanie komputera, by akceptował żądania programu Remote Assistance (Pomoc zdalna)
- Używanie jednej z dostępnych metod żądania i nawiązywania sesji programu Remote Assistance (Pomoc zdalna)

Szacunkowy czas lekcji: 5 minut

Realizacja żądań pomocy

W programie Help (Pomoc) systemu Windows Server 2003 znajduje się moduł w postaci kreatora przeznaczony dla programu Remote Assistance (Pomoc zdalna). Pierwsza strona tego modułu została przedstawiona na rysunku 2-6.



Rysunek 2-6. Ekran powitalny modułu Remote Assistance (Pomoc zdalna) w programie Help and Support Center (Centrum pomocy i obsługi technicznej)

Połączenie, którego obsługa jest podobna do programów typu kreator, pozwala wysyłać żądania za pomocą konta usługi Microsoft .NET Passport, poprzez wysłanie pliku Jub za pomocą konta poczt{'

elektronicznej (poza usługą Passport) wraz z możliwością wysyłania żądania za pomocą programu Windows Messenger. Aby żądanie dotarło poprzez przesłanie wiadomości e-mail, oba komputery muszą używać klienta poczty e-mail zgodnego z interfejsem MAPI (Messaging Application Programming Interface)

Wykorzystywanie usługi Windows Messenger dla połączenia programu Remote Assistance (Pomoc zdalna) wymaga, by użytkownik umieścił na swojej liście kontaktowej nazwę użytkownika asystenta usługi Windows Messenger, a żądania realizował za pomocą klienta programu Windows Messenger. Program Windows Messenger wyświetla, czy dana osoba obsługuje komputer (online), czy też jej komputer jest wyłączony (offline). Żądania bezpośrednie do programu Remote Assistance (Pomoc zdalna) mogą być kierowane tylko, jeśli asystent obsługuje swój komputer (tryb online). Program Remote Assistant (Pomoc zdalna) wymaga, aby oba komputery działały pod kontrolą systemów Windows XP lub Windows Server 2003.



Informacja Wskaźnik statusu pracy (online) w oknie pomocy programu Remote Assistance (Pomoc zdalna) nie jest dynamiczny i dlatego użytkownik musi odświeżać ekran, aby przekonać się o aktualnym statusie asystenta.

Po odebraniu żądania pomocy zdalnej, pomocnik (ekspert) może połączyć się z komputerem zdalnie i bezpośrednio przeglądać ekrany komputera, aby rozwiązać problem. Zainicjowanie żądania pomocy powoduje, że klient programu Remote Assistance (Pomoc zdalna) wysyła do eksperta zaszyfrowany bilet bazujący na języku XML (Extensible Markup Language) z prośbą o akceptację zaproszenia.



Alert bezpieczeństwa Program Remote Assistance (Pomoc zdalna), jeśli jest włączony, zezwala na połączenia do komputera przy obniżonym poziomie ochrony. Należy upewnić się, że dla sesji pomocy zdalnej umożliwiony został dostęp jedynie do zaufanych podmiotów.

Korzystanie z programu Remote Assistance (Pomoc zdalna)

Użytkownik może wysyłać żądania pomocy innego użytkownika usługi Windows Messenger poprzez umieszczenie jego żądania w programie Help and Support Center (Centrum pomocy i obsługi technicznej) lub bezpośrednio za pomocą programu Windows Messenger. Obie aplikacje używają tych samych mechanizmów do określania, czy ekspert pracuje w trybie online i do wysyłania żądania pomocy. Rysunek 2-7 przedstawia wysyłanie żądania pomocy zdalnej korzystając z programu Windows Messenger.



Rysunek 2-7. Wysyłanie żądania pomocy zdalnej

Po otwarciu okna programu Windows Messenger użytkownik wybiera konto eksperta. Ekspert odbiera zaproszenie w postaci wiadomości błyskawicznej (Instant Message). Ekspert klika przycisk **Accept** (Akceptuj) i rozpoczyna sesję programu Remote Assistance (Pomoc zdalna). Użytkownik żądający sesji potwierdza kliknięciem przycisku **Yes** (Tak).

Po nawiązaniu połączenia zdalnego, sesja rozpoczyna się na komputerze eksperta. Ekspert i użytkownik mogą współdzielić kontrolę pulpitu, możliwości przesyłania plików oraz korzystać z okna rozmowy (chat), za pomocą którego obaj współpracują rozwiązując problem.



Alert bezpieczeństwa Jeśli użytkownik wybierze żądanie wysłania wiadomości e-mail lub pliku, wymagane będzie hasło jako wspólna tajemnica sesji programu Remote Assistance (Pomoc zdalna). Użytkownik powinien zdefiniować trudne hasło i przekazać je ekspertowi korzystając z innej metody komunikacji, takiej jak telefon bądź bezpieczna poczta elektroniczna.

Oferowanie użytkownikowi pomocy zdalnej

Program Remote Assistance (Pomoc zdalna) jest szczególnie użyteczny, jeśli zachodzi potrzeba rozpoczęcia procesu rozwiązywania problemów komputera użytkownika. W tym celu, na lokalnym komputerze docelowym (użytkownika), należy dla zasady grupy komputera lokalnego Local Group Policy włączyć opcję **Offer Remote Assistance** (Oferuj pomoc zdalną):

1. Na komputerze użytkownika kliknij polecenia **Start, Run** (Uruchom), a następnie wpisz polecenie **gpedit.msc**. Wyświetlone zostanie okno edytora obiektów zasad grupy komputera lokalnego - Group Policy.



informacja Domain Group Policy (Zasada grupy domeny) może uniemożliwić dostosowywanie omawianej zasady.

2. W węźle *Computer Configuration* (Konfiguracja komputera) rozwiń węzeł **Administrative Templates** (Szablony administracyjne), następnie **System** i kliknij obiekt **Remote Assistance** (Pomoc zdalna).

- 3- Dwukrotnie kliknij obiekt **Offer Remote Assistance** (Oferuj pomoc zdalną), a następnie zaznacz opcję **Enabled** (Włączone). 4. Następnie kliknij przycisk **Show** (Pokaż) i określ poszczególnych użytkowników, którzy będą dopuszczeni do oferowania pomocy, poprzez przydzielenie pomocników wewnątrz kontekstu tej zasady. Pomocnik dodawany jest w postaci **domain\username** (domena\nazwa_użytkownika) i musi być członkiem grupy administratorów lokalnego komputera.

Inicjowanie pomocy zdalnej

Po zakończeniu powyższej konfiguracji, można ze swojego komputera rozpocząć realizację pomocy na komputerze użytkownika w oparciu o te uprawnienia, które zostały określone podczas definiowania pomocnika w zasadzie grupy komputera docelowego:

1. Otwórz program **Help And Support Center** (Centrum pomocy i obsługi technicznej), kliknij menu **Tools** (Narzędzia), a następnie kliknij opcję **Help And Support Center Tools** (Narzędzia centrum pomocy i obsługi technicznej). Kliknij opcję **Offer Remote Assistance** (Oferuj pomoc zdalną). Na rysunku 2-8 pokazany został omawiany ekran *Help And Support Center Tools* (Narzędzia centrum pomocy i obsługi technicznej).



Rysunek 2-8. Ekran *Help And Support Center Tools* (Narzędzia centrum pomocy i obsługi technicznej)

2. W oknie dialogowym wpisz nazwę lub adres IP komputera docelowego, a następnie kliknij przycisk **Connect** (Połącz). Wybierz sesję użytkownika, jeśli zalogowanych jest kilku użytkowników. Następnie kliknij przycisk **Start Remote Assistance** (Uruchom pomoc zdalną).
Na ekranie komputera użytkownika pojawi się okno informujące, że osoba z działu wsparcia technicznego rozpoczyna sesję programu *Remote Assistance* (Pomoc zdalna).
- 3- Użytkownik akceptuje zaproszenie, co rozpoczyna wykonywanie procedur pomocy zdalnej.



Alert bezpieczeństwa Istnieje szereg zagadnień, które należy rozważyć podczas zarządzania i administrowania za pomocą programu Remote Assistance (Pomoc zdalna) w środowisku korporacji bądź dużej organizacji. Administrator może określić otwarte środowisko, w którym pracownicy otrzymują pomoc zdalną poza ścianą ogniową (firewall) przedsiębiorstwa lub może ograniczyć pomoc zdalną za pomocą zasady grupy i zdefiniować kilka różnych poziomów uprawnień, jak na przykład umożliwienie dostępu programu Remote Assistance (Pomoc zdalna) wyłącznie wewnątrz organizacji. Połączenia poza ścianą ogniową wymagają otwarcia portu 3389.

Ograniczenia używania programu Remote Assistance (Pomoc zdalna) związane ze ścianą ogniową w sieci (firewall)

Program Remote Assistance (Pomoc zdalna) działa ma szczycie technologii Terminal Services (Usługi terminalowe), co oznacza że musi być używany ten sam port stosowany w programie Terminal Services (Usługi terminalowe): port 3389. Program Remote Assistance (Pomoc zdalna) nie będzie działał, jeśli zablokowany jest ruch zewnętrzny tego portu. Oprócz tego jest jeszcze kilka innych aspektów stosowania ściany ogniowej, w szczególności dotyczących translacji adresów sieciowych NAT (Network Address Translation).

- Program Remote Assistance (Pomoc zdalna) obsługuje technologię UPnP (Universal Plug and Play) przy współpracy z urządzeniami wykorzystującymi NAT (Network Address Translation). Jest to metoda przydatna w małych, biurowych sieciach, gdzie używane są technologie takie jak ICS (Internet Connection Sharing) systemu Windows XP. Jednak program ICS systemu Windows 2000 *nie* obsługuje UPnP.



Wskazówka egzaminacyjna Należy zwrócić uwagę na pytania, które zakładają stosowanie programu ICS systemu Windows 2000 w dużych, korporacyjnych działach wsparcia technicznego przy korzystaniu z pomocy zdalnej skierowanej do filii tej organizacji. Ponieważ program Windows 2000 ICS nie obsługuje technologii UPnP, będą mnożyć się problemy programu Remote Assistance (Pomoc zdalna).

- Program Remote Assistance (Pomoc zdalna) wykryje adres IP i port TCP urządzenia UPnP NAT i umieści ten adres w zaszyfrowanym bilecie. Ten adres i port będą używane do nawiązania połączenia 7. wykorzystaniem urządzenia NAT podczas rozpoczynania przez pomocnika lub żądającą stację roboczą sesji programu Remote Assistance (Pomoc zdalna). Żądanie połączenia programu Remote Assistance (Pomoc zdalna) będzie następnie przekierowane do klienta przez urządzenie NAT.
- Program Remote Assistance (Pomoc zdalna) nie połączy się, jeśli żądający jest za urządzeniem NAT, które nie obsługuje UPnP w sytuacji, kiedy wiadomość e-mail jest używana do przesłania pliku zaproszenia. W sytuacji, kiedy zaproszenie jest wysyłane za pomocą programu Windows Messenger, urządzenie NAT nie obsługujące UPnP będzie współpracować, jeśli jeden klient umieszczony jest za urządzeniem NAT. Jeśli oba komputery (pomocnika i żądającego) znajdują się za urządzeniem NAT, które nie obsługuje UPnP, połączenie programu Remote Assistance nie zostanie nawiązane.

Jeśli użytkownik w domu uruchamia oprogramowanie korzystające ze ściany ogniowej lub usługi NAT, to może używać programu Remote Assistance (Pomoc zdalna) w oparciu o typową konfigurację. Jedynym ograniczeniem jest konieczność otwierania portu 3389-

Informacja Usługa Instant Messenger Service działa w oparciu o port 1863.



Zadanie kontrolne: Korzystanie z programu Remote Assistance (Pomoc zdalna) za pomocą aplikacji Windows Messenger

Zadanie to wymaga do nawiązania sesji programu Remote Assistance (Pomoc zdalna) drugiego komputera lub współpracy z partnerem. Oba serwery Server01 i Server02 powinny mieć zainstalowane programy Windows Messenger i skonfigurowane dla dwóch różnych kont. Jeśli dysponujemy tylko jednym komputerem, sesję programu Remote Assistance (Pomoc zdalna) można nawiązać za pomocą dwóch odrębnych kont aplikacji Windows Messenger skonfigurowanych na tym samym komputerze, ale w takim przypadku nie będzie możliwa kontrola ekranu.

1. Na serwerze Server02 (lub innym komputerze) otwórz program **Windows Messenger** i zaloguj się używając konta Account #2 (konta programu Messenger).
2. W drugim programie **Windows Messenger** (logowanie za pomocą konta Account #1) z menu **Actions** (Akcje) wybierz polecenie **Ask For Remote Assistance** (Uzyskaj pomoc zdalną).
3. W oknie dialogowym *Ask for Remote Assistance* wybierz konto **Account #2**, a następnie kliknij przycisk OK.
4. Na tym etapie pojawia się sekwencja żądań i potwierdzeń pomiędzy dwoma aplikacjami Windows Messenger. Wybieraj przycisk **Accept** (Akceptuj) lub OK dla każdego pytania dotyczącego nawiązania sesji programu *Remote Assistance*.
5. Początkowo, sesja programu *Remote Assistance* działa w trybie *Screen View Only* (Widok ekranów). Aby przejąć kontrolę komputera — nowicjusza, należy wybrać opcję **Take Control** (Przejmij kontrolę) znajdującą się w górnej części okna programu *Remote Assistance*. Użytkownik - nowicjusz musi zaakceptować próbę przejęcia kontroli nad jego komputerem.



Informacja Zarówno nowicjusz, jak i ekspert mogą w dowolnym momencie zakończyć lub rozłączyć sesję.

Bez względu na to, czy ekspert przejmie kontrolę komputera nowicjusza, zostały włączone funkcje przeglądania ekranów, transferu plików i „rozmowy” (chat).

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć mater' lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pyt— i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Jakie są podobieństwa programów Remote Assistance (Pomoc zdalna) i Remote Desktop for Administration (Pulpit zdalny dla administracji)? Jakie są różnice?

2. Jakie są zalety programu Remote Assistance (Pomoc zdalna)?
3. Które z poniżej wymienionych ograniczeń dotyczących ściany ogniowej odnoszą się do programu Remote Assistance (Pomoc zdalna)?
 - a. Port 3389 musi być otwarty
 - b. NAT nie może być używany
 - c. Stosowanie usługi Internet Connection Sharing (Współużytkowanie połączenia internetowego) nie jest możliwe
 - d. Program Remote Assistance (Pomoc zdalna) nie może być używany z wykorzystaniem połączeń prywatnych sieci wirtualnych VPN (Virtual Private Network).

Podsumowanie lekcji

Program Remote Assistance (Pomoc zdalna) charakteryzuje się wspólnym działaniem: użytkownik może uzyskać pomoc od eksperta lub jeśli zostało to prawidłowo skonfigurowane w obiekcie Group Policy (Zasady grupy), ekspert może sam rozpocząć sesję. W obu przypadkach, użytkownik musi akceptować nawiązanie sesji i zgodzić się na przejęcie kontroli, a także w każdym momencie może zakończyć umożliwianie kontroli swojego komputera. W żadnym momencie ekspert nie może przejąć kontroli komputera użytkownika bez powiadamiania. Program Remote Assistance (Pomoc zdalna) jest zbudowany w oparciu o aplikację Terminal Services (Usługi terminalowe) oraz wykorzystuje interfejs systemu pomocy i programu Windows Messenger, aby umożliwić rozpoczęcie sesji, rozmowę, przeglądanie ekranów oraz przysyłanie plików. Technologie programów Terminal Services (Usługi terminalowe) i Remote Assistance (Pomoc zdalna) są ze sobą ściśle powiązane tak, że obie usługi używają tego samego portu sieci 3389, który musi być otwarty, aby możliwe było nawiązywanie sesji programu Remote Assistance (Pomoc zdalna) poprzez ścianę ogniową.

Zadanie praktyczne

Jako fragment procedur zdalnej administracji w przedsiębiorstwie zdecydowano włączyć na każdym komputerze program Remote Assistance (Pomoc zdalna). Przedstawiciele handlowi często podróżują i w trakcie tych podróży używają do pracy komputerów przenośnych.

W wewnętrznej sieci firmy, program Windows Messenger jest używany do komunikacji z klientami oraz dla programu Remote Assistance (Pomoc zdalna). Jednakże na ścianie ogniowej został zamknięty port 1863, stosowany przez program Instant Messenger dla ruchu w sieci Internet.

Użytkownicy zdalni powinni używać programu Remote Assistance (Pomoc zdalna), ale nie można się z nimi połączyć za pomocą programu Windows Messenger, aby stwierdzić, czy w danym momencie pracują na komputerze (status online).

Czy możliwe jest wykorzystywanie programu Remote Assistance (Pomoc zdalna) przez użytkowników zdalnych? Jeśli tak, w jaki sposób można zrealizować to zadanie?

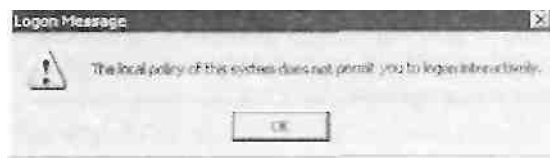
Należy korzystać z jednej z dwóch alternatywnych metod żądania wykorzystywanych w programie Remote Assistance (Pomoc zdalna).

- **Metoda wiadomości E-Mail** Wysyłanie wiadomości e-mail do eksperta za pomocą programu Help and Support Tools (Centrum pomocy i obsługi technicznej). Po otrzymaniu odsyłacza w wiadomości e-mail, ekspert będzie mógł ustawić sesję programu Remote Assistance (Pomoc zdalna).
- **Metoda pliku** Utworzenie pliku programu Remote Assistance (Pomoc zdalna) za pomocą aplikacji Help and Support Tools (Centrum pomocy i obsługi technicznej). Wysłanie pliku do eksperta za pomocą poczty elektronicznej lub udostępnienie pliku ekspertowi w współużytkowanym folderze. Po otrzymaniu odsyłacza w pliku, ekspert będzie mógł ustawić sesję programu Remote Assistance (Pomoc zdalna).

W obu metodach jest bardzo zalecane, aby hasło utworzone dla sesji programu Remote Assistance (Pomoc zdalna) było bezpiecznie dostarczone do eksperta, dzięki czemu nieupoważnione osoby nie będą mogły uzyskać dostępu do sesji.

Rozwiązywanie problemów

Podczas prób połączenia się z systemem Windows Server 2003 za pomocą programu Remote Desktop Connection (Podłączanie pulpitu zdalnego) stale wyświetlany jest komunikat pokazany na rysunku 2-9.



Rysunek 2-9. Błąd wyświetlany podczas prób połączenia do konsoli programu Remote Desktop For Administration (Pulpit zdalny dla administracji)

Zostały sprawdzone i potwierdzone następujące ustawienia serwera:

- Użytkownik należy do grupy Remote Desktop Users (Użytkownicy pulpitu zdalnego).
- Użytkownik nie należy do grupy Administrators (Administratorzy).
- Użytkownik mógł połączyć się z punktami współdzielonymi na komputerze, na którym uruchomiony jest program Terminal Server (Serwer terminali), a polecenie ping wysłane do komputera daje odpowiedź potwierdzającą.

Jakie inne ustawienia należy jeszcze sprawdzić na komputerze, na którym uruchomiono program Terminal Server (Serwer-terminali), aby rozwiązać ten problem?

Jest prawdopodobne, że Terminal Server (Serwer terminali) jest jednocześnie kontrolerem domeny (Domain Controller), a obiekt Default Domain Controller Group Policy (Domyślna zasada grupy kontrolera domeny) nie zezwala na połączenia zdalne dla grupy Remote Administrative Users (Użytkownicy administracji zdalnej). Obiekt Local Group Policy (Lokalna zasada grupy) na kon-

trolerach domen zezwala na połączenia tylko dla administratorów i musi zostać zmodyfikowany. Najprostszym sposobem modyfikacji lokalnej zasady grupy jest taka zmiana, aby zasada ta stała się domyślną zasadą grupy kontrolera domeny (Default Domain Controller Group Policy).

Podsumowanie rozdziału

- Konsole MMC są wspólnym interfejsem narzędzi systemu Windows Server 2003-
- Przystawki są poszczególnymi narzędziami, które można dodawać do konsoli MMC.
- Niektóre przystawki mogą być używane do konfigurowania komputerów zdalnych, działanie innych jest ograniczone tylko do komputera lokalnego.
- Konsole MMC mogą być zapisywane w dwóch trybach: z pełnym dostępem — tryb Author (autorski) lub z ograniczonym dostępem - tryb User (użytkownika). Tryb konsoli MMC nie uprawnia ani nie uniemożliwia użytkownikowi wykonywania tego, do czego ma uwierzytelnienie i dostęp poprzez swoje uprawnienia.
- Program Remote Desktop for Administration (Pulpit zdalny dla administracji) umożliwia administrację serwera przeprowadzaną z lokalizacji zdalnej w taki sam sposób, jak po interaktywnym zalogowaniu się na konsoli lokalnej.
- Spośród systemów operacyjnych dla stacji roboczych, jedynie Windows XP umożliwia obsługę programu Remote Desktop for Administration (Pulpit zdalny dla administracji).
- Program Remote Assistance (Pomoc zdalna), podobnie jak program Remote Desktop for Administration (Pulpit zdalny dla administracji) dla pulpitu, umożliwia zdalne przeglądanie i kontrolę pulpitów komputerów systemu Windows XP.
- Program Remote Assistance (Pomoc zdalna) działa także w systemie Windows Server 2003.
- Zrealizowanie pomocy zdalnej wymaga współpracy dwóch osób: użytkownika na komputerze docelowym oraz eksperta obsługującego inny komputer. Podczas sesji obaj użytkownicy muszą zaakceptować czynności kontrolne, a sesja może być w dowolnym momencie zakończona przez każdego z nich.

Informacje dla zdających egzamin

Przed przystąpieniem do egzaminu należy zapoznać się z przedstawionymi poniżej najważniejszymi faktami i pojęciami, aby określić, które tematy wymagają przejrzania. Należy powrócić do lekcji, aby osiągnąć większą wprawę oraz przejrzeć znajdujące się w części 2 działu „Materiały dodatkowe”, które skierowują do materiałów uzupełniających tematy objęte zadaniami egzaminacyjnymi.

Najważniejsze fakty

- Konsole MMC są kontenerami dla przystawek.
- Przystawki mogą być używane w kontekście lokalnym lub zdalnym, nie mogą natomiast być jednocześnie połączone do komputerów zdalnych i lokalnych.
- W pojedynczej konsoli, przystawki mogą być łączone dla dostosowania preferencji związanych z administracją.

- Konsole MMC mogą być zapisywane w trybie User (użytkownika), aby ograniczyć konfigurację, jednak możliwość wykonywania zadań jest określona przez uprawnienia, a nie przez ograniczenia zdefiniowane przez daną konsolę MMC. Jeśli użytkownik ma wystarczające uprawnienia do zarządzania komputerem, może tworzyć konsole MMC dodając dowolne przystawki.
- Program Remote Desktop for Administration (Pulpit zdalny dla administracji) wymaga odpowiednich uprawnień do połączenia za pomocą klienta programu Remote Desktop (Pulpit zdalny). Ustawienia domyślne określają, że uprawnienia te są przydzielone administratorom.
- Program Remote Assistance (Pomoc zdalna) jest dwukierunkową sesją wymagającą akceptacji. W żadnym momencie ekspert nie może przejąć nieautoryzowanej kontroli nad komputerem użytkownika.
- Port 3389 — taki sam port jest używany przez program Remote Desktop for Administration (Pulpit zdalny dla administracji), musi być otwarty dla ściany ogniowej, aby sesja programu Remote Assistance (Pomoc zdalna) mogła zostać ustanowiona.

Najważniejsze pojęcia

Porównanie programów Remote Assistance (Pomoc zdalna) i Remote Desktop for Administration (Pulpit zdalny dla administracji) Program Remote Assistance (Pomoc zdalna) umożliwia ekspertowi nawiązanie sesji kontroli zdalnej, jeśli został o to poproszony przez użytkownika — nowicjusza. Dokumenty uwierzytelnienia dostarczane są w postaci współdzielonego tajnego hasła, utworzonego przez nowicjusza podczas zapraszania do sesji. Program Remote Desktop for Administration (Pulpit zdalny dla administracji) wymaga tylko jednego użytkownika, który przyłączony jest zdalnie **do** komputera, na którym uruchomione są usługi programu Terminal Server (Serwer terminali) oraz który jest skonfigurowany tak, aby dopuszczał połączenia programu Remote Desktop (Pulpit zdalny).

Microsoft Management Console (konsola MMC) Jakie funkcje można realizować za pomocą połączeń zdalnych przystawek oraz jakie wymagane są uprawnienia.

Remote Desktop for Administration (Pulpit zdalny dla administracji) Uprawnienia i konfiguracja serwera wymagana dla połączeń programu Remote Desktop for Administration (Pulpit zdalny dla administracji).

Pytania i odpowiedzi

4) Pytania do lekcji 1

1. Który tryb jest domyślnym trybem tworzenia konsoli MMC?
Domyślnym trybem konsoli MMC jest tryb Author (autorski).
2. Czy przystawka może jednocześnie śledzić komputer lokalny i komputer zdalny?
Nie. Przystawki mogą być skonfigurowane, aby łączyły się z komputerem lokalnym lub zdalnym, ale nie mogą łączyć się z nimi jednocześnie.

- 3- Jeśli zachodzi potrzeba ograniczenia dostępu do danej przystawki, w jaki sposób należy zbudować konsolę MMC zawierającą tę przystawkę?

Należy zapisać konsolę w jednym z trybów użytkownika (User), w zależności od wymaganego poziomu ograniczeń.

Pytania do lekcji 2

1. Jakie uprawnienia są wymagane do administrowania komputerem zdalnym za pomocą konsoli MMC?

Do przeprowadzania administracji zdalnej użytkownik musi mieć uprawnienia administracji dotyczące komputera zdalnego.

2. Czy można dla istniejącej przystawki konsoli MMC zmienić kontekst z lokalnego na zdalny lub też konieczne jest załadowanie przystawki takiego samego typu przy skonfigurowaniu jej dla połączenia zdalnego?

Kontekst przystawek może być zmieniony przez zmianę właściwości danej przystawki. Przystawka nie musi być ponownie uruchamiana, aby została zmieniona jej konfiguracja.

3. Czy wszystkie funkcje przystawki dla komputera lokalnego mogą być używane na komputerze zdalnym?

Nie, nie wszystkie funkcje są dostępne. Na przykład element Device Manager (Menedżer urządzeń) w przystawce Computer Management (Zarządzanie komputerem) może być używany jedynie do przeglądania konfiguracji komputera zdalnego, ale nie można przeprowadzać zmian konfiguracji urządzeń komputera.

Pytania do lekcji 3

1. Jaka jest maksymalna liczba jednoczesnych połączeń do programu Terminal Server uruchomionego w trybie administracji zdalnej? Dlaczego?

Trzy; dwa połączenia zdalne i jedno połączenie do konsoli (ale to nie jest fair, prawda?). Tak więc, z technicznego punktu widzenia ograniczenie do dwóch połączeń wynika z tego, że w programie Terminal Server (Serwer terminali) skonfigurowanym dla administracji zdalnej w trybie programu Remote Desktop (Pulpit zdalny) nie są instalowane komponenty współużytkowania aplikacji.

2. Jaki jest najlepszy sposób udostępnienia administratorom możliwości zarządzania zdalnego serwerem za pomocą programu Terminal Services (Usługi terminalowe)?

- Nie trzeba wykonywać żadnych czynności, administratorzy mają już taki dostęp.
- Usunięcie administratorów z listy uprawnień połączenia programu Terminal Server (Serwer terminali) i przesunięcia tych kont do grupy Remote Desktop for Administration (Pulpit zdalny dla administracji).
- Utworzenie oddzielnego, o niższym niż administratorzy poziomie uwierzytelnienia konta użytkownika, które będzie używane codziennie i umieszczenie tego konta w grupie Remote Desktop for Administration (Pulpit zdalny dla administracji).

Prawidłowa odpowiedź to c. Jest to zalecana praktyka, aby logować się za pomocą konta o minimalnych uprawnieniach, zamiast uruchamiać narzędzia administracyjne przy najwyższych uprawnieniach za pomocą polecenia RunAs.

- 3- Które narzędzie jest używane do włączenia na serwerze programu Remote Desktop (Pulpia zdalny)?
- Terminal Services Manager (Menedżer usług terminalowych)
 - Terminal Services Configuration (Konfiguracja usług terminalowych)
 - Właściwości modułu System w programie Control Panel (Panel sterowania)
 - Terminal Services Licensing (Licencjonowanie usług terminalowych)

Prawidłowa odpowiedź: c.

Pytania do lekcji 4

1. Jakie są podobieństwa programów Remote Assistance (Pomoc zdalna) i Remote Desktop for Administration (Pulpit zdalny dla administracji)? Jakie są różnice?

Program Remote Assistance (Pomoc zdalna) umożliwia kontrolę zdalną komputera tak, jakby użytkownik znajdował się przed pulpitem komputera zdalnego, program realizuje połączenie do serwera terminali (Terminal Server) poprzez aplikację Remote Desktop for Administration (Pulpit zdalny dla administracji).

Program Remote Desktop for Administration (Pulpit zdalny dla administracji) jest kontrolowany wyłącznie przez katalog kont, lokalnych lub domenowych, które są skonfigurowany na tym komputerze dla połączeń programu Terminal Server (Serwer terminali). Program Remote Assistance (Pomoc zdalna) wymaga pewnych typów potwierdzeń pomiędzy użytkownikiem a pomocnikiem — ekspertem.

2. Jakie są zalety programu Remote Assistance (Pomoc zdalna)?

Aby udzielić pomocy, ekspert nie musi przebywać w siedzibie użytkownika. Zostały usunięte trudności związane z usuwaniem problemów „przez telefon”.

3. Które z poniżej wymienionych ograniczeń dotyczących ściany ogniowej odnoszą się do programu Remote Assistance (Pomoc zdalna)?
- Port 3389 musi być otwarty
 - NAT nie może być używany
 - Nie jest możliwe stosowanie usługi Internet Connection Sharing (Współużytkowanie połączenia internetowego)
 - Program Remote Assistance (Pomoc zdalna) nie może być używany z wykorzystaniem połączeń prywatnych sieci wirtualnych VPN (Virtual Private Network).

Prawidłowa odpowiedź: a.

3 Konta użytkowników



Zadania egzaminacyjne omawiane w tym rozdziale:

- Tworzenie i zarządzanie kontami użytkowników
- Tworzenie i modyfikowanie kont użytkowników za pomocą przystawki konsoli MMC (Microsoft Management Console) - Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory)
- Automatyzacja tworzenia i modyfikowania kont użytkowników
- Importowanie kont użytkowników
- Zarządzanie lokalnymi, mobilnymi i obowiązkowymi profilami użytkowników
- Rozwiązywanie problemów dotyczących kont użytkowników
- Diagnostyka i rozwiązywanie problemów zablokowanych kont
- Diagnostyka i rozwiązywanie zagadnień dotyczących właściwości kont użytkowników
- Rozwiązywanie problemów dotyczących uwierzytelnień

Cele rozdziału

Przed udostępnieniem dostępu do zasobów dla poszczególnych pracowników firmy, administrator musi włączyć procesy uwierzytelniania tych osób. Rzecz jasna, głównym elementem uwierzytelnienia jest identyfikacja użytkownika, obsługiwana jako konto w usłudze katalogowej Microsoft Active Directory. W rozdziale tym student zapoznaje się i pogłębia swoją wiedzę o tworzeniu, obsłudze i rozwiązywaniu problemów dotyczących kont użytkowników i ich uwierzytelnienia.

Każdy dzień, w każdym przedsiębiorstwie przynosi unikalny zestaw problemów dotyczących zarządzania użytkownikami. Właściwości konfiguracji typowego konta użytkownika są prawdopodobnie inne niż właściwości członków zespołu wsparcia pomocy technicznej, a na pewno inne niż dla wbudowanego w systemie konta administratora. Umiejętności wystarczające do tworzenia i modyfikowania pojedynczego konta użytkownika stają się nieporadne i mało efektywne podczas pracy z dużą liczbą kont, jak w przypadku zarządzania kontami nowoprzyjętych pracowników.

Aby zarządzanie kontami było sprawne w rozmaitych sytuacjach praktycznych, w rozdziale tym przeanalizowane zostaną różne narzędzia i metody zamieszczone w przystawce Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) oraz w programach narzędziowych wiersza poleceń.

Lekcje rozdziału:

- Lekcja 1: Tworzenie i zarządzanie obiektami użytkowników 67
- Lekcja 2: Tworzenie wielokrotne obiektów użytkownika 79
- Lekcja 3: Zarządzanie profilami użytkowników 92
- Lekcja 4: Bezpieczeństwo i rozwiązywanie problemów związanych z uwierzytelnieniem 102

Wymagania

W rozdziale tym zostały przedstawione umiejętności i pojęcia dotyczące kont usługi Active Directory. Opracowując niniejszy zestaw szkoleniowy założono, że student ma co najmniej 18-miesięczne doświadczenia w obsłudze usługi Active Directory, konsoli MMC oraz przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory). Jeśli jednak student chciałby przeprowadzić ćwiczenia praktyczne w oparciu o prezentowane w rozdziale przykłady, to powinien przygotować następujące elementy:

- Komputer z zainstalowanym systemem Microsoft Windows Server 2003 (Standard lub Enterprise). Serwer powinien być nazwany **Server01** i skonfigurowany jako kontroler domeny w domenie *contoso.com*
- Jednostki organizacyjne (OU) pierwszego poziomu: *Administrative Groups*, *Employees* i *Security Groups*
- Grupy globalne znajdujące się w jednostce organizacyjnej Security Groups OU o nazwach *Sales Representatives* oraz *Sales Managers*
- Konsola *Active Directory Users And Computers* (Użytkownicy i komputery usługi Active Directory) lub niestandardowa konsola MMC, zawierająca przystawkę *Active Directory Users And Computers*.

Lekcja 1: Tworzenie i zarządzanie obiektami użytkowników

Usługa Active Directory wymaga, aby przed umożliwieniem poszczególnym jednostkom dostępu do zasobów, przeprowadzona została weryfikacja tożsamości tych jednostek. Proces ten nazywany jest uwierzytelnieniem. Podstawą uwierzytelnienia jest konto użytkownika wraz z jego nazwą logowania, hasłem i unikalnym identyfikatorem zabezpieczeń (SID). Podczas logowania usługa Active Directory uwierzytelnia wprowadzoną nazwę użytkownika i hasło. Następnie podsystem zabezpieczeń tworzy żeton (token) dostępu reprezentujący użytkownika. Żeton dostępu zawiera identyfikator SID konta użytkownika, jak również identyfikator SID grup, do których należy użytkownik. Żeton ten może być następnie używany do sprawdzania praw przypisanych użytkownikowi, wliczając w to prawo lokalnego logowania się na komputerze oraz uwierzytelnionego dostępu do zasobów zabezpieczonych przez listy kontroli dostępu (ACL).

Konto użytkownika jest 7-integrowane z obiektem użytkownika w usłudze Active Directory. Obiekt użytkownika oprócz nazwy użytkownika i hasła oraz identyfikatora SID, zawiera również informacje kontaktowe (takie jak numer telefonu bądź adres), informacje związane ze stanowiskiem w przedsiębiorstwie (takie jak stanowisko czy tytuł), informacje o członkostwie w grupach oraz informacje o konfiguracji takie jak profil mobilny, usługi terminalowe bądź ustawienia kontroli zdalnej. Niniejsza lekcja stanowi przegląd i pogłębienie wiedzy o obiektach usługi Active Directory.

Materiały omówione podczas lekcji pozwalają na

- Tworzenie obiektów użytkownika w usłudze Active Directory za pomocą przystawki Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory)
- Konfigurowanie właściwości obiektu użytkownika
- Wyjaśnienie istotnych opcji dotyczących kont, które nie są oczywiste, jeśli opierać się tylko na ich opisach.
- Jednoczesne modyfikowanie właściwości wielu obiektów

Szacunkowy czas lekcji: 15 minut

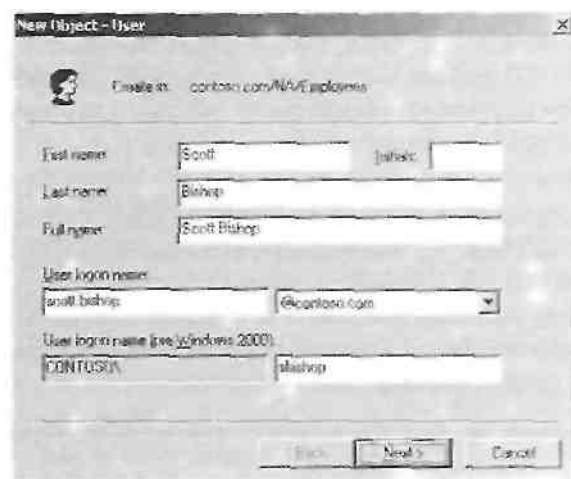
Tworzenie obiektów użytkownika za pomocą konsoli Active Directory Users and Computers

Obiekt użytkownika można tworzyć za pomocą przystawki *Active Directory Users and Computers* (Użytkownicy i komputery usługi Active Directory). Pomimo, że obiekty użytkownika mogą być tworzone w domenie lub w dowolnym kontenerze domyślnym, zalecane jest tworzenie użytkowników w jednostkach organizacyjnych tak, aby w pełni można było korzystać z zalet delegowania administracji czy funkcji obiektów zasady grupy GPO (*Group Policy Object*).

Aby utworzyć obiekt użytkownika, należy wybrać kontener, w którym obiekt ten ma się znajdować, kliknąć menu **Action** (Akcja), a następnie wybrać kolejno polecenia **New** (Nowy) i **User** (Użytkownik). Aby utworzyć obiekt użytkownika w kontenerze, użytkownik musi być członkiem grupy *Enterprise Admins* (Administratorzy przedsiębiorstwa), *Domain Admins* (Administratorzy domeny) lub *Account Operators* (Operatorzy kont), albo też użytkownikowi temu zostały przekazane (delegowanie)

uprawnienia administracyjne pozwalające tworzyć obiekty użytkownika w kontenerze. Jeśli uprawnienia są niewystarczające, polecenie *New User* jest nieaktywne.

Wyświetlone zostanie okno dialogowe *New Object—User* (Nowy obiekt — Użytkownik), pokazane na rysunku 3-1. Pierwsza strona tego okna dotyczy nazwy użytkownika. W tabeli 3-1 opisane zostały właściwości dostępne na pierwszej stronie okna dialogowego.



Rysunek 3-1. Okno dialogowe *New Object-User*

Tabela 3-1. Właściwości użytkownika zamieszczone na pierwszej stronie okna dialogowego *New Object-User*

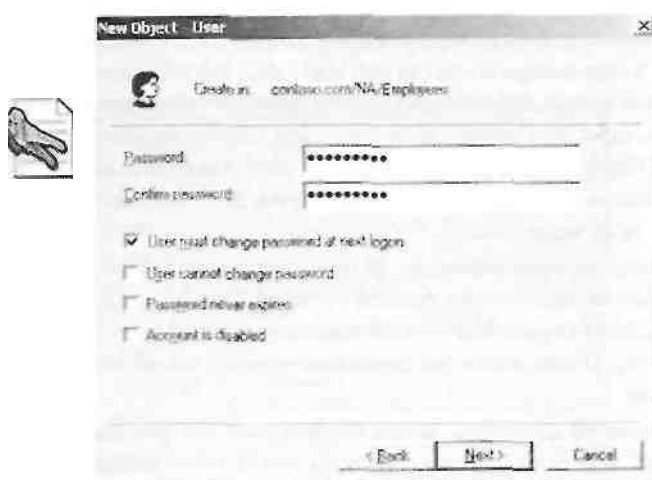
Właściwość	Opis
Imię Inicjały	Imię użytkownika. Nie wymagane. Inicjały
Nazwisko Pełna nazwa	nazwy użytkownika. Nie wymagane. Nazwiska użytkownika. Nie wymagane. Pełna nazwa użytkownika. Jeśli zostały wprowadzone wartości w polach do wprowadzania imienia i nazwiska, pole pełnej nazwy użytkownika wypełniane jest automatycznie. Podpowiadaną nazwę można zmodyfikować. Wypełnienie pola jest wymagane.
User Logon Name (Nazwa logowania użytkownika)	Główna nazwa użytkownika UPN (User Principal Name) składa się z nazwy logowania i przyrostka UPN. Przyrostkiem domyślnie jest nazwa DNS domeny, w której tworzony jest obiekt. Właściwość jest wymagana, a cała nazwa UPN, mająca składnię nazwa_logowania@przyrostek_UPN, musi być unikatowa wewnątrz lasu usługi Active Directory. Przykładem nazwy UPN może być <u>bysomeonc@contoso.com</u> . Nazwa UPN może być używana do logowania się w dowolnym systemie, na którym uruchomione są systemy Microsoft Windows 2000, Windows XP lub Windows Server 2003.

ciąg dalszy na następnej stronie

ciąg dalszy ze strony poprzedniej

Właściwość	Opis
User Logon Name (Pre-Windows 2000) (nazwa logowania dla systemów starszych niż Windows 2000)	Ta nazwa logowania jest używana do logowania za pomocą klientów niższego poziomu, takich jak klienci systemów Microsoft Windows 95, Windows 98, Windows Millennium Edition (Windows Me), Windows NT 4 lub Windows NT 3.51. Wypełnienie pola jest wymagane, a wewnątrz domeny nazwa musi być unikatowa.

Po wypełnieniu pól pierwszej strony okna dialogowego *New Object—User* (Nowy obiekt — Użytkownik) należy kliknąć przycisk *Next* (Dalej). Następną stronę pokazaną została na rysunku 3-2 i w oknie tym można wpisywać hasło użytkownika oraz można określać flagi konta.



Rysunek 3-2. Druga strona okna dialogowego *New Object—User* (Nowy obiekt — Użytkownik)

Alert bezpieczeństwa Domyślne zasady kont domeny systemu Windows Server 2003, definiowane w obiekcie GPO - Default Domain Policy (Domyślna zasada domeny), wymuszają stosowanie złożonych haseł, które mają przynajmniej 7 znaków. Złożoność hasła oznacza też, że musi ono zawierać trzy z czterech rodzajów znaków: duże litery, małe litery, cyfry oraz znaki inne niż alfanumeryczne. Podczas używania systemu Windows Server 2003 w środowisku testowym, powinno się stosować tę samą praktykę, wymaganą dla sieci produkcyjnych. Dlatego w niniejszym zestawie szkoleniowym użytkownik jest zachęcany do stosowania haseł złożonych dla tworzonych kont. Podczas logowania zmusza to jednak do pamiętania trudnych haseł.

Właściwości, które są dostępne na drugiej stronie okna dialogowego *New Object—User*, zostały zebrane i przedstawione w tabeli 3-2.

Tabela 3-2 Właściwości obiektu użytkownika znajdujące się na drugiej stronie okna dialogowego New Object-User

Właściwość	Opis
Password (Hasło)	Hasło używane do uwierzytelnienia użytkownika. Ze względów bezpieczeństwa hasło powinno być zawsze przydzielane. Podczas wprowadzania hasło nie jest wyświetlane.
Confirm Password (Potwierdzenie hasła) User Must Change Password At Next Logon (Użytkownik musi zmienić hasło przy następnym logowaniu)	Pole, w którym ponownie wprowadzane jest hasło, aby upewnić się, że przy pierwszym wprowadzaniu hasła nie nastąpiła pomyłka. To pole wyboru należy zaznaczyć, jeśli chcemy, aby przy pierwszym logowaniu użytkownik zmienił wprowadzone przez administratora hasło. Opcji tej nie można zaznaczyć, jeśli wybrana została opcja Password Never Expires (Hasło nigdy nie wygasa). Zaznaczenie omawianej opcji wyklucza zaznaczenie opcji User Cannot Change Password (Użytkownik nie może zmienić hasła).
User Cannot Change Password (Użytkownik nie może zmienić hasła)	Zaznaczenie tego pola wyboru jest przydatne, jeśli kilku użytkowników korzysta z tego samego konta (na przykład Gość) lub jeśli należy kontrolować hasła konta użytkownika. Opcja ta jest często stosowana do zarządzania hasłami kont usług. Opcje User Must Change Password At Next Logon (Użytkownik musi zmienić hasło przy następnym logowaniu) i User Cannot Change Password (Użytkownik nie może zmienić hasła) wykluczają się wzajemnie.
Password Never Expires (Hasło nigdy nie wygasa)	Zaznaczenie tej opcji powoduje, że hasło jest zawsze ważne. Wybranie opcji automatycznie usuwa zaznaczenie opcji User Must Change Password At Next Logon (Użytkownik musi zmienić hasło przy następnym logowaniu). Ustawienia to jest często stosowane do zarządzania hasłami kont usług.
Account Is Disabled (Konto jest wyłączone)	Zaznaczenie opcji wyłącza konto użytkownika. Na przykład, opcja może być przydatna podczas tworzenia konta nowo zatrudnionego pracownika, który nie potrzebuje jeszcze dostępu do sieci.



Nieoficjalnie Podczas tworzenia obiektów nowych użytkowników, dla każdego z nich należy definiować unikatowe, złożone hasła, które nie są zgodne z łatwym do przewidzenia szablonem. Należy również zaznaczać opcję wymuszającą zmianę hasła przy pierwszym logowaniu. Jeśli prawdopodobnie użytkownik nie będzie się logował w określonym czasie, konto należy wyłączyć. Kiedy dla użytkownika potrzebny staje się dostęp do sieci, należy sprawdzić, czy konto jest włączone. Użytkownik zostanie poproszony o utworzenie nowego, znanemu tylko jemu, unikatowego hasła.

Niektóre opcje konta przedstawione w tabeli 3-2 mogą być potencjalnie w sprzeczności z ustawieniami zasad domeny. Na przykład, domyślna zasada domeny wprowadza najlepszą praktykę zabraniającą zachowywania haseł za pomocą odwracalnego szyfrowania. Jednakże, w rzadko spotykanych sytuacjach, kiedy potrzebne jest szyfrowanie odwracalne, właściwość użytkownika *Store Password Using Reversible Encryption* (Zachowaj hasło przy użyciu szyfrowania odwracalnego), będzie miała pierwszeństwo w stosunku do tego konkretnego obiektu. Podobnie domena może określać maksymalny wiek hasła lub wymuszać zmianę hasła użytkownika przy następnym logowaniu. Tak więc, jeśli

dla obiektu użytkownika została zaznaczona opcja *Password never expires* (Hasło nigdy nie wygasa), to konfiguracja ta zostanie zastąpiona przez ustawienia zasad domeny.

Zarządzanie obiektami użytkownika za pomocą konsoli Active Directory Users And Computers

Podczas tworzenia użytkowników należy skonfigurować najważniejsze właściwości obiektu, takie jak nazwa logowania i hasło. Obiekty użytkownika mają jednak wiele innych, dodatkowych właściwości, które w dowolnym momencie można konfigurować za pomocą konsoli *Active Directory Users And Computers* (Użytkownicy i komputery usługi Active Directory). Jej funkcje ułatwiają administrowanie i wyszukiwanie obiektów.

Aby skonfigurować właściwości obiektu użytkownika, należy zaznaczyć obiekt, kliknąć menu **Action** (Akcja), a następnie wybrać polecenie **Properties** (Właściwości). Wyświetlone zostanie okno dialogowe właściwości użytkownika, pokazane na rysunku 3-3. Alternatywnym sposobem wyświetlenia tego okna jest kliknięcie obiektu prawym przyciskiem myszy i wybranie z rozwijanego menu polecenia **Properties**.



Rysunek 3-3. Okno dialogowe *Users Properties* (Właściwości użytkownika) Strony

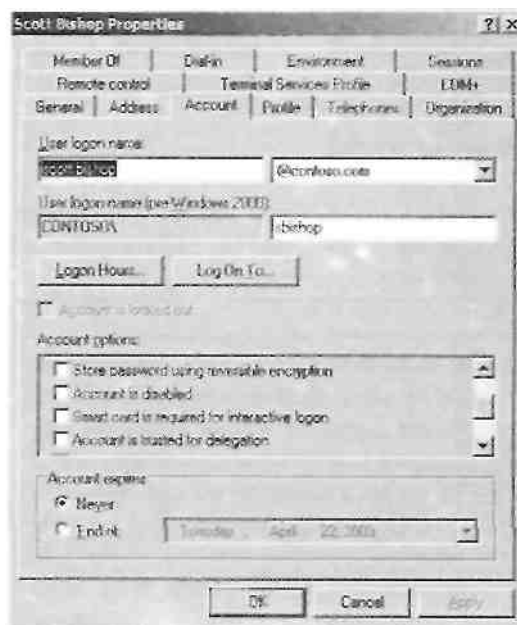
okna dialogowego przedstawiają właściwości podzielone na kilka kategorii:

- **Właściwości konta:** zakładka **Account** (Konto) Właściwości te dotyczą tych cech, które są konfigurowane podczas tworzenia obiektu użytkownika, wliczając w to nazwy logowania, hasła czy flagi konta.
- **Informacje osobowe:** zakładki **General** (Ogólne), **Address** (Adres), **Telephones** (Telefony) oraz **Organization** (Organizacja) Zakładka General (Ogólne) prezentuje właściwości nazwy, która powstała podczas tworzenia obiektu użytkownika.

- **Zarządzanie konfiguracją użytkownika: zakładka Profile (Profil)** W tym miejscu można przeprowadzić konfigurację profilu użytkownika obejmującą ścieżkę, skrypt logowania oraz lokalizację katalogu macierzystego.
- **Członkostwo w grupach: zakładka Member Of (Członek grupy)** Na tej zakładce można dodawać lub usuwać grupy, do których należy użytkownik oraz można określić podstawową grupę użytkownika.
- **Usługi terminalowe: zakładki Terminal Services Profile (Profil usług terminalowych), Environment (Środowisko), Remote Control (Zdalne sterowanie) oraz Sessions (Sesje)** Te cztery zakładki umożliwiają skonfigurowanie i zarządzanie właściwościami sesji programu Terminal Services (Usługi terminalowe).
- **Dostęp zdalny: zakładka Dial-in (Telefonowanie)** Umożliwia włączenie i konfigurowanie dla użytkownika uprawnień dostępu zdalnego.
- **Aplikacje: zakładka COM+** Przypisuje użytkownikowi zbiór partycji COM+ usługi Active Directory. Właściwość ta jest nową cechą systemu Windows Server 2003 i ułatwia zarządzanie aplikacjami rozproszonymi.

Właściwości konta

Najważniejsze właściwości konta użytkownika znajdują się na zakładce *Account* (Konto) w oknie dialogowym właściwości użytkownika. Przykład takiej zakładki został pokazany na rysunku 3-4.



Rysunek 3-4. Zakładka *Account* (Konto użytkownika)

Kilka właściwości zostało opisanych w tabeli 3-2. Właściwości te są określane podczas tworzenia obiektu użytkownika i mogą być modyfikowane, tak jak większy zbiór właściwości, za pomocą zakładki

Account. Znaczenie niektórych właściwości nie jest oczywiste i warto przyjrzeć się ich definicjom zamieszczonym w tabeli 3-3-

Tabela 3-3. Właściwości konta użytkownika

Właściwość	Opis
Logon Hours (Godziny logowania)	Aby określić, w których godzinach użytkownik może zalogować się do sieci, należy kliknąć przycisk Logon Hours (Godziny logowania). Po kliknięciu przycisku Log On To (Zaloguj do) otwarte zostanie okno umożliwiające zdefiniowanie, do których stacji roboczych użytkownik będzie mógł się logować. W innej części interfejsu użytkownika, właściwość ta nazywana jest Computer Restrictions (Ograniczenia komputera). Aby wprowadzić te ograniczenia, musi być włączony protokół NetBIOS poprzez TCP/IP, ponieważ cecha ta w celu ograniczenia logowania użytkownika używa nazwy komputera, a nie adresu MAC (Media Access Control) karty sieciowej.
Log On To (Zaloguj do)	
Store Password Using Reversible Encryption (Zachowaj hasło przy użyciu szyfrowania odwracalnego)	Opcja ta przy zapisywaniu hasła w usłudze Active Directory nie korzysta z jej mocnego, nieodwracalnego algorytmu szyfrowania i jest przydatna do obsługi aplikacji, którym niezbędne są informacje o hasle użytkownika. Jeśli cecha ta nie jest absolutnie konieczna, nie należy włączać tej opcji, ponieważ znacząco zostaje zmniejszona ochrona hasła. Hasła przechowywane przy użyciu szyfrowania odwracalnego są podobne do haseł zapisanych tekstem otwartym.
Smart Card Is Required For Interactive Logon (Logowanie interakcyjne wymaga karty inteligentnej)	Karty inteligentne są przenośnymi urządzeniami sprzętowymi, których modyfikacje są trudne do przeprowadzenia. Przechowują unikatowe informacje identyfikacyjne użytkownika. Są przyłączane lub wkładane do systemu i stanowią dodatkowy, fizyczny komponent procesu uwierzytelnienia.
Account Is Trusted For Delegation (Konto jest zaufane w kwestii delegowania)	Opcja ta włącza usługę konta, która umożliwia dostęp do zasobów sieci w imieniu użytkownika. Najczęściej opcja ta nie jest wybierana, z pewnością nie dla obiektów użytkownika reprezentujących ludzi. Najczęściej jest używana dla kont usług w infrastrukturach trój- lub wielowarstwowych aplikacji. Używane do określania, kiedy konto wygasa.
Account Expires (Wygasanie konta)	

Jednoczesne zarządzanie właściwościami wielu kont

System Windows Server 2003 umożliwia jednoczesne modyfikowanie właściwości wielu kont użytkownika. Kilka kont wybiera się po prostu przez klikanie każdego konta przy jednocześnie wciśniętym przycisku CTRL lub za pomocą innej metody wyboru wielokrotnego. Należy upewnić się, że zaznaczone zostały obiekty należące tylko do jednej klasy, takie jak użytkownicy. Po zaznaczeniu kilku użytkowników, w menu Action (Akcja) należy wybrać polecenie Properties (Właściwości).

Przy zaznaczeniu wielu obiektów użytkowników, dla modyfikacji dostępny jest podzbiór właściwości.

- Zakładka General (Ogólne) Description (Opis), Office (Biuro), Telephone Number (Numer telefonu), Fax (Faks), Web Page (Strona sieci Web), E-mail

MCSE Training Kit: Egzamin 70-290

- **Zakładka Account (Konto)** UPN Suffix (przyrostek nazwy UPN), Logon Hours (Godziny logowania), Computer Restrictions (logon workstations) (Zaloguj do), Account Options (Opcje konta) — wszystkie, Account Expires (Wygasanie konta)
- **Address (Adres)** Street (Ulica), PO Box (Skrytka), City (Miasto), State/Province (Województwo), ZIP/Postal Code (Kod pocztowy), Country/Region (Kraj/Region),
- **Profile (Profil)** Profile Path (Ścieżka profilu), Logon Script (Skrypt logowania) oraz Home Folder (Folder macierzysty)
- **Organization (Organizacja)** Title (Tytuł), Department (Dział), Company (Firma), Manager (Menedżer)



Wskazówka Należy dobrze orientować się, które właściwości mogą być jednocześnie modyfikowane dla wielu użytkowników. Pytania egzaminacyjne, które sugerują potrzebę zmiany wielu właściwości obiektów tak szybko, jak to jest możliwe, często sprawdzają zrozumienie zagadnień związanych z wyborem wielokrotnym.

Jest wiele właściwości, które muszą być określone osobno dla każdego użytkownika. Także niektóre zadania administracyjne, jak na przykład usuwanie haseł bądź zmiana nazwy konta, w danym momencie mogą być wykonywane tylko dla jednego użytkownika.

Przenoszenie użytkownika

Jeśli wewnątrz organizacji użytkownik jest przenoszony, prawdopodobnie trzeba będzie przenieść również obiekt użytkownika tak, aby nastąpiły odpowiednie zmiany w administrowaniu lub konfiguracji tego obiektu. Aby przesunąć obiekt za pomocą konsoli *Active Directory Users and Computers*, należy zaznaczyć obiekt i z menu **Action** (Akcja) wybrać polecenie Move (Przenieś). To samo można osiągnąć, klikając obiekt prawym przyciskiem myszy i wybierając z menu polecenie Move (Przenieś).



Wskazówka Nową cechą systemu Windows Server 2003 jest obsługa operacji typu „przesuń i upuść”. W przystawce Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) użytkownik może przenosić obiekty między jednostkami organizacyjnymi „przesuwając je i upuszczając” w odpowiednim miejscu.

Zadanie kontrolne: Tworzenie i zarządzanie obiektami użytkownika

W zadaniu tym zostaną utworzone trzy obiekty użytkownika, a następnie będą modyfikowane ich właściwości.

Ćwiczenie 1: Tworzenie obiektu użytkownika

1. Do serwera Server01 zaloguj się jako administrator.
2. Otwórz konsolę *Active Directory Users And Computers* (Użytkownicy i komputery usługi Active Directory).
3. Zaznacz jednostkę organizacyjną **Employees**.
4. Utwórz/ konto użytkownika zgodnie z podanymi poniżej informacjami pamiętając, że należy użyć złożonego hasła:

<u>Nazwa pola tekstowego</u>	<u>Wpis</u>
First Name (Imię)	Dan
Last Name (Nazwisko)	Holme
User Logon Name (Nazwa logowania użytkownika)	Dan.Holme
User Logon Name (Pre-Windows 2000) (Nazwa logowania użytkownika — systemy starsze niż Windows 2000)	Dholme

5. Utwórz innego użytkownika zgodnie z podanymi poniżej informacjami:

<u>Nazwa pola tekstowego</u>	<u>Wpis</u>
First Name (Imię)	Hank
Last Name (Nazwisko)	Carbeck
User Logon Name (Nazwa logowania użytkownika)	Hank.Carbeck
User Logon Name (Pre-Windows 2000) (Nazwa logowania użytkownika - systemy starsze niż Windows 2000)	Hcarbeck

6. Utwórz trzeci obiekt użytkownika zachowując tę samą konwencję dla nazw logowania użytkownika.

Ćwiczenie 2: Modyfikacja właściwości obiektu użytkownika

1. Dla obiektu użytkownika otwórz okno dialogowe właściwości.
2. Skonfiguruj odpowiednie właściwości dla obiektu użytkownika na zakładkach *General* (Ogólne), *Address* (Adres), *Profile* (Profil), *Telephones* (Telefony) oraz *Organization* (Organizacja).
3. Sprawdź inne właściwości obiektu użytkownika, ale nie zmieniaj ich w tym momencie.
4. Aby zakończyć, kliknij przycisk OK.

Ćwiczenie 3: Modyfikacja właściwości wielu obiektów użytkownika

1. Otwórz konsolę *Active Directory Users And Computers* (Użytkownicy i komputery usługi Active Directory) i przejdź do jednostki organizacyjnej Employees w domenie Contoso.com. W oknie drzewa zaznacz jednostkę **Employees**, która wyświetli w oknie szczegółów listę obiektów użytkownika utworzonych w ćwiczeniu 1.
2. Kliknij obiekt użytkownika **Dan Holme**.

3. Przytrzymaj przycisk CTRL i kliknij obiekt użytkownika **Hank Carbeck**.
4. Kliknij menu **Action** (Akcja), a następnie kliknij polecenie **Properties** (Właściwości),
5. Należy zwrócić uwagę na różnice pomiędzy tym oknem dialogowym właściwości a bardziej rozbudowanym oknem używanym w ćwiczeniu 2. Sprawdź, czy właściwości są dostępne, jeśli zaznaczonych zostało wiele obiektów, ale ich nie modyfikuj.
6. Skonfiguruj następujące właściwości dla dwóch obiektów użytkownika:

Strona właściwości	Właściwość	Wpis
General (Ogólne)	Description (Opis)	Zapoznaj mnie z wszystkim, co należy wiedzieć o systemie Windows Server 200 (425) 555-0175
General (Ogólne)	Telephone Number (Numer telefonu)	
General (Ogólne)	Web Page (Strona sieci Web)	http://www.microsoft.com/mspress/
Address (Adres)	Street (Ulica)	One Microsoft Way
Address (Adres)	City (Miasto)	Redmond
Address (Adres)	State/Province (Województwo)	Washington
Address (Adres)	ZIP/Postal Code (Kod pocztowy)	98052
Organization (Organizacja)	Title (Tytuł)	Author
Organization (Organizacja)	Company (Firma)	Microsoft Press

7. Po zakończeniu konfigurowania właściwości, kliknij przycisk OK.
8. Otwórz właściwości obiektu **Dan Holme**.
9. Sprawdź, czy właściwości skonfigurowane w punkcie 6 dotyczą w rzeczywistości tego obiektu. Po zakończeniu kliknij przycisk OK.
10. Kliknij obiekt użytkownika **Dan Holme**.
11. Przytrzymaj przycisk CTRL i kliknij obiekt użytkownika **Hank Carbeck**. Kliknij menu Action (Akcja).
12. Należy zauważyć, że po zaznaczeniu kilku użytkowników, polecenie **Reset Password** (Resetuj hasło) nie jest dostępne. Które jeszcze polecenia nie są dostępne? Sprawdź to, przeglądając menu **Action** przy zaznaczeniu jednego użytkownika oraz przy zaznaczeniu dwóch obiektów.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Za pomocą konsoli Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) użytkownik konfiguruje obiekty użytkowników w domenie oraz może zmieniać adres i numer telefonu obiektu użytkownika, który reprezentuje jego samego. Polecenie New User (Nowy Użytkownik) nie jest dla niego dostępne. Jakie jest najbardziej prawdopodobne wyjaśnienie takiej sytuacji?
2. Administrator tworzy pewną liczbę obiektów użytkownika dla zespołu firmy, skupiającej pracowników zatrudnionych na okres próbny. Przyszli pracownicy będą zatrudnieni od godziny 9.00 do 17.00, a ich umowy podpisane zostaną za miesiąc lub dwa. Pracownicy będą pracować zgodnie z tym harmonogramem. Które z wymienionych poniżej właściwości powinien skonfigurować administrator, aby zapewnić największe bezpieczeństwo dla tych obiektów?
 - a. Password (Hasło)
 - b. Logon Hours (Godziny logowania)
 - c. Account expires (Wygasanie hasła)
 - d. Store password using reversible encryption (Zachowaj hasło przy użyciu szyfrowania odwracalnego)
 - e. Account is trusted for delegation (Konto jest zaufane w kwestii delegowania)
 - f. User **must** change password at **next** logon (Użytkownik musi zmienić hasło przy następnym logowaniu)
 - g. Account is disabled (Konto jest wyłączone)
 - h. Password never expires (Hasło nigdy nie wygasa)
3. Które z poniżej wymienionych właściwości i zadań administracyjnych mogą być jednocześnie konfigurowane dla kilku obiektów użytkownika?
 - a. Last Name (Nazwisko)
 - b. User Logon Name (Nazwa logowania użytkownika)
 - c. Wyłączenie konta
 - d. Włączenie konta
 - e. Wyczyszczenie hasła
 - f. Password Never Expires (Hasło nigdy nie wygasa)
 - g. User Must Change Password At Next Logon (Użytkownik musi zmienić hasło przy następnym logowaniu)
 - h. Logon Hours (Godziny logowania)
 - i. Computer Restrictions (Logon Workstations) (Ograniczenia komputera, Logowanie na stacjach roboczych)
 - j. Title (Tytuł)
 - k. Direct Reports (Bezpośredni podwładni)

Podsumowanie lekcji

- Aby utworzyć obiekt użytkownika, użytkownik musi być członkiem grupy Enterprise Admins (Administratorzy przedsiębiorstwa), Domain Admins (Administratorzy domeny) bądź Account Operators (Operatorzy kont) lub użytkownikowi zostały przekazane (delegowanie) uprawnienia administracyjne pozwalające tworzyć obiekty użytkownika.
- Obiekt użytkownika zawiera właściwości najczęściej kojarzone z „kontem” użytkownika - nazwa i hasło logowania oraz unikatowy identyfikator użytkownika SID.
- Obiekty użytkownika zawierają również właściwości dotyczące reprezentowanych osób, wliczając w to informacje osobowe, członkostwo w grupach oraz ustawienia administracyjne. System Windows Server 2003 umożliwia jednocześnie zmiany niektórych właściwości dla wielu użytkowników.

Lekcja 2: Tworzenie wielokrotnie obiektów użytkownika

Zdarzają się sytuacje, w których zachodzi potrzeba szybkiego utworzenia wielu obiektów **użytkowników**. To może być przykładowo nowa grupa studentów w szkole lub nowo zatrudniani pracownicy przedsiębiorstwa. W takich sytuacjach trzeba stosować metody ułatwiające lub **automatyzujące** tworzenie obiektów użytkowników, gdyż tworzenie pojedynczych kont będzie mało efektywne. W lekcji 1 opisane zostały sposoby tworzenia i zarządzania obiektami użytkownika za pomocą konsoli Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory). Niniejsza lekcja rozwija te zagadnienia i umiejętności omawiając narzędzia pozwalające na tworzenie obiektów użytkowników za pomocą szablonów, importowania oraz skryptów wiersza poleceń.

Materiały omówione podczas lekcji pozwalają na

- Tworzenie i stosowanie szablonów obiektu użytkownika
- Import obiektów użytkowników za pomocą plików, w których wartości rozdzielane są przecinkami
- Znaczenie nowych narzędzi wiersza poleceń w procesie tworzenia i zarządzania obiektami użytkowników

Szacunkowy czas lekcji: 15 minut

Tworzenie i wykorzystywanie szablonów obiektu użytkownika

Często zdarza się, że grupa obiektów ma podobne właściwości. Przykładowo, wszyscy przedstawiciele handlowi mogą należeć do tej samej grupy, mogą logować się do sieci w tych samych godzinach oraz mają foldery macierzyste i profile mobilne przechowywane na tym samym serwerze. W takim przypadku byłoby pomocne, aby podczas tworzenia obiektu użytkownika, jego niektóre właściwości były już zdefiniowane. Można to osiągnąć poprzez utworzenie ogólnego obiektu użytkownika, nazywanego często *szablonem*, a następnie kopiowanie tego szablonu w celu utworzenia nowego obiektu.

Aby utworzyć szablon użytkownika, należy utworzyć obiekt użytkownika i określić jego właściwości oraz umieścić obiekt w odpowiedniej grupie.



Alert bezpieczeństwa Należy upewnić się, czy konto użytkownika jest *wyłączone*. Ponieważ jest to tylko szablon, dostęp do zasobów sieci za pomocą tego obiektu musi być zablokowany.

Aby utworzyć użytkownika w oparciu o szablon, należy zaznaczyć dany szablon i z menu **Action** (Akcja) wybrać polecenie **Copy** (Kopiuj). Użytkownik będzie musiał określić niektóre właściwości podobnie, jak podczas tworzenia nowego użytkownika: imię i nazwisko, inicjały, nazwy logowania, hasło oraz opcje konta. Po utworzeniu obiektu można zauważyć, że właściwości określone w szablonie zostały skopiowane według poniżej przedstawionego opisu bazującego na podziale na strony właściwości:

- **General (Ogólne)** Żadne właściwości nie są kopiowane
- **Address (Adres)** Wszystkie właściwości są kopiowane, za wyjątkiem jednej - *Street* (Ulica)

- **Account (Konto)** Wszystkie właściwości są kopiowane, za wyjątkiem nazw logowania, które trzeba definiować podczas kopiowania szablonu
- **Profile (Profil)** Wszystkie właściwości są kopiowane, a profil i folder macierzysty zostają zmodyfikowane zgodnie z nową nazwą logowania
- **Telephones (Telefony)** Żadne właściwości nie są kopiowane
- **Organization (Organizacja)** Wszystkie właściwości są kopiowane, za wyjątkiem jednej — *Titk* (Tytuł)
- **Member Of (Członek grupy)** Wszystkie właściwości są kopiowane
- **Dial-in (Telefonowanie), Environment (Środowisko), Sessions (Sesje), Remote Control (Zdalne sterowanie), Terminal Services Profile (Profil usług terminalowych), COM+** Żadne właściwości nie są kopiowane



Wskazówka Użytkownik utworzony poprzez skopiowanie szablonu, domyślnie należy do tej samej grupy, jaka została określona w szablonie. Uprawnienia i prawa przypisane tej grupie będą stosowały się do nowego użytkownika. Jednakże bezpośrednia zmiana uprawnień samego szablonu obiektu użytkownika *nie* spowoduje skopiowania bądź zmodyfikowania uprawnień nowego użytkownika.

Importowanie obiektów użytkowników za pomocą programu CSVDE

CSVDE jest programem narzędziowym wiersza poleceń, który umożliwia import lub eksport obiektów w usłudze Active Directory. Import lub eksport przeprowadzany jest na podstawie pliku tekstowego, w którym wartości rozdzielane są przecinkami. Jest to popularny format pliku czytany przez wiele programów, na przykład Notatnik lub Microsoft Excel. Jest to bardzo efektywne narzędzie w przypadku, kiedy zachodzi konieczność szybkiego tworzenia obiektów. Podstawowa składnia polecenia przedstawia się następująco:

`csvde [-i] [-f FileName] [-k]`

-i Opcja ta określa tryb importu. Jeśli nie została wyspecyfikowana, oznacza to, że domyślnym trybem będzie eksport. -f *FileName* Określa nazwę pliku importu.

-k Podczas importu ignoruje błędy i kontynuuje działanie. Ignorowane błędy to między innymi „obiekt już istnieje”, „naruszenia dostępu” oraz „atrybut lub wartość już istnieje”.

Plik importu jest tekstowym plikiem o wartościach rozdzielanych przecinkami (*.csv lub *.txt), w którym pierwszym wierszem jest lista nazw atrybutów protokołu LDAP (Lightweight Directory Access Protocol) dla importowanych atrybutów, po którym następuje jeden wiersz dotyczący każdego obiektu. Każdy obiekt musi zawierać dokładnie te atrybuty, który zostały wyspecyfikowane w pierwszym wierszu. Poniżej zamieszczony został przykład takiego pliku:

```
DN.objectClass.sAMAccountName.sn.givenName.userPrincipalName "CN=Scott
Bishop,OU=Employees,OC=contoso,DC=com", user,sbishop,Bishop,
Scott,scott.bishop@contoso.com
```

Zaimportowanie tego pliku utworzy w jednostce organizacyjnej Employees obiekt użytkownika o nazwie Scott Bishop. Nazwy logowania, imię i nazwisko zostaną zdefiniowane przez plik. Obiekt początkowo jest wyłączony, a po wyczyszczeniu hasła obiekt można włączyć.



Zobacz także Więcej informacji o poleceniu CSVDE, wliczając w to szczegóły dotyczące jego parametrów i używania podczas *eksportu* obiektów katalogu, można znaleźć w programie Help and Support Center (Centrum pomocy i obsługi technicznej) systemu Windows Server 2003. Polecenie LDIFDE, również omówione w programie Help and Support Center (Centrum pomocy i obsługi technicznej), umożliwia import i eksport kont za pomocą formatu protokołu LDAP. Polecenie to i struktura jego pliku nie są dla administratorów tak intuicyjne, jak obsługiwane przez polecenie CSVDE pliki o wartościach rozdzielanych przecinkami.

Korzystanie z narzędzi wiersza poleceń usługi Active Directory

System Windows Server 2003 obsługuje szereg efektywnych programów narzędziowych wiersza poleceń, które ułatwiają zarządzanie usługą Active Directory. Poniżej przedstawiona została lista tych narzędzi wraz z krótkim opisem każdego z nich:

- **DSADD** Dodaje obiekty do katalogu.
- **DSGET** Wyświetla („gets”) właściwości obiektów katalogu.
- **DSMOD** Modyfikuje wybrane atrybuty istniejącego obiektu katalogu.
- **DSMOVE** Przenosi obiekt z bieżącego kontenera do nowej lokalizacji.
- **DSRM** Usuwa obiekt, podzawo znajdujące się poniżej obiektu lub oba elementy (obiekt wraz z podzawem).
- **DSOJJERY** Umożliwia badanie obiektów usługi Active Directory, które spełniają określone kryteria wyszukiwania. Polecenie to jest często używane do tworzenia listy obiektów, która jest następnie dostarczana do innych narzędzi wiersza poleceń, celem modyfikacji lub zarządzania wyszukanych obiektów.

Narzędzia te, w przełącznikach wiersza poleceń, stosują jeden lub kilka wymienionych poniżej elementów:

- **Typ obiektu docelowego** Jest to jeden z predefiniowanych zestawów wartości, które skorelowane są z klasą obiektu usługi Active Directory. Typowe przykłady to: komputer, użytkownik, jednostka organizacyjna OU, grupa czy serwer (w znaczeniu kontrolera domeny).
- **Identyfikacja obiektu docelowego** Nazwa wyróżniająca (DN) obiektu, z którą związane jest wykonywanie rozkazu. Nazwa DN obiektu jest atrybutem każdego obiektu, reprezentującym nazwę obiektu i jego lokalizację w lesie usługi Active Directory. Przykładowo, w lekcji 1 w ćwiczeniu 1 utworzony został obiekt o następującej nazwie wyróżniającej: CN=Dan Holme, OU=Employees, DC=Contoso, DC=com.



Informacja Jeśli podczas stosowania nazw DN w parametrze polecenia, nazwy zawierają spacje, należy obejmować je nawiasami. Jeśli natomiast podelementy nazwy wyróżniającej zawierają ukośnik (backslash) lub przecinek, należy sprawdzić informacje zamieszczone w tematach modułu pomocy, które zostały wymienione na następnej stronie.

MCSE Training Kit: Egzamin 70-290

- **Serwer** Można wyspecyfikować nazwę kontrolera domeny, z którą związane jest wykonywanie rozkazu.
- **Użytkownik** Można wyspecyfikować nazwę użytkownika i hasło, z którymi związane jest uruchamianie polecenia. Jest to przydatna opcja, jeśli użytkownik zalogowany jest za pomocą konta, które nie ma uprawnień administracyjnych, a chce uruchomić polecenie wymagające większych uprawnień niż bieżące.

Dodatkowo należy pamiętać, że w składni przełączników i parametrów uwzględniana jest wielkość liter oraz że mogą być poprzedzane znakami myślnika („-”) lub ukośnika („/”).



Zobacz także Niniejsza lekcja dotyczy głównie najczęściej używanych poleceń i parametrów, a także ich używania w odniesieniu do obiektów użytkownika. Więcej informacji dotyczących omawianych programów narzędziowych, w tym pełną listę akceptowanych parametrów, znaleźć można uruchamiając program Help and Support Center (Centrum pomocy i obsługi technicznej) i wyszukując informacje według tematu „directory service command-line tools” (narzędzia wiersza poleceń usługi katalogowej). Należy pamiętać, aby wpisując temat objąć go znakami cudzysłowu. Po kliknięciu przycisku Search (Wyszukaj), na liście rezultatów wyszukiwania tematów pomocy wyświetlona zostanie lista Command Linę Reference (Odwołania do wiersza poleceń).

DSQUERY

Polecenie DSQUERY bada usługę Active Directory wyszukując obiekty spełniające określone kryteria. Składnia polecenia jest następująca:

```
dsquery object type [(StartNode | forestroot | domainroot)] [~o {dn | rdn | samid}] [-scope Isubtree | onelevel | base)] [-name Name] [-desc Description] [-upn UPN] [-samid SAMName] [-inactive NumberOfWeeks] [-stalepwd NumberOfDays] [-disabled] [{-s Server | -d Domain)] [-u UserName] [-p iPassword | *)]
```



Wskazówka Warto zapamiętać, że polecenie to jest często używane do wygenerowania listy obiektów, potrzebnych do uruchomienia innego programu narzędziowego wiersza poleceń. Realizacja polega na wprowadzaniu wyników tego polecenia do następnego rozkazu (praca potokowa). Na przykład, pokazane poniżej polecenie wyszukuje w usłudze Active Directory obiekty, których nazwa zaczyna się od znaków „Dan”, a następnie przekazuje wyniki do polecenia DSMOD, które wyłącza każdy obiekt:

```
dsquery user -name Dan* | dsmod user -disabled yes
```

Inne programy narzędziowe akceptują format nazwy DN, jak również jest to domyślny format ich danych wyjściowych.

Podstawowe parametry zebrane zostały w tabeli 3-4.

Tabela 3-4. Parametry polecenia DSQUERY

Parametr	Opis
Zakres zapytania	
<i>object_type</i>	Wymagany. Typ obiektu reprezentuje klasy obiektu, które będą przeszukiwane. Typ obiektu może być określony jako komputer, kontakt, grupa, OU, serwer lub znak zastępczy „*”, który przedstawia dowolną klasę obiektu. W niniejszej lekcji omawiane będą przede wszystkim polecenia, które wyszukują obiekty użytkowników. Opcjonalny. Określa węzeł, od którego rozpoczyna się wyszukiwanie. Można wyspecyfikować las główny (forestroot), domenę główną (domainroot) lub nazwę wyróżniającą węzła (StartNode). Jeśli określony został las główny, do wyszukiwania wykorzystywany jest katalog globalny. Wartość domyślna wskazuje na domenę główną. Określa zakres wyszukiwania. Wartość „subtree” wskazuje, że zakresem jest poddrzewo liczone od węzła początkowego (startnode). Wartość „onelevel” wskazuje tylko na bezpośredni węzeł potomny węzła początkowego. Wartość „base” wskazuje pojedynczy obiekt reprezentowany przez węzeł początkowy. Jeśli jako węzeł początkowy określony został las główny, prawidłowym zakresem jest jedynie poddrzewo. Domyślne ustawienia określają, że używanym zakresem będzie poddrzewo.
Sposoby wyświetlania wyników	
-o (dn, rdn, samidj)	Opcje określają format, za pomocą którego wyprowadzana będzie lista znalezionych elementów. Wartość „dn” dla każdego wpisu, powoduje wyświetlenie nazwy wyróżniającej. Wartość „rdn” wyświetla względną nazwę wyróżniającą każdego wpisu. Wartość „samid” dla każdego wpisu powoduje wyświetlenie nazwy konta SAM (Security Accounts Manager). Domyślnie używany jest format określony opcją „dn”.
Kryteria wyszukiwania	
-name <i>Name</i>	Wyszukiwani są użytkownicy, dla których atrybuty nazwy (wartość atrybutu CN) są zgodne z wyrażeniem <i>Name</i> . Można używać znaków zastępczych, na przykład: „jn*”, „*ith” lub „j*th”. Wyszukiwani są użytkownicy, dla których atrybut opisu zgadza się z wyrażeniem „ <i>Description</i> ”. Można używać znaków zastępczych. Wyszukiwani są użytkownicy, dla których numer UPN zgadza się z wyspecyfikowaną wartością „ <i>UPN</i> ”.
-desc <i>Description</i>	
-upn <i>UPN</i>	
-sam id <i>SAM Name</i> -	Wyszukiwani są użytkownicy, dla których nazwa konta SAM zgadza się z wyrażeniem „ <i>SAMName</i> ”. Można używać znaków zastępczych.
inacive <i>NumberOfWeeks</i> -	Wyszukiwani są użytkownicy, którzy byli nieaktywni określoną liczbę tygodni.
stalepwd <i>NumberOfDays</i> -	Wyszukiwani są użytkownicy, którzy nie zmienili swojego hasła określoną liczbę dni. Wyszukiwani są użytkownicy, których konta są
disabled	wyłączone.

ciąg dalszy na następnej stronie

[poprzedniej](#)

Parametr

Opis

Kontroler domeny i uprawnienia używane przy poleceniach

{-s *Server* \ -d *Domain*)-u *UserName*

Następuje połączenie do określonego serwera zdalnego lub domeny.

Określa nazwę użytkownika, za pomocą której użytkownik loguje się do serwera zdalnego. Domyślnie opcja —u stosuje nazwę użytkownika taką, jakiej używa do logowania. Do określania nazwy użytkownika, można używać następujących formatów:

- Nazwa użytkownika (na przykład: *Linda*)
- ♦ domena\nazwa użytkownika (na przykład: *widgets\Linda*)
- * UPN (na przykład: *Linda@widgets.microsoft.com*)

-p *{Password | *}*

Podczas logowania na serwerze zdalnym określa albo hasło albo znak zastępczy „*„. Po wprowadzeniu gwiazdki „*„, użytkownik będzie poproszony o wpisanie hasła.



Wskazówka Brak aktywności wyrażany jest liczbą tygodni, natomiast liczba dni dotyczy hasła, które nie było zmieniane.

DSADD

Polecenie DSADD umożliwia utworzenie obiektów usługi Active Directory. Jeśli tworzony jest obiekt użytkownika, używane jest polecenie DSADD USER. Parametry polecenia DSADD pozwalają konfigurować określone właściwości obiektów. Chociaż nazwa parametrów wyjaśnia ich rolę, to w przypadku konieczności znalezienia dokładniejszych opisów parametrów polecenia DSADD, można posłużyć się programem Help And Support Center (Centrum pomocy i obsługi technicznej).

dsadd user *UserDN...*

Parametr *UserDN...* jest jedną lub kilkoma nazwami wyróżniającymi nowego obiektu (lub nowych obiektów). Jeśli nazwa DN zawiera spacje, należy objąć całą nazwę DN znakami cudzysłowu. Do wprowadzania parametru *UserDN...* może być używany jeden z następujących sposobów:

- Wprowadzenie listy nazw DN z innego polecenia (wprowadzanie potokowe), takiego jak DSQUERY.
- Wprowadzenie każdej nazwy DN w wierszu poleceń, przy czym nazwy te oddzielane są spacjami.
- Pozostawienie pustego parametru nazw DN. W tym momencie, w wierszu poleceń, można wprowadzać nazwy DN pojedynczo, z klawiatury konsoli. Każdą nazwę DN trzeba zakończyć naciśnięciem przycisku ENTF.R. Jednoczesne naciśnięcie przycisków CTRL+Z oznacza, że wprowadzona została ostatnia nazwa DN.

Za parametrem DN, w poleceniu DSADD USER może stosować następujące parametry opcjonalne:

- -samid *SAMName*
- -upn *UPN*
- -fn *FirstNarnc*
- -mi *Initial*

- -In *LastName*
- -display *DisplayName*
- -empid *EmployeeID*
- -pwd *{Password \ *}* gdzie * oznacza, że użytkownik będzie poproszony o wprowadzenie hasła
- -desc *Description*
- -memberof *GroupDN*;
- -office *Office*
- -tel *PhoneNumber*
- ' -email *Email*
- -hometel *HomePhoneNumber*
- -pager *PagerNumber*
- -mobile *CellPhoneNumber*
- -fax *FaxNumber*
- -iptel *IPPhoneNumber*
- -webpg *WebPage*
- -title *Title*
- -dept *Department*
- -company *Company*
- -mgr *ManagerDN*
- -hmdir *HomeDirectory*
- -hmdrv *DriveLetter*.
- -profile *ProfilePath*
- -loscr *ScriptPath*
- -mustchpwd {yes | no}
- -canchpwd {yes | no}
- -reversiblepwd {yes | no}
- -pwdneverexpires {yes | no}
- -acctxpires *NumberOfDays*
- -disabled {yes | no}

Podobnie jak dla polecenia DSQUERY, parametry -s, -u oraz -p mogą być dodawane w celu określania kontrolera domeny, Z którym związane jest wykonywanie rozkazu DSADD, a nazwa użytkownika i hasło będą określać odpowiednie uprawnienia.

- j-s *Server \ -d Domain*)
- -u *UserName*
- -p *{Password \ *}*

Specjalny znacznik \$username\$ (uwzględniane są duże i małe litery) może zastępować nazwę SAM konta dla wartości parametrów -email, -hmdir, -profile oraz -webpg. Na przykład, jeśli „Denise” jest

nazwą SAM konta, parametr `-hmdir` może być zapisany za pomocą jednego z pokazanych poniżej formatów:

- `-hmdir\users\Denise\home`
- `-hmdir\users\%username%\home`

DSMOD

Polecenie `DSMOD` modyfikuje wartości istniejących obiektów (jednego lub kilku).

`dsmod user UserDN ... parameters`

Polecenie obsługuje parametr `UserDN...` dokładnie w taki sam sposób, jak polecenie `DSADD`. Oczywiście, w tym przypadku zamiast tworzenia obiektów o odpowiednich właściwościach następuje modyfikacja istniejących obiektów. Należy odnotować wyjątki — za pomocą polecenia `DSMOD USER` nie można modyfikować właściwości obiektu użytkownika: nazwy *SAMName* (parametr `-samid`) lub członkostwa w grupie (parametr `-memberof`). Do zmiany członkostwa w grupie można zastosować polecenie wiersza poleceń `DSMOD GROUP` omawiane w rozdziale 4 „Konta grup”.

Polecenie `DSMOD` umożliwia również stosowanie parametru `-c`. Parametr ten wprowadza polecenie `DSMOD` w tryb operacji ciągłej, w którym polecenie zgłasza występowanie błędów, ale nie przerywa modyfikowania obiektu. Bez parametru `-c`, polecenie `DSMOD` przerywa działania po napotkaniu pierwszego błędu.

DSGET

Polecenie `DSGET` pobiera i wyświetla wybrane właściwości jednego lub kilku istniejących obiektów.

`dsget user UserDN ... parameters`

Polecenie obsługuje parametr nazwa `UserDN...` dokładnie w taki sam sposób, jak polecenie `DSADD` oraz stosuje te same parametry za wyjątkiem tego, że polecenie `DSGET` używa *wyłącznie* parametrów, nie używa natomiast skojarzonych z parametrami wartości. Przykładowo, w poleceniu `DSGET` można zasrosować parametr `-samid parameter`, a nie można zastosować tego parametru wraz z jego wartością (`-samid SAMName`). Powód jest oczywisty: polecenie wyświetla, a nie dodaje bądź modyfikuje właściwości. Oprócz tego, polecenie `DSGET` nie obsługuje parametru `—password`, ponieważ nie można wyświetlać haseł. W poleceniu `DSGET` można dodawać parametry `-dn` oraz `-sid`, za pomocą których wyświetlana jest odpowiednio nazwa wyróżniająca i identyfikator SID obiektu.



Wskazówka egzaminacyjna Warto prześledzić różnice między poleceniami `DSQUERY` a `DSGET`. Polecenie `DSQUERY` wyszukuje i zwraca wyniki w postaci zestawu obiektów, którego podstawą utworzenia było kryterium wyszukiwania bazujące na właściwościach obiektów. Polecenie `DSGET` zwraca właściwości jednego lub kilku wyspecyfikowanych obiektów.

DSMOVE

Polecenie `DSMOVE` umożliwia przesuwanie i zmianę nazwy obiektów w obrębie domeny. Obiekty nie mogą być przenoszone pomiędzy domenami. Składnia polecenia jest następująca::

`dsmove ObjectDN [-newname NewName'] [-newparent ParentDN]`

Polecenie DSMOVE obsługuje również parametry -s, -u oraz -p opisane w sekcji dotyczącej polecenia DSQUERY.

Obiekt określany jest za pomocą nazwy wyróżniającej wyspecyfikowanej w parametrze *ObjectDN*. Aby zmienić nazwę obiektu, należy określić nową nazwę zwykłą w parametrze *NewName*. Wyspecyfikowanie nazwy wyróżniającej kontenera (w parametrze *ParentDN*) przemieści dany obiekt do tego kontenera.

DSRM

Polecenie DSRM jest używane do przesunięcia obiektu, jego podrzewa lub obu elementów (obiektu i podrzewa). Składnia polecenia jest następująca:

```
dsrcm ObjectDN ... [-subtree [- exclude]] [-noprompt] [-c]
```

Polecenie obsługuje parametry -s, -u oraz -p opisane w sekcji dotyczącej polecenia DSQUERY.

Obiekt określany jest za pomocą nazwy wyróżniającej wyspecyfikowanej w parametrze *ObjectDN*. Przełącznik -subtree powoduje, że polecenie DSRM przemieści zawartość obiektu, o ile obiekt ten jest kontenerem. Przełącznik —exclude wyklucza sam obiekt i może być używany jedynie w koniunkcji z przełącznikiem -subtree. Przykładowo, wyspecyfikowanie przełączników -subtree oraz -exclude spowoduje usunięcie obiektów podrzewa jednostki OU, samą jednostkę pozostawi natomiast nienaruszoną. Domyślne ustawienia określają, że przy braku przełączników -subtree lub -exclude usuwany jest tylko obiekt.

Użytkownik będzie poproszony o potwierdzenie usunięcia każdego obiektu, chyba że wyspecyfikowany został parametr -noprompt. Przełącznik -c wprowadza polecenie DSRM w ciągły tryb operacji, w którym zgłaszane są błędy operacji, ale polecenie kontynuuje przetwarzanie następnych obiektów. Przy braku przełącznika -c operacja zostanie zatrzymana po napotkaniu pierwszego błędu.

Zadanie kontrolne: Tworzenie wielu obiektów

W zadaniu tym za pomocą szablonów i narzędzi wiersza poleceń będą tworzone i zarządzane obiekty użytkownika.

Ćwiczenie 1: Tworzenie szablonu użytkownika

1. Zaloguj się na serwerze Server01 jako Administrator.
2. Otwórz konsolę *Active Directory Users And Computers*.
- 3- W oknie drzewa konsoli zaznacz jednostkę organizacyjną **Employees**. 4.

Utwórz konto użytkownika na podstawie następujących informacji:

Nazwa pola tekstowego	Wpis
First Name (Imię)	Template
Last Name (Nazwisko)	Sales Representative
User Logon Name: (Nazwa logowania użytkownika)	Template.salcs.rep
User Logon Name (Pre-Windows 2000): (Nazwa logowania użytkownika (systemy starsze niż Windows 2000))	Templatesalcsrep

MCSE Training Kit: Egzamin 70-290

5. Kliknij przycisk **Next** (Dalej).
6. Zaznacz opcję **Account Is Disabled** (Konto jest wyłączone). Kliknij przycisk **Next** (Dalej).
7. Wyświetlona zostanie strona podsumowania. Kliknij przycisk **Finish** (Zakończ).



Informacja Jak nadmieniono w części zatytułowanej „Wymagania”, przed ćwiczeniami należało utworzyć grupę Sales Representatives w jednostce organizacyjnej Security Groups. Jeśli grupa ta nie została utworzona, trzeba utworzyć ją teraz. Należy skonfigurować globalną grupę zabezpieczeń o nazwie Sales Representative.

8. Wyświetl właściwości obiektu **Template Sales Representative**.
9. Dla konta szablonu skonfiguruj podane poniżej właściwości:

Zakładka	Właściwość	Wartość
Member Of (Członek grupy)	Member Of (Członek grupy)	Sales Representatives
Account (Konto)	Logon Hours (Godziny logowania)	poniedziałek-piątek, 9:00 - 17:00
Account (Konto)	Expires (Wygasanie konta)	Po trzech miesiącach
Organization (Organizacja) Profile (Profil)	Company (Firma)	Contoso
	Profile pathi (Ścieżka profilu)	\\Server1\Profiles\%Username%

10. Po zakończeniu konfigurowania właściwości konta kliknij przycisk OK.

Ćwiczenie 2: Tworzenie użytkowników poprzez kopiowanie szablonu użytkownika

1. W drzewie konsoli zaznacz jednostkę organizacyjną **Employees**.
2. Zaznacz obiekt **Template Sales Representative**.
3. Kliknij menu **Action** (Akcja), a następnie kliknij polecenie **Copy** (Kopiuj).
4. Utwórz nowe konto użytkownika zgodnie z następującymi informacjami:

Nazwa pola tekstowego	Wpis
First Name (Imię)	Scott
Last Name (Nazwisko)	Bishop
User Logon Name: (Nazwa logowania użytkownika)	Scott.Bishop
User Logon Name (Pre-Windows 2000): (Nazwa logowania użytkownika (systemy starsze niż Windows 2000))	Sbishop
Account Is Disabled (Konto jest wyłączone)	Usuń zaznaczenie
Password/Confirm Password (Hasło/ Potwierdzenie hasła)	Wprowadź i potwierdź złożone hasło, zgodnie z opisem we wcześniejszym fragmencie rozdziału.

- 5- Kliknij przycisk **Next** (Dalej), a następnie kliknij przycisk **Finish** (Zakończ).
6. Wyświetl właściwości obiektu **Scott Bishop**.
- 7- Sprawdź, czy informacje skonfigurowane dla szablonu, dotyczące właściwości znajdujących się na zakładkach *Member Of* (Członek grupy), *Account* (Konto) oraz *Organization* (Organizacja) zastosowane zostały do nowego obiektu.
8. Ponieważ w rozdziale konto to będzie używane w innym ćwiczeniu, zmień dwie właściwości. Na zakładce *Account* (Konto) określ właściwość *Account Expires* (Wygasanie konta) wpisując opcję **Never** (Nigdy) oraz ustaw właściwość *Logon Hours* (Godziny logowania) tak, aby logowanie było zawsze możliwe.

Ćwiczenie 3: Importowanie obiektów użytkownika za pomocą polecenia CSVDE

1. Otwórz program Notepad (Notatnik).
2. Wpisz uważnie następujące informacje, tworząc 3 wiersze tekstu:
 DN.objectClass,sAMAccountName.sn,givenName,userPrincipal Name
 "CN=Danielle Tiedt.OU=Employees .
 DC=contoso,DC=com",user.dtiedt.Tiedt, Danielle,danielle.tiedt@contoso.
 com
 "CN=Lorrin Smith- Bates,OU=Employees, DC=contoso,DC=com",user,
 lsmithbates.Smith-Bates.Lorrin,lorrin.smithbates@contoso.com
3. Zapisz plik nadając mu nazwę **„C:\USERS.CSV”** upewniając się, że nazwa została objęta znakami cudzysłowu. Bez tych znaków plik zostanie zapisany jako C:\USERS.CSV.TXT.
4. Otwórz okno wiersza poleceń i wpisz następujące polecenie: csvde
 —i -f **c:\users.csv**
5. Jeśli wyświetlony zostanie komunikat potwierdzający pomyślne wykonanie operacji, uruchom konsolę *Active Directory Users and Computers*, aby przekonać się, czy obiekt ten został utworzony. Jeśli natomiast podczas wykonywania polecenia pojawiły się błędy, w Notatniku otwórz plik **USERS.CSV** i popraw błędy.
6. W dalszej części rozdziału konta tych użytkowników będą używane do logowania. Ponieważ konta są importowane bez haseł, należy hasła te wyczyścić. Po skonfigurowaniu haseł należy włączyć konta. Polecenia **Reset Password** (Resetuj hasło) oraz **Enable Account** (Konto włączone) znajdują się w menu **Action** (Akcja) lub **Objects** (Obiekty).
7. Jeśli masz dostęp do aplikacji, która otwiera pliki tekstowe o wartościach rozdzielanych przecinkami, takie jak Microsoft Excel, otwórz plik C:\USERS.CSV. Za pomocą takiej aplikacji, przy uporządkowanym w kolumny widoku, w porównaniu do programu Notatnik, łatwiej jest rozpoznać strukturę pliku.

Ćwiczenie 4: Korzystanie z narzędzi wiersza poleceń dotyczących usługi Active Directory

1. Otwórz okno wiersza poleceń i wprowadź następujące polecenie:
dsquery user ,>OU=Employees, DC=Contoso,DC=Com" — stalepwd 7
2. Polecenie wyszukuje obiekty użytkownika, dla których hasło nie zostało zmienione przez 7 dni, a po jego wykonaniu powinny przynajmniej zostać wyświetlone obiekty utworzone w ćwiczeniu 1

- i 2. Jeśli tak się nie stało, utwórz jeden lub dwa nowe obiekty użytkowników, a następnie wykonaj polecenie opisane w punkcie 1.
- 3- Wpisz następujące polecenie i naciśnij ENTER:
- OU=Employees, DC=Contoso, DC=Com" — stalepwd 7 | dsmod user - mustchpwd yes**
4. W poleceniu wykorzystywane są wyniki polecenia DSQUERY jako informacje wejściowe dla rozkazu DSMOD. Polecenie DSMOD dla każdego obiektu konfiguruje opcję „User must change password at next logon” (Użytkownik musi zmienić hasło przy następnym logowaniu). Dla tych obiektów sprawdź na zakładce Account (Konto), czy opcja ta jest odpowiednio ustawiona.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Która opcja będzie najbardziej przydatna do wygenerowania 100 nowych obiektów użytkownika, przy czym dla każdego powinny być jednakowe ustawienia następujących właściwości: Profile path (ścieżka profilu), Home folder path (ścieżka katalogu macierzystego), Title (tytuł), Web Page (Strona sieci Web), Company (firma), Department (dział) oraz Manager (menedżer)?
2. Które narzędzie pozwala zidentyfikować konta nieużywane od dwóch miesięcy?
 - a. DSADD
 - b. DSGET
 - c. DSMOD
 - d. DSRM
 - e. DSQUERY
- 3- Która zmienna może być używana razem z poleceniami DSMOD oraz DSADD do utworzenia katalogów macierzystych i folderów profili specyficznych dla użytkownika?
 - a. % Username%
 - b. \$ Username\$
 - c. Cbl=Useratne
 - d. < Usernamo
4. Które narzędzia umożliwiają wyświetlenie numerów telefonicznych wszystkich użytkowników jednostki organizacyjnej OU?
 - a. DSADD
 - b. DSGET
 - c. DSMOD

- d. DSRM
- e. DSQUERY

Podsumowanie lekcji

- Szablon obiektu użytkownika jest obiektem kopiowanym w celu utworzenia nowego użytkownika. Jeśli szablon nie jest „rzeczywistym” użytkownikiem, konto to powinno być wyłączone. Na podstawie szablonu kopiowana jest tylko część właściwości użytkownika.
- Polecenie CSVDE umożliwia import obiektów katalogu na podstawie pliku tekstowego, w którym wartości rozdzielane są przecinkami.
- System Windows Server 2003 obsługuje nowe, efektywne narzędzia wiersza poleceń do tworzenia, zarządzania oraz usuwania obiektów katalogu: DSQUERY, DSGET, DSADD, DSMOVŁ, DSMOD oraz DSRM. Polecenie DSOJUERY jest często używane do wygenerowania wyniku, który jest traktowany jako informacje wejściowe innych poleceń (praca potokowa).

Lekcja 3: Zarządzanie profilami użytkowników

Każdy, kto obsługiwał użytkowników w sieci komputerowej wie, że są elementy systemu, których brak jest dla użytkownika dużą uciążliwością. Na przykład, jeśli użytkownik zalogował się i nie ma dostępu do katalogu Ulubione w przeglądarce lub musi ponownie konfigurować niestandardowy słownik lub też nie ma dostępu do dokumentów czy skrótów na swoim pulpicie, to jego wydajność spada gwałtownie i na pewno zadzwoni do działu wsparcia technicznego. Te wszystkie przykłady dotyczą elementów profilu użytkownika. Profile mogą być konfigurowane, aby poprawić dostępność, zabezpieczenia i niezawodność. Podczas tej lekcji omówione zostaną sposoby zarządzania lokalnymi, mobilnymi, grupowymi oraz obowiązkowymi profilami.

Materiały omówione podczas lekcji pozwalają na

- Zrozumienie stosowania lokalnych i mobilnych profili użytkownika
- Skonfigurowanie mobilnego profilu użytkownika
- Utworzenie wstępnie skonfigurowanego mobilnego profilu użytkownika lub grupy
- Skonfigurowanie profilu obowiązkowego

Szacunkowy czas lekcji: 15 minut

Profil użytkownika

Profil użytkownika jest zbiorem folderów i plików danych zawierających elementy środowiska pulpitu, utworzone zgodnie z potrzebami użytkownika. Ustawienia te dotyczą:

- Skrótów menu *Start* pulpitu i paska *Quick Launch* (Szybkie uruchamianie)
- Dokumentów pulpitu i foldera *My Document* (Moje dokumenty), chyba że skonfigurowane zostało przekierowanie.



Wskazówka Właściwości foldera My Documents (Moje dokumenty) oraz reguły w zasadzie grupy dotyczące foldera przekierowania (Folder Redirection) umożliwiają przekierowanie foldera My Documents (Moje dokumenty) tak, aby miejscem docelowym był określony folder sieci. Jest to najlepsze rozwiązanie umożliwiające przechowywanie na serwerze zawartości foldera użytkownika My Documents (Moje dokumenty), gdzie dane są archiwizowane, sprawdzane programami antywirusowymi oraz mogą być łatwo udostępnione innym użytkownikom danej organizacji i dzięki temu inaczej wykorzystywane niż na zwykłym pulpicie. Folder My Documents (Moje dokumenty) może być także dostępny w trybie offline, co oznacza, że użytkownicy mogą mieć dostęp do swoich plików również przy braku połączenia z siecią.

¹ Ulubionych odsyłaczy i plików typu „cookie” przeglądarki Internet Explorer

¹ Certyfikatów (jeśli zostały wprowadzone)

¹ Określonych plików aplikacji, takich jak niestandardowy słownik dziennika programu Microsoft Office, szablony użytkownika czy list samouzupełnień

- My Network Places (Moje miejsca sieciowe)
- Ustawień wyświetlania pulpitu, takich jak wygląd, tapeta i wygaszacz ekranu

Te istotne elementy są inne dla każdego użytkownika. Byłoby pożądane, aby ustawienia te nie zmieniały się między kolejnymi sesjami w sieci, były dostępne dla użytkownika nawet jeśli loguje się on na innym komputerze, a także żeby były dostępne po wymuszonej awarii ponownej instalacji systemu.

Lokalne profile użytkownika

Ustawienia domyślne określają, że profile użytkownika są przechowywane lokalnie w folderze *"%SystemDrive%\Documents and Settings\%Username%".* Ich działanie można opisać następująco:

- Podczas pierwszego logowania użytkownika system tworzy profil tego użytkownika, kopiując profil użytkownika domyślnego (Default User). Folder nowego profilu zostaje utworzony w oparciu o nazwę logowania (podczas pierwszego logowania).
- Wszystkie zmiany pulpitu użytkownika i środowiska oprogramowania są zapisywane w lokalnym profilu użytkownika. Każdy użytkownik ma swój indywidualny profil, tak więc określone ustawienia dotyczą tylko tego użytkownika.
- Środowisko użytkownika jest rozszerzane przez profil znajdujący się w folderze *Ali Users*. Profil ten może zawierać skróty pulpitu lub menu Start, miejsca sieciowe, a nawet dane aplikacji. Elementy profilu *Ali Users* są łączone z profilem użytkownika tworząc środowisko użytkownika. Ustawienia domyślne określają, że jedynie użytkownicy grupy Administratorzy mogą modyfikować ten profil (profil *Ali Users*).
- Profil jest przechowywany lokalnie i dlatego jeśli użytkownik loguje się w innym systemie, dokumenty i ustawienia jego profilu nie będą dostępne. Zamiast tego, jak było to wcześniej wspomniane, system wygeneruje nowy profil lokalny, jeśli użytkownik logował się po raz pierwszy w tym systemie.

Mobilny profil użytkownika

Jeśli użytkownicy pracują na kilku komputerach, istnieje możliwość skonfigurowania dla nich mobilnego profilu użytkownika (RUP), co zapewni, że bez względu na to, w którym systemie użytkownik się zaloguje, jego dokumenty i ustawienia środowiska będą niezmiennie. Profile RUP są przechowywane na serwerze, co oznacza ponadto, że profil może być archiwizowany, sprawdzany za pomocą programów antywirusowych i centralnie kontrolowany. Nawet w środowiskach, w których użytkownicy nie przemieszczają się, profile RUP zapewniają zwiększoną niezawodność. Jeśli system użytkownika ulegnie awarii i musi być ponownie instalowany, profil mobilny zapewni, że na nowym systemie środowisko użytkownika będzie identyczne jak poprzednio.

Aby skonfigurować profil RUP, na serwerze należy udostępnić folder. Najlepiej, jeśli serwer jest serwerem plików, gdzie często wykonywane są kopie zapasowe.



Informacja Należy pamiętać, aby dla udostępnionego foldera wszystkim przydzielić uprawnienia Everyone Full Control (Pełna kontrola). W systemie Windows Server 2003 domyślnym ustawieniem dla udostępnionych folderów jest prawo Read (Odczyt), które nie jest wystarczające dla współdzielenia profilu mobilnego.

Na zakładce *Profile* (Profil) okna dialogowego właściwości użytkownika należy wpisać ścieżkę profilu (Profile Path) w następującym formacie: `\\<sen>er >|<share>|\"%Username%\"`. Zmienna `%Username%` będzie automatycznie zastąpiona nazwą logowania użytkownika.

Dzięki temu prostemu mechanizmowi, pr/y następnym logowaniu system zidentyfikuje lokalizację profilu mobilnego.



Wskazówka egzaminacyjna Mobilne profile użytkownika nie są niczym innym, jak udostępnionym folderem i określeniem lokalizacji profilu w tym folderze (ścieżka określona jest we właściwościach obiektu użytkownika: ścieżka profilu). W żadnym wypadku profile mobilne nie są właściwościami obiektu komputera.

Podczas wylogowywania użytkownika, system aktualizuje profil znajdujący się na serwerze. Użytkownik może się teraz zalogować na dowolnym komputerze w domenie, a zastosowane zostaną jego aktualne dokumenty i ustawienia środowiska przechowywane w profilu RUP.



Informacja W systemie Windows Server 2003 wprowadzona została nowa zasada: Only Allow Local User Profiles (Zezwalaj tylko na lokalne profile użytkowników). Zasada ta powiązana z jednostką organizacyjną zawierającą konta komputera będzie zapobiegać stosowaniu profili mobilnych na tych komputerach. Użytkownicy będą obsługiwać profile lokalne.

Jeśli użytkownik, dla którego zdefiniowany został profil RUP, loguje się po raz pierwszy w nowym systemie, to system nie będzie kopiował profilu domyślnego użytkownika (Default User). Zamiast tego, będzie pobierał profil RUP z lokalizacji sieciowej. Podczas wylogowywania lub podczas logowania się w innym systemie, na którym użytkownik pracował poprzednio, system kopiuje jedynie pliki, które zostały zmienione.

Synchronizacja profilu mobilnego

Inaczej niż w poprzednich wersjach systemów Microsoft Windows, systemy Windows 2000, Windows XI' oraz Windows Server 2003 podczas operacji logowania i wylogowywania nie przesyłają bądź nie pobierają całego profilu użytkownika. Zamiast tych operacji, profil jest *synchronizowany*. Pomiędzy systemem lokalnym a sieciowym folderem profilu RUP przesyłane są jedynie pliki, które zostały zmienione. Oznacza to, że przy korzystaniu z profili RUP operacje logowania i wylogowywania są znacznie szybsze niż w poprzednich wersjach systemu Windows. Organizacje, które właśnie z tych powodów (wpływ na ruch w sieci i procesy logowania) nie korzystały z profili RUP, powinny ponownie ocenić swoją konfigurację.

Tworzenie wstępnie skonfigurowanych profili użytkowników

Istnieje możliwość utworzenia niestandardowego profilu użytkownika w celu przygotowania zaplanowanego i wstępnie skonfigurowanego środowiska oprogramowania. Podejście takie jest przydatne w następujących sytuacjach:

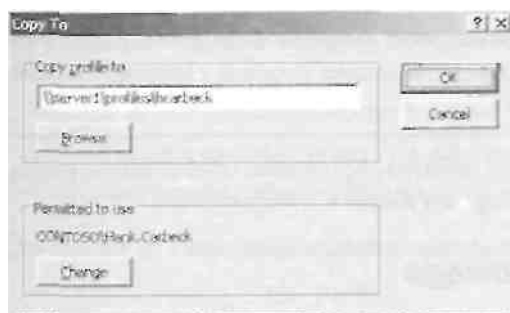
- Udostępnianie wydajnego środowiska pracy charakteryzującego się łatwym dostępem do potrzebnych zasobów sieci i aplikacji
- Ograniczanie dostępu do niezbędnych zasobów i aplikacji
- Uproszczenie czynności związanych ze wsparciem technicznym poprzez stosowanie bardziej prostego i spójnego pulpitu

W celu utworzenia wstępnie skonfigurowanego profilu użytkownika nie są wymagane żadne specjalne narzędzia. Po prostu trzeba zalogować się do systemu i odpowiednio zmodyfikować pulpit oraz oprogramowanie. Zaleca się wykonywanie tych czynności w oparciu o inne niż bieżąco używane konto, aby nie modyfikować niepotrzebnie swojego własnego profilu.

Po utworzeniu profilu należy zalogować się w systemie jako użytkownik posiadający uprawnienia administratora. W programie *Contro! Panel* (Panel sterowania) należy otworzyć moduł System i kliknąć zakładkę **Advanced** (Zaawansowane), a następnie przycisk **Settings** (Ustawienia) w ramce **User Profiles** (Profil użytkownika). Następnie należy zaznaczyć profil, który został utworzony i kliknąć przycisk Copy To (Kopiuj do). Ścieżkę profilu w formacie UNC (Universal Naming Convention) wprowadza się w postaci: \\<server>\<share>\<username>. W sekcji **Permitted To Use** (Pozwolenie na używanie) należy kliknąć przycisk **Change** (Zmień), aby wybrać użytkownika, dla którego przygotowywany jest profil. Czynność ta określa listę ACL foldera profilu, która zezwala na dostęp dla danego użytkownika. Na rysunku 3-5 przedstawiony został przykład okna kopiowania profilu. Kliknięcie przycisku OK spowoduje skopiowanie profilu do jego lokalizacji w sieci.



Informacja Aby skopiować profil, użytkownik musi być członkiem grupy Administratorzy.



Rysunek 3-5. Kopiowanie do lokalizacji w sieci wstępnie skonfigurowanego profilu użytkownika

Na koniec należy otworzyć okno właściwości obiektu użytkownika i na zakładce *Profile* (Profil) wpisać tę samą ścieżkę UNC profilu. I to wszystko. Następnym razem użytkownik zaloguje się do komputera domeny, a pobrany profil będzie określał jego środowisko.



Wskazówka Podczas używania wstępnie skonfigurowanych profili mobilnych lub dokładniej każdego profilu mobilnego, należy zwrócić uwagę na potencjalne zagadnienia dotyczące różnic urządzeń systemów, w których loguje się użytkownik. Przykładowo, jeśli skróty pulpitu były utworzone przy założeniu rozdzielczości ekranu XGA (1024*768), a użytkownik zalogował się w systemie wyposażonym w kartę grafiki o rozdzielczości SVGA (800x600), to niektóre skróty mogą stać się niewidoczne. Ponadto profile nie zawsze można w pełni przenosić pomiędzy różnymi platformami. Profil opracowany dla systemu Windows 98 nie będzie prawidłowo funkcjonował w systemie Windows Server 2003. Niektóre niespójności występują nawet pomiędzy systemami Windows Server2003, Windows XP lub Windows 2000 Professional.

Tworzenie wstępnie skonfigurowanego profilu grupy

Profile mobilne umożliwiają tworzenie typowego środowiska pulpitu dla wielu użytkowników mających podobne obowiązki. Proces jest podobny do tworzenia wstępnie skonfigurowanego profilu użytkownika za wyjątkiem tego, że utworzony profil udostępniany jest wielu użytkownikom.

Należy utworzyć profil zgodnie z procedurą opisaną powyżej. Podczas kopiowania profilu do serwera ścieżka powinna mieć następującą postać: `\\<serwer>\<udostępniony folder>\<nazwa profilu grupy>`. Należy umożliwić dostęp wszystkim użytkownikom korzystającym z tego profilu, czyli w ramce Per-mitted To Use (Pozwolenie na używanie) trzeba kliknąć przycisk Change (Zmień) i zaznaczyć grupę zawierającą wszystkich użytkowników lub grupę BUILTINUSERS, która zawiera wszystkich użytkowników domeny. Jedynie użytkownicy, do których profil będzie się rzeczywiście odnosił, są użytkownikami, dla których skonfigurowana zostanie ścieżka profilu obiektu użytkownika.

Po skopiowaniu profilu do lokalizacji w sieci, należy skonfigurować ścieżkę profilu dla użytkowników, do których profil ten ma być zastosowany. System Windows Server 2003 ułatwia wykonanie tego zadania, w którym trzeba zaznaczyć wielu użytkowników i dla wszystkich jednocześnie zmienić ścieżkę profilu. Należy wpisać tę samą nazwę UNC, która była użyta do skopiowania profilu do sieci, na przykład:

Wskazówka Ścieżka profilu jest konfigurowana jako właściwość jednego lub kilku obiektów *użytkownika*. Ścieżka nie jest przypisywana do obiektu, jakim jest grupa. Chociaż idea profilu grupy właśnie na tym polega, trzeba pamiętać, aby nie „wpaść” w pułapkę związaną z kojarzeniem profilu z obiektem grupy.



Na koniec, ponieważ dostęp do profilu grupy uzyskiwać będzie kilku użytkowników, profil grupy musi być obowiązkowy. Odpowiednie czynności opisane zostały w następnej sekcji.

`\\<serweri>\<udostępnionyfolder>\<nazwa profilu grupy>`.

Q | Wskazówka Ścieżka profilu jest konfigurowana jako właściwość jednego lub kilku obiektów *użytkownika*. Ścieżka nie jest przypisywana do obiektu, jakim jest grupa. Chociaż idea profilu grupy właśnie na tym polega, trzeba pamiętać, aby nie „wpaść” w pułapkę związaną z kojarzeniem profilu z obiektem grupy.

Na koniec, ponieważ dostęp do profilu grupy uzyskiwać będzie kilku użytkowników, profil grupy musi być obowiązkowy. Odpowiednie czynności opisane zostały w następnej sekcji.

Konfigurowanie profilu obowiązkowego

Profil obowiązkowy nie zezwala na modyfikowanie środowiska profilu. Dokładniej mówiąc, profil obowiązkowy nie obsługuje zmian, jakie nastąpiły pomiędzy sesjami. Dlatego też, pomimo że użytkownik może przeprowadzać modyfikacje, to przy następnym logowaniu pulpit będzie wyglądał identycznie, jak przy poprzednim logowaniu. Zmiany nie są zapisywane.

Profile obowiązkowe są przydatne, jeśli zachodzi potrzeba zablokowania pulpitu. Praktyczne zastosowanie wprowadzania profili grupy dotyczy sytuacji, kiedy nie chcemy, aby zmiany poczynione przez jednego użytkownika miały wpływ na środowisko innych użytkowników.

Aby określić profil jako obowiązkowy wystarczy po prostu zmienić nazwę pliku w folderze głównym profilu. Profile obowiązkowe *nie* są konfigurowane za pomocą uprawnień. Plik, który musi mieć zmienioną nazwę to: Ntuser.dat. Plik jest ukryty i dlatego należy sprawdzić, czy w menu Folder Options (Opcje folderów) w programie Control Panel (Panel sterowania) zaznaczona została opcja „Show hid-den files and folders” (Pokaż ukryte pliki i foldery) lub czy w wierszu poleceń użyte zostało polecenie attrib, które usunęło atrybut Hidden (Ukryty). Być może, trzeba będzie również skonfigurować program Windows Explorer (Eksplorator Windows) tak, aby wyświetlał rozszerzenia plików.

Nazwę znalezionej kopii profilu — Ntuser.dat, który ma być profilem obowiązkowym, należy zmienić na Ntuser.man. Po takiej zmianie, profil bez względu na to czy jest mobilny czy lokalny, stanie się profilem obowiązkowym.

Zadanie kontrolne: Zarządzanie profilami użytkowników

W zadaniu tym utworzony zostanie profil mobilny, wstępnie skonfigurowany profil mobilny oraz obowiązkowy profil grupy. Będzie zachodziła konieczność kilkakrotnego logowania i wylogowywania. Ponieważ typowe konto użytkownika nie może logować się lokalnie w kontrolerze domeny, zadanie należy rozpocząć od utworzenia użytkowników w grupie Print Operators (Operatorzy drukowania), gdyż użytkownicy ci mogą się bez przeszkód logować lokalnie w kontrolerze domeny.

Ćwiczenia 1: Konfiguracja użytkowników pozwalająca logować się na kontrolerze domeny

W rzeczywistości rzadko zachodzi potrzeba, aby dla użytkowników wymagane był)' uprawnienia zezwalające na lokalne logowanie w kontrolerze domeny. Jednak w podczas testów taka możliwość jest bardzo potrzebna. Najprostszym sposobem realizacji tego zadania jest dodanie grupy Domain Users (Użytkownicy domeny) do grupy Print Operators (Operatorzy drukowania). Grupa Print Operators (Operatorzy drukowania) ma prawa do lokalnego logowania.

1. Otwórz konsolę *Active Directory Users And Computers* (Użytkownicy i komputery usługi Active Directory).
2. W oknie drzewa przystawki zaznacz kontener **Builtin**.
3. Otwórz menu właściwości grupy *Print Operators* (Operatorzy drukowania).
4. Za pomocą zakładki *Members* (Członkowie) dodaj grupę *Domain Users* do grupy *Print Operators*.

Ćwiczenie 2: Tworzenie udostępnionego foldera profilu

1. Na dysku C: utwórz folder **Profiles**.
2. Prawym przyciskiem myszy kliknij folder **Profiles** i wybierz opcję **Sharing and Security** (Udostępnianie i zabezpieczenia).
3. Kliknij zakładkę **Sharing** (Udostępnianie).
4. Udostępnij folder używając nazwy domyślnej: **Profiles**.
5. Kliknij przycisk **Permissions** (Uprawnienia).

6. Zaznacz pole wyboru zezwalające na pełną kontrolę - **Fuli Control**. 7-
Kliknij przycisk OK.



Alert bezpieczeństwa System Windows Server 2003 w momencie tworzenia współużytkowanych zasobów przydziela do nich ograniczone uprawnienia. Większość organizacji stosuje najlepsze rozwiązanie polegające na przydzielaniu pełnych uprawnień Fuli Control (Pełna kontrola) do współużytkowanych zasobów, natomiast ograniczone uprawnienia przydzielane są do folderów za pomocą zakładki Security (Zabezpieczenia) znajdującej się w oknie dialogowym właściwości foldera. Jeśli jednak administrator nie odblokował zasobu przed jego udostępnieniem, system Windows Server 2003 „nadgorliwie” w odniesieniu do zabezpieczeń, używać będzie uprawnień domyślnych, które zezwalają na dostęp typu Read-Only (tylko do odczytu).

Ćwiczenie 3: Tworzenie szablonu profilu użytkownika

1. Utwórz konto użytkownika, które będzie używane jedynie w celu tworzenia szablonów profilu. Konto powinno być utworzone zgodnie z poniższymi informacjami:

Nazwa pola tekstowego	Wpis
First Name (Imię)	Profile
Last Name (Nazwisko)	Account
User Logon Name: (Nazwa logowania użytkownika)	Profile
User Logon Name (Pre-Windows 2000) (Nazwa logowania użytkownika (systemy starsze niż Windows 2000))	Profile

2. Wyloguj się z serwera Server01.
3. Zaloguj się używając konta **Profile**.
4. Utwórz niestandardowy pulpit dodając na przykład skróty do lokalnych lub sieciowych zasobów.
5. Dostosuj pulpit za pomocą programu **Display** (Ekran) znajdującego się w programie *Control Panel* (Panel sterowania). W oknie dialogowym *Display Properties* (Właściwości ekranu), na stronie *Desktop* (Pulpit) można skonfigurować tło pulpitu oraz klikając przycisk **Customize Desktop** (Dostosuj pulpit) można do pulpitu dodawać ikony **My Documents** (Moje dokumenty), **My Computer** (Mój komputer), **My Network Places** (Moje miejsca sieciowe) oraz **Internet Explorer**.
6. Wyloguj się z konta **Profile**.

Ćwiczenie 4: Ustawianie wstępnie skonfigurowanego profilu użytkownika

1. Zaloguj się jako administrator.
2. W programie *Control Panel* (Panel sterowania), klikając dwukrotnie ikonę **System** otwórz właściwości tego modułu.
3. Kliknij zakładkę **Advanced** (Zaawansowane).
4. W sekcji *User Profiles* (Profil użytkownika) kliknij przycisk **Settings** (Ustawienia), co powoduje otwarcie okna dialogowego **CopyTo** (Kopiuj do).
5. Zaznacz profil konta użytkownika - **Profile**.
6. Kliknij przycisk **CopyTo** (Kopiuj do).

7. W ramce **Copy Profile To** (Kopiowanie profilu do) wpisz **\\server01\profiles\hcarbeck**.
8. W ramce **Permitted To Use** (Pozwolenie na używanie) kliknij przycisk **Change** (Zmień).
9. Wpisz **Hank** i kliknij przycisk OK.
10. Sprawdź wpisy w oknie dialogowym *Copy To* (Kopiuj do) i kliknij przycisk OK.
11. Po skopiowaniu profilu do sieci kliknij dwa razy przycisk OK, aby zamknąć okna dialogowe *User Profiles* (Profil użytkownika) i *System Properties* (Właściwości systemu).
12. Otwórz folder **C:\Profiles**, aby sprawdzić, czy utworzony został folder profilu „Hcarbeck”.
13. Otwórz przystawkę *Active Directory Users And Computers* i w oknie drzewa przystawki zaznacz jednostkę organizacyjną **Employees**.
14. Otwórz właściwości obiektu użytkownika **Hank Carbeck**.
15. Kliknij zakładkę **Profile (Profil)**.
16. W polu **Profile Path** (Ścieżka profilu) wpisz **Wserver01\profiles\%username%**.
17. Kliknij przycisk **Apply** (Zastosuj) i sprawdź czy zmienna *%Username%* została zastąpiona przez „hcarbeck”. Jest rzeczą ważną, aby ścieżka profilu była zgodna z rzeczywistą ścieżką sieci odnoszącą się do foldera profilu.
18. Kliknij przycisk OK.
19. Sprawdź wstępnie skonfigurowany mobilny profil użytkownika poprzez wylogowanie się i ponowne zalogowanie przy użyciu nazwy *bank.carbeck@contoso.com*. Powinny pojawić się zmiany, które przeprowadzone zostały podczas sesji dla konta Profile.

Ćwiczenie 5: Ustawianie wstępnie skonfigurowanego, obowiązkowego profilu grupy

1. Zaloguj się jako administrator.
2. W programie *Control Panel*, klikając dwukrotnie ikonę **System** otwórz właściwości tego modułu.
3. Kliknij zakładkę **Advanced** (Zaawansowane).
4. W ramce *User Profiles* (Profil użytkownika) kliknij przycisk *Settings* (Ustawienia).
5. Zaznacz profil konta użytkownika — **Profile**.
6. Kliknij przycisk **Copy To** (Kopiuj do).
7. W ramce *Copy Profile To* (Kopiuj profil do) wpisz **Wserver01\profiles\sales**.
8. W ramce *Permitted To Use* (Pozwolenie na używanie) kliknij przycisk **Change** (Zmień).
9. Wpisz **Users**, a następnie kliknij przycisk OK.
10. Sprawdź wpisy w oknie dialogowym *Copy To* (Kopiuj do) i kliknij przycisk OK.
11. Po skopiowaniu profilu do sieci kliknij dwa razy przycisk OK, aby zamknąć okna dialogowe *User Profiles* (Profil użytkownika) i *System Properties* (Właściwości systemu).
12. Otwórz folder **C:\Profiles**, aby sprawdzić, czy utworzony został folder profilu „Sales”.
13. W programie *Control Panel* (Panel sterowania) otwórz moduł *Folder Options* (Opcje folderów) i na zakładce *View* (Widok), w ramce *Advanced Settings* (Ustawienia zaawansowane) sprawdź, czy zaznaczona jest opcja **Show Hidden Files And Folders** (Pokaż ukryte pliki i foldery).
14. Otwórz folder **C:\Profiles\Sales** i zmień nazwę pliku *Ntuser.dat* na *Ntuser.man*. Zmiana ta spowoduje, że profil stanie się profilem obowiązkowym.

15. Otwórz przystawkę *Active Directory Users And Computers* i w oknie drzewa przystawki zaznacz jednostkę organizacyjną **Employees**.
16. W oknie drzewa przystawki *zaznacz*, następujące obiekty (kliknięcie przy jednocześnie wciśniętym przycisku CTRL): **Scott Bishop, Danielle Tiedt, Lorrin Smith-Bates**.
- 17- Kliknij menu **Action** (Akcja) i wybierz polecenie **Properties** (Właściwości).
18. Kliknij zakładkę **Profile** (Profil), a następnie zaznacz pole wyboru **Profile Path** (Ścieżka profilu).
19. W polu *Profile Path* (Ścieżka profilu) wpisz \\server01\profiles\sales.
20. Kliknij przycisk OK.
21. Sprawdź wstępnie skonfigurowany mobilny profil użytkownika poprzez wylogowanie się i ponowne zalogowanie przy użyciu nazwy danielle.tiedt@contoso.com.
22. Sprawdź „obowiązkową” naturę profilu poprzez modyfikację wyglądu pulpitu. Przeprowadzanie modyfikacji powinno być możliwe, natomiast zmiany te nie są zachowywane w następnych sesjach.
- 23- Wyloguj się i następnie ponownie zaloguj jako użytkownik **Danielle Tiedt**. Ponieważ profil jest obowiązkowym profilem, zmiany poczynione w poprzednim kroku nie powinny być widoczne.
24. Wyloguj się i następnie ponownie zaloguj jako użytkownik **Scott Bishop**, za pomocą nazwy scott.bishop@contoso.com. Powinien pojawić się taki sam pulpit.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Opisz, w jaki sposób powstaje pulpit użytkownika, jeśli nie są stosowane profile mobilne.
2. Utwórz/ odpowiadając kolejność przedstawionych poniżej czynności tak, aby odzwierciedlał proces tworzenia wstępnie skonfigurowanego mobilnego profilu użytkownika. Należy uwzględnić wszystkie kroki.
 - Utwórz niestandardowy pulpit i środowisko użytkownika.
 - Zaloguj się jako użytkownik o uprawnieniach wystarczających do modyfikowania właściwości konta użytkownika.
 - Skopiuj profil do sieci.
 - Utwórz konto użytkownika tak, żeby profil można było utworzyć bez modyfikowania żadnego aktualnego profilu użytkownika.
 - Zaloguj się za pomocą konta profilu.
 - Na stronie właściwości użytkownika Profile wpisz ścieżkę UNC do profilu.
 - Zaloguj się jako administrator lokalny lub administrator domeny.
- 3- W jaki sposób powstaje profil obowiązkowy?

- a. Skonfigurowanie uprawnień na stronie właściwości foldera Security (Zabezpieczenia) tak, aby nie był możliwy zapis.
- b. Skonfigurowanie uprawnień na stronie właściwości foldera Security (Zabezpieczenia) tak, aby możliwy był tylko odczyt.
- c. Modyfikacja atrybutów foldera profilu i określenie atrybutu Read Only (Tylko do odczytu).
- d. Zmiana nazw pliku Ntuser.dat na Ntuser.man.

Podsumowanie lekcji

- Dla każdego użytkownika logującego się w systemie, system Windows Server 2003 udostępnia indywidualne profile. Domyślne ustawienia określają, że profile są przechowywane na lokalnym systemie w folderach `%Systemdrive%\Documents` oraz `Settings\% Username%`.
- Dla profilu mobilnego wymagany jest tylko udostępniony folder oraz skonfigurowanie ścieżki profilu we właściwościach obiektu użytkownika.
- Wstępnie skonfigurowane profile są po prostu profilami skopiowanymi do ścieżki profilu przed jej skonfigurowaniem w obiekcie użytkownika.
- Profile grupy muszą być obowiązkowe (zmiana nazwy pliku Ntuser.dat na Ntuser.man), aby zmiany przeprowadzone przez jednego z użytkowników nie wpływały na pracę innych użytkowników.

Lekcja 4: Bezpieczeństwo i rozwiązywanie problemów związanych z uwierzytelnieniem

Po skonfigurowaniu obiektów użytkownika, użytkownicy mogą za pomocą tych kont dokonywać uwierzytelnienia w systemie. I wtedy wyłaniają się dwa dodatkowe wyzwania: luki w zabezpieczeniach, które pozostawione bez „opieki” zagrażają integralności sieci przedsiębiorstwa oraz zagadnienia „socjalno-inżynieryjne”, a w szczególności problemy uwierzytelnienia związane z budową sieci, która powinna być wygodna w użyciu oraz niezawodna. Niestety te dwa tematy są ze sobą w sprzeczności — dobrze zabezpieczona sieć staje się trudniejsza w obsłudze. W niniejszej lekcji omawiane są zagadnienia dotyczące uwierzytelnienia użytkowników. Opisany jest wpływ zasad kont domeny, w tym zasad haseł i zasad blokowania konta. Oprócz tego poruszone zostały zagadnienia dotyczące sposobów konfigurowania inspekcji zdarzeń związanych z logowaniem oraz wykonywaniem szeregu zadań dotyczących uwierzytelnienia obiektów użytkownika.

Materiały omówione podczas lekcji pozwalają na

- Rozpoznawanie zasad kont domeny oraz ich wpływu na uwierzytelnienie i wymagania dotyczące haseł.
- Konfigurowanie inspekcji dla zdarzeń związanych z logowaniem.
- Modyfikacja atrybutów obiektów użytkownika dotyczących uwierzytelnienia.

Szacunkowy czas lekcji: 15 minut

Stosowanie zasad dla zabezpieczania uwierzytelnienia

Usługa Active Directory systemu Windows Server 2003 obsługuje zasady zabezpieczeń, które wzmacniają hasła i ich użycie wewnątrz przedsiębiorstwa. Oczywiście zasada hasła musi zostać zaprojektowana tak, aby wystarczająco zniechęcała włamywaczy, a jednocześnie była wygodna dla użytkowników, gdyż zbyt trudne hasła są zapomniane (co w rezultacie kończy się telefonem do działu wsparcia technicznego) lub co gorsza zapisywaniem trudnych haseł.

System Windows Server 2003 uruchomiony jako serwer członkowski obsługuje zasadę dotyczącą jego lokalnych kont użytkownika. Lokalna zasada zabezpieczeń może być zarządzana za pomocą odpowiednio nazwanej przystawki: *Local Security Policy*.

Dużo częściej spotykane będą zagadnienia związane z zasadami odnoszącymi się do obiektów użytkownika należących do domeny. Zasada konta domeny jest zarządzana przez *Default Domain Policy* (Domyślna zasada domeny). W celu jej sprawdzania i modyfikacji należy otworzyć konsolę *Active Directory Users and Computers* (Użytkownicy i komputery usługi Active Directory). Następnie zaznaczyć węzeł domeny i z menu **Action** (Akcja) wybrać polecenie **Properties** (Właściwości). Na zakładce *Group Policy* (Zasady grupy), obiekt GPO wyświetlony jako pierwszy lub jako odsyłacz do najwyższego obiektu jest obiektem zasady, który będzie kierował zasadami kont domeny. Najczęściej (i jest to dobra praktyka) obiektem tym jest *Default Domain Policy* (Domyślna zasada domeny). Należy zaznaczyć tę zasadę i kliknąć przycisk **Edit** (Edytuj). Uruchomione zostanie okno *Group Policy Object Editor* (Edytor obiektów zasad grupy), które przeznaczone jest dla domyślnej zasady domeny. Następnie należy kolejno przejść przez węzły: *Computer Configuration* (Konfiguracja komputera), *Windows*

Settings (Ustawienia systemu Windows), *Security Settings* (Ustawienia zabezpieczeń), *Account Policies* (Zasady konta).

Zasada haseł

Zasady haseł domeny umożliwiają zabezpieczenie sieci dzięki wprowadzaniu najbardziej praktycznych technik zarządzania hasłami. Zasady zostały opisane w tabeli 3-5.

Tabela 3-5 Zasady haseł

Zasada	Opis
Enforce Password History (Wymuszaj tworzenie historii haseł)	Włączenie tej zasady powoduje, że usługa Active Directory obsługuje listę ostatnio używanych haseł i nie pozwala, aby użytkownicy tworzyli hasła używane poprzednio. W rezultacie, użytkownik poproszony o zmianę hasła nie może ponownie użyć tego samego hasła, co zapobiega wydłużaniu czasu życia haseł. Ustawienia domyślne określają, że zasada jest włączona przy maksymalnej wartości 24 pamiętanych haseł. W wielu organizacjach używana jest wartość 6 lub 12.
Maximum Password Age (Maksymalny okres ważności hasła)	Zasada ta określa, kiedy użytkownik będzie zmuszony zmienić hasło. Hasła zmieniane rzadko lub w ogóle są bardziej podatne na złamanie i wykorzystanie przez włamywaczy. Wartość domyślna to 42 dni. W różnych organizacjach parametr ten najczęściej przyjmuje wartości od 30 do 90 dni. Kiedy użytkownik jest zmuszony do zmiany hasła, bez względu na to czy włączone jest zapamiętywanie poprzednio używanych haseł, użytkownik może po prostu zmieniać szereg razy swoje hasło, aż ponownie zacznie używać pierwotnego hasła.
Minimum Password Age (Minimalny okres ważności hasła)	Omawiana zasada zapobiega temu wymuszając, aby przerwa pomiędzy kolejnymi zmianami wynosiła określoną liczbę dni. Oczywiście hasło może być w usłudze Active Directory wyczyszczone w dowolnym momencie przez administratora lub osobę o odpowiednich uprawnieniach. Użytkownik jednak w wyspecyfikowanym okresie nie może zmieniać hasła częściej niż raz.
Minimum Password Length (Minimalna długość hasła) Passwords Must Meet Complexity Requirements (Hasło musi spełniać wymagania co do złożoności)	Zasada ta wymusza reguły lub filtry dotyczące tworzenia nowych haseł. Domyślny filtr hasła w systemie Windows Server 2003 (passfilt.dll) wymaga spełnienia następujących warunków: • Hasło nie może być zbudowane w oparciu o nazwę konta użytkownika. • Hasło składa się z co najmniej 6 znaków. • Hasło zawiera znaki należące do trzech spośród czterech typów wymienionych dalej: • Wielkie litery alfabetu (A...Z) • Małe litery alfabetu (a...z)

ciąg dalszy na następnej stronie

Zasada	Opis
	- Cyfry arabskie (0... 9) - Znaki inne niż alfanumeryczne (na przykład !\$,%,) Domyślne ustawienia systemu Windows Server 2003 określają, że zasada ta jest włączona.



Informacja Konfigurowanie długości hasła i wymagań co do jego złożoności nie ma wpływu na istniejące hasła. Zmiany te dotyczą nowotworzonych i modyfikowanych haseł po zastosowaniu zasady.

Zasada blokady konta

Blokowanie konta dotyczy koncepcji reagowania systemu na kilka nieudanych prób logowania się w systemie przez pojedynczego użytkownika. System powinien taką sytuację rozpoznać jako próbę włamania, której pierwszym etapem jest złamanie hasła i w takiej sytuacji system powinien zablokować konto, aby uniemożliwić dalsze próby. Zasady blokowania konta domeny określają maksymalną liczbę nieprawidłowych prób logowania, które miały miejsce w określonym czasie oraz okres czasu, w ciągu którego konto pozostaje zablokowane (w tym okresie użytkownik po prostu czeka lub kontaktuje się z administratorem). W tabeli 3-6 zamieszczone zostało podsumowanie zasad blokady konta (Account Lockout).

Tabela 3-6. Zasady blokady konta

Zasada	Opis
Account Lockout Threshold (Próg blokady konta)	Zasada ta określa liczbę nieprawidłowych prób logowania, po przekroczeniu której konto zostanie zablokowane. Można wybierać wartości z zakresu od 0 do 999. Wartości zbyt małe (na przykład: 3) mogą powodować blokadę konta wynikającą z typowych pomyłek użytkownika. Wartość 0 określa, że konto nigdy nie będzie zablokowane.
Account Lockout Duration (Czas trwania blokady konta)	Zasada ta definiuje okres, który musi upłynąć po zablokowaniu konta, aby usługa Active Directory automatycznie odblokowała konto użytkownika, Zasada domyślnie nie jest włączana, gdyż staje się przydatna dopiero w połączeniu z zasadą Account Lockout Threshold (Próg blokady konta). Chociaż zasada umożliwia definiowanie wartości z zakresu 0 do 99999 minut, czyli do około 10 tygodni, ustawienia 5 do 15 minut są wystarczające, aby praktycznie uniemożliwić atak, a jednocześnie nie będzie to miało znaczenia dla uprawnionych użytkowników, którzy przez błędne wprowadzanie hasła zablokowali konto. Wartość 0 powoduje, że konto musi być odblokowane ręcznie i tym samym użytkownik musi skontaktować się z administratorem.
Reset Account Lockout Counter After (Wyzeruj licznik blokady konta po)	Ustawienia te określają czas, który musi upłynąć od próby nieudanego logowania, zanim licznik zostanie wyzerowany. Można wybrać wartość z zakresu od 1 do 99999 minut, a wartość ta musi być równa lub mniejsza niż wartość określająca czas trwania blokady.

Zagadnienia związane z różnymi platformami

Bardzo często organizacje stosują różne usługi katalogowe, serwery i platformy aplikacji klienckich. W środowisku domeny Active Directory, w którym znajdują się systemy Windows 95, Windows 98, Windows Me, lub Windows NT 4, administrator musi zdawać sobie sprawę z kilku problemów.

- Hasła: Systemy Windows 2000, Windows XP Professional oraz Windows Server 2003 obsługują hasła o długości 127 znaków, natomiast w systemach Windows 95, Windows 98 oraz Windows ME można stosować tylko 14-znakowe hasła.
- Klient usługi Active Directory: Program klienta usługi Active Directory można pobrać z witryny firmy Microsoft i zainstalować na systemach Windows 95, Windows 98, Windows Me oraz Windows NT 4. Umożliwia to systemom działającym pod kontrolą poprzednich wersji Windows wykorzystywanie wielu funkcji usługi Active Directory, dostępnych w systemach Windows 2000 Professional lub Windows XP Professional, w tym:
 - » Podejście ukierunkowane na lokalizację: system klienta usługi Active Directory będzie próbował zalogować się w kontrolerze domeny swojej lokalizacji, a nie w dowolnym kontrolerze domeny przedsiębiorstwa.
 - » Active Directory Service Interfaces (ADSI): korzystanie ze skryptów podczas zarządzania usługą Active Directory.
 - » Distributed File System (Dfs): możliwość dostępu do współużytkowanych zasobów rozproszonego systemu plików (Dfs) serwerów działających pod kontrolą systemów Windows 2000 i Windows Server 2003.
 - » Uwierzytelnienie programu NT LAN Manager (NTLM) wersja 2: możliwość korzystania z poprawionych funkcji uwierzytelnienia programu NTLM wersja 2. »
- Active Directory Windows Address Book (WAB): strony właściwości
- » Możliwości wyszukiwania usługi Active Directory zintegrowane w poleceniach Start—Find lub Start—Search.

Wymienione poniżej funkcje, obsługiwane w systemach Windows 2000 Professional i Windows XP Professional, *nie są* udostępniane przez programy klienta usługi Active Directory w systemach Windows 95, Windows 98 i Windows NT 4:

- Uwierzytelnienie Kerberos V5
- Obsługa Group Policy (Zasady grupy) lub Change and Configuration Management (Zarządzanie konfiguracją i zmianami)
- Główna nazwa usługi (SPN) lub uwierzytelnienie wzajemne.

Oprócz tego, należy zdawać sobie sprawę z następujących zagadnień, które występują w mieszanych środowiskach:

- System Windows 98 obsługuje hasła o długości do 14 znaków, natomiast systemy Windows 2000, Windows XP i Windows Server 2003 mogą obsługiwać 127 znakowe hasła. Należy o tym pamiętać konfigurując hasła dla użytkowników, którzy logują się za pomocą systemu Windows 98.

Przy braku klienta usługi Active Directory użytkownicy systemów wcześniejszych niż Windows 2000 mogą zmieniać swoje hasła tylko, jeśli system miał dostęp do kontrolera domeny wykonującego pojedyncze operacje wzorca, nazywanego emulatorem głównego kontrolera domeny (PDC). Aby określić, który system w domenie jest emulatorem PDC, należy otworzyć konsolę *Active Directory Users And Computers*, zaznaczyć węzeł domeny, z menu **Action** (Akcja) wybrać polecenie **Operations Masters** (Wzorce operacji), a następnie kliknąć zakładkę **PDC**. Jeśli emulator PDC jest niedostępny (to znaczy jest wyłączony lub znajduje się w niedostępnej sieci), użytkownik nie będzie mógł zmienić swojego hasła.

Jak było już wcześniej nadmienione, obiekty użytkownika obsługują dwie właściwości nazwy logowania użytkownika. Są to: nazwa logowania systemów Windows wcześniejszych niż system Windows 2000 lub nazwa SAM, będące ekwiwalentem nazwy użytkownika systemów Windows 95, Windows 98 lub Windows NT 4. Podczas logowania, użytkownik wprowadza nazwę logowania i w oknie dialogowym *Log On To* (Zaloguj do) musi wybrać domenę. W innych przypadkach nazwa użytkownika może być wprowadzana w postaci `<NazwaDomeny>\<NazwaLogou>aniaUżytkownika>`.

Użytkownicy systemu Windows 2000 lub późniejszych mogą logować się w ten sam sposób, jak do tej pory lub za pomocą bardziej sprawnej nazwy UPN. Nazwa UPN ma postać `<NazwaLogowaniaUżytkownika>@<przyrostek UPN>`, gdzie przyrostek UPN jest domyślnie nazwą domeny DNS, w której znajduje się obiekt użytkownika. Jeśli podczas logowania używana jest nazwa UPN, nie jest konieczne wybieranie domeny w oknie dialogowym *Log On To*. W rzeczywistości okno to zostaje wyłączone w momencie wpisania znaku „@”.

Inspekcja uwierzytelnienia

Jeśli przewidujemy, że może zdarzyć się atak polegający na próbie złamania hasła użytkownika lub chcemy rozwiązywać problemy związane z uwierzytelnieniem, można skonfigurować zasadę inspekcji, która będzie generować wpisy w dzienniku Security (Zabezpieczenia) log. Rekordy dziennika mogą okazać się bardzo przydatne i pomóc w znalezieniu rozwiązania.

Zasady inspekcji

Aby dojść do wymienionych poniżej zasad, należy rozwinąć następujące węzły edytora *Group Policy/Object Editor* (Edytor obiektów zasady grupy) lub przystawki *Local Security Policy* (Lokalna zasada zabezpieczeń): *Computer Configuration* (Konfiguracja komputera), *Windows Settings* (Ustawienia systemu Windows), *Security Settings* (Ustawienia zabezpieczeń), *Local Policies* (Zasady lokalne), węzeł *Audit Policy* (Zasada inspekcji). Inspekcja może rejestrować zdarzenia, które zakończyły się sukcesem lub zdarzenia, które zakończyły się niepowodzeniem.

- * **Audit Account Logon Events (Przeprowadź inspekcję zdarzeń logowania na kontach)** Zasada ta sprawdza każdą instancję logowania użytkownika, która wywołała proces uwierzytelnienia w kontrolerze domeny. Dla kontrolerów domeny zasada ta jest definiowana w obiekcie GPO domyślnego kontrolera domeny. Warto odnotować, że po pierwsze, zasada ta będzie generować wpisy dziennika zabezpieczeń (Security log) na kontrolerze domeny każdorazowo, kiedy użytkownik loguje się w trybie interakcyjnym lub loguje się poprzez sieć za pomocą konta domeny. Po drugie, należy

zapamiętać, że dla pełnego sprawdzenia wyników inspekcji, należy przeanalizować dzienniki zabezpieczeń na wszystkich kontrolerach domeny, ponieważ uwierzytelnienie użytkownika jest rozdzielone pomiędzy wszystkimi kontrolerami domeny lub lokacji.

- **Audit Account Management (Przeprowadź inspekcję zarządzania kontami)** Zasada powoduje rejestrowanie zdarzeń tworzenia, usuwania lub modyfikacji użytkownika, grup bądź kont komputera. Pity włączonej zasadzie zarządzania kontami rejestrowane jest również resetowanie hasła.
- **Audit Logon Events (Przeprowadź inspekcję zdarzeń logowania)** Zdarzenia logowania obejmują logowania i wylogowania w trybie interakcyjnym oraz poprzez połączenia sieciowe. Jeśli zasada ta jest włączona i skonfigurowana tak, aby rejestrowane były pomyślnie zakończone logowania w kontrolerze domeny, to logowania na stacji roboczej nie wygenerują wpisu dziennika inspekcji. Jedynie logowania w trybie interakcyjnym lub poprzez sieć generują zdarzenia logowania. Zdarzenia logowania konta generowane są na komputerze lokalnym dla kont lokalnych, a na kontrolerze domeny dla kont sieci. Zdarzenia logowania powstają gdziekolwiek ma miejsce logowanie.



Wskazówka Warto zapamiętać różnice pomiędzy zdarzeniami Logon (logowanie) a zdarzeniami Account Logon (logowanie na koncie). Jeśli użytkownik loguje się na stacji roboczej za pomocą konta domeny, stacja robocza rejestruje zdarzenie logowania, natomiast kontroler domeny rejestruje zdarzenie logowania na koncie. Kiedy użytkownik łączy się z udostępnionym folderem serwera sieci, serwer rejestruje zdarzenie logowania, natomiast kontroler domeny rejestruje zdarzenie logowania na koncie.

Dziennik zdarzeń zabezpieczeń

Po skonfigurowaniu inspekcji, wiadomości o zdarzeniach zaczynają wypełniać dzienniki zabezpieczeń. Informacje te można przeglądać wybierając dziennik Security (Zabezpieczenia) w przystawce Event Viewer (Podgląd zdarzeń) dwukrotnie klikając konkretne zdarzenie.



Wskazówka egzaminacyjna Należy zapamiętać, że zdarzenia Account Logon (Logowanie na koncie) powinny być monitorowane na każdym kontrolerze domeny. Zdarzenia logowania muszą być monitorowane na wszystkich systemach.

Administrowanie uwierzytelnieniem użytkownika

Jeśli użytkownik zapomni hasła, został przeniesiony lub zwolniony, to każda z tych sytuacji powoduje odpowiednie zarządzanie obiektem użytkownika. Większość zadań administracyjnych dotyczących zabezpieczeń konta użytkownika to blokowanie konta, czyszczenie hasła, włączanie, wyłączanie, zmiana nazwy oraz usuwanie obiektów użytkownika.

Odblokowywanie konta użytkownika

Zasada blokowania konta powoduje, że po przekroczeniu liczby dozwolonych prób nieprawidłowego logowania, konto zostaje zablokowane i przez określony czas odrzucane są wszystkie próby logowania, chyba że administrator odblokuje konto.

Aby odblokować użytkownika, należy zaznaczyć obiekt użytkownika i z menu **Action** (Akcja) wybrać polecenie **Properties** (Właściwości). Następnie należy kliknąć zakładkę **Account** (Konto) i zmienić zaznaczenie pola wyboru: **Account Is Locked Out** (Konto jest zablokowane).

Czyszczenie haseł użytkownika

Jeśli użytkownik zapomni hasła, administrator musi je wyczyścić. Aby przeprowadzić taką operację, administrator nie musi znać zapomnianego hasła. Po prostu, zaznacza obiekt i w menu Action (Akcja) wybiera polecenie Reset Password (Resetuj hasło). Następnie dwukrotnie (aby potwierdzić zgodność) wprowadza nowe hasło i zgodnie z dobrą praktyką zabezpieczeń zaznacza opcję User Must Change Password At Next Logon (Użytkownik musi zmienić hasło przy następnym logowaniu).

Wyłączanie, włączanie, zmiana nazwy i usuwanie obiektów użytkownika

Zmiany osobowe w firmie wymuszają zarządzanie obiektami użytkowników polegające na wyłączaniu, włączaniu lub zmianie nazwy obiektów. Dla każdej z tych czynności operacje są podobne. Należy zaznaczyć użytkownika i z menu Action (Akcja) wybrać odpowiednie polecenie zgodnie z poniższym opisem:

- **Disabling And Enabling A User** (Odlączenie i włączanie użytkownika) Jeśli użytkownik nie potrzebuje dostępu do sieci przez dłuższy okres, powinno się zablokować jego konto. Konto zostanie włączone ponownie, jeśli użytkownik znowu będzie potrzebował dostępu do sieci. Warto zauważyć, że w menu Action (Akcja) występuje tylko jedno polecenie Disable (Wyłącz) lub Enable (Włącz), w zależności od bieżącego statusu obiektu.
- **Deleting A User** (Usuwanie użytkownika) Jeśli użytkownik zwalnia się z przedsiębiorstwa i *na jego miejsce nie przewiduje się szybko zastępstwa*, należy usunąć obiekt użytkownika. Należy zwrócić uwagę, że usuwając użytkownika, usuwa się jednocześnie jego członkostwo w grupie, identyfikator SID oraz jego uprawnienia. Jeśli utworzony zostanie obiekt o takiej samej nazwie, będzie miał inny identyfikator SID i trzeba będzie ponownie przydzielać uprawnienia i definiować członkostwo w grupach.
- **Renaming A User** (Zmiana nazwy użytkownika) Zmiana nazwy obiektu użytkownika ma miejsce, jeśli użytkownik zmieni swoje nazwisko, na przykład z powodu małżeństwa lub jeśli zwolnił się z przedsiębiorstwa, ale na jego miejsce przewidziana jest inna osoba, która powinna mieć przydzielone takie same prawa czy inne właściwości.



Wskazówka Należy dobrze rozumieć różnice między wyłączeniem a usunięciem obiektu oraz między włączeniem a odblokowaniem użytkownika.

Zadanie kontrolne: Zabezpieczenia i rozwiązywanie problemów dotyczących uwierzytelnienia

W zadaniu tym konfigurowane będą zasady inspekcji domeny, a następnie wygenerowane zostaną zdarzenia logowania. Końcowym etapem zadania będzie analiza wyników zawartych w informacjach o zarejestrowanych zdarzeniach.

Ćwiczenie 1: Konfiguracja zasad

1. Otwórz konsolę *Active Directory Users And Computers* (Użytkownicy i komputery usługi Active Directory).
2. Zaznacz węzeł domeny contoso.com.
3. Z menu Action (Akcja) wybierz polecenie **Properties** (Właściwości).
4. Na zakładce *Group Policy* (Zasada grupy) zaznacz domyślną zasadę domeny (Default Domain Policy) i kliknij przycisk **Edit**.
5. Poprzez węzły *Computer Configuration* (Konfiguracja komputera), *Windows Settings* (Ustawienia systemu Windows), *Security Settings* (Ustawienia zabezpieczeń) i *Account Policies* (Zasady kont) przejdź do **Account Lockout Policy** (Zasada blokady konta).
6. Dwukrotnie kliknij zasadę **Account Lockout Duration** (Czas trwania blokady konta).
7. Zaznacz pole wyboru **Deny This Policy Setting** (Definiuj następujące ustawienia zasad).
8. Wpisz 0 jako określenie czasu trwania blokady i kliknij przycisk **Apply** (Zastosuj).
System powiadomi, że skonfiguruje próg blokady konta i zresetuje licznik zasad. Kliknij przycisk OK.
9. Kliknij przycisk OK, aby potwierdzić ustawienia, a następnie kliknij przycisk OK, aby zamknąć okno dialogowe zasady.
10. Sprawdź, czy wartość parametru zasady *Account Lockout Duration* (Czas trwania blokady konta) wynosi zero, czy próg ma wartość 5, a licznik zasady ustawiony został na 30 minut.
11. Zamknij okno *Group Policy Object Editor* (Edytor obiektów zasady grupy).
12. Kliknij przycisk OK, aby zamknąć okno dialogowe *Properties* (Właściwości) domeny contoso.com.
13. Po rozwinięciu węzła domeny zaznacz kontener **Domain Controllers**.
14. W menu **Action** (Akcja) wybierz polecenie **Properties** (Właściwości).
15. Na zakładce *Group Policy* (Zasady grupy) zaznacz zasadę **Default Domain Controllers Policy** i kliknij przycisk **Edit** (Edytuj).
16. Poprzez węzły *Computer Configuration* (Konfiguracja komputera), *Windows Settings* (Ustawienia systemu Windows), *Security Settings* (Ustawienia zabezpieczeń) i *Local Policies* (Zasady lokalne) przejdź do **Audit Policy** (Zasada inspekcji).
17. Dwukrotnie kliknij zasadę **Audit Account Logon Events** (Przeprowadź inspekcję zdarzeń logowania na kontach).
18. Zaznacz opcję **Deny These Policy Settings** (Definiuj następujące ustawienia zasad), zaznacz obie opcje **Success** (Sukces) i **Failure** (Niepowodzenie), a następnie kliknij przycisk OK.
19. Dwukrotnie kliknij zasadę **Audit Logon Events** (Przeprowadź inspekcję zdarzeń logowania).

20. Zaznacz opcję **Define ITiese Policy Settings** (Definiuj następujące ustawienia zasad), zaznacz obie opcje **Success** (Sukces) i **Failure** (Niepowodzenie), a następnie kliknij przycisk OK
21. Dwukrotnie kliknij zasadę **Account Management** (Przeprowadź inspekcję zarządzania kontami).
22. Zaznacz opcję **Define These Policy Settings** (Definiuj następujące ustawienia zasad), zaznacz opcję **Success** (Sukces), a następnie kliknij przycisk OK.
23. Zamknij okno *Group Policy Object Editor* (Edytor obiektów zasady grupy).
24. Kliknij przycisk OK, aby zamknąć okno dialogowe *Properties* (Właściwości) dla obiektu *Domain Controllers Properties*.

Ćwiczenie 2: Generowanie zdarzeń logowania

1. Wyloguj się z serwera *Scriver01*.
2. Wygeneruj dwa zdarzenia nieprawidłowego logowania próbując się zalogować za pomocą nazw użytkownika **sbishop** i *nieprawidłowego* hasła.
3. Prawdłowo zaloguj się jako **sbishop**.
4. Wyloguj się.

Ćwiczenie 3: Generowanie zdarzeń związanych z zarządzaniem kontami

1. Zaloguj się jako Administrator.
2. Otwórz konsolę *Active Directory Users And Computers*.
3. W oknie drzewa przystawki przejdź do jednostki organizacyjnej **Employees**.
4. W oknie szczegółów zaznacz obiekt użytkownika **Scott Bishop**, a następnie kliknij menu Action (Akcja).
5. Kliknij polecenie **Reset Password** (Resetuj hasło).
6. Wprowadź i potwierdź nowe hasło dla użytkownika Scott Bishop, a następnie kliknij przycisk OK

Ćwiczenie 4: Analiza wiadomości o zdarzeniach związanych z zabezpieczeniami uwierzytelnienia

1. W grupie programów **Administrative Tools** otwórz konsolę **Computer Management** (Zarządzanie komputerem).
2. Rozwiń węzeł **Event Viewer** (Podgląd zdarzeń) i wybierz dziennik **Security** (Zabezpieczenia).
3. Upewnij się, że kolumna **Category** (Kategoria) jest odpowiedniej szerokości, aby można było rozpoznać typy zaprotokołowanych zdarzeń.
4. Przejrzyj zdarzenia, które zostały ostatnio wygenerowane — nieprawidłowe logowania, prawidłowe logowania oraz wyczyszczenie hasła użytkownika **Scott Bishop**.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nic potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materia! lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Dla domeny włączona została zasada wymagań złożoności hasła. Należy opisać wymagania dla haseł oraz kiedy te wymagania zaczynają obowiązywać.
2. Jaka jest najlepsza pojedyncza zasada inspekcji pozwalająca w przedsiębiorstwie monitorować „słownikowy” atak przeprowadzany w celu złamania haseł użytkowników oraz który dziennik lub dzienniki należy w tym celu przeanalizować?
3. Użytkownik zapomniał hasła i kilka razy próbował zalogować się za pomocą nieprawidłowego hasła. W końcu użytkownik odebrał komunikat informujący, że konto jest wyłączone lub zablokowane. Komunikat sugeruje, aby użytkownik skontaktował się z administratorem. Co musi zrobić administrator?
 - a. Usunąć i ponownie utworzyć obiekt użytkownika.
 - b. Zmienić nazwę obiektu użytkownika.
 - c. Włączyć obiekt użytkownika.
 - d. Odblokować obiekt użytkownika.
 - e. Zresetować hasło obiektu użytkownika.

Podsumowanie lekcji

- Domyślna zasada domeny — Default Domain Policy, zarządza zasadami kont, wliczając w to zasady blokowania i zasady haseł.
- Domyślna zasada kontrolerów domeny - Default Domain Controllers Policy, określa najważniejsze zasady inspekcji dla kontrolerów domeny.
- Zasada inspekcji uwierzytelnienia powoduje rejestrowanie zdarzeń w dzienniku zabezpieczeń każdego kontrolera domeny.

Zadanie praktyczne

Jeden z członków domeny Contoso powiadomił niedawno, że padł ofiarą złamania zabezpieczenia hasła, co spowodowało ujawnienie jego ważnych danych. Administrator zdecydował się sprawdzić konfigurację zabezpieczeń domeny Contoso oraz wprowadzić następujące wymagania:

- **Wymaganie 1:** Ponieważ była przeprowadzona aktualizacja kontrolerów domeny działających pod kontrolą systemu Windows 2000 Server do systemu Windows Server 2003, to zasada kont domeny zachowuje wymagania systemu Windows 2000 Server. Tak więc zasady konta domeny powinny wymagać:
 - » Zmiany hasła co 60 dni
 - » Hasła o długości 8 znaków
 - » Złożonych hasła
 - » Minimalnego czasu obowiązywania hasła - tydzień
 - » Zapamiętywania 20 poprzednich hasła
 - » Blokowania konta po pięciu nieudanych próbach logowania przy 60 minutowej przerwie
 - » Interwencji administratora w celu odblokowania kont.
- **Wymaganie 2:** Dodatkowo należy zapewnić, żeby zasady te zaczęły obowiązywać w ciągu % godzin. Zasady hasła zostaną wprowadzone w momencie zmiany hasła przez użytkownika - zasady nie mają wpływu na istniejące hasła. Administrator wymaga, by użytkownicy zmienili swoje hasła w możliwie najkrótszym czasie oraz żeby nie dotyczyły kont używanych przez usługi. Konta usług są przechowywane w jednostce organizacyjnej Service Accounts domeny Contoso. Konta użytkowników są przechowywane w jednostce organizacyjnej Employees oraz w 15-tu jednostkach OU zlokalizowanych poniżej jednostki Employees.
- **Wymaganie 3:** Zablokowanie pulpitów przedstawicieli handlowych, dzięki temu będzie mniej prawdopodobne, że zainstalują niestandardowe paski narzędzi sieci Web, prognozy pogody, programy narzędziowe typu „tapeta dnia” lub inne oprogramowanie, które może połączyć się z Internetem i umożliwić zaatakowanie pulpitu.

Wymaganie 1

Aby spełnić pierwsze wymaganie należy zmodyfikować ustawienia dotyczące hasła i blokady konta.

1. Co powinno zostać zmodyfikowane, aby spełnić wymagania numer 1 ?
 - a. Plik szablonu zabezpieczeń kontrolera domeny Hisccdc.inf
 - b. Zasada Default Domain (Domyślna zasada domeny).
 - c. Zasada Default Domain Controller (Domyślna zasada kontrolera domeny)
 - d. Szablon zabezpieczeń kontrolera domeny Ssetup Securiry.inf

Poprawna odpowiedź to b.
2. Która zasada musi zostać określona do takiego skonfigurowania blokady konta, aby w celu odblokowania konta użytkownicy musieli skontaktować się z działem wsparcia technicznego?
 - a. Czas trwania blokady konta: 999
 - b. Próg blokady konta: 999

- c. Czas trwania blokady konta: 0
- d. Próg blokady konta: 0

Prawidłowa odpowiedź to c. Należy odpowiednio skonfigurować zasady domeny. Opis procedury zawiera ćwiczenie 1 w lekcji 4.

Wymaganie 2

Opisane w tym punkcie wymagania wskazują, że należy zmusić użytkowników do możliwie najszybszej zmiany hasła. Podpowiedzią jest informacja, że konta użytkownika obsługują flagę User Must Change Password At **Next** Logon (Użytkownik musi zmienić hasło przy następnym logowaniu).

1. Która procedura będzie najszybszym i najbardziej efektywnym sposobem skonfigurowania konta użytkownika tak, aby zmuszony był do zmiany hasła przy następnym logowaniu?
 - a. Należy zaznaczyć konto użytkownika, otworzyć okno jego właściwości i na stronie Account (Konto) zaznaczyć opcję User Must Change Password At **Next** Logon (Użytkownik musi zmienić hasło przy następnym logowaniu). Procedurę należy powtórzyć dla każdego konta.
 - b. Należy nacisnąć CTRL+A, aby zaznaczyć wszystkich użytkowników jednostki organizacyjnej Employees. Wybrać polecenie Properties (Właściwości) i na stronie Account (Konto) zaznaczyć opcję User Must Change Password At **Next** Logon (Użytkownik musi zmienić hasło przy następnym logowaniu). Procedurę należy powtórzyć dla każdej jednostki organizacyjnej.
 - c. Należy użyć polecenia DSADD.
 - d. Należy użyć polecenia DSRM.
 - e. Należy użyć polecenia DSQUERY oraz DSMOD.

Prawidłowa odpowiedź to e.

2. Polecenie DSOJQUERY umożliwia utworzenie listy obiektów w oparciu o interesujące w zadaniu właściwości i lokalizację, a następnie przekazać listę tych obiektów do polecenia DSMOD, za pomocą którego zostaną odpowiednio zmodyfikowane. Należy otworzyć wiersz poleceń i wpisać następujące polecenie:

DSOJQUERY user „OU=Employees,DC=Contoso,DC=Com”

Polecenie wygeneruje listę obiektów użytkownika jednostki organizacyjnej Employees. Zaletą tego podejścia jest to, że polecenie uwzględni użytkowników znajdujących się w jednostkach organizacyjnych umieszczonych poniżej jednostki Employees. W zadaniu określono, że istnieje 15 takich jednostek. Wszystkie te jednostki OU będą uwzględnione podczas generowania listy obiektów za pomocą polecenia DSOJQUERY

W tym momencie, aby spełnić wymagania należy wpisać następujące polecenie:

DSOJQUERY user „OU=Employees,DC=Contoso,DC=Com” | DSMOD user -mustchpwd yes

Wymaganie 3

W zadaniu tym należy zmodyfikować profile użytkownika przedstawicieli handlowych.

1. Który profil będzie najbardziej użyteczny dla obsługi „zablokowanego” pulpitu, przeznaczonego dla wszystkich przedstawicieli handlowych?

- a. Profil lokalny
 - b. Lokalny, obowiązkowy profil
 - c. Profil Ali Users (Wszyscy użytkownicy)
 - d. Wstępnie skonfigurowany, mobilny profil grupy
 - c. Wstępnie skonfigurowany, obowiązkowy, mobilny profil grupy
- Prawidłowa odpowiedź to b.
2. W ćwiczeniu 5 lekcji 3 utworzony został profil nazwany Sales. Poprzez zmianę nazwy pliku Ntuser.dat na Ntuser.man, profil ten stał się profilem obowiązkowym. Ostatecznie profil został przypisany do kilku użytkowników. W jaki sposób można przekonać się, że każdy nowy przedstawiciel handlowy używa tego samego profilu?
- Należy zmodyfikować szablon konta Sales Representative, który był utworzony w ćwiczeniu 1 lekcji 2. Na zakładce Profile (Profil) należy wpisać ścieżkę profilu: \\server01\profiles\sales. Prawidłowość przeprowadzanych czynności można sprawdzić kopiując szablon w celu utworzenia nowego konta użytkownika, a następnie zalogować się jako ten nowy użytkownik. Po przeprowadzeniu modyfikacji pulpitu należy wylogować się i ponownie zalogować. Pomiedzy sesjami modyfikacje pulpitu nie powinny się zachować.

Rozwiązywanie problemów

W tym ćwiczeniu zostanie wygenerowanych kilka rodzajów zdarzeń dotyczących niepowodzeń logowania i operacji na kontach. Następnie przeprowadzana będzie procedura rozpoznawania i odpowiedniego korygowania tych niepowodzeń.

Przed przystąpieniem do ćwiczenia należy utworzyć konta użytkowników. Potrzebne konta użytkowników były utworzone w ćwiczeniu 3 lekcji 2. Potrzebne będzie także skonfigurowanie zasad kont | domeny tak, jak było przeprowadzone w ćwiczeniu 1 lekcji 4.

Ćwiczenie 1: Generowanie zdarzeń dotyczących niepowodzeń logowania i operacji na kontach

1. Wyloguj się z serwera ServcrO 1.
2. Wywołaj blokadę konta logując się sześciokrotnie za pomocą nazwy użytkownika lsmithbates i *nieprawidłowego* hasła. Warto zwrócić uwagę na różnice w komunikatach otrzymywanych po nieudanej próbie logowania w sytuacji, kiedy konto nic jest zablokowane i kiedy już zostało zablokowane.
3. Zaloguj się jako Daniclle Tiedt za pomocą nazwy użytkownika dtiedt.
4. Naciśnij CTRL+ALT+DELETE i zmień hasło na inne.
5. Naciśnij CTRL+ALT+DELETE i spróbuj zmienić hasło na poprzednie. Czy jest to możliwe? Dlaczego jest możliwe lub dlaczego nie jest możliwe?
6. Spróbuj zmienić hasło na jeszcze inne nowe hasło. Czy jest to możliwe? Dlaczego jest możliwe lub dlaczego nie jest możliwe?
- 7- Wyloguj się.

Ćwiczenie 2: Monitorowanie oraz rozpoznawanie zdarzeń dotyczących logowania i zarządzania kontem.

1. Zaloguj się jako administrator.
2. W grupie programów Administrative Tools (Narzędzia administracyjne) otwórz konsolę Computer Management (Zarządzanie komputerem).
3. Rozwiń węzeł Event Viewer (Podgląd zdarzeń) i zaznacz dziennik Security (Zabezpieczenia).
4. Upewnij się, że kolumna Category (Kategoria) jest odpowiedniej szerokości, aby rozpoznać rodzaje zarejestrowanych zdarzeń.
5. Przeanalizuj ostatnio wygenerowane zdarzenia. Należy zwrócić uwagę na nieudane próby logowania, blokady oraz próby wyczyszczenia hasła użytkownika Danielle Tiedt.

Ćwiczenie 3: Naprawa problemów dotyczących kont i uwierzytelnienia

1. Otwórz konsolę Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory).
2. W oknie drzewa przystawki zaznacz jednostkę organizacyjną Employees.
3. W oknie szczegółów zaznacz obiekt użytkownika Danielle Tiedt.
4. W menu Action (Akcja) kliknij polecenie Reset Password (Resetuj hasło).
5. Wpisz stare i nowe hasło użytkownika Danielle Tiedt. Dlaczego możesz przeprowadzić te operacje, jeśli będąc zalogowany jako użytkownik Danielle Tiedt nie mogłeś?
6. Zaznacz obiekt użytkownika Lorrin Smith-Bates.
7. W menu Action (Akcja) kliknij polecenie Properties (Właściwości).
8. Na zakładce Account (Konta) usuń zaznaczenie pola wyboru Account Is Locked Out (Konto jest zablokowane).
9. Kliknij przycisk OK.

Podsumowanie rozdziału

- Tylko użytkownik, który jest członkiem grup Enterprise Admins (Administratorzy przedsiębiorstwa), Domain Admins (Administratorzy domeny) i Account Operators (Operatorzy kont) lub użytkownik, w stosunku do którego nastąpiła delegacja uprawnień, może tworzyć obiekty użytkownika.
- Obiekty użytkownika zawierają właściwości najczęściej kojarzone z kontami użytkownika, w tym nazwy logowania i hasło czy unikatowy identyfikator użytkownika SID. Zawierają również szereg właściwości dotyczących osób, które reprezentują, wliczając w to informacje osobowe, członkostwo w grupie bądź ustawienia administracyjne. W systemie Windows Server 2003 niektóre te właściwości mogą być zmieniane jednocześnie dla wielu użytkowników.
- Szablon obiektu użytkownika jest obiektem, który jest kopiowany w celu utworzenia nowego użytkownika. Jeśli szablon nie jest „rzeczywistym” użytkownikiem, powinien być wyłączony. W oparciu o szablon kopiowany jest tylko podzbiór właściwości.
- Polecenie CSVDE umożliwia import obiektów katalogu na podstawie pliku tekstowego, w którym wartości rozdzielane są przecinkami.

- System Windows Server 2003 obsługuje nowe efektywne narzędzia wiersza poleceń, które umożliwiają tworzenie, zarządzanie oraz usuwanie obiektów katalogu. Te nowe narzędzia to: DSQUERY, DSGET, DSADD, DSMOVE, DSMOD oraz DSRM. Najczęściej polecenie DSQUERY służy do generowania listy obiektów, która jest następnie wykorzystywana jako informacje wejściowe innego polecenia (praca potokowa).
- System Windows Server 2003 udostępnia indywidualne profile dla każdego użytkownika, który zalogował się w systemie. Domyślnie profile są przechowywane w lokalnym systemie w folderze `%Systemdrive%\Documents and Settings\%Username%`.
- Korzystanie z profili mobilnych wymaga jedynie udostępnionego foldera oraz ścieżki profilu skonfigurowanej we właściwościach obiektu użytkownika.
- Wstępnie skonfigurowane profile są profilami skopiowanymi do ścieżki profilu, zanim ścieżka ta została określona w obiekcie użytkownika.
- Profile grupy muszą być profilami obowiązkowymi, aby zmiany poczynione przez jednego użytkownika nie miały wpływu na pracę innych użytkowników. Zmiana nazwy pliku Ntuser.dat na Ntuser.man powoduje, że profil staje się profilem obowiązkowym.
- Domyślna zasada domeny, Default Domain Policy, kieruje zasadami konta, wliczając w to zasady hasła i blokady konta, podczas gdy zasada Default Domain Controllers Policy (Domyślna zasada kontrolerów domeny) określa podstawowe zasady inspekcji kontrolerów domeny.
- Inspekcja uwierzytelnienia generuje wpisy dziennika zabezpieczeń każdego kontrolera domeny.

Informacje dla zdających egzamin

Przed przystąpieniem do egzaminu należy zapoznać się z przedstawionymi poniżej najważniejszymi faktami i pojęciami, aby określić które tematy wymagają pogłębienia. Należy powrócić do lekcji, aby osiągnąć większą wprawę oraz przejrzeć działy znajdujące się w części 2 — „Materiały dodatkowe”. Informacje tu zawarte kierują do materiałów uzupełniających tematy objęte zadaniami egzaminacyjnymi.

Najważniejsze fakty

- Do utworzenia konta użytkownika wymagane jest odpowiednie członkostwo w grupie lub odpowiednie uprawnienia.
- Opcje udostępnione w celu tworzenia lub zarządzania wieloma kontami użytkowników to: szablony użytkowników, importowanie oraz programy narzędziowe wiersza poleceń. Warto zapoznać się z różnicami między poszczególnymi opcjami oraz słabymi i mocnymi stronami każdej z nich.
- Dostęp i modyfikowanie właściwości możliwe jest podczas tworzenia użytkownika, modyfikowania za pomocą konsoli Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory), kopiowania szablonu, wykonywania polecenia DSQUERY lub podczas dodawania bądź modyfikowania użytkowników za pomocą poleceń DSADD i DSMOD.
- Proces konfigurowania mobilnych profili użytkownika, wstępnie skonfigurowanych profili lub wstępnie skonfigurowanych, obowiązkowych profili grup.
- Wpływ zasady grupy na hasło i ustawienia blokady konta.
- Sposoby inspekcji zdarzeń dotyczących uwierzytelnienia.

Najważniejsze pojęcia

Szablon konta użytkownika Określenia te dotyczą również innych pojęć, ale koncepcja jest taka sama. Szablon konta jest używany jako baza dla nowego konta. Szablon jest *kopiowany* w celu utworzenia nowego użytkownika oraz niektórych jego właściwości, w szczególności kopiowane jest członkostwo w grupach.

Porównanie konta zablokowanego i wyłączonego Konto jest wyłączone, jeśli wygasło lub jeśli zostało wyłączone przez administratora. Konto jest natomiast zablokowane, jeśli przekroczony został próg ilości nieudanych prób dostępu, określony dla danego konta przez zasadę blokady konta.

Profil obowiązkowy Jest to profil użytkownika, który nie obsługuje modyfikacji zachodzących między sesjami. Użytkownik *może* modyfikować profil, ale podczas wylogowywania się z systemu, zmiany nie są zapisywane. Profile grupy muszą być profilami obowiązkowymi, w przeciwnym razie zmiany poczynione przez jednego z użytkowników, będą wpływać na pracę pozostałych.

Pytania i odpowiedzi

77 Pytania do lekcji 1

1. Za pomocą konsoli Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) użytkownik konfiguruje obiekty użytkowników w domenie i może zmieniać adres i numer telefonu obiektu użytkownika, który reprezentuje jego samego. Polecenie New User (Nowy Użytkownik) nie jest dla niego dostępne. Jakie jest najbardziej prawdopodobne wyjaśnienie takiej sytuacji?

Użytkownik nie ma wystarczających uprawnień do tworzenia w kontenerze obiektu użytkownika. Polecenia przystawki są dostosowane tak, aby odzwierciedlały uprawnienia administracyjne użytkownika. Jeśli użytkownik nie ma praw do tworzenia obiektu, niedostępne będzie dla niego odpowiednie polecenie New (Nowy).

2. Administrator tworzy pewną liczbę obiektów użytkownika dla zespołu firmy, skupiającej pracowników zatrudnionych na okres próbny. Przyszli pracownicy będą zatrudnieni od godziny 9.00 do 17.00, a ich umowy podpisane zostaną za miesiąc lub dwa. Pracownicy będą pracować zgodnie z tym harmonogramem. Które z wymienionych poniżej właściwości powinien skonfigurować administrator, aby zapewnić największe bezpieczeństwo dla tych obiektów?
 - a. Hasło
 - b. Godziny logowania
 - c. Account expires (Wygasanie hasła)
 - d. Store password using reversible encryption (Zachowaj hasło przy użyciu szyfrowania odwracalnego)
 - e. Account is trusted for delegation (Konto jest zaufane w kwestii delegowania)
 - f. User must change password at next logon (Użytkownik musi zmienić hasło przy następnym logowaniu)
 - g. Account is disabled (Konto jest wyłączone)
 - h. Password never expires (Hasło nigdy nie wygasa)

Prawidłowe odpowiedzi to a, b, c, f, g.

3. Które z wymienionych poniżej właściwości i zadań administracyjnych mogą być jednocześnie konfigurowane dla kilku obiektów użytkownika??
- Last Name (Nazwisko)
 - User Logon Name (Nazwa logowania użytkownika)
 - Wyłączenie konta
 - Włączenie konta
 - Resetowanie hasła
 - Password Never Expires (Hasło nigdy nie wygasa)
 - User Must Change Password At Next Logon (Użytkownik musi zmienić hasło przy następnym logowaniu)
 - Logon Hours (Godziny logowania)
 - Computer Restrictions (Logon Workstations) (Ograniczenia komputera. Logowanie na stacjach roboczych)
 - Title (tytuł)
 - Direct Reports (Bezpośredni podwładni)
- Prawidłowe odpowiedzi to c, d, f, g, h, i, j.

Pytania do lekcji 2

1. Która opcja będzie najbardziej przydatna do wygenerowania 100 nowych obiektów użytkownika, przy czym dla każdego powinny być jednakowe ustawienia następujących właściwości: Profile path (ścieżka profilu), Home folder path (ścieżka katalogu macierzystego), Title (tytuł), Web Page (Strona sieci Web), Company (firma), Department (dział) oraz Manager (menedżer)?
- Polecenie DSADD będzie najbardziej przydatną opcją. Można wprowadzić jeden wiersz polecenia zawierający wszystkie parametry. Pozostawiając pusty parametr *UserDN*, można za jednym razem w konsoli polecenia wprowadzić nazwę wyróżniającą użytkownika. Szablon obiektu użytkownika nie umożliwia skonfigurowania niektórych opcji, w tym: Title (Tytuł), Telephone Number (Numer telefonu) i Web Page (Strona sieci Web). Utworzenie tekstowego pliku, w którym wartości rozdzielane są przecinkami, w porównaniu do innych metod, jest czasochłonne i byłoby przesadą tworzenie takiego pliku, w szczególności, jeśli tak wiele parametrów jest identycznych.
2. Które narzędzie pozwala zidentyfikować konta nieużywane od dwóch miesięcy?
- DSADD
 - DSGET
 - DSMOD
 - DSRM
 - DSQUERY
- Prawidłowa odpowiedź to e.
3. Która zmienna może być używana razem z poleceniami DSMOD oraz DSADD do utworzenia katalogów macierzystych i folderów profili specyficznych dla użytkownika?
- % Username%
 - \$ UsernameS

c. `CN=Username` d.

<Username> Prawidłowa

odpowiedź to b.

4. Które narzędzia umożliwiają wyświetlenie numerów telefonicznych wszystkich użytkowników jednostki organizacyjnej OU?
 - a. DSADD
 - b. DSGET
 - c. DSMOD
 - d. DSRM
 - e. DSQUERY

Prawidłowe odpowiedzi to b oraz e. Polecenie DSQUERY generuje listę obiektów użytkownika w jednostce OU, która może być przekazana do polecenia DSGET. To polecenie może wyświetlić poszczególne właściwości, jak na przykład numery telefoniczne.

Pytania do lekcji 3

1. Opisz, w jaki sposób powstaje pulpit użytkownika, jeśli nie są stosowane profile mobilne.
Podczas pierwszego logowania się użytkownika, system kopiuje profil nazwany Default User (Użytkownik domyślny) i na tej podstawie w folderze `%Systemdrive%\Documents and Settings\%Username%` (lokalizacja domyślna) tworzy profil dotyczący danego użytkownika. Środowisko użytkownika jest połączeniem jego profilu i profilu All Users (Wszyscy użytkownicy).
2. Utwórz odpowiednią kolejność przedstawionych poniżej czynności tak, aby odzwierciedlały proces tworzenia wstępnie skonfigurowanego mobilnego profilu użytkownika. Należy uwzględnić wszystkie kroki.
 - Utwórz niestandardowy pulpit i środowisko użytkownika.
 - Zaloguj się jako użytkownik o wystarczających uprawnieniach do modyfikowania właściwości konta użytkownika.
 - Skopiuj profil do sieci.
 - Utwórz konto użytkownika tak, żeby profil można było utworzyć bez modyfikowania żadnego aktualnego profilu użytkownika.
 - Zaloguj się za pomocą konta profilu.
 - Na stronie właściwości użytkownika Profile wpisz ścieżkę UNC do profilu.
 - Zaloguj się jako administrator lokalny lub administrator domeny.
 1. Utwórz konto użytkownika tak, żeby profil można było utworzyć bez modyfikowania żadnego aktualnego profilu użytkownika.
 2. Zaloguj się za pomocą konta profilu.
 3. Utwórz niestandardowy pulpit i środowisko użytkownika.
 4. Zaloguj się jako administrator lokalny lub administrator domeny.
 5. Skopiuj profil do sieci.
 6. Zaloguj się jako użytkownik o wystarczających uprawnieniach do modyfikowania właściwości konta użytkownika.

7. Na stronie właściwości użytkownika Profile wpisz ścieżkę UNC do profilu.
3. W jaki sposób powstaje profil obowiązkowy?
- Skonfigurowanie uprawnień na stronie właściwości foldera Security (Zabezpieczenia) tak, aby nie był możliwy zapis.
 - Skonfigurowanie uprawnień na stronie właściwości foldera Security (Zabezpieczenia) tak, aby możliwy był tylko odczyt.
 - Modyfikacja atrybutów foldera profilu i określenie atrybutu Read Only (Tylko do odczytu).
 - Zmiana nazwy pliku Ntuser.dat na Ntuser.man.

Prawidłowa odpowiedź to d.

111 Pytania do lekcji 4

1. Dla domeny włączona została zasada wymagań złożoności hasła. Należy opisać wymagania dla haseł oraz kiedy te wymagania zaczynają obowiązywać.
- Hasło nie może być zbudowane na nazwie konta użytkownika. Musi zawierać co najmniej sześć znaków, przy czym co najmniej po jednym znaku z trzech spośród czterech kategorii: duże litery, małe litery, cyfry arabskie oraz znaki inne niż alfanumeryczne. Wymagania te od razu obowiązują nowe konta. Dla kont istniejących wymagania zaczną być stosowane przy następnej zmianie hasła.
2. Jaka jest najlepsza pojedyncza zasada inspekcji pozwalająca w przedsiębiorstwie monitorować „słownikowy” atak przeprowadzany w celu złamania haseł użytkowników oraz który dziennik lub dzienniki należy w tym celu przeanalizować?
- Przy tych założeniach, najlepiej nadającą się zasadą sprawdzania nieudanych zdarzeń logowania na koncie jest Audit Policy (Zasada inspekcji). Nieudane logowania będą generować zdarzenia rejestrowane w dzienniku Security (Zabezpieczenia) każdego kontrolera domeny.
3. Użytkownik zapomniał hasła i kilka razy próbował zalogować się za pomocą nieprawidłowego hasła. W końcu użytkownik odebrał komunikat informujący, że konto jest wyłączone lub zablokowane. Komunikat sugeruje, aby użytkownik skontaktował się z administratorem. Co musi zrobić administrator?
- Usunąć i ponownie utworzyć obiekt użytkownika.
 - Zmienić nazwę obiektu użytkownika.
 - Włączyć obiekt użytkownika.
 - Odblokować obiekt użytkownika.
 - Resetować hasło obiektu użytkownika.

Prawidłowe odpowiedzi to d oraz e. Pomimo, że podczas logowania w systemie Windows 2000 tekst komunikatu informuje, że konto jest wyłączone, w rzeczywistości konto jest zablokowane. W systemie Windows Server 2003 komunikaty są dokładne. Jak jest w rzeczywistości, można również sprawdzić, patrząc jaka była przyczyna komunikatu: użytkownik zapomniał hasła. W tej sytuacji należy odblokować konto i zresetować hasło.

4 Konta grup



Zadania egzaminacyjne omawiane w tym rozdziale:

- Tworzenie i zarządzanie grupami
 - » Tworzenie i modyfikowanie grup za pomocą przystawki konsoli MMC — Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory)
 - » Rozpoznawanie i modyfikacja zakresu grupy
 - » Zarządzanie członkostwem grupy
 - » Automatyzacja tworzenia i modyfikowania grup

Cele rozdziału

Użytkownicy, grupy i komputery są podstawowymi obiektami usługi katalogowej Active Directory, ponieważ umożliwiają pracownikom, ich menedżerom, administratorom systemu czy komukolwiek korzystającemu z sieci, bezpiecznie określać swoją tożsamość. Bez określania tożsamości nie byłoby możliwe uzyskiwanie dostępu do komputerów, aplikacji bądź do danych potrzebnych w codziennej pracy. Chociaż prawdą jest, że minimalne wymagania tożsamości dotyczą użytkowników i komputerów, to zarządzanie zasadami zabezpieczeń pojedynczych użytkowników staje się niepotrzebnie skomplikowane, o ile użytkownicy nie są przypisani do grup. Indywidualne przypisywanie uprawnień setkom użytkowników jest problemem, którego „rozmiary” są trudne do przewidzenia. Natomiast rozsądny podział na grupy czyni proces tworzenia i zarządzania uprawnieniami znacznie prostszym.

System Microsoft Windows Server 2003 ma dwa rodzaje grup, a każdy z nich można podzielić na trzy różne zakresy. Zrozumienie konstrukcji tych grup w granicach prawidłowego zakresu umożliwia lepsze wykorzystanie zasobów administracyjnych podczas ich tworzenia, przydzielania czy zarządzania dostępem. Możliwości konstrukcji grup zależą od tego czy domena bądź las, w którym grupy zostały utworzone, działa w mieszanym, tymczasowym lub macierzystym poziomie funkcjonalności domeny systemu Windows Server 2003. System Windows Server 2003 jest wyposażony w szereg wbudowanych grup. Oprócz tego, użytkownik zgodnie ze swoimi potrzebami, może stworzyć dowolną ilość grup.

Lekcje rozdziału:

- Lekcja 1: Omówienie rodzajów grup i ich zakresów 123
- Lekcja 2: Zarządzanie kontami grup..... 129
- Lekcja 3: Automatyzacja zarządzania kontami grup 133

Wymagania

W celu przeprowadzenia ćwiczeń zamieszczonych w rozdziale potrzebny będzie:

- Komputer nazwany Servcr01 i działający pod kontrolą systemu Windows Server 2003.
- Serwer Server01 powinien być kontrolerem domeny w domenie contoso.com.

Lekcja 1: Omówienie rodzajów grup i ich zakresów

Grupy są kontenerami zawierającymi obiekty użytkowników i komputerów. Obiekty te są członkami grup. Jeśli w liście kontroli dostępu (ACL) zasobu określone zostały uprawnienia dla grupy, wszyscy członkowie danej grupy otrzymują te uprawnienia.

System Windows Server 2003 został wyposażony w dwa rodzaje grup: zabezpieczeń i dystrybucyjne. *Grupy zabezpieczeń* są używane do przypisywania uprawnień określających dostęp do zasobów sieci. *Grupy dystrybucyjne* są wykorzystywane do łączenia użytkowników w celu utworzenia dystrybucyjnych list poczty elektronicznej. Grupy zabezpieczeń mogą być używane jako grupy dystrybucyjne, natomiast sytuacja odwrotna nie jest możliwa. Prawidłowe zaplanowanie struktury grup wpływa na zarządzanie i możliwości skalowania, w szczególności w środowisku przedsiębiorstwa, w którym zainstalowanych zostało wiele domen.



Wskazówka Pomimo, że ustawienia dla pojedynczych podmiotów zabezpieczeń (użytkownicy i komputery) mogą być określone przez listę ACL, ustawienia takie są raczej rozszerzeniem możliwości niż zalecaną regułą administrowania. Jeśli na przykład liczba wyjątków list ACL jest nietypowo długa, członkostwo tej grupy powinno być ponownie przeanalizowane.

Materiały omówione podczas lekcji pozwalają na

- Rozpoznawanie typu grupy i prawidłowe ich wykorzystanie
- Rozpoznawanie trzech zakresów grupy i prawidłowe ich wykorzystanie
- Omówienie różnic pomiędzy grupami a tożsamościami specjalnymi

Szacunkowy czas lekcji: 15 minut

Poziomy funkcjonalności domeny

W systemie Windows Server 2003 dostępne są cztery poziomy funkcjonalności domeny: mieszany systemu Windows 2000 (domyślny), macierzysty systemu Windows 2000, tymczasowy systemu Windows Server 2003 oraz poziom systemu Windows Server 2003.

- **Mieszany Windows 2000** Służy do obsługi kontrolerów domen systemów Windows NT 4, Windows 2000 oraz Windows Server 2003
- **Macierzysty Windows 2000** Służy do obsługi kontrolerów domen systemów Windows 2000 oraz Windows Server 2003
- **Tymczasowy Windows Server 2003** Służy do obsługi kontrolerów domen systemów Windows NT 4 oraz Windows Server 2003
- **Poziom systemu Windows Server 2003** Służy do obsługi kontrolerów domen systemu Windows Server 2003

Ograniczenia właściwości grup omawiane w niniejszej książce dotyczą tych czterech poziomów funkcjonalności domeny.

Zakresy grupy

Zakres grupy określa sposób przypisania uprawnień członkom grupy. *Grupy systemu* Windows Server 2003, zarówno zabezpieczeń, jak i dystrybucyjne, podzielone zostały na cztery zakresy: domeny, lokalny, globalny oraz uniwersalny.



Informacja Choć grupy lokalne nie są traktowane jako część zakresu grup systemu Windows Server 2003, zostały dołączone dla uzupełnienia.

Grupy lokalne

Grupy lokalne (lub grupy lokalne komputera) są głównie używane dla zapewnienia kompatybilności z systemem Windows NT 4. Istnieją użytkownicy i grupy lokalne na komputerach działających pod kontrolą systemu Windows Server 2003, które są skonfigurowane jako serwery członkowskie. Kontrolery domen nie wykorzystują grup lokalnych.

- Grupy lokalne mogą zawierać członków dowolnej domeny lasu, członków zaufanej domeny innych lasów oraz członków zaufanych domen niskiego poziomu.
- Zakres grupy lokalnej dotyczy przydzielania zasobów tylko tego komputera, na którym dana grupa istnieje.

Lokalne grupy domeny

Lokalne grupy domeny są głównie używane do przypisywania dla grup globalnych uprawnień umożliwiających dostęp do lokalnych zasobów domeny. Lokalne grupy domeny:

- Istnieją we wszystkich domenach i lasach o mieszanym, tymczasowym bądź macierzystym poziomie funkcjonalności.
- W całej domenie są dostępne tylko dla domen o macierzystym poziomie funkcjonalności systemu Windows 2000 lub dla domen o poziomie systemu Windows Server 2003. Lokalne grupy domeny funkcjonują na kontrolerze domeny jako grupa lokalna, o ile domena ma mieszany poziom funkcjonalności.
- Mogą zawierać członków dowolnej domeny lasu, członków zaufanych domen innych lasów oraz członków zaufanych domen niskiego poziomu.
- Mają zakres obejmujący całą domenę dla domen o następujących poziomach funkcjonalności: Windows 2000 macierzysty lub Windows Server 2003. Mogą być także używane do przydzielania uprawnień do zasobów na dowolnym komputerze systemu Windows Server 2003, który znajduje się wewnątrz, a nie poza domeną, w której istnieje dana grupa.

Grupy globalne

Grupy globalne są głównie używane do udoskonalania klasyfikowanego członkostwa w lokalnych grupach domeny dla pojedynczych podmiotów zabezpieczeń lub dla bezpośredniego przypisania uprawnień (w szczególności dla domen o mieszanym bądź tymczasowym poziomie funkcjonalności). Grupy globalne są często używane do gromadzenia użytkowników lub komputerów tej samej domeny i współdzielących takie same zadania, role bądź funkcje. Grupy globalne:

- Istnieją we wszystkich domenach i lasach o mieszanym, tymczasowym bądź macierzystym poziomie funkcjonalności.
- Mogą mieć członków, którzy znajdują się w tej samej domenie.
- Mogą być członkiem lokalnej grupy komputera lub domeny.
- Mogą mieć uprawnienia w dowolnej domenie (wliczając w to zaufane domeny innych lasów i domeny systemów wcześniejszych niż Windows 2003)
- Mogą zawierać inne grupy globalne (tylko dla macierzystego poziomu funkcjonalnego domeny systemu Windows 2000 lub dla poziomu funkcjonalnego domeny systemu Windows Server 2003)

Grupy uniwersalne

Grupy uniwersalne są głównie używane do przydzielania dostępu do zasobów wszystkich zaufanych domen, przy czym grupy uniwersalne mogą być jedynie używane jako podmioty zabezpieczeń (typ grupy zabezpieczeń) tylko dla macierzystego poziomu funkcjonalnego domeny systemu Windows 2000 lub dla poziomu funkcjonalnego domeny systemu Windows Server 2003

- Grupy uniwersalne mogą mieć członków w dowolnej domenie lasu.
- Dla macierzystego poziomu funkcjonalności domeny systemu Windows 2000 lub dla poziomu funkcjonalnego domeny systemu Windows Server 2003, grupy uniwersalne mogą mieć uprawnienia dowolnej domeny, wliczając w to zaufane domeny innych lasów.



Wskazówka Grupy uniwersalne mogą być pomocne przy przedstawianiu i konsolidacji grup, które obejmują kilka domen oraz przy wykonywaniu wspólnych zadań w obrębie przedsiębiorstwa. Przydatną wskazówką może być wyznaczenie rzadko zmieniających się grup używanych w dużym zakresie, jako grup uniwersalnych.

Konwersja grupy

Zakres grupy jest określany w momencie jej tworzenia. Jednakże, dla macierzystego poziomu funkcjonalnego domeny systemu Windows 2000 lub dla poziomu funkcjonalnego domeny systemu Windows Server 2003, lokalne lub globalne grupy domeny mogą zostać przekształcone w grupy uniwersalne, pod warunkiem, że grupy te nie są członkami innych grup tego samego zakresu. Przykładowo, grupa globalna, która jest członkiem innej grupy globalnej, nie może być przekształcona w grupę uniwersalną. Tabela 4-1 jest podsumowaniem wykorzystania grup domeny systemu Windows Server 2003, jako podmiotów zabezpieczeń (typ: grupy zabezpieczeń).

Tabela 4-1. Zakres grupy i dozwolone obiekty

Zakres grupy	Dozwolone obiekty
Macierzysty poziom funkcjonalności domeny systemu Windows 2000 lub poziom funkcjonalności domeny systemu Windows Server 2003	
Domain Local (lokalny domeny)	Konta komputerów, użytkownicy, grupy globalne oraz grupy uniwersalne dowolnej domeny lub zaufanych domen. Grupy lokalne domeny (tej samej domeny). Zagnieżdżone grupy lokalne domeny (tej samej domeny).

ciąg dalszy na następnej stronie

ciąg dalszy ze strony poprzedniej

Zakres grup	Dozwolone obiekty
Global (globalny)	Użytkownicy, komputery i grupy globalne tej samej domeny. Zagnieżdżone grupy globalne (tej samej domeny), zagnieżdżone grupy lokalne domeny lub zagnieżdżone grupy uniwersalne.
Universal (uniwersalny)	Grupy uniwersalne, grupy globalne, użytkownicy i komputery dowolnej domeny lasu. Zagnieżdżone grupy globalne, zagnieżdżone grupy lokalne domeny lub zagnieżdżone grupy uniwersalne.
Mieszany poziom funkcjonalności domeny systemu Windows 2000 lub tymczasowy poziom funkcjonalności domeny systemu Windows Server 2003	
Domain Local (lokalny)	Konta komputerów, użytkownicy lub grupy globalne
domeny) Global	dowolnej domeny.
(globalny)	Nie mogą być zagnieżdżane.
	Jedynie komputery i użytkownicy tej samej domeny. Nie mogą być zagnieżdżane.
	Niedostępne.
Universal (uniwersalny)	

Tożsamości specjalne

Istnieją również specjalne grupy nazwane *tożsamościami specjalnymi*, które są obsługiwane przez system operacyjny. Tożsamości specjalne nie mogą być tworzone lub usuwane. Administratorzy nie mogą również modyfikować członkostwa tych grup. Tożsamości specjalne nie pojawiają się w przystawce Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) ani innych narzędziach służących do zarządzania komputerem, ale uprawnienia mogą być przydzielane poprzez listę ACL. W tabeli 4-2 zamieszczone zostały niektóre tożsamości specjalne systemu Windows Server 2003-

Tabela 4-2. Tożsamości specjalne i reprezentowane przez nich obiekty

Tożsamość	Reprezentowane obiekty
Everyone (Wszyscy)	Reprezentuje wszystkich aktualnych użytkowników sieci, wliczając w to użytkowników Go/coraz użytkowników innych domen. Każdorazowo, kiedy użytkownik loguje się do sieci, jest automatycznie dodawany do grupy <i>Everyone</i> . Reprezentuje użytkowników, którzy aktualnie uzyskali dostęp do danego zasobu za pośrednictwem sieci (w przeciwieństwie do użytkowników, którzy uzyskali dostęp do zasobów logując się lokalnie na komputerze, na którym znajdują się te zasoby). Każdorazowo, kiedy użytkownik uzyskuje dostęp do danego zasobu poprzez sieć, jest automatycznie dodawany do grupy <i>Network</i> .
Network (Sieć)	
Anonymous Logon (Logowanie anonimowe)	Grupa <i>Anonymous Logon</i> dotyczy użytkowników, którzy korzystają z zasobów sieci z pominięciem procesu uwierzytelnienia.

ciąg dalszy na następnej stronie

ciąg dalszy ze strony poprzedniej

Tożsamość	Reprezentowane obiekty
Interactive (Interakcyjni)	Reprezentuje wszystkich użytkowników, którzy są aktualnie zalogowani na danym komputerze i którzy uzyskali dostęp do danego zasobu zlokalizowanego na tym komputerze (w przeciwieństwie do użytkowników, którzy uzyskali dostęp do zasobu za pośrednictwem sieci). Każdorazowo, kiedy użytkownik uzyskuje dostęp do zasobu komputera, na którym się zalogował, automatycznie dodawany jest do grupy <i>Interakcyjni</i> . Grupa <i>Authenticated Users</i> zawiera wszystkich użytkowników, którzy zostali uwierzytelnieni w sieci za pomocą ważnego konta użytkownika. Podczas przydzielania uprawnień, grupę <i>Authenticated Users</i> można używać zamiast grupy <i>Everyone</i> , dzięki czemu zabroniony zostanie anonimowy dostęp do zasobów.
Authenticated Users (Użytkownicy uwierzytelnieni)	
Creator Owner (Twórca właściciel)	Grupa <i>Creator Owner</i> dotyczy użytkowników, którzy utworzyli lub są właścicielami zasobu. Przykładowo, jeśli użytkownik utworzył zasób, ale administrator stał się właścicielem tego zasobu, to administrator stanie się członkiem grupy <i>Creator Owner</i> .
Dialup	Grupa <i>Dialup</i> zawiera użytkowników, którzy połączyli się z siecią za pomocą łącza telefonicznego.



Uwaga Grupom tym mogą być przydzielane uprawnienia dostępu do zasobów sieci, chociaż przydzielając uprawnienia do niektórych grup należy zachować szczególną ostrożność. Członkowie tych grup nie muszą być użytkownikami, którzy zostali uwierzytelnieni w domenie. Na przykład, jeśli grupie *Everyone* (Wszyscy) przydzielone zostały pełne uprawnienia do udostępnionego zasobu, przyłączeni użytkownicy innych domen uzyskają dostęp do tego zasobu.

Zadanie kontrolne: Zmiana typu i zakresu grupy

W zadaniu tym przeprowadzane są ćwiczenia praktyczne dotyczące tworzenia grup i modyfikowania ich zakresu.

Ćwiczenie 1: Tworzenie i modyfikowanie grupy

W ćwiczeniu tym zmieniony zostanie typ grupy i jej zakres.

1. W przystawce *Active Directory Users And Computers* (Użytkownicy i komputery usługi Active Directory) utwórz globalną grupę dystrybucyjną. Grupa ma znajdować się w kontenerze *Users* (Użytkownicy) nazwanym *Agents*.
2. Prawym przyciskiem myszy kliknij grupę **Agents**, a następnie wybierz polecenie **Properties** (Właściwości).

Czy można zmieniać zakres i typ grupy? Jeśli nie, dlaczego nie jest to możliwe?

Jeśli nie można zmieniać typu i zakresu grupy, domena, w której wykonywane są operacje jest wciąż domeną mieszanego lub tymczasowego poziomu funkcjonalności systemu Windows Server 2003. Aby zmieniać typ lub zakres grupy, należy zwiększyć poziom funkcjonalności domeny do poziomu

macierzystego domeny systemu Windows 2000 lub do poziomu domeny systemu Windows Server 2003.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Który typ grupy domeny jest najbardziej podobny do grupy lokalnej na serwerze członkowskim! Jakie są podobieństwa tych grup?
2. Jeśli w domenie lub lesie używane są grupy uniwersalne i dla członków tej grupy zachodzi potrzeba uzyskiwania dostępu w oparciu o uprawnienia, jakie muszą być spełnione wymagania odnośnie konfiguracji grupy uniwersalnej?
3. Które podmioty zabezpieczeń mogą być członkiem grupy globalnej w domenie o poziomie funkcjonalności domeny systemu Windows Server 2003?

Podsumowanie lekcji

- Istnieją dwa typy grup: grupa zabezpieczeń i grupa dystrybucji. Grupom zabezpieczeń mogą być przypisywane uprawnienia, natomiast grupy dystrybucyjne używane są w kontenerach kwerend, takich jak pocztowe grupy dystrybucyjne i do tych grup nie mogą być przydzielane uprawnienia do zasobów.
- Uprawnienia zabezpieczeń grup są przydzielane poprzez listę ACL, podobnie jak dla innych podmiotów zabezpieczeń, takich jak użytkownik lub komputer.
- Dla macierzystego poziomu funkcjonalności domeny systemu Windows 2000 lub dla pozioma funkcjonalności domeny systemu Windows Server 2003, grupy zabezpieczeń i dystrybucyjne mogą być zbudowane jako domeny lokalne, globalne lub uniwersalne, a każda dla innego zakresu umieszczanych w grupie podmiotów zabezpieczeń.

Lekcja 2: Zarządzanie kontami grup

Przystawka konsoli MMC - *Active Directory Users And Computers* (Użytkownicy i komputery usługi Active Directory) jest podstawowym narzędziem administrowania podmiotami zabezpieczeń domeny, czyli użytkownikami oraz komputerami. Podczas tworzenia grup określany jest zakres, typ oraz członkostwo grupy. Przystawkę *Active Directory UsersAnd Computers* można również stosować do modyfikowania członkostwa istniejących grup.

Materiały omówione podczas lekcji pozwalają na

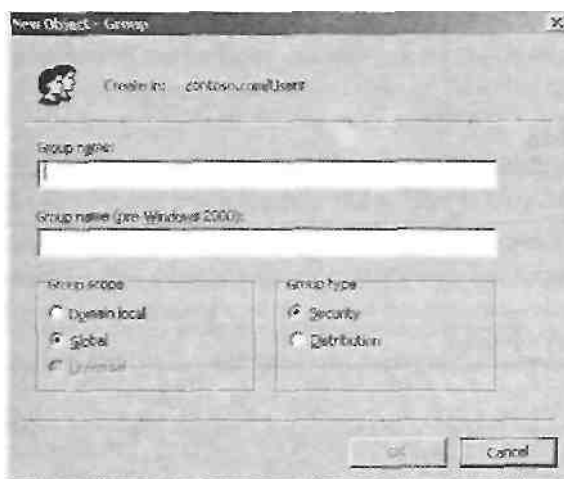
- Tworzenie grup
- Modyfikowanie członkostwa grup
- Wyszukiwanie grup domeny, do których należy dany użytkownik

Szacunkowy czas lekcji: 10 minut

Tworzenie grupy zabezpieczeń

Przystawka *Active Directory Users And Computers* jest narzędziem najczęściej używanym do tworzenia grup. Przystawka znajduje się w folderze *Administrative Tools* (Narzędzia administracyjne). W oknie szczegółów przystawki należy prawym przyciskiem myszy kliknąć kontener, w którym ma być utworzona grupa i z menu wybrać polecenie **New, Group** (Nowy, Grupa). Następnie dla tworzonej grupy należy wybrać zakres i typ.

Podstawowym typem grupy, która prawdopodobnie będzie tworzona, jest grupa zabezpieczeń, ponieważ ten typ grupy jest używany do określania uprawnień w liście ACL. Dla mieszanego i tymczasowego poziomu funkcjonalnego domeny można jedynie określić grupę zabezpieczeń dla zakresu domeny lokalnej lub globalnej. Rysunek 4-1 ilustruje, że nie można tworzyć grupy zabezpieczeń, która ma uniwersalny zakres w przypadku mieszanego lub tymczasowego poziomu funkcjonalności domeny.

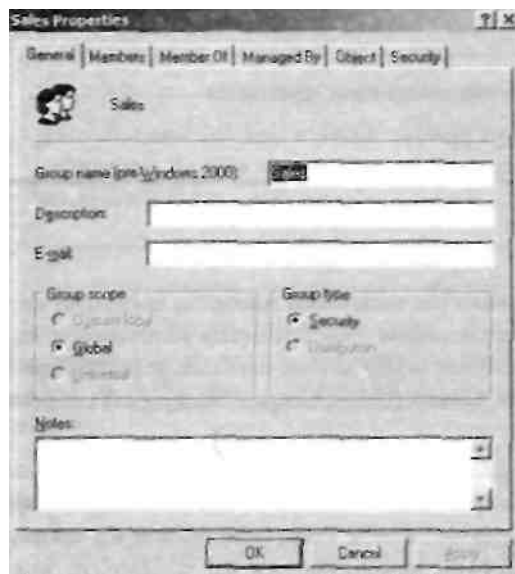


Rysunek 4-1. Grupy zabezpieczeń mieszanego lub tymczasowego poziomu funkcjonalności domeny

W przypadku mieszanego lub tymczasowego poziomu funkcjonalności domeny, grupy lokalne, globalne i uniwersalne mogą być jednak utworzone jako grupy dystrybucyjne. Dla mieszanego lub tymczasowego poziomu funkcjonalności domeny, grupy dystrybucyjne mogą być tworzone dla dowolnego zakresu.

Modyfikowanie członkostwa grup

Dodawanie lub usuwanie członków grupy jest również realizowane za pomocą przystawki *Active Directory Users And Computers*. Prawym przyciskiem myszy należy kliknąć dowolną grupę i wybrać polecenie **Properties** (Właściwości). Rysunek 4-2 przedstawia okno dialogowe *Properties* (Właściwości) dla globalnej grupy zabezpieczeń nazwanej Sales.



Rysunek 4-2. Strona *Properties* (Właściwości) grupy zabezpieczeń nazwanej *Sales*

W tabeli 4-3 zostały wyjaśnione zakładki dotyczące konfiguracji członkostwa, umieszczone w oknie dialogowym *Properties* (Właściwości).

Tabela 4-3. Konfiguracja członkostwa

Zakładka	Funkcja
Members (Członkowie)	Dodawanie, usuwanie lub tworzenie listy podmiotów zabezpieczeń, które są przechowywane w tym kontenerze, jako jego członkowie.
Member Of (Członek grupy)	Dodawanie, usuwanie lub tworzenie listy kontenerów, które przechowują dany kontener.



Zobacz także Dodatkowe informacje, dotyczące używania narzędzi wiersza poleceń usługi katalogowej służących przeglądaniu i modyfikowaniu członkostwa grupy, można znaleźć w rozdziale 3, „Konta użytkowników”. Narzędzia te to polecenia DSQUERY, DSGET, DSMOD, oraz DSGROUP. Polecenie DSGET jest szczególnie przydatne przy tworzeniu listy wszystkich grup, do których należy dany użytkownik.

Wyszukiwanie grup domeny, do których należy dany użytkownik

Usługa Active Directory umożliwia elastyczne i pomysłowe zagnieżdżanie grup, przy czym:

- Grupy globalne mogą być zagnieżdżane w innych grupach globalnych, uniwersalnych lub lokalnych grupach domeny.
- Grupy uniwersalne mogą być członkami innych grup uniwersalnych lub lokalnych grup domeny.
- Lokalne grupy domeny mogą należeć do innych lokalnych grup domeny.

Elastyczność zagnieżdżania grup jest potencjalnym źródłem złożoności i bez odpowiednich narzędzi byłoby bardzo trudno dokładnie określić, do których grup należy użytkownik, czy należy bezpośrednio lub pośrednio. Na szczęście, system Windows Server 2003 został wyposażony w polecenie DSGET, za pomocą którego można rozwiązywać takie problemy. W wierszu poleceń należy wpisać:

```
dsget uset UserDN -memberof [-expand]
```

Przełącznik -memberof zwraca wartość atrybutu MemberOf pokazując, do których grup użytkownik należy bezpośrednio. Poprzez dodanie przełącznika -expand, grupy te będą przeszukiwane rekurencyjnie, co utworzy pełną listę wszystkich grup, do których należy dany użytkownik domeny.

Zadanie kontrolne: Modyfikowanie członkostwa grupy

W zadaniu tym omawiane będą członkostwa grupy oraz zagnieżdżanie grup pod kątem rozpoznawania, które kombinacje członkostwa grup są możliwe.

Ćwiczenie 1: Zagnieżdżone członkostwo grupy

1. Jeśli poziom funkcjonalności domeny jest inny niż dla systemu Windows Server 2003, należy za pomocą przystawki *Active Directory UsersAnd Computers* podnieść go do poziomu funkcjonalności domeny systemu Windows Server 2003.
2. Utwórz trzy grupy globalne w jednostce organizacyjnej Users: Group 1, Group 2 i Group 3.
3. Utwórz trzy konta użytkowników: User 1, User 2 i User 3.
4. Skonfiguruj tak, aby konta User 1, User 2 i User 3 były członkami grupy Group 1.
5. Skonfiguruj tak, aby grupa Group 1 była członkiem grupy Group 2.

Które grupy można teraz przekształcić w grupę uniwersalną? Sprawdź swoją teorię (dla dwóch grup spośród trzech przekształcenie takie powinno być możliwe).

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiały lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Która zakładka w oknie właściwości grupy jest używana do dodawania użytkowników do grupy?

2. Wewnątrz grupy Sales należy zagnieździć grupę IT Administrators, odpowiedzialną za grupę Sales tak, aby jej członkowie mieli dostęp do tych samych zasobów (określonych przez uprawnienia listy ACL). Którą zakładką na stronie Properties (Właściwości) grupy IT Administrators należy się posłużyć, aby określić te ustawienia?

- 3- Pewne środowisko składa się z dwóch domen: jednej domeny systemu Windows Server 2003 oraz jednej domeny systemu Windows NT 4. Jakim zakresem grupy należy się posłużyć do przydzielania uprawnień do dowolnych zasobów umieszczonych na komputerze w dowolnej domenie?

Podsumowanie lekcji

- Modyfikowanie członkostwa grupy jest realizowane za pomocą konsoli Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory).
- Określenie członkostwa w grupie dla podmiotów zabezpieczeń jest realizowane za pomocą zakładki Members Of (Członek grupy) znajdującej się na zakładce Security (Zabezpieczenia) we właściwościach podmiotu zabezpieczeń. Określanie członków kontenera (grupy) jest realizowane za pomocą zakładki Members (Członkowie).
- Grupy mogą być zagnieżdżane, jeśli domena, w której grupy są umieszczone, ma macierzysty poziom funkcjonalności domeny systemu Windows 2000 lub poziom funkcjonalności domeny systemu Windows Server 2003- Dla mieszanego lub tymczasowego poziomu funkcjonalności domeny (obsługa kontrolerów domeny systemu Windows NT 4) nie jest możliwe zagnieżdżanie grup.
- Zmiana typu i zakresu grupy jest możliwa tylko, jeśli domena ma macierzysty poziom funkcjonalności domeny systemu Windows 2000 lub poziom funkcjonalności domeny systemu Windows Server 2003.

Lekcja 3: Automatyzacja zarządzania kontami grup

Konsola Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) jest wygodnym narzędziem tworzenia i modyfikowania pojedynczych grup, nie jest natomiast najbardziej wydajną metodą tworzenia dużej liczby podmiotów zabezpieczeń. I dlatego system Windows Server 2003 został wyposażony w program Ldifde.exe, który ułatwia importowanie bądź eksportowanie dużej liczby podmiotów zabezpieczeń, wliczając w to grupy.

Materiały omówione podczas lekcji pozwalają na

- Import podmiotów zabezpieczeń za pomocą programu LDIFDE
- Eksport podmiotów zabezpieczeń za pomocą programu LDIFDE
- Tworzenie i modyfikowanie grup za pomocą poleceń DSADD i DSMOD

Szacunkowy czas lekcji: 30 minut

Korzystanie z programu LDIFDE

Format LDIF (Data Interchange Format) protokołu LDAP (Lightweight Directory Access Protocol) jest pierwszą wersją standardu sieci Internet dla formatu plików, które mogą być używane do przeprowadzania operacji wsadowych w usłudze katalogowej podporządkowanej standardom protokołu LDAP. Format LDIF może być stosowany do eksportu i importu danych przy przetwarzaniu wsadowym dla operacji usługi Active Directory, takich jak dodawanie i modyfikowanie. Program narzędziowy nazwany LDIFDE został dołączony do systemu Windows Server 2003 dla obsługi operacji wsadowych bazujących na standardzie formatu plików LDIF.

Program narzędziowy wiersza poleceń LDIFDE został dołączony do wszystkich wersji systemu Windows Server 2003. Program LDIFDE można uruchamiać stosując odpowiednie przełączniki w oknie wiersza poleceń lub powłoce polecenia. Na rysunku 4-3 przedstawione zostały główne polecenia programu wyświetlone za pomocą wprowadzonego w wierszu polecenia **Ldifde /?**



Rysunek 4-3. *Plik pomocy programu wiersza poleceń LDIFDE*

Tabela 4-4 zawiera listę głównych poleceń programu LDIFDE.

Tabela 4-4. Polecenia programu LDIFDE (główne)

Polecenie	Wykorzystanie
Parametry główne	
-i	Załącza rryb importu (domyślnym trybem jest eksport)
-f filename (nazwa_pliku)	Nazwa pliku wejściowego lub wyjściowego
-s servername (nazwa_serwera)	Serwer do powiązania
-c FromDN ToDN	Zamiana wystąpień FromDN na ToDN
-v	Włącza tryb pełnej informacji
-j path (ścieżka)	Lokalizacja pliku dziennika
-t port	Numer portu (domyślnie 389)
->	Pomoc
Określone parametry eksportu	
-d RootDN	Katalog główny wyszukiwania LDAP (domyślnie kontekst nazw)
-r Filier (filtr)	Filtr wyszukiwania LDAP(domyślnie „(objectClass=*)”)
-p SearchScope (zakres wyszukiwania)	Zakres wyszukiwania (Base/OneLevel/Subtrce)
-l list (lista)	Lista atrybutów (rozdzielane przecinkami), które będą przeglądane w procesie wyszukiwania LDAP
-o list (lista)	Lista atrybutów (rozdzielane przecinkami), które trzeba pominąć w informacjach wejściowych
"g	Wyłącza wyszukiwanie stronicowane

ciąg dalszy ze strony poprzedniej

Polecenie	Wykorzystanie
-m	Dla eksportu włącza logikę menedżera SAM (Security Accounts Manager)
-n	Nie eksportuje wartości binarnych
Określone parametry importu	
-k	Funkcja importu zignoruje błędy „Constraint Violation” (naruszenie więzów) oraz „Object Already Exists” (obiekt już istnieje)
Parametry poświadczeń	
-a UserDN	Polecenie zostanie uruchomione przy użyciu wyspecyfikowanej nazwy wyróżniającej użytkownika i hasła. Na przykład: „cn=adminstrator,dc=contoso,dc=com password”
-b UserName Domain (nazwa_użytkownika domena)	Polecenie zostanie uruchomione dla parametrów nazwa_użytkownika, domena, hasło. Ustawienia domyślne określają, że polecenie zostanie uruchomione dla poświadczeń dotyczących aktualnie zalogowanego użytkownika.



Informacja Program narzędziowy LDIFDE dołączony do systemu Windows Server 2003 może zostać skopiowany do systemu Windows 2000 Professional lub Windows XP, a następnie powiązany i używany zdalnie w usłudze Active Directory systemu Windows Server 2003.



W praktyce Tworzenie konta

Często zdarza się, że dysponujemy danymi, których duża część będzie publikowana w usłudze katalogowej systemu Windows Server 2003. Dane te mogą być przechowywane w domenach niskiego poziomu (Windows NT 4, Windows 2000, Novell Directory Services (NDS) lub w innego typu bazach danych (działy kadr są znane z opracowywania takich danych).

Jeśli te dane o użytkownikach są dostępne, można je wykorzystać do umieszczenia „hurtem” w usłudze Active Directory. Jest wiele narzędzi, które ułatwiają uzyskiwanie danych, na przykład Addusers w systemie Windows NT 4 czy LDIFDE w systemie Windows 2000.

Oprócz tego, większość programów baz danych ma wbudowane funkcje eksportu rekordów do plików o wartościach rozdzielanych przecinkami (CSV). Program LDIFDE może importować dane na podstawie takiego pliku. W przypadku plików CSV należy zaznaczyć, że nie można utworzyć obiektu bez niektórych elementów i jeśli w pliku brakuje wymaganego elementu, podczas importu pojawiają się błędy.

ciąg dalszy na następnej stronie

ciąg dalszy ze strony poprzedniej

Tworzenie grup wymaga co prawda tylko dwóch elementów: nazwy wyróżniającej (CN=User) oraz lokalizacji (DC=Domain, DC=OU), które to elementy prawdopodobnie nie zostaną pominięte.

Po niewielkiej edycji, dane o jednostce organizacyjnej i grupach można dodać do pliku importu, a następnie za pomocą programu LDIFDE znacznie szybciej zbudować usługę Active Directory.

Tworzenie grup za pomocą polecenia DSADD

Polecenie DSADD omawiane w rozdziale 2 jest używane do tworzenia obiektów w usłudze Active Directory. Aby dodać obiekt, należy zastosować następującą składnię polecenia:

dsadd group GroupDN...

Parametr *GroupDN...* jest jedną lub kilkoma nazwami wyróżniającymi nowego obiektu grupy. Jest i nazwa DN zawiera spacje, całą nazwę DN należy objąć znakami cudzysłowu. Parametr *GroupDN...* może być wprowadzany za pomocą jednej z poniżej wymienionych metod:

- Poprzez wprowadzenie listy nazw DN za pośrednictwem innego polecenia takiego jak dsquery.
- Poprzez wpisanie w wierszu poleceń każdej nazwy DN oddzielonej znakami spacji.
- Poprzez pozostawienie pustego parametru nazwy DN. W tym momencie z klawiatury konsoli można wpisywać w wierszu poleceń pojedyncze nazwy DN. Po każdej nazwie DN należy nacisnąć ENTER, a po ostatniej nazwie DN należy nacisnąć CTRL+Z.

W poleceniu DSADD GROUP, po parametrze DN można używać następujących parametrów opcjonalnych:

-secgrp {yes | no} określa czy grupa jest grupą zabezpieczeń (yes) lub grupą dystrybucyjną (no). Wartość domyślna parametru — yes.

-scope {1 g | u} określa czy grupa jest lokalną grupą domeny (1), grupą globalną (g, wartość domyślna) lub grupą uniwersalną (u). -

saraid SAMName (nazwa SAM) -

desc Description (opis)

-memberof GroupDN... określa grupy, do których nowa grupa ma zostać dodana. -

members MemberDN... określa członków nowotworzonej grupy.

Zgodnie z opisem zamieszczonym w rozdziale 3, można dodawać parametry -s, -u oraz -p określają, kontroler domeny, z którym związane jest wykonywanie rozkazu DSADD, a nazwa użytkownika i hasło, czyli poświadczenia, będą używane do wykonania polecenia.

{-s Server | -d Domain} -

u UserName -p

{Password | *}

Modyfikowanie grup za pomocą polecenia DSMOD

Polecenie DSMOD, omawiane w rozdziale 2, jest używane do modyfikowania obiektów usługi Active Directory. Aby zmodyfikować obiekt, należy użyć następującej składni:

dsmod group GroupDN...

W omawianym poleceniu można stosować wiele takich samych przełączników, co w poleceniu DSADD, wliczając w to — samid, -desc, -secgrp oraz -scope. Dla istniejących grup, najczęściej nie zachodzi potrzeba modyfikowania tych atrybutów. Natomiast najbardziej przydatnymi przełącznikami są przełączniki umożliwiające zmianę członkostwa grupy, a w szczególności:

-addmbr Member... dodaje członków do grupy, która została wyspecyfikowana w parametrze Group
-rmmbr Member... usuwa członków grupy, która została wyspecyfikowana w parametrze Group
 gdzie, tak jak we wszystkich poleceniach usługi katalogowej, nazwa DN jest pełną nazwą wyróżniającą innego obiektu usługi Active Directory, objętą znakami cudzysłowu, jeśli nazwa DN zawiera spacje.



Uwaga W dowolnym wierszu poleceń można użyć tylko jednego przełącznika -addmbr lub -rmmbr. Obu przełączników nie można stosować jednocześnie w pojedynczym poleceniu DSMOD GROUP.

Zadanie kontrolne: Wykorzystanie programu LDIFDE do zarządzania kontami grup

W poniższych ćwiczeniach pokazane zostanie, w jaki sposób wyświetlić opcje dostępne w poleceniu LDIFDE, jak wyeksportować użytkowników usługi Active Directory oraz jak w katalogu utworzyć obiekt grupy.

Ćwiczenie 1: Uruchomienie programu LDIFDE

W ćwiczeniu tym wyświetlone zostaną opcje dostępne w poleceniu LDIFDE.

1. Otwórz okno Command Prompt (Wiersz polecenia)
2. Aby wyświetlić listę poleceń, wpisz w wierszu poleceń polecenie: **ldifde /?**.

Ćwiczenie 2: Eksport użytkowników z jednostki organizacyjnej

W ćwiczeniu tym przeprowadzony zostanie eksport całej zawartości (wszyscy użytkownicy) jednostki organizacyjnej nazwanej Marketing, znajdującej się w domenie contoso.com.

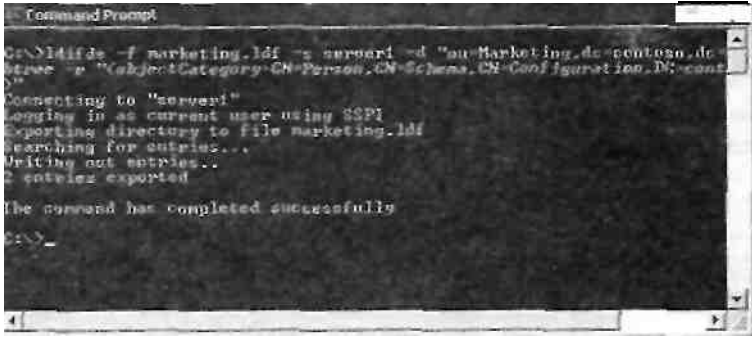
1. W domenie contoso.com (serwer Server01 jest kontrolerem domeny contoso.com) utwórz jednostkę organizacyjną Marketing.
2. W jednostce organizacyjnej Marketing utwórz dwóch lub trzech użytkowników. Nazwy użytkowników mogą być wybrane dowolnie.
3. Otwórz okno wiersza poleceń i wpisz następujące polecenie programu LDIFDE (znak dwukropka : oznacza kontynuację w następnej linii):

```
ldifde -f marketing.ldf -s server01 :
-d "ou=Marketing,dc=contoso,dc=com" :
-p subtree -r :
```


"(objectCategory=CN=Person.CN=Schema,CN=Configuration.:
DOcontoso.DC=com)"

Rysunek 4-4 przedstawia komunikaty wyświetlane po uruchomieniu polecenia.

PoT3fl



```
Command Prompt
C:\>ldifde -f marketing.ldf -s server1 -d "ou=Marketing,dc=contoso,dc=com" -p "(objectCategory=CN=Person.CN=Schema,CN=Configuration,DC=contoso,DC=com)"
Connecting to "server1"
Logging in as current user using SSPI
Exporting directory to file marketing.ldf
Searching for entries...
Writing out entries...
2 entries exported
The command has completed successfully
C:\>
```

Rysunek 4-4. Komunikaty wyświetlone po wykonaniu polecenia programu LDIFDE dotyczącej eksportu jednostki organizacyjnej Marketing

Polecenie tworzy plik formatu LDIF nazwany Marketing.ldf poprzez połączenie się z serwerem Server01 i przejście poddrzewa jednostki organizacyjnej Marketing OU w celu wyszukania wszystkich obiektów kategorii Person (osoba)

Ćwiczenie 3: Tworzenie grup za pomocą polecenia LDIFDE

W ćwiczeniu tym polecenie LDIFDE będzie używane do tworzenia jednostki organizacyjnej contoso.com.

1. Uruchom edytor tekstowy, jak na przykład Notatnik i utwórz plik tekstowy nazwany Newgroup.ldf" (Plik należy zapisać jako plik LDIF, a nie jako plik tekstowy).
2. Przeprowadź edycję pliku Newgroup.ldf i dodaj następujący tekst:
dn: CN=Management,OU=Marketing,DC=contoso.DC=com
changetype: add en: Management objectClass:
group samAccountName: Marketing
- 3- Zapisz i zamknij plik LDIF.
4. Otwórz okno wiersza poleceń, wpisz poniższe polecenie i naciśnij ENTER:
ldifde -i -f newgroup.ldf -s server01



Wskazówka Należy zwrócić uwagę na dodatkowe znaki niewidoczne (tabulacje, spacje, znaki CR i LR umieszczone w pliku. Znaki te spowodują nieprawidłowe działanie polecenia,

5. Za pomocą przystawki Active Directory Users And Computers (Użytkownicy i komputery ushij Active Directory) sprawdź, czy nowa grupa została utworzona.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Które z poniżej wymienionych poleceń programu LDIFDE zmienia jego działanie z funkcji eksportowania na funkcję importowania?
 - a. -i
 - b. -t
 - c. -f
 - d. -s
2. Które klasy obiektów można eksportować lub importować za pomocą programu LDIFDE?
3. W bazie danych użytkowników istnieje możliwość eksportowania informacji do pliku CSV. Czy taki plik można wykorzystać do importowania lub też trzeba ręcznie utworzyć plik *.ldf?

Podsumowanie lekcji

- Program LDIFDE jest narzędziem dołączonym do systemu Windows Server 2003, które umożliwia import i eksport danych do/z usługi Active Directory.
- Jeśli dysponujemy istniejącym katalogiem danych użytkownika, program LDIFDE można wykorzystać do eksportu potrzebnych danych, a następnie do zaimportowania ich do usługi Active Directory. Ogólnie mówiąc, jest to bardziej wydajny proces niż ręczne tworzenie pojedynczo każdego elementu. Pliki CSV są przydatne, o ile dane są prawidłowo sformatowane i posiadają wszystkie wymagane elementy ułożone w odpowiedniej kolejności.
- W celu wykorzystania w usłudze Active Directory, program LDIFDE może zostać skopiowany do systemów Windows 2000 lub Windows XP.

Zadanie praktyczne

Administrator uczestniczy w procesie budowania usługi Active Directory i dysponuje niektórymi danymi o użytkownikach, które dostarczył dział kadr. Dane te to imię, nazwisko, adres oraz numer I telefonu. Zasada przedsiębiorstwa stanowi, że nazwa logowania użytkownika powinna być połączeniem imienia lub inicjału oraz nazwiska (na przykład dla użytkownika Ben Smith nazwą logowania może być bsmith),

W przedsiębiorstwie jest 500 użytkowników, 30 grup i 10 jednostek organizacyjnych. W ujęciu praktycznym, jaki jest najlepszy sposób umożliwiający skonfigurowanie usługi Active Directory najprościej i najszybciej jak jest to możliwe?

Chociaż nie istnieje „absolutnie” poprawna odpowiedź, to należy rozważyć różne poziomy złożoności zagadnienia. Połączenie metod jest prawdopodobnie najlepszym rozwiązaniem przy uwzględnieniu następujących rozważań:

- Dane użytkownika mogą być w razie potrzeby edytowane, ale tych czynności jest niewiele, a do usługi Active Directory użytkownicy wprowadzeni będą za pomocą programu LDIFDE.
- Konstrukcja jednostki organizacyjnej może być fragmentem konstrukcji użytkownika, wszystko w oparciu o ten sam plik przy zminimalizowanych czynnościach edycyjnych. Dla jednostek organizacyjnych również używany będzie program LDIFDE.
- Innym zagadnieniem są grupy. Ponieważ członkostwo grupy jest w usłudze Active Directory wielowartościowym atrybutem, musi być wyspecyfikowane indywidualnie dla każdej grupy w momencie jej tworzenia. Przy użyciu pojedynczego pliku zadanie to byłoby skomplikowane, a prawdopodobieństwo popełnienia błędów wzrosłoby znacznie. Lepszym rozwiązaniem jest indywidualne określanie członkostwa grup.

Rozwiązywanie problemów

W usłudze Active Directory tworzenie pojedynczych obiektów (użytkowników, grupy i komputery) jest prostym procesem, natomiast w sytuacji, kiedy istnieje wiele obiektów, wyszukiwanie obiektów i ich skojarzeń może stać się prawdziwym wyzwaniem. W dużym, wielodomenowym środowisku (lub w mniejszym środowisku, lecz o skomplikowanej konstrukcji), rozwiązywanie problemów związanych z dostępem do zasobów może być trudne. Na przykład, jeśli użytkownik Karol może uzyskiwać dostęp do pewnych, ale nie do wszystkich zasobów, które zostały dla niego przewidziane, to prawdopodobnie nie jest członkiem grup, do których przydzielone zostały uprawnienia do tych zasobów.

Jeśli w środowisku istnieje wiele domen, z których każda zawiera wiele jednostek organizacyjnych, a w tych jednostkach znajduje się wiele zagnieżdżonych grup, to przeanalizowanie członkostwa tych grup w celu określenia, czy dany użytkownik jest członkiem odpowiednich grup, jest bardzo czasochłonne. W takiej sytuacji, przystawka Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) nie jest najlepszym narzędziem.

Aby uzyskać pełną listę wszystkich grup, których członkiem jest dany użytkownik, można używać polecenia DSGET. Podczas realizacji tego ćwiczenia używany będzie obiekt użytkownika Ben Smith w domenie contoso.com i jednostka organizacyjna Users.

1. W usłudze Active Directory wybierz użytkownika, dla którego przeprowadzone zostaną opisane poniżej etapy ćwiczenia. Jeśli konstrukcja usługi nie jest odpowiednia, należy utworzyć parę grup zagnieżdżonych w kilku jednostkach organizacyjnych, przy czym użytkownik nie może być członkiem wszystkich grup.
2. Otwórz okno wiersza poleceń.
3. Wpisz poniższe polecenie (zastępując nazwę OU i użytkownika nazwą użytkownika wybranego w punkcie 1):

dsget user „CN=Ben Smith,CN=Users,DC=contoso,DC=com” -memberof -expand

Wyświetlona zostanie pełna lista wszystkich grup, których członkiem jest dany użytkownik.

Podsumowanie rozdziału

- Grupy mogą być tworzone w dowolnej jednostce organizacyjnej usługi Active Directory.
- Istnieją dwa rodzaje grup: grupy zabezpieczeń oraz grupy dystrybucyjne.
- Istnieją trzy zakresy: grupy lokalne domeny, grupy globalne oraz grupy uniwersalne.
- Ręczne tworzenie grup jest realizowane za pomocą przystawki konsoli MMC — Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory).
- Automatyzacja tworzenia grup realizowana jest przy użyciu narzędzia wiersza poleceń LDIFDE.
- Narzędzia usługi katalogowej takie jak DSQUERY, DSGET oraz DSMOD mogą być używane do utworzenia, modyfikowania oraz wygenerowania listy grup i ich członków.
- Typy grup mogą być zmieniane jedynie, jeśli poziom funkcjonalności domeny jest nie mniejszy niż macierzysty poziom funkcjonalności domeny systemu Windows 2000.
- Zaawansowane zagnieżdżanie grup jest możliwe tylko, jeśli poziom funkcjonalności domeny jest nie mniejszy niż macierzysty poziom funkcjonalności domeny systemu Windows 2000.

Informacje dla zdających egzamin

Przed przystąpieniem do egzaminu należy zapoznać się z przedstawionymi poniżej najważniejszymi faktami i pojęciami, aby określić, które tematy wymagają pogłębienia. Należy powrócić do lekcji, aby osiągnąć większą wprawę oraz przejrzeć działy znajdujące się w części 2 - „Materiały dodatkowe”. Informacje tu zawarte, kierują do materiałów uzupełniających tematy objęte zadaniami egzaminacyjnymi.

Najważniejsze fakty

- Typy grup i możliwości ich wykorzystywania zależą od poziomu funkcjonalności domeny
- Zakres grup oraz różne sposoby zagnieżdżania grup zależą od poziomu funkcjonalności domeny
- Podstawowe przeznaczenie przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) to tworzenie grup i modyfikowanie ich członkostwa
- Podstawowe przeznaczenie programu LDIFDE to tworzenie grup oraz eksportowanie grup z jednego katalogu do innego
- Podstawowe przeznaczenie polecenia DSGET to tworzenie pełnej listy członkostwa danego użytkownika

Najważniejsze pojęcia

Lokalne grupy domeny (zakres) Dla mieszanego i tymczasowego poziomu funkcjonalności, grupy lokalne nie są dostępne w całej domenie, ale tylko na kontrolerach domeny.

Grupy globalne (zakres) Grupy te są dostępne w całej domenie przy dowolnym poziomie funkcjonalności.

Grupy uniwersalne (zakres) Grupy te są dostępne w całej domenie przy dowolnym poziomie funkcjonalności, przy czym dla mieszanego poziomu funkcjonalnego domeny systemu Windows 2000 i tymczasowego poziomu funkcjonalności systemu Windows Server 2003 stwierdzenie powyższe dotyczy tylko grup dystrybucyjnych.

Grupy zabezpieczeń (typ) Uprawnienia tych grup mogą być przydzielane w liście ACL.

Grupy dystrybucyjne (typ) Uprawnienia tych grup nie mogą być przydzielane w liście ACL.

Pytania i odpowiedzi

128 Pytania do lekcji 1

1. Który typ grupy domeny jest najbardziej podobny do grupy lokalnej na serwerze członkowskim; Jakie są podobieństwa tych grup?

Lokalne grupy domeny są bardzo podobne do grup lokalnych na serwerze członkowskim w tym, że dla mieszanego lub tymczasowego poziomu funkcjonalności domeny systemu Windows Server 2003 ograniczone są do komputerów, na których zostały umieszczone, natomiast w przypadku lokalnych grup domeny, do kontrolera domeny. Dopóki poziom funkcjonalności domeny nie zostanie podniesiony do macierzystego poziomu domeny systemu Windows 2000 lub do poziomu domeny systemu Windows Server 2003, lokalne grupy domeny nie mogą być używane do przydzielania uprawnień na żadnym serwerze domeny oprócz kontrolerów domeny.

2. Jeśli w domenie lub lesie używane są grupy uniwersalne i dla członków takiej grupy zachodzi potrzeba uzyskiwania dostępu w oparciu o uprawnienia, jakie muszą być spełnione wymagania odnośnie konfiguracji grupy uniwersalnej?

Dla grupy uniwersalnej:

- » Wymagany poziom funkcjonalności domeny to poziom macierzysty dla systemu Windows 2000 lub poziom funkcjonalności domeny systemu Windows Server 2003.
 - » Grupa uniwersalna musi być grupą zabezpieczeń (nie może być grupą dystrybucyjną).
3. Które podmioty zabezpieczeń mogą być członkiem grupy globalnej w domenie o poziomie funkcjonalności domeny systemu Windows Server 2003?
 - » Użytkownicy
 - » Komputery
 - » Grupy uniwersalne
 - » Grupy globalne

132 Pytania do lekcji 2

1. Która zakładka w oknie właściwości grupy jest używana do dodawania użytkowników do grupy?

Zakładka Members (Członkowie) jest używana do dodawania członków do grupy.

2. Wewnątrz grupy Sales należy zagnieździć grupę IT Administrators, odpowiedzialną za grupę Sales tak, aby jej członkowie mieli dostęp do tych samych zasobów (określonych przez uprawnienia listy ACL), co grupa Sales. Którą zakładką na stronie Properties (Właściwości) grupy IT Administrators należy się posłużyć, aby określić te ustawienia?

Zakładka Members Of (Członek grupy) jest używana do dodawania grupy IT Administrators do grupy Sales.

3. Pewne środowisko składa się z dwóch domen: jednej domeny systemu Windows Server 2003 oraz jednej domeny systemu Windows NT 4. Jakim zakresem grupy należy się posłużyć do przydzielania uprawnień do dowolnych zasobów umieszczonych na komputerze w dowolnej domenie?

Dla tymczasowego poziomu funkcjonalności domeny systemu Windows Server 2003, który jest wymagany do obsługi domen systemu Windows NT 4, jako podmioty zabezpieczeń używać można tylko grupy globalne. Lokalne grupy domeny są przydatne jedynie na kontrolerach domen systemu Windows Server 2003, natomiast grupy uniwersalne nie mogą być używane jako grupy zabezpieczeń w domenach o tymczasowym poziomie funkcjonalności domeny systemu Windows Server 2003.

Pytania do lekcji 3

1. Które z wymienionych poniżej poleceń programu LDIFDE zmienia jego działanie z funkcji eksportowania na funkcję importowania?
 - a. -i
 - b. -t
 - c. -f**
 - d. -s**

Prawidłowa odpowiedź to a. Polecenie -i zmienia domyślną funkcję programu LDIFDE z eksportowania na importowanie.
2. Które klasy obiektów można eksportować lub importować za pomocą programu LDIFDE?

Za pomocą programu LDIFDE można wyeksportować lub zaimportować dowolny obiekt usługi Active Directory, wliczając w to użytkowników, grupy, komputery lub jednostki organizacyjne. Oprócz tego, przy użyciu programu LDIFDE można modyfikować dowolne właściwości tych obiektów.
3. W bazie danych użytkowników istnieje możliwość eksportowania informacji do pliku CSV. Gdzie taki plik można wykorzystać do importowania lub też trzeba ręcznie utworzyć plik *.ldf?

Plik CSV może być używany do importowania danych o użytkownikach do usługi Active Directory. Tam, gdzie jest to możliwe, brakujące wartości zostaną zastąpione przez system Windows Server 2003 wartościami domyślnymi, natomiast brak wartości obowiązkowych w pliku podczas importowania powoduje błędy, a obiekt nie zostanie utworzony.

Zadania egzaminacyjne omawiane w tym rozdziale:

- Tworzenie i zarządzanie kontami komputerów w środowisku usługi katalogowej Microsoft Active Directory
- Rozwiązywanie problemów kont komputerów
 - » Diagnostyka i rozwiązywanie zagadnień dotyczących kont komputerów za pomocą przystawki konsoli MMC (Microsoft Management Console) — Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory)
 - » Zerowanie kont komputerów

Cele rozdziału

Każdy administrator sieci zdaje sobie sprawę, że wraz z upływem czasu, w przedsiębiorstwie przybywa sprzętu, komputery ulegają awariom, zmieniają się role i użytkownicy danego komputera, a stary sprzęt jest wyłączany z eksploatacji lub rozbudowywany, co prowadzi do nabywania systemów zastępczych. Wszystkie te czynności wymuszają aktualizacje kont komputerów usługi Active Directory.

Po przeprowadzeniu uwierzytelnienia użytkownika za pomocą nazwy obiektu użytkownika i hasła, komputer obsługuje konto, które ma nazwę oraz hasło służące do utworzenia bezpiecznych relacji pomiędzy komputerem a domeną. Użytkownik może zapomnieć swoje hasło, co powoduje konieczność wyczyszczenia hasła przez administratora lub może być na urlopie, co z kolei wymaga wyłączenia obiektu użytkownika. Podobnie, konto komputera może wymagać zerowania lub wyłączenia.

W niniejszym rozdziale omawiane są sposoby tworzenia obiektów komputera, które zawierają właściwości zabezpieczeń wymaganych, aby obiekt stał się „kontem” oraz sposoby zarządzania tymi obiektami za pomocą graficznego interfejsu użytkownika przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory), jak również za pomocą wydajnych narzędzi wiersza poleceń systemu Microsoft Windows Server 2003. W rozdziale opisany jest również proces łączenia komputera z domeną tak, aby można było rozpoznać potencjalne miejsca awarii i bardziej efektywnie rozwiązywać problemy dotyczące kont komputerów. Na koniec przedstawione będą ćwiczenia służące opanowaniu podstawowych umiejętności wymaganych do rozwiązywania problemów i naprawy kont komputerów.

Lekcje rozdziału:

- Lekcja 1: Dołączanie komputera do domeny 147
- Lekcja 2: Zarządzanie kontami komputerów 157
- Lekcja 3: Rozwiązywanie problemów związanych z kontami komputerów 162

Wymagania

W rozdziale tym przedstawione są umiejętności i pojęcia dotyczące kont komputerów usługi Active Directory. Jeśli student chciałby przeprowadzić ćwiczenia praktyczne w oparciu o prezentowane w rozdziale przykłady i ćwiczenia, powinien przygotować następujące elementy:

- Komputer z zainstalowanym systemem Windows Server 2003 (Standard Edition lub Enterprise Edition). Serwer nazwany powinien być Server01 i skonfigurowany jako kontroler domeny w domenie contoso.com.
- Jednostki organizacyjne pierwszego poziomu to: „Administrative Groups,” „Desktops,” ora „Servers.”
- W jednostce organizacyjnej Administrative Groups powinna znajdować się globalna grupa zabezpieczeń nazwana „Deployment.”
- Konsolę Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) lub niestandardową konsolę MMC zawierającą przystawkę Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory).
- Jedno z ćwiczeń, dołączenie komputera do domeny, jest możliwe tylko wtedy, kiedy dysponujemy dodatkowym komputerem działającym pod kontrolą jednego z systemów: Microsoft Windows 2000 Professional, Windows XP lub Windows Server 2003 i połączonym z serwerem Server01. Serwer Server01 lub inny musi mieć prawidłowo skonfigurowane usługi DNS, a komputer dodatkowy musi być skonfigurowany, by używał właśnie tego serwera DNS, dzięki czemu będzie mógł zlokalizować kontroler domeny (Server01) i domenę contoso.com.

Lekcja 1: Dołączanie komputera do domeny

Domyślna konfiguracja dla systemu Windows Server 2003, a także wszystkich systemów operacyjnych Microsoft Windows określa, że komputer należy do grupy roboczej. W grupie roboczej, komputer bazujący na systemie Windows NT (co dotyczy też systemów Windows NT 4, Windows 2000, Windows XP oraz Windows Server 2003) może uwierzytelniać użytkowników jedynie w oparciu o lokalną bazę danych SAM (Security Accounts Manager). Uwzględniając wszystkie jego zadania i przeznaczenie, jest to system autonomiczny. Jego członkostwo w grupie roboczej odgrywa mniejszą rolę, w szczególności dla usługi przeglądania. Pomimo, że użytkownik może połączyć się z udostępnionym zasobem innego komputera grupy roboczej lub domeny, w rzeczywistości za pomocą konta domeny użytkownik nie jest nigdy zalogowany do komputera.

Zanim możliwe będzie zalogowanie się na komputerze za pomocą konta użytkownika domeny, komputer ten musi należeć do domeny. Dwa kroki wymagane do przyłączenia komputera do domeny to: utworzenie konta komputera oraz skonfigurowanie komputera tak, aby przyłączył się do domeny za pomocą tego konta. Niniejsza lekcja omawia umiejętności dotyczące tworzenia kont komputerów oraz dołączania komputerów do domen. Bardziej szczegółowy opis samych kont komputerów został zamieszczony w następnej lekcji.

Obsługa kont komputerów, podobnie jak dla użytkowników, obejmuje nazwę, hasło i identyfikator zabezpieczeń (SID). Właściwości te są zawarte w klasie obiektu komputera usługi Active Directory. Z tego powodu, przygotowanie komputera, aby stał się częścią domeny, jest procesem bardzo podobnym do przypadku użytkownika: należy utworzyć obiekt komputera w usłudze Active Directory.

Materiały omówione podczas lekcji pozwalają na

- Tworzenie kont komputerów za pomocą konsoli Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory)
- Tworzenie kont komputerów za pomocą programu narzędziowego wiersza poleceń DSADD
- Tworzenie kont komputerów za pomocą programu narzędziowego wiersza poleceń NETDOM
- Dołączanie komputera do domeny poprzez zmianę właściwości identyfikacji sieciowej
- Zapoznanie się z istotnymi zagadnieniami tworzenia konta komputera przed przyłączeniem do domeny

Szacunkowy czas lekcji: 20 minut

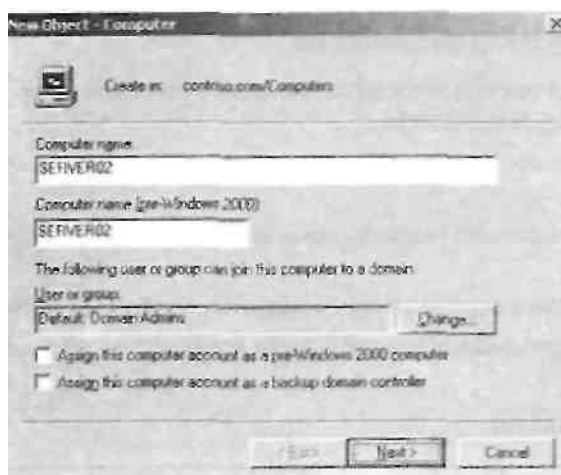
Tworzenie kont komputerów

Aby utworzyć obiekt komputera w usłudze Active Directory, administrator musi być członkiem grupy Administratorzy lub *Account Operators* (Operatorzy kont), znajdujących się na kontrolerach domyślnych. Domyślne ustawienia określają, że grupy *Domain Admins* (Administratorzy domeny) oraz *Enterprise Admins* (Administratorzy przedsiębiorstwa) są członkami grupy Administratorzy. Alternatywnym rozwiązaniem jest przekazanie administracji (delegowanie) tak, aby inni użytkownicy bądź grupy mogli tworzyć obiekty komputera.

Użytkownicy domeny mogą również tworzyć obiekty komputera przy użyciu interesującego, pośredniego procesu. Jeśli komputer został przyłączony do domeny, a konto komputera nie istnieje, usługa Active Directory automatycznie tworzy taki obiekt. Obiekt komputera domyślnie powstaje w jednostce organizacyjnej *Computers*. Każdy użytkownik grupy *Authenticated Users* (Użytkownicy uwierzytelnieni), czyli w rezultacie dotyczy to wszystkich użytkowników, może przyłączyć 10 komputerów do domeny i w ten sposób utworzyć do 10 obiektów komputera.

Tworzenie obiektów komputera za pomocą konsoli Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory)

W celu utworzenia obiektu komputera lub „konta” należy utworzyć przystawkę *Active Directory Users and Computers* i zaznaczyć kontener lub jednostkę organizacyjną, w której obiekt ma zostać utworzony. W menu *Action* (Akcja) lub w menu skrótów (po kliknięciu kontenera prawym przyciskiem myszy) należy wybrać polecenie *New-Computer* (Nowy-Komputer). Wyświetlone zostanie okno dialogowe *New Object-Computer* (Nowy obiekt — Komputer), takie jak przedstawione na rysunku 5-1.



Rysunek 5-1. Okno dialogowe *New Object-Computer* (Nowy obiekt- Komputer)

W oknie dialogowym *New Object-Computer* należy wpisać nazwę komputera. Pozostałe właściwości tego okna będą omawiane w następnej lekcji. Po kliknięciu przycisku **Next** (Dalej), wyświetlane jest okno dialogowe, w którym należy określić identyfikator GUID. Identyfikator GUID jest używany do nazwania konta komputera w procesie instalacji zdalnej RIS (Remote Installation Services), który nie będzie omawiany w tym rozdziale. Wpisanie identyfikatora GUID nie jest wymagane podczas

tworzenia konta komputera, gdyż połączenie z domeną będzie uzyskiwane za pośrednictwem innych metod. Tak więc należy po prostu kolejno kliknąć przyciski Next (Dalej) oraz **Finish** (Zakończ).

Tworzenie obiektów komputera przy użyciu polecenia DSADD

Wszystko wskazuje na to, że można zaryzykować stwierdzenie: „nic nowego pod słońcem”. Jednak przed ostatecznym wyrażeniem takiej opinii, w przypadku systemu Windows Server 2003 trzeba zapoznać się z przydatnym narzędziem wiersza poleceń DSADD, które umożliwia utworzenie obiektów komputera z wiersza poleceń lub za pomocą pliku wsadowego.

W rozdziale 2 „Administracja systemu Microsoft Windows Server 2003”, polecenie DSADD było omawiane w celu utworzenia obiektów użytkownika. Aby utworzyć obiekty komputera, wystarczy wpisać polecenie **dsadd computer *ComputerDN***, gdzie *ComputerDN* jest nazwą wyróżniającą (DN) komputera, jak na przykład CN=Desktop123,OU=Desktops,DC=contoso,DC=com.

Jeśli nazwa DN zawiera spację, należy całą nazwę DN objąć znakami cudzysłowu. Parametr *ComputerDN...* jest jedną lub kilkoma nazwami wyróżniającymi nowego obiektu komputera. Parametr *ComputerDN* może zawierać jedną lub kilka nazw wyróżniających nowych obiektów komputera, dzięki czemu polecenie DSADD Computer jest wygodną metodą jednoczesnego tworzenia wielu obiektów. Parametr *ComputerDN...* może być wprowadzany za pomocą jednej z wymienionych poniżej metod:

- Poprzez wprowadzenie listy nazw DN za pośrednictwem innego polecenia, takiego jak dsquery
- Poprzez wpisanie w wierszu poleceń każdej nazwy DN oddzielanej znakami spacji.
- Poprzez pozostawienie pustego parametru nazwy DN. W tym momencie z klawiatury konsoli można wpisywać w wierszu poleceń pojedyncze nazwy DN. Po każdej nazwie DN należy nacisnąć ENTER, a po ostatniej nazwie DN należy nacisnąć CTRL+Z.

W poleceniu DSADD COMPUTER, po parametrze DN można używać następujących parametrów opcjonalnych:

- -samid *SAMName* (nazwa SAM)
- -desc *Description* (opis)
- -loc *Location* (lokalizacja)

Tworzenie konta użytkownika za pomocą polecenia NETDOM

Polecenie NETDOM jest udostępnione w zestawie Support Tools i instalowane z dysku CD-ROM systemu Windows Server 2003 z katalogu Support\Tools. Polecenie jest także umieszczone na dyskach CD systemów Windows XP oraz Windows 2000. Należy używać wersji zgodnej z platformą. Polecenie NETDOM z wiersza poleceń umożliwia tworzenie szeregu kont domeny oraz wykonywanie zadań związanych z zabezpieczeniami.

Aby utworzyć konto komputera w domenie, należy wpisać następujące polecenie:

```
netdom add ComputerName / domain: DomainName /userd-User
/Password-UserPassword [/ou:0i/DA/]
```

Polecenie to tworzy konto komputera o nazwie *ComputerName* w domenie o nazwie *DomainName* za pośrednictwem poświadczeń domeny: *User* oraz *UserPassword*. Parametr / ou powoduje, że obiekt zostanie utworzony w jednostce organizacyjnej wyspecyfikowanej za pomocą nazwy wyróżniającej

*OU*DN, która umieszczana jest za parametrem. Jeśli nazwa *OU*DN nie została określona, to domyślnie konto komputera zostanie utworzone w jednostce organizacyjnej *Computers*. Poświadczeni!; użytkownika muszą mieć, rzecz jasna, odpowiednie uprawnienia pozwalające na tworzenie obiektów komputera.

Dołączenie komputera do domeny

Samo konto komputera nie wystarczy, aby utworzyć relacje zabezpieczeń pomiędzy domeną a komputerem. Komputer musi być połączony z domeną.

Aby przyłączyć komputer do domeny, należy postępować zgodnie z następującą procedurą:

1. Otwórz właściwości komputera dotyczące jego nazwy — okno *Computer Name* (Nazwa komputera).! Okno to można otworzyć różnymi metodami:
 - » Otwórz program **Control Panel** (Panel sterowania), kliknij moduł **System**, po czym kliknij zakładkę **Computer Name** (Nazwa komputera).
 - » Prawym przyciskiem myszy kliknij ikonę **My Computer** (Mój komputer) i wybierz poleceniek **Properties** (Właściwości). Następnie kliknij zakładkę **Computer Name** (Nazwa komputera).

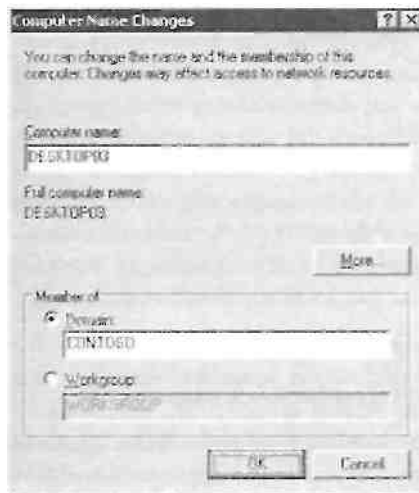


Informacje Zakładka *Computer Name* (Nazwa komputera) w systemach Windows 2000 jest nazywana *Network Identification* (Identyfikacja sieciowa), a przycisk *Change* (Zmień) opisany jest *Properties* (Właściwości). Jednakże funkcjonalność jest identyczna.

2. W programie **Control Panel** (Panel sterowania) otwórz folder **Network Connections** (Połączeni. sieciowe) i w menu **Advanced** (Zaawansowane) wybierz polecenie **Network Identification** (Identyfikacja sieciowa).
3. Na zakładce **Computer Name** (Nazwa komputera) kliknij przycisk **Change** (Zmień). Wyświetlone zostanie okno dialogowe *Computer Name Changes* (Zmiany nazwy komputera), pokazani na rysunku 5-2. W oknie tym można zmienić nazwę, domenę i członkostwo grupy roboczej komputera.



Wskazówka egzaminacyjna Nazwy komputera lub członkostwa nie można zmieniać, jeśli użytkownik nie zalogował się za pomocą konta o uprawnieniach administracyjnych na tym komputerze. Jedynie użytkownicy, którzy należą do grupy lokalnych administratorów, będą mogli modyfikować te właściwości (aktywny przycisk Zmień).



Rysunek 5-2. Okno dialogowe *Computer Name Changes* (Zmiany nazwy komputera)

4. W oknie dialogowym *Computer Name Changes* kliknij przycisk **Domain** (Domena) i wpisz nazwę domeny.



Wskazówka Pomimo, że nazwy NetBIOS domeny (płaskie) można z powodzeniem używać do zlokalizowania domeny docelowej, zaleca się wprowadzanie nazwy DNS. Konfiguracja DNS jest istotna dla komputera systemów DNS Windows 2000, Windows XP lub Windows Server 2003. Stosując nazwę DNS domeny określamy preferowany proces rozpoznawania nazwy oraz sprawdzamy konfigurację DNS komputera. Jeśli komputer nie mógł zlokalizować domeny, do której miał się przyłączyć, należy sprawdzić prawidłowość wpisów konfiguracji połączenia sieciowego określających serwer DNS.

5. Kliknij przycisk OK- Komputer kontaktuje się z kontrolerem domeny. Jeśli podczas dołączania do domeny pojawiły się problemy, należy sprawdzić połączenie sieciowe, jego konfigurację, jak również konfigurację usługi DNS.

Jeśli natomiast połączenie zostało nawiązane, użytkownik będzie poproszony o podanie nazwy użytkownika i hasła, które posiada uprawnienia umożliwiające połączenie z domeną (rysunek 5-3 przedstawia odpowiednie okno dialogowe). Warto zwrócić uwagę, że wymagane poświadczenie tożsamości dotyczy hasła i nazwy użytkownika *domeny*.



Rysunek 5-3. Wpisywanie poświadczeń tożsamości przy połączeniu do domeny

Jeśli wcześniej *nie* zostało utworzone konto komputera domeny o nazwie, która zgadza się z nazwą komputera, usługa Active Directory automatycznie utworzy konto w domyślnym kontenerze *Computers*. Po utworzeniu i zlokalizowaniu konta komputera domeny, komputer ustanawia relacje zaufania z domeną, zmienia swój identyfikator SID tak, aby był zgodny z tym kontem oraz dokonuje modyfikacji członkostwa grup. Aby zakończyć proces, komputer musi zostać ponownie uruchomiony.



Informacje Do połączenia stacji roboczej lub serwera z domeną może być również używane polecenie NETDOM JOIN. Jego funkcjonalność jest identyczna jak dla interfejsu użytkownika *Computer Name Changes*, za wyjątkiem tego, że można także wyspecyfikować jednostkę organizacyjną, jeśli obiekt komputera nie istnieje w usłudze Active Directory.

Porównanie kontenerów i jednostek organizacyjnych komputerów

Kontener *Computers* jest domyślną lokalizacją obiektów komputera w usłudze Active Directory. Po aktualizacji domeny systemu Windows NT 4 do systemu Windows 2000, początkowo wszystkie komputery znajdują się w tym kontenerze. Ponadto, jeśli komputer łączy się z domeną, w której nie istnieje konto dla tego komputera, obiekt komputera zostanie automatycznie utworzony w kontenerze *Computers*.



Wskazówka Zestaw programów narzędziowych *Microsoft Windows Server 2003 Resource Kit* zawiera program REDIRCOMP umożliwiający przekierowanie automatycznie tworzonych obiektów komputera do wskazanej jednostki organizacyjnej. Domena musi mieć poziom funkcjonalności systemu Windows Server 2003, co oznacza, że wszystkie kontrolery domen muszą działać pod kontrolą systemu Windows Server 2003. Narzędzie to jest przydatne w organizacjach, w których tworzenie konta komputera jest mniej ściśle kontrolowane. Ponieważ obiekty komputera zostają automatycznie utworzone w jednostce organizacyjnej, mogą być zarządzane przez zasady powiązane z tą jednostką OU. Więcej informacji o programie REDIRCOMP można znaleźć w zestawie *Windows Server 2003 Resource Kit*.

Chociaż kontener *Computers* jest kontenerem domyślnym dla obiektów komputera, nie jest idealnym kontenerem dla takich obiektów. Inaczej niż dla jednostek organizacyjnych, kontenery takie jak *Computers*, *Users* i *Builtin* nie mogą być powiązane do zasad, co ogranicza potencjalny zakres stosowania

zasady grupy dotyczącej komputerów. Zalecana praktyką projektowania usługi Active Directory jest dołączanie co najmniej jednej jednostki organizacyjnej przeznaczonej dla komputerów. Często dla komputerów przeznaczonych jest wiele jednostek organizacyjnych, które tworzone są w oparciu o regiony administracyjne lub do oddzielenia administracji komputerów przenośnych, stacjonarnych, serwerów druku i plików czy serwerów aplikacji. Przykładowo, w usłudze Active Directory istnieje domyślna jednostka organizacyjna dla kontrolerów domeny, która jest powiązana z zasadą *Default Domain Controller Policy* (Domyślna zasada kontrolera domeny). Dzięki utworzeniu jednej lub kilku jednostek organizacyjnych dla komputerów, organizacja może poprzez zasady grupy bardziej elastycznie przekazywać administrację i zarządzanie konfiguracją komputerów.

Jeśli w organizacji utworzono dla komputerów jedną lub kilka jednostek organizacyjnych, należy każdy automatycznie utworzony obiekt komputera (w kontenerze *Computers*) przesunąć do odpowiedniej jednostki OU. W tym celu należy zaznaczyć komputer i z menu **Action** (Akcja) wybrać polecenie Move (Przenieś). Innym sposobem przeniesienia obiektu jest skorzystanie z nowej funkcji konsoli MMC — „przeciągnij i upuść”.



Wskazówka Ponieważ obiekt komputera w jednostce organizacyjnej *Computers* nie jest zarządzany przez zasady grupy powiązane ze specjalnie utworzonymi dla komputerów jednostkami organizacyjnymi przedsiębiorstwa oraz ponieważ przeniesienie obiektu komputera z jednostki organizacyjnej *Computers* do innej jednostki OU wymaga dodatkowych czynności, to zalecaną metodą jest *utworzenie obiektów komputera zanim komputer zostanie przyłączony do domeny*. Obiekt komputera można najpierw utworzyć we właściwej jednostce organizacyjnej, i dzięki temu, jeśli system komputerowy przytacza się do domeny, stosując się do niego zasady powiązane z tą jednostką organizacyjną.

Obiekt komputera lub każdy inny obiekt można również, przenieść przy użyciu polecenia DSMOVE. Składnia polecenia DSMOVE jest następująca:

```
dsmove ObjectDN [-newname NewName] [-newparent ParentDN]
```

Parametr *-newname* umożliwia zmianę nazwy obiektu. Parametr *-newparent* pozwala przesunąć obiekt. W celu przeniesienia komputera nazwanego DesktopABC z kontenera *Computers* do jednostki organizacyjnej *Desktops*, należy wprowadzić następujące polecenie:

```
dsmove ?CN=DesktopABC,CN=Computers.DC=Contoso,DC=com? -newparent  
?OU=Desktops.DC=Contoso,DC=com?
```

Polecenie to ponownie pokazuje różnicę między *kontenerem* (CN) *Computers* a *jednostką organizacyjną* (OU) *Desktops*.

Aby w usłudze Active Directory przenosić obiekty, należy mieć odpowiednie uprawnienia. Uprawnienia domyślne grupy *Account Operators* (Operatorzy kont) pozwalają przenosić obiekty komputerów między kontenerami i jednostkami organizacyjnymi, wliczając w to kontener *Computers*, *za wyjątkiem jednostki organizacyjnej* *Domain Controllers* (Kontrolery domeny). Administratorzy, w tym *Domain Admins* (Administratorzy domeny) oraz *Enterprise Admins* (Administratorzy przedsiębiorstwa), mogą przenosić obiekty pomiędzy dowolnymi kontenerami i jednostkami organizacyjnymi, w tym także między kontenerem *Computers* i jednostką organizacyjną *Domain Controllers* (Kontrolery domeny).

Zadanie kontrolne: Dołączenie komputera do domeny usługi Active Directory

W zadaniu tym, za pomocą przystawki Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) oraz polecenia DSADD, utworzone zostaną konta komputerów. Następnie komputery będą przyłączane do domeny, pod warunkiem posiadania dostępu do innego systemu.

Ćwiczenie 1: Tworzenie kont komputerów za pomocą przystawki Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory)

1. Otwórz przystawkę *Active Directory Users And Computers*.
2. W jednostce organizacyjnej Servers utwórz obiekt komputera dla komputera nazwanego „SERVER02.” Skonfiguruj jedynie nazwę komputera. Nie zmieniaj pozostałych właściwości domyślnych.
Warto zauważyć, że podobnie jak dla użytkowników, komputer ma dwie nazwy - nazwę komputera i nazwę komputera dla systemów wcześniejszych niż system Windows 2000”. Zalecaną praktyką jest, aby obie nazwy były takie same.

Ćwiczenie 2: Tworzenie kont komputerów za pomocą polecenia DSADD

1. Otwórz okno wiersza poleceń.
2. Wpisz polecenie:
dsadd computer ?cn=desktop03,ou=servers,dc=contoso,dc=com?

Ćwiczenie 3: Przesuwanie obiektu komputera

1. Otwórz przystawkę *Active Directory Users And Computers*.
2. Za pomocą polecenia **Move** (Przenieś), przesuń obiekt komputera Desktop03 z jednostki organizacyjnej Servers do jednostki Desktops.
3. Przeciągnij obiekt Server02 z kontenera Servers do kontenera *Computers*.
4. Zaznacz kontener *Computers*, aby upewnić się, że obiekt Server02 znalazł się na właściwym miejscu. Podczas stosowania metody „przeciągnij i upuść” łatwo o popełnienie błędu.



Nieoficjalnie Konsola MMC jest stałym źródłem „umiarkowanych” ataków paniki. Okna konsoli nie są automatycznie odświeżane. Po przeprowadzeniu zmian, takich jak przesunięcie obiektu, należy użyć polecenia Refresh (Odśwież) lub klawisza skrótu (F5), aby odświeżyć konsolę.

5. Otwórz okno właściwości kontenera Computers. W oknie tym nie występuje zakładka Group Policy (zasada grupy), inaczej niż dla właściwości jednostek organizacyjnych, takich jak Servers. I to jest jednym z powodów, dla których w przedsiębiorstwach dla komputerów tworzone są dodatkowe jednostki organizacyjne.
6. Otwórz okno wiersza poleceń.
7. Wpisz polecenie:

dsmove ?CN=Server02,CN=Computers,DC=contoso,DC=com? -newparent ?OU=Servers,DC=contoso,DC=com?

Polecenie to z powrotem przesuwa obiekt komputera do jednostki organizacyjnej Servers. 8.
Sprawdź, czy komputer znalazł się z powrotem w jednostce organizacyjnej Servers.

Ćwiczenie 4 (Opcjonalne): Przyłączenie komputera do domeny

Ćwiczenie to wymaga dodatkowego systemu połączonego w sieci z serwerem Server01. Oprócz tego, system DNS musi być prawidłowo skonfigurowany tak, aby utworzone zostały rekordy usługi (SRV) serwera Server01. Konfiguracja DNS dodatkowego komputera musi umożliwiać lokalizację serwera Server01, jako kontrolera domeny contoso.com.

1. Jeśli dysponujesz dodatkowym systemem umożliwiającym przyłączenie do domeny, urwórz za pomocą przystawki *Active Directory Users And Computers* lub polecenia DSADD, konto dla systemu dodatkowego. Upewnij się, że użyta nazwa jest identyczna z nazwą komputera.
2. Zaloguj się do komputera. Należy zalogować się za pomocą konta, które należy do grupy lokalnych administratorów, aby możliwa była zmiana członkostwa w domenie.
3. Znajdź zakładkę **Computer Name** (Nazwa komputera) otwierając moduł **System** w programie **Control Panel** (Panel sterowania) lub polecenie **Network Identification** (Identyfikacja sieciowa) znajdujące się w menu **Advanced** (Zaawansowane) w katalogu **Network Connections** (Połączenia sieciowe).
4. Kliknij przycisk **Change** (Zmień).
5. Kliknij opcję **Domain** (Domena) i wpisz nazwę domeny DNS - contoso.com.
6. Kliknij przycisk OK.
7. Wpisz poświadczenia tożsamości dla konta Administrator w domenie contoso.com.
8. Kliknij przycisk OK.
9. Komputer poinformuje, że niezbędne będzie ponowne uruchomienie systemu. Kliknij przycisk OK dla każdego pojawiającego się komunikatu i zamknij wszystkie okna dialogowe. Ponownie uruchom system.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Jaką *minimalną* tożsamość musi użytkownik poświadczyć, aby mógł utworzyć konto komputera systemu Windows Server 2003 w jednostce organizacyjnej domeny? Należy rozważyć wszystkie kroki procesu przy założeniu, że konto tego komputera nie było wcześniej utworzone w usłudze w Active Directory.
 - a. Domain Admins (Administratorzy domeny)
 - b. Enterprise Admins (Administratorzy przedsiębiorstwa)
 - c. Administrators on a domain controller (Administratorzy na kontrolerze domeny)
 - d. Account Operators on a domain controller (Operatorzy kont na kontrolerze domeny)
 - e. Server Operators on a domain controller (Operatorzy serwerów na kontrolerze domeny)

- f. Account Operators on the server (Operatorzy kont na tym serwerze)
 - g. Server Operators on the server (Operatorzy serwera, na danym serwerze)
 - h. Administrators on the server (Administratorzy na tym serwerze)
2. W którym miejscu można zmienić członkostwo domeny komputera systemu Windows Server 2003?
- a. Właściwości modułu My Computer (Mój komputer)
 - b. Moduł System w programie Control Panel (Panel sterowania)
 - c. Przystawka Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory)
 - d. Folder Network Connections (Połączenia sieciowe)
 - e. Moduł Users (Użytkownicy) w programie Control Panel (Panel sterowania)
- 3- Za pomocą którego programu narzędziowego wiersza poleceń można utworzyć w usłudze Active Directory konto komputera domeny?
- a. NETDOM
 - b. DSADD
 - c. DSGET
 - d. NETSH
 - e. NSLOOKUP

Podsumowanie lekcji

- Ustawienia domyślne określają, że członkowie grup Administratorzy oraz Account Operators (Operatorzy kont) mają uprawnienia do tworzenia obiektów komputera w usłudze Active Directory.
- Przystawka Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) oraz programy DSADD i NETDOM mogą być używane do tworzenia kont komputerów.
- Aby dla komputera zmienić członkostwo domeny, należy zalogować jako członek grupy *Administratorzy lokalni*.

Lekcja 2: Zarządzanie kontami komputerów

W poprzedniej lekcji omówione zostały podstawowe elementy relacji komputer - domena, czyli konto komputera i połączenie komputera do domeny. Teraz opisany zostanie bardziej szczegółowo obiekt komputera w usłudze Active Directory, jego pozostałe właściwości, uprawnienia będące motorem jego działania oraz sposoby zarządzania tymi właściwościami przeprowadzane za pomocą interfejsu GUI bądź narzędzi wiersza poleceń.

Materiały omówione podczas lekcji pozwalają na

- Konfigurowanie uprawnień nowego obiektu komputera usługi Active Directory
- Konfigurowanie właściwości obiektu komputera usługi Active Directory
- Wyszukiwanie i zarządzanie kontami komputerów za pomocą przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory)

Szacunkowy czas lekcji: 10 minut

Zarządzanie uprawnieniami obiektu komputera

Jak nadmieniono w lekcji 1, komputer może być przyłączony do domeny, jeśli w trakcie tego procesu użytkownik poświadczy tożsamość o uprawnieniach administratora domeny. Jednakże kwestie bezpieczeństwa wymagają, aby do realizacji danego zadania wykorzystywane były tylko te uprawnienia, które są niezbędne. Wymóg posiadania uprawnień konta administratora domeny dla dodania komputera do domeny wydaje się być przesadą.

Na szczęście, usługa Active Directory umożliwia dokładne sterowanie grupami lub użytkownikami, którzy mogą połączyć się do konta komputera domeny. Pomimo, że domyślne ustawienia wymagają uprawnień administratorów domeny, można pozwolić, by dowolna grupa (na przykład nazwana Instalatorzy) mogła dołączać komputer do konta. Jest to duże ułatwienie w procesie tworzenia obiektu komputera.

Podczas tworzenia obiektu komputera, na pierwszej stronie okna dialogowego New Object-Computer (Nowy obiekt — Komputer), pokazanej poprzednio na rysunku 5-1, znajduje się ramka opisana: The Following User Or Group Can Join This Computer To A Domain (Poniższy użytkownik lub grupa mogą dołączać ten komputer do domeny). Należy kliknąć przycisk Change (Zmień) i wskazać grupę lub użytkownika. Zmiana ta modyfikuje szereg uprawnień komputera usługi Active Directory.

Na następnej stronie okna dialogowego New Object-Computer (Nowy obiekt — Komputer) dla komputera należy określić globalny unikatowy identyfikator (GUID), który jest potrzebny podczas instalacji przeprowadzanej z pomocą usług instalacji zdalnej RIS (Remote Installation Services). Dodatkowe informacje o usłudze RIS można znaleźć w dziale firmy Microsoft - Knowledge Base pod adresem <http://support.microsoft.com/>.

Jeśli komputer, który korzysta z utworzonego konta, działa pod kontrolą systemu Windows wersji wcześniejszej niż 2000, należy zaznaczyć pole wyboru Assign This Computer Account As A Pre-Windows 2000 Computer (Przypisz to konto komputera jako komputer z systemem starszym,

niż Windows 2000). Jeśli konto jest przeznaczone dla zapasowego kontrolera domeny systemu Windows NT, należy zaznaczyć pole wyboru Assign This Computer Account As A Backup Domain Controller (Przypisz to konto jako zapasowy kontroler domeny).

a

Wskazówka Warto zapamiętać, że jedynie komputery bazujące na technologii systemu Windows NT mogą należeć do domeny, natomiast systemy Windows 95, Windows 98 oraz Windows Millennium Edition (Windows Me) nie mogą dołączać lub utrzymywać kont komputerów. Dlatego omawiane poprzednio pole wyboru odnosi się tak naprawdę do systemu Windows NT 4.

Konfigurowanie właściwości komputera

Obiekty komputera mają szereg właściwości, które nie są podczas tworzenia konta komputera uwidaczniane w interfejsie użytkownika. Aby określić lokalizację obiektu i opis, skonfigurować członkostwo grupy, uprawnienia połączeń telefonicznych czy powiązać z obiektem użytkownika, który ma zarządzać komputerem, należy dla obiektu komputera otworzyć okno dialogowe Properties (Właściwości) Stronę właściwości systemu operacyjnego (Operating System) można tylko odczytywać. Informacje są automatycznie publikowane w usłudze Active Directory, a odpowiednie rekordy są puste, dopóki komputer nie połączy się z domeną przy użyciu tego konta.

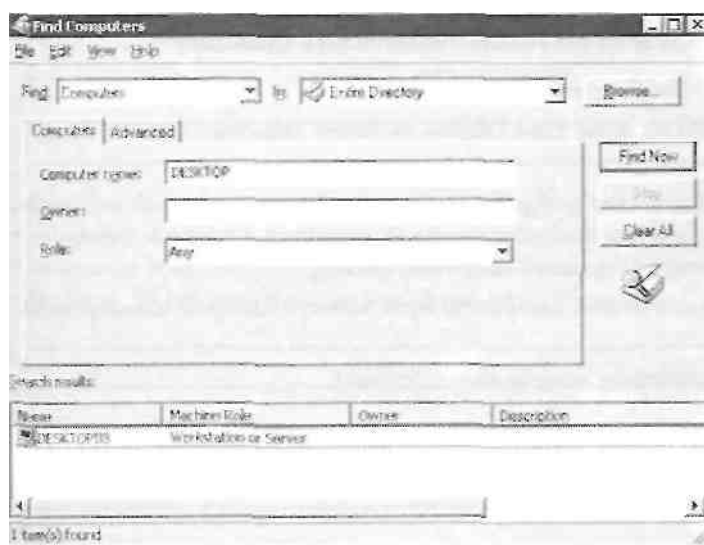
Kilka klas obiektu usługi Active Directory obsługuje właściwości zarządcy komputera, które zostały zebrane na stronie właściwości komputera — Managed By (Zarządzany przez). Te powiązane właściwości tworzą odniesienia do obiektu użytkownika. Wszystkie inne właściwości, takie jak adresy czy numery telefonów, są wyświetlane bezpośrednio w obiekcie użytkownika i nie są przechowywane jako część obiektu komputera.

Tak jak było nadmienione w rozdziale 2, za pomocą polecenia DSMOD można modyfikować szereg właściwości obiektu komputera. Działanie polecenia DSMOD będzie omówione w kolejnej sekcji w odniesieniu do zagadnień rozwiązywania problemów obiektu komputera.

Wyszukiwanie i dołączanie do obiektów usługi Active Directory

Jeśli użytkownik dzwoni do działu wsparcia technicznego, administrator chciałby wiedzieć, jaki system operacyjny oraz jakie pakiety serwisowe zostały zainstalowane na komputerze użytkownika. Informacje te są przechowywane jako właściwości obiektu komputera. Problemem staje się wyszukanie tego obiektu komputera, w szczególności jeśli mamy do czynienia ze złożoną usługą Active Directory, w której znajduje się kilka domen i wiele jednostek organizacyjnych.

Przystawka Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) została wyposażona w sprawne i proste narzędzie umożliwiające wyszukiwanie różnego typu obiektów. W tym rozdziale pokazane będą sposoby wyszukiwania obiektów komputera. W tym celu, na pasku narzędzi konsoli, należy kliknąć przycisk Find Objects In Active Directory (Znajdź obiekty w usłudze Active Directory). Okno dialogowe Find Computers (Znajdowanie: Komputery) pokazane zostało na rysunku 5-4. Po uruchomieniu wyszukiwania, czyli przed naciśnięciem przycisku Find Now (Znajdź teraz), można określić typ wyszukiwanego obiektu (Znajdź:), zakres wyszukiwania (W:) oraz można określić kryteria wyszukiwania.



Rysunek 5-4. Okno dialogowe *Find Computers (Znajdowanie: Komputer)*, pokazane po wyszukaniu obiektu

Na liście wyszukanych obiektów można zaznaczyć komputer i z menu File (Plik) lub z menu skrótów wybrać zadanie do wykonania. Wielu administratorów docenia możliwość wykorzystywania polecenia Manage (Zarządzaj) pozwalającego bezpośrednio otworzyć konsolę Computer Management (Zarządzanie komputerem) i połączyć się z wybranym komputerem, dzięki czemu można przeanalizować jego dzienniki zdarzeń, program zarządzający urządzeniami, informacje o systemie, konfigurację dysku i usług, a także informacje o użytkownikach lokalnych czy kontach grup.

Zadanie kontrolne: Zarządzanie kontami komputerów

W zadaniu tym wyszukiwany będzie obiekt komputera oraz modyfikowane będą jego właściwości.

Ćwiczenie 1: Zarządzanie kontami komputerów

1. Otwórz przystawkę *Active Directory Users And Computers*.
2. Zaznacz jednostkę organizacyjną Security Groups i utwórz globalną grupę zabezpieczeń nazwaną Deployment.
3. Zaznacz jednostkę organizacyjną Desktops.
4. Utwórz konto komputera — Desktop04. Na pierwszej stronie okna dialogowego New Object- Computer (Nowy obiekt — Komputer) kliknij przycisk Change (Zmień) znajdujący się poniżej opcji The Following User Or Group Can Join This Computer To A Domain (Poniższy użytkownik lub grupa mogą dołączać ten komputer do domeny). W polu Select User or Group (Użytkownik lub grupa) wpisz **deployment**, a następnie kliknij przycisk OK.
5. Zakończ tworzenie obiektu komputera Desktop04.

Ćwiczenie 2: Wyszukiwanie obiektów usługi Active Directory

1. Otwórz przystawkę *Active Directory Users And Computers*.
2. Na pasku narzędzi kliknij ikonę **Find Objects in Active Directory** (Znajdź obiekty w usłudze Active Directory).
3. Domyślnie, okno dialogowe jest przygotowane do wyszukiwania użytkowników, kontaktów i grup. Z menu rozwijanego wybierz opcję **Computers (Komputery)**, a na liście zakresu wyszukiwania (W:), zaznacz opcję **Entire Directory (Cały obiekt: Katalog)**.
4. W polu **Computer Name (Nazwa komputera)** wpisz **server**, a następnie kliknij przycisk **Find Now (Znajdź teraz)**.

Na liście wyników wyświetlony zostanie obiekt: **Server01**.

Ćwiczenie 3: Zmiana właściwości komputera

1. Na liście wyników wyszukiwania uzyskanej w ćwiczeniu 1, otwórz okno dialogowe właściwości obiektu **Server01**.
2. Kliknij zakładkę **Location (Lokalizacja)**.
3. Wpisz **Headquarters Server Room**.
4. Kliknij zakładkę **Managed By (Zarządzany przez)**, a następnie kliknij przycisk **Change (Zmień)**.
5. Wpisz **Hank**, a następnie kliknij przycisk **OK**.
6. Warto zwrócić uwagę, że wyświetlona została nazwa użytkownika oraz informacje kontaktowe.
- 7- Kliknij zakładkę **Operating System (System operacyjny)**. Zanotuj wersję systemu oraz poziom pakietu serwisowego.
8. (Opcjonalne) Jeśli dysponujesz przyłączonym do domeny dodatkowym komputerem (lekcja 1, ćwiczenie 4), otwórz okno właściwości tego obiektu komputera oraz zanotuj cechy systemu operacyjnego.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezenrowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Która platforma umożliwia przyłączenie do domeny?
 - a. Windows 95
 - b. Windows NT 4
 - c. Windows 98
 - d. Windows 2000
 - e. Windows Me
 - f. Windows XP
 - g. Windows Server 2003

2. Po otwarciu obiektu komputera, na zakładce Operating System (System operacyjny) nie są wyświetlane żadne właściwości. Co może być tego przyczyną?
3. Dyrektor ma komputer przenośny nazwany „TopDog”, działający pod kontrolą systemu Windows XP. Należy umożliwić dołączenie tego komputera do domeny oraz zapewnić, że konfiguracja tego komputera będzie bezpośrednio określana przez zasady grupy powiązane z jednostką organizacyjną Desktops. W jaki sposób można zrealizować takie zadanie?
4. Dlaczego zalecaną praktyką jest utworzenie obiektu komputera *przed* przyłączeniem komputera do domeny?

Podsumowanie lekcji

- Dowolny użytkownik lub grupa mogą dołączać komputer do konta domeny. Jest to określone przy użyciu opcji: The Following User Or Group Can Join This Computer To A Domain (Poniższy użytkownik lub grupa może przyłączyć ten komputer do domeny).
- Przycisk The Find Objects In Active Directory (Znajdź obiekty w usłudze Active Directory), znajdujący się na pasku narzędzi przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) umożliwia wyszukiwanie, a następnie zarządzanie komputerami i innymi obiektami usługi Active Directory.

Lekcja 3: Rozwiązywanie problemów związanych z kontami komputerów

Domeny usługi Active Directory traktują komputery jako podmioty zabezpieczeń. Oznacza to, że komputer, tak jak użytkownik, ma konto lub bardziej dokładnie, obiekt komputera ma właściwości takie jak nazwa, hasło oraz identyfikator SID. Podobnie jak konta użytkowników, konta komputerów wymagają obsługi, a czasami rozwiązania problemów. Niniejsza lekcja omawia właśnie umiejętności i pojęcia dotyczące rozwiązywania problemów związanych z obiektami komputerów.

Materiały omówione podczas lekcji pozwalają na

- Omówienie istotnych różnic dotyczących usuwania, wyłączania bądź zerowania kont komputerów
- Rozpoznawanie symptomów występowania problemów konta komputera
- Rozwiązywanie problemów kont komputerów poprzez usuwanie, wyłączanie, zerowanie lub odłączanie kont przy użyciu programów narzędziowych wiersza poleceń i narzędzi interfejsu użytkownika

Szacunkowy czas lekcji: 20 minut

Usuwanie, wyłączanie bądź zerowanie kont komputerów

Konta komputerowe, podobnie jak konta użytkowników, obsługują unikatowy identyfikator SID, który umożliwia administratorowi przydzielanie uprawnień do komputerów. Również podobnie jak dla kont użytkownika, konta komputerów należą do grup. Dlatego, również tak jak dla kont użytkownika, ważnym zagadnieniem jest zrozumienie rezultatów usunięcia konta komputera. Po usunięciu konta komputera, usunięte zostają jego członkostwa w grupach oraz identyfikator SID. Jeśli konto zostało usunięte przypadkowo, pomimo tego, że nowo utworzone konto ma taką samą nazwę, będzie miało nowy identyfikator SID. Dla nowego konta, członkostwa grup oraz wszystkie uprawnienia muszą być ponownie określone. Dlatego przed usunięciem konta komputera należy upewnić się, że nie będą już dłużej potrzebne atrybuty zabezpieczeń tego obiektu.

Aby usunąć konto komputera za pomocą przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory), należy zlokalizować i zaznaczyć obiekt komputera, a następnie z menu Action (Akcja) lub z menu skrótów wybrać polecenie Delete (Usuń). System poprosi o potwierdzenie czynności usuwania, ponieważ usunięcie jest operacją nieodwracalną (domyślna odpowiedź określona jest jako Nie). Po naciśnięciu przycisku Tak, obiekt zostanie usunięty.

Program wiersza poleceń DSRM omawiany w rozdziale 3, również umożliwia usuwanie obiektu komputera. W tym celu należy wpisać następujące polecenie DSRM:

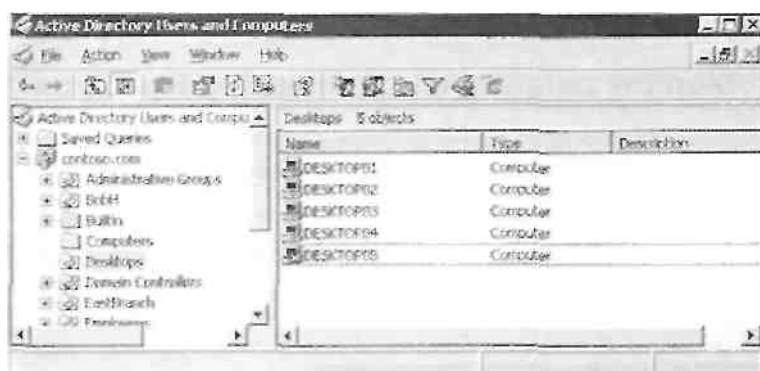
DSRM ObjectDN

Gdzie *ObjectDN* jest nazwą wyróżniającą komputera, jak na przykład „CN=Desktop15, OU=Desktops, DC=contoso, DC=com”. Również i w tym programie użytkownik będzie poproszony o potwierdzenie wykonania operacji.

Wskazówka Jeśli komputer jest odłączony od domeny (podczas przeprowadzanej przez administratora zmiany członkostwa komputera w grupie lub innej domenie), komputer próbuje usunąć swoje konto w domenę. Jeśli nie było to możliwe, ze względu na brak połączenia bądź problemy związane z siecią lub uprawnieniami, konto pozostanie w usłudze Active Directory. Konto może sprawiać wrażenie konta wyłączonego. Jeśli nie jest ono już potrzebne, powinno być usunięte ręcznie.

Jeśli przez dłuższy okres komputer nie będzie używany lub będzie odłączony od sieci, można wyłączyć jego konto. Takie działania odzwierciedlają zasadę bezpieczeństwa, nakazującą przechowywanie jedynie minimalnej liczby „tożsamości” wymaganej dla procesów uwierzytelnienia w danej organizacji. Wyłączenie konta nie modyfikuje identyfikatora SID lub członkostwa grupy, tak więc, jeśli zajdzie potrzeba ponownego użycia tego komputera, wystarczy włączyć jego konto.

Dla danego obiektu komputera, w menu kontekstowym lub w menu Action (Akcja) umieszczone jest polecenie Disable Account (Wyłącz konto). Konto wyłączone oznaczone jest w przystawce Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) czerwonym krzyżykiem (X), tak jak pokazane to zostało na rysunku 5-5.



Rysunek 5-5. Wyłączone konto komputera

Jeśli konto jest wyłączone, komputer nie może utworzyć pomiędzy domeną bezpiecznego kanału. Z tego powodu, użytkownicy, którzy nie logowali się poprzednio do tego komputera i tym samym nie mają na komputerze zapisanych poświadczeń tożsamości, nie będą mogli zalogować się, o ile, poprzez włączenie konta nie zostanie ponownie ustanowiony kanał bezpieczeństwa.

Aby włączyć konto komputera wystarczy po prostu zaznaczyć komputer i z menu Action (Akcja) lub menu skrótów wybrać polecenie Enable Account (Włącz konto).

Do załączania lub wyłączania konta komputera w wierszu poleceń służy program DSMOD. Polecenie DSMOD modyfikuje obiekty usługi Active Directory. Składnia używana do wyłączenia lub załączenia konta komputera jest następująca:

```
DSMOD COMPUTER ComputerDN -DISABLED YES
DSMOD COMPUTER ComputerDN -DISABLED NO
```

Jeśli członkostwa grupy konta oraz identyfikator SID, a także uprawnienia przydzielone do tego identyfikatora są istotne dla operacji domeny, nie należy usuwać takiego konta. Nasuwa się więc pytanie, co należy zrobić, jeśli komputer został zastąpiony przez nowy system, poprzez wymianę starych

urządzeń sprzętu. W takim przypadku należy przeprowadzić operację nazwaną *zerowanie (resetowanie)* konta komputera.

Zerowanie konta komputera usuwa hasło, ale pozostawia wszystkie właściwości obiektu komputera. W rezultacie takiej operacji konto staje się „dostępne”. W tym momencie, dowolny komputer (w tym aktualizowany system) za pomocą tego konta może przyłączyć się do domeny.

W rzeczywistości, komputer, który był poprzednio połączony z domeną za pomocą tego konta, może używać wyzerowanego konta łącząc się po prostu ponownie z domeną. Zagadnienia te będą omawiane bardziej szczegółowo w lekcji dotyczącej rozwiązywania problemów.

Polecenie Reset Account (Resetuj konto) jest dostępne po zaznaczeniu obiektu komputera w menu Action (Akcja) oraz w menu kontekstowym. Do zerowania konta komputera można również używać polecenia DSMOD. Składnia polecenia jest następująca:

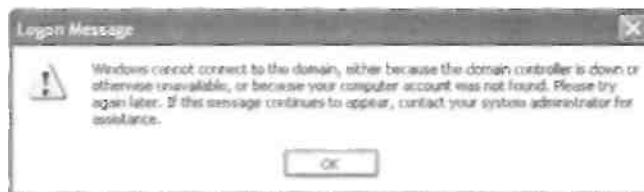
```
dsmod computer ComputerDN -reset
```

Polecenie NETDOM, dołączone w zestawie narzędziowym Windows Server 2003 Support Tools, również umożliwia zerowanie konta komputera. Program ten znajduje się w katalogu SupportATools na dysku CD-ROM systemu Windows Server 2003-

Rozpoznawanie problemów związanych z kontami komputerów

Relacje zabezpieczeń pomiędzy domeną a kontami komputerów są silne. W rzadko spotykanych sytuacjach, kiedy konto lub kanał bezpieczeństwa nie działa, symptomy uszkodzenia są ogólnie mówiąc oczywiste. Częste problemy związane z kontem komputera to:

Komunikaty podczas logowania wskazują na brak kontaktu z kontrolerem domeny, na brak konta lub brak relacji zaufania pomiędzy komputerem a domeną. Przykład takiego komunikatu przedstawiony został na rysunku 5-6.



Rysunek 5-6. Komunikat podczas logowania w systemie Windows XP, wskazujący na możliwość wystąpienia problemów konta komputera

- Komunikaty błędów lub zdarzeń zapisane w dzienniku zdarzeń wskazują na występowanie podobnych problemów lub sugerują nieprawidłowe hasła, zaufania, kanały bezpieczeństwa czy relacje pomiędzy domeną lub kontrolerem domeny.
- Brak konta komputera w usłudze Active Directory.

Jeśli ma miejsce jedna z opisanych sytuacji, należy rozwiązać problem. W poprzedniej części rozdziału omówione zostały sposoby usuwania, wyłączania i zerowania kont komputerów oraz sposoby dołączania komputera do domeny.

Wymienione poniżej reguły są stosowane podczas rozwiązywania problemów związanych z kontami komputerów:

- A. Jeśli konto istnieje w usłudze Active Directory, musi zostać wyzerowane.
- B. Jeśli w usłudze Active Directory brak konta komputera, należy konto takie utworzyć.
- C. Jeśli komputer wciąż należy do domeny, musi zostać z niej usunięty poprzez zmianę członkostwa z domeny do grupy roboczej. Nazwa grupy roboczej jest bez znaczenia. Zaleca się, aby wybrać nazwę nieużywanej grupy roboczej.
- D. Ponowne przyłączenie komputera do domeny. Alternatywnym rozwiązaniem jest przyłączenie innego komputera do domeny, ale komputer ten musi mieć taką samą nazwę jak konto komputera.

Podczas rozwiązywania dowolnego problemu związanego z kontem komputera należy stosować *wszystkie cztery reguły*. Reguły mogą być używane w dowolnej kolejności za wyjątkiem reguły D, ponowne połączenie komputera do domeny musi być zawsze wykonywane na końcu procedury. Poniżej przeanalizowane zostaną dwa przykłady praktyczne.

W pierwszym przykładzie użytkownik powiadomił administratora, że podczas logowania system wyświetla komunikat informujący o prawdopodobnym braku konta komputera. Stosując regułę A, należy otworzyć przystawkę Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) i sprawdzić, czy takie konto komputera istnieje. Następnie konto należy wyzerować. Reguła B nie ma zastosowania — konto istnieje. Następnie, stosując regułę C, należy odłączyć system od domeny, a później zgodnie z regułą D ponownie go przyłączyć.

W drugim zadaniu praktycznym, jeśli konto komputera zostało przypadkowo wyzerowane, zostanie zastosowana reguła A. Pomimo, że wyzerowanie konta jest przypadkowe, do jego odtworzenia trzeba zastosować wszystkie trzy pozostałe reguły. Reguła B nie ma zastosowania, ponieważ konto istnieje w domenie. Reguła C wskazuje, że komputer jest wciąż połączony z domeną i musi być z niej usunięty. Następnie, stosując regułę D, można ponownie przyłączyć komputer do domeny.

Stosując te cztery reguły w pracy bądź podczas egzaminu, można podjąć właściwe decyzje, co do sposobu rozwiązywania dowolnego problemu, w którym konto komputera przestało działać.

Zadanie kontrolne: Rozwiązywanie problemów związanych z kontami komputera

W zadaniu tym będzie rozwiązywany problem oparty na rzeczywistym zdarzeniu. Użytkownik domeny contoso.com powiadomił administratora, że podczas logowania do komputera Desktop03 wyświetlony zostaje następujący komunikat:

„System Windows nie może połączyć się do domeny, ponieważ kontroler domeny jest niedostępny bądź wyłączony lub konto komputera nie zostało znalezione. Proszę później ponowić próbę logowania. Jeśli w dalszym ciągu wyświetlany będzie ten sam komunikat, należy skontaktować się z administratorem systemu”.

Po odczekaniu kilku minut użytkownik wykonał jeszcze dwie próby i za każdym razem wyświetlany był taki sam komunikat. Użytkownik, próbując się zalogować, stracił 20 minut, po czym zniechęcony skontaktował się z administratorem systemu.

Ćwiczenie 1: Rozwiązywanie problemów związanych z kontami komputera

1. Rozpoznawanie najbardziej prawdopodobnych przyczyn problemu:
 - a. Użytkownik wprowadził nieprawidłową nazwę użytkownika.
 - b. Użytkownik wprowadził nieprawidłowe hasło.
 - c. Na liście okna logowania (Log On To), użytkownik wybrał nieprawidłową domenę.
 - d. Brak kanału bezpieczeństwa pomiędzy komputerem a domeną.
 - e. Uszkodzony został rejestr komputera.
 - f. Zasada komputera zabrania logowania interakcyjnego.

W kontekście opisanego przykładu, najbardziej prawdopodobna przyczyna opisana została w punkcie d — brak kanału bezpieczeństwa pomiędzy komputerem a domeną.

2. Rozpoznawanie etapów procesu rozwiązywania problemu na podstawie listy przedstawionej poniżej. Należy określić prawidłową kolejność etapów. Nie wszystkie etapy są wymagane.
 - a. Włączenie konta komputera.
 - b. Skonfigurowanie komputera Desktop03 tak, aby należał do domeny contoso.com.
 - c. Sprawdzenie, czy konto komputera istnieje w usłudze Active Directory.
 - d. Zerowanie lub ponowne utworzenie konta komputera.
 - e. Skonfigurowanie komputera Desktop03 tak, aby należał do grupy roboczej.
 - f. Usunięcie konta komputera.
 - g. Wyłączenie konta komputera.

Prawidłowa odpowiedź to kroki e, c, d oraz b. Krok e nie musi być wykonany jako pierwszy, wystarczy, że będzie wykonany przed krokiem b. Kolejność kroków c oraz d musi być zachowana i muszą być wykonane przed krokiem b, który jest krokiem ostatnim.

Ćwiczenie 2: Odtwarzanie konta komputera po wystąpieniu problemów

1. Otwórz przystawkę Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory).
2. Kliknij ikonę Find Objects In Active Directory (Znajdź obiekty w usłudze Active Directory) i wyszukaj komputer Desktop03.
3. Komputer Desktop03 pojawi się na liście wyników wyszukiwania, ponieważ był utworzony podczas lekcji 1.
4. Po sprawdzeniu, że konto istnieje, wyzeruj je klikając prawym przyciskiem myszy obiekt komputera Desktop03, a następnie wybierając polecenie Reset Account (Resetuj konto).

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Po okresie rozwoju przedsiębiorstwo utworzyło drugą domenę. W zeszłym tygodniu kilka komputerów zostało przeniesionych ze starej do nowej domeny. Po uruchomieniu przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory), obiekty tych komputerów w dalszym ciągu znajdowały się w starej domenie, a ich ikony oznaczone były czerwonym krzyżykiem „X”. Który kierunek działań będzie najbardziej odpowiedni?
 - a. Włączenie kont
 - b. Wyłączenie kont
 - c. Zerowanie kont
 - d. Usunięcie kont
2. Użytkownik powiadomił, że podczas logowania na monitorze pojawił się komunikat informujący, że komputer nie mógł połączyć się z domeną z powodu wyłączenia kontrolera domeny lub braku konta komputera. Wyszukiwanie konta w przystawce Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) pozwoliło ustalić, że rzeczywiście takie konto nie istnieje. Jakie kroki należy podjąć?
3. Użytkownik powiadomił, że podczas logowania na monitorze pojawił się komunikat informujący, że komputer nie mógł połączyć się z domeną z powodu wyłączenia kontrolera domeny lub braku konta komputera. Wyszukiwanie konta w przystawce Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) pozwoliło ustalić, że konto istnieje i sprawia wrażenie poprawnie działającego konta- Jakiego kroki należy podjąć?

Podsumowanie lekcji

- Podobnie jak użytkownicy, komputery obsługują konta, w tym identyfikatory SID oraz członkostwo grupy. Należy ostrożnie postępować podczas usuwania obiektu konta. Wyłączenie obiektu komputera pozostawia możliwość włączenia komputera, jeśli komputer ten musi być ponownie częścią domeny.
- Problemy dotyczące kont komputerów mówiąc ogólnie są dość oczywiste, dzięki komunikatom, które wskazują na rodzaj problemów związanych z hasłami, kanałem bezpieczeństwa bądź relacjami zaufania.
- Korzystając w czterech reguł opisanych w lekcji 3, można praktycznie rozwiązać dowolny problem związany z kontem komputera.

Zadanie praktyczne

Firma Contoso zdecydowała otworzyć dwie nowe filie: East oraz West. W każdym biurze zakupionych zostało 10 komputerów przeznaczonych dla przedstawicieli handlowych. Przyjęte indeksy dla nowych komputerów przedstawione zostały w poniższej tabeli.

Filia East	Filia West
EB-2841	WB-3748
EB-2842	WB-3749
EB-2843	WB-3750
EB-2844	WB-3751
EB-2845	WB-3752
EB-2846	WB-3753
EB-2847	WB-3754
EB-2848	WB-3755
EB-2849	WB-3756
EB-2850	WB-3757

Zadanie polega na przygotowaniu usługi Active Directory do rozmieszczenia tych komputerów.

Ćwiczenie 1: Utworzenie jednostek organizacyjnych OU

Utwórz dwie jednostki organizacyjne w domenie contoso.com: EastBranch oraz WestBranch. Nazwy wpisz tak, jak zostały przedstawione, bez spacji pomiędzy wyrazami.

Ćwiczenie 2: Utwórz skrypt potrzebny do utworzenia kont komputerów

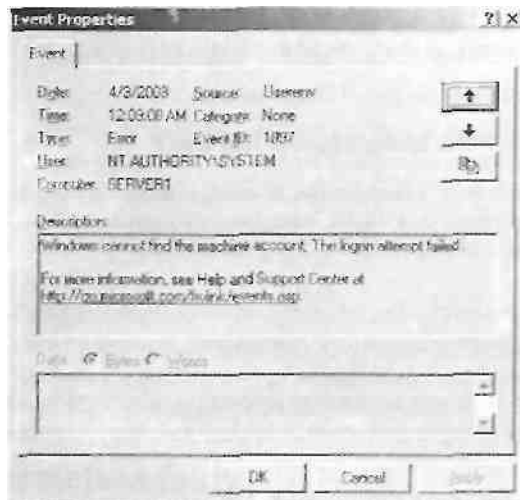
1. Otwórz program Notepad (Notatnik).
2. Dla każdego komputera wpisz wiersz wzorując się na poniższym przykładzie:

```
DSADD COMPUTER ?CN=EB-2841.OU=EastBranch,DC=Contoso,DC=COM? -desc  
?Sales Rep Computer? -loc ?East Branch Office?
```

Należy pamiętać, aby modyfikować parametr *CN=* tak, aby był zgodny z indeksem każdego komputera oraz aby parametry *OU=* i *-loc* odzwierciedlały nazwy i opis lokalizacji filii.
3. Zapisz plik jako „C:\ScriptComputers.bat” i zwróć uwagę, czy nazwa została objęta znakami cudzo-
słowa, gdyż w przeciwnym razie Notatnik automatycznie utworzy plik z rozszerzeniem .txt.
4. Otwórz okno wiersza poleceń i wpisz polecenie c:\scriptcomputers.
5. Przeglądając jednostki organizacyjne EastBranch oraz WestBranch sprawdź, czy konta komputerów zostały poprawnie wygenerowane. Jeśli nowe komputery nie są widoczne, należy nacisnąć klawisz F5, ponieważ konsola MMC nie odświeża automatycznie ekranu.

Rozwiązywanie problemów

Po weekendzie, podczas którego konsultant pracował na komputerach w filii EAST, użytkownicy zaczęli zgłaszać problemy związane z logowaniem. W dzienniku zdarzeń na jednym z komputerów filii zarejestrowane zostało następujące zdarzenie:



Na tej podstawie można sądzić, że problem ma związek z kontem komputera. Które z poniżej wymienionych kroków należy podjąć, aby rozwiązać problem?

1. Usunąć konta komputerów
2. Wyzerować konta użytkowników
3. Przyłączyć komputery do grupy roboczej
4. Wyłączyć konta komputerów
5. Wyzerować konta komputerów
6. Włączyć konta komputerów
- 7- Utworzyć nowe konta komputerów
8. Dołączyć komputery do domeny

Prawidłowa odpowiedź to 5, 3 oraz 8. Jest to najbardziej skuteczne rozwiązanie — wyzerowanie kont komputerów i ponowne ich przyłączenie do domeny.

Ćwiczenie 1 (Opcjonalne): Symulacja problemu

Jeśli w podczas lekcji 1 dołączony został do domeny Contoso dodatkowy komputer, należy go teraz przenieść do jednostki organizacyjnej EastBranch. Następnie, za pomocą przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory), wyzerować konto komputera.

Po ponownym uruchomieniu komputera należy spróbować zalogować się do domeny. Czy ta operacja powiodła się? Czy można zalogować się za pomocą kont domeny Contoso używanych przedtem? Dlaczego? Wskazówka: logowania buforowane.

Czy można zalogować się za pomocą nowego konta domeny, które nigdy przedtem nie było używane do logowania na komputerze? Wykonanie takiej próby powoduje wyświetlenie typowego komunikatu informującego, że konto komputera nie zostało znalezione.

Zaloguj się jako administrator lokalny i przeanalizuj dziennik zdarzeń. Jaki komunikat o błędzie został tam zarejestrowany?

Ćwiczenie 2: Zerowanie wszystkich kont komputerów filii East

Najszybszym sposobem zerowania wszystkich kont komputerów, w szczególności dlatego, że wszystkie konta znajdują się w tej samej jednostce organizacyjnej, będzie zastosowanie narzędzia wiersza poleceń.

1. Otwórz/ okno wiersza poleceń.
2. Wpisz następujące polecenie:

```
DSQUERY COMPUTER ?OU=EastBranch,DC=contoso,DC=com?
```

Polecenie to wyszukuje w usłudze Active Directory komputery jednostki organizacyjnej EastBranch. Powstała lista powinna zgadzać się z listą komputerów utworzonych w zadaniu praktycznym.

3. Wpisz następujące polecenie:

```
DSQUERY COMPUTER ?OU=EastBranch.DC=contoso,DC=com? | DSMOD COMPUTER -  
RESET
```

W tym momencie wyniki polecenia DSQUERY są przekazywane i stanowią informację wejściową dla polecenia DSMOD. Polecenie DSMOD COMPUTER -RESET wyzeruje każde konto, czyli zadanie zostało wykonane.

Ćwiczenie 3 (Opcjonalne): Ponowne przyłączenie do domeny

W poprzednim ćwiczeniu wyzerowane zostało konto komputera dodatkowego. Teraz można w praktyce przeprowadzić operację usunięcia komputera z domeny poprzez przeniesienie jego członkostwa do grupy roboczej. Po ponownym uruchomieniu komputera należy ponownie przyłączyć komputer do domeny.

Podsumowanie rozdziału

- Aby utworzyć obiekt komputera w usłudze Active Directory, należy mieć odpowiednie uprawnienia. Uprawnienia takie mają członkowie grup Administrators (Administratorzy) oraz Account Operators (Operatorzy kont). Uprawnienia te mogą zostać przekazane innym użytkownikom bądź grupom.
- Po utworzeniu obiektu komputera można wyspecyfikować, który użytkownik lub grupa może przyłączyć komputer do domeny za pomocą tego konta.

- Przystawka Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) umożliwia tworzenie, modyfikowanie, usuwanie, włączanie, wyłączanie i zerowanie obiektów komputera.
- Za pomocą rozkazu DSADD Computer można w wierszu poleceń utworzyć obiekt komputera oraz modyfikować jego właściwości.
- Polecenie DSMOD Computer jest również używane do zerowania, wyłączania i włączania obiektu komputera. Polecenie DSRM usuwa obiekt komputera. Program narzędziowy NETDOM wyposażony jest w szereg przełączników, dzięki którym można wykonywać podobne zadania.
- Najczęściej stosowane sposoby rozwiązywania problemów związane z odtwarzaniem kont komputera to ponowne utworzenie lub zerowanie konta komputera, usunięcie komputera z domeny oraz ponowne przyłączenie komputera do domeny.

Informacje dla zdających egzamin

Przed przystąpieniem do egzaminu należy zapoznać się z przedstawionymi poniżej najważniejszymi faktami i pojęciami, aby określić, które tematy wymagają pogłębienia. Należy powrócić do lekcji, aby osiągnąć większą wprawę oraz przejrzeć działy znajdujące się w części 2 — „Materiały dodatkowe”. Informacje tu zawarte kierują do materiałów uzupełniających tematy objęte zadaniami egzaminacyjnymi.

Najważniejsze fakty

- Identyfikacja minimalnych uprawnień wymaganych do utworzenia obiektu komputera w usłudze Active Directory oraz uprawnień wymaganych do zmiany członkostwa komputera pomiędzy domeną a grupą roboczą.
- Znajomość składni poleceń DSADD, DSMOD oraz DSRM. Warto zapamiętać, że do stosowania poleceń DSMOD oraz DSADD wymagane jest użycie jako parametrów jednej lub kilku nazw wyróżniających. Do sporządzenia listy tych parametrów (nazw) może być wykorzystywane polecenie DSQUERY.
- Zrozumienie różnic pomiędzy wyłączaniem, zerowaniem i usuwaniem kont komputerów. Jaki jest wpływ każdej z tych czynności na obiekt komputera, jego identyfikator SID, członkostwo w grupach oraz na sam system?
- Znajomość czterech reguł rozwiązywania problemów związanych z kontami komputerów. Zawsze należy stosować wszystkie cztery reguły, co pozwoli rozwiązać prawie każdy problem dotyczący konta komputera.
- Należy dobrze opanować sposoby wyszukiwania obiektów w usłudze Active Directory, a także metody zarządzania wyszukanymi obiektami. Umiejętności te dotyczą wielu obiektów usługi Active Directory i szeregu zadań podczas egzaminu certyfikującego.

Najważniejsze pojęcia

Konto komputera Utworzone w usłudze Active Directory konto jednoznacznie identyfikujące komputer w domenie.

Pytania i odpowiedzi

155 Pytania do lekcji 1

1. Jaka *minimalna* tożsamość musi użytkownik poświadczyć, aby mógł utworzyć konto komputera systemu Windows Server 2003 w jednostce organizacyjnej domeny? Należy rozważyć wszystkie kroki procesu przy założeniu, że konto tego komputera nie było wcześniej utworzone w usłudze w Active Directory.
 - a. Domain Admins (Administratorzy domeny)
 - b. Enterprise Admins (Administratorzy przedsiębiorstwa)
 - c. Administrators on a domain controller (Administratorzy kontrolera domeny)
 - d. Account Operators on a domain controller (Operatorzy kont kontrolera domeny)
 - e. Server Operators on a domain controller (Operatorzy serwerów kontrolera domeny)
 - f. Account Operators on the server (Operatorzy kont serwera)
 - g. Server Operators on the server (Operatorzy serwera, na danym serwerze)
 - h. Administrators on the server (Administratorzy serwera)

Prawidłowa odpowiedź to d oraz h. Członkowie grupy Account Operators (Operatorzy kont) kontrolera domeny mają przydzielone minimalne uprawnienia potrzebne do utworzenia w domenie obiektu komputera. Aby zmienić członkostwo domeny konta komputera, trzeba być członkiem grupy administratorów lokalnych serwera.

2. W którym miejscu można zmienić członkostwo domeny komputera systemu Windows Server 2003?
 - a. Właściwości modułu My Computer (Mój komputer)
 - b. Moduł System w programie Control Panel (Panel sterowania)
 - c. Przystawka Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory)
 - d. Folder Network Connections (Połączenia sieciowe)
 - e. Moduł Users (Użytkownicy) w programie Control Panel (Panel sterowania)

Prawidłowe odpowiedzi to a, b oraz d.

- 3- Za pomocą którego programu narzędziowego wiersza poleceń można utworzyć w usłudze Active Directory konto komputera domeny?
 - a. NETDOM
 - b. DSADD
 - c. DSGET
 - d. NETSH
 - e. NSLOOKUP

Prawidłowe odpowiedzi to a oraz b.

Pytania do lekcji 2

1. Która platforma umożliwia przyłączenie do domeny?

- a. Windows 95
- b. Windows NT 4
- c. Windows 98
- d. Windows 2000
- e. Windows Me
- f. Windows XP
- g. Windows Server 2003

Prawidłowe odpowiedzi to b, d, f oraz g.

2. Po otwarciu obiektu komputera, na zakładce Operating System (System operacyjny) nie są wyświetlane żadne właściwości. Co może być tego przyczyną?

Komputer nie przyłączył się do domeny za pomocą tego konta. Domyślne ustawienia określają, że po przyłączeniu systemu do domeny, jego właściwości są umieszczane na zakładce Operating System (System operacyjny).

3. Dyrektor ma komputer przenośny nazwany „TopDog”, działający pod kontrolą systemu Windows XP. Należy umożliwić dołączenie tego komputera do domeny oraz zapewnić, że konfiguracja tego komputera będzie bezpośrednio określana przez zasady grupy powiązane z jednostką organizacyjną Desktops. W jaki sposób można zrealizować takie zadanie?

Dla komputera TopDog należy utworzyć obiekt komputera w jednostce organizacyjnej Desktops. Podczas tworzenia konta należy w polu opcji The Following User Or Group Can Join This Computer To A Domain (Poniższy użytkownik lub grupa może przyłączyć ten komputer do domeny) wybrać konto użytkownika dyrektora.

4. Dlaczego zalecaną praktyką jest utworzenie obiektu komputera *przed* przyłączeniem komputera do domeny?

Jest kilka powodów, dlaczego w domenie warto utworzyć konto komputera przed przyłączeniem komputera do domeny. Pierwszy powód dotyczy faktu, że jeżeli konto nie zostanie wcześniej utworzone, to podczas dołączania komputera do domeny konto zostanie automatycznie wygenerowane i umieszczone w domyślnym kontenerze nazwanym Computers (Komputery). W rezultacie zasady komputera, które najczęściej są powiązane z określoną jednostką organizacyjną, nie będą stosowane do dołączonego komputera. Oprócz tego, ponieważ większość organizacji tworzy specjalne jednostki organizacyjne dla komputerów, po przyłączeniu do domeny trzeba będzie wykonać dodatkowy krok: przeniesienie obiektu komputera do odpowiedniej jednostki organizacyjnej. W końcu, dzięki wcześniejszemu utworzeniu obiektu komputera można wyspecyfikować, które grupy (lub użytkownicy) mogą za pomocą tego konta dołączać komputer do domeny. Krótko mówiąc, podejście takie jest bardziej elastyczne oraz zapewnia większą kontrolę podczas instalowania komputerów.

Pytania do lekcji 3

1. Po okresie rozwoju przedsiębiorstwo utworzyło drugą domenę. W zeszłym tygodniu, kilka komputerów zostało przeniesionych ze starej do nowej domeny. Po uruchomieniu przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory), obiekty tych

komputerów w dalszym ciągu znajdowały się w starej domenie, a ich ikony oznaczone były czerwonym krzyżykiem „X”. Który kierunek działań będzie najbardziej odpowiedni?

- a. Włączenie kont
- b. Wyłączenie kont
- c. Zerowanie kont
- d. Usunięcie kont

Prawidłowa odpowiedź to d. Podczas przesuwania komputera do innej domeny, konto jego nie zostało usunięte, prawdopodobnie ze względu na ustawienia uprawnień. Obecnie komputer należy do innej domeny, a konto nie jest już potrzebne.

2. Użytkownik powiadomił, że podczas logowania na monitorze pojawił się komunikat informujący, że komputer nie mógł połączyć się z domeną z powodu wyłączenia kontrolera domeny lub braku konta komputera. Wyszukiwanie konta w przystawce Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) pozwoliło ustalić, że rzeczywiście takie konto nie istnieje. Jakie kroki należy podjąć?

Utworzyć konto komputera, odłączyć komputer użytkownika od domeny, a następnie ponownie go przyłączyć.

3. Użytkownik powiadomił, że podczas logowania na monitorze pojawił się komunikat informujący, że komputer nie mógł połączyć się z domeną z powodu wyłączenia kontrolera domeny lub braku konta komputera. Wyszukiwanie konta w przystawce Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) pozwoliło ustalić, że konto istnieje i sprawia wrażenie poprawnie działającego konta. Jakie kroki należy podjąć?

Wyzerować konto komputera, odłączyć komputer użytkownika od domeny, a następnie ponownie go przyłączyć.

6 Pliki i foldery



Zadania egzaminacyjne omawiane w tym rozdziale:

- Konfigurowanie dostępu do współdzielonych folderów »
Zarządzanie uprawnieniami udostępnionych folderów
- Konfigurowanie uprawnień systemu plików » Sprawdzanie uprawnień
czynnych po przydzieleniu uprawnień » Przejmowanie własności
plików lub folderów
- Rozwiązywanie problemów związanych z dostępem do plików i udostępnionych folderów.
- Zarządzanie serwerem sieci Web
» Zarządzanie programem Internet Information Services (Internetowe usługi informacyjne) »
Zarządzanie zabezpieczeniami programu IIS (Internet Information Services)

Cele rozdziału

Wiele zadań, spośród codziennych czynności administratora, dotyczy obsługi plików i folderów w sieci, czyli zasobów potrzebnych użytkownikom każdej organizacji. Jeśli użytkownik nie może uzyskać dostępu do potrzebnych mu zasobów, kontaktuje się z działem wsparcia technicznego. W rezultacie, aby rozwiązać problem, administrator modyfikuje uprawnienia lub członkostwo grupy tracąc czas i pieniądze. Jeśli natomiast dostęp do ważnych danych uzyskuje nieupoważniona osoba, do działu wsparcia technicznego również zadzwoni telefon, a administrator straci czas i pieniądze szukając nowej pracy.

Z pewnością każdy administrator miał do czynienia z podstawowymi elementami zabezpieczeń zasobów dostępnych w systemach Windows, czyli z przydzielaniem grupom lub użytkownikom uprawnień dostępu. System Microsoft Windows Server 2003 w porównaniu do systemów Windows 2000 i Windows XP wyposażony został w ulepszone narzędzia i funkcje, natomiast w porównaniu do systemu Windows NT 4 są to zupełnie inne rozwiązania. Te wszystkie dodatkowe możliwości wymagają większej praktyki w zarządzaniu i rozwiązywaniu problemów dotyczących plików i folderów.

W niniejszy rozdziale omówione zostaną pojęcia i umiejętności związane z zarządzaniem udostępnionymi folderami oraz przeanalizowane zostaną możliwości przystawki Shared Folders (Foldery udostępnione). Czytelnik zostanie zapoznany z edytorem ACL (Access Control List Editor), jego wieloma oknami dialogowymi, za pomocą których można obsługiwać ważne funkcje. Po analizie kilku konfiguracji uprawnień, sprawdzane będą *uprawnienia czynne*, czyli zestaw uprawnień użytkownika wynikający z sumy uprawnień obiektu użytkownika i grupy, a następnie konfigurowane będą funkcje inspekcji pozwalające monitorować operacje i dostęp do danego pliku. Na koniec omówione zostaną usługi IIS, które podobnie jak usługi File and Print Sharing (Udostępnianie plików i drukarek), umożliwiają w sieci dostęp do plików i folderów.

Lekcje rozdziału:

- Lekcja 1: Konfiguracja folderów udostępnionych..... 177
- Lekcja 2: Konfiguracja uprawnień systemu plików 187
- Lekcja 3: Inspekcja dostępu do systemu plików 205
- Lekcja 4: Administracja IIS (Internet Information Services) 212

Wymagania

W rozdziale tym prezentowane są umiejętności i pojęcia dotyczące kont komputerów usługi katalogowej Microsoft Active Directory. Jeśli student chciałby przeprowadzić ćwiczenia praktyczne w oparciu o prezentowane w rozdziale przykłady i ćwiczenia, powinien przygotować następujące elementy:

- Komputer z zainstalowanym systemem Windows Server 2003 (Standard Edition lub Enterprise Edition). Serwer powinien zostać nazwany Server01 i skonfigurowany jako kontroler domeny w domenie contoso.com.
- Jednosdci organizacyjne pierwszego poziomu to: Security Groups oraz Employees.
- Grupa *Domain Users* (Użytkownicy domeny) musi być członkiem grupy *Print Operators* (Operatorzy drukowania), dzięki czemu podczas ćwiczeń „zwykli” użytkownicy będą mogli logować się w kontrolerze domeny.
- Pięć lokalnych grup zabezpieczeń domeny utworzonych w jednostce organizacyjnej Security Groups: Project 101 Team, Project 102 Team, Engineers, Managers oraz Project Contractors.
- Konta użytkowników utworzone w jednostce organizacyjnej Employees: Scott Bishop, Danielle Tiedt oraz Lorrin Smith-Bates, przy czym Scott Bishop należy do grup Engineers, Project Contractors oraz Project 101 Team, Danielle Tiedt należy do grup Engineers oraz Project 101 Team, a Lorrin Smith-Bates należy do grup Managers oraz Project 101 Team.
- Dostęp do przystawki *Shared Folders* (Foldery udostępnione) za pośrednictwem konsoli *Computer Management* (Zarządzanie komputerem), konsoli *File Server Management* (Zarządzanie serwerem plików), która udostępniana jest w programie *Manage Your Server* (Zarządzanie tym serwerem) lub niestandardowej konsoli MMC.

Lekcja 1: Konfiguracja folderów udostępnionych

Nie istniałyby sieci, a administratorzy nie mieliby pracy, jeśli nie byłoby potrzebne udostępnianie informacji pomiędzy komputerami użytkowników w przedsiębiorstwach. Dlatego też tworzenie udostępnionych folderów umożliwiających taki dostęp jest podstawowym zadaniem każdego administratora sieci. Foldery udostępnione w systemie Windows Server 2003 są zarządzane przez przystawkę *Shared Folders* (Foldery udostępnione).

Materiały omówione podczas lekcji pozwalają na

- Utworzenie udostępnionego foldera za pomocą programu Windows Explorer (Eksplorator Windows) oraz przystawki Shared Folders (Foldery udostępnione)
- Konfigurowanie uprawnień i innych właściwości folderów udostępnionych
- Zarządzanie sesjami użytkownika i otwartymi plikami

Szacunkowy czas lekcji: 15 minut

Udostępnianie foldera

Udostępnianie foldera konfiguruje usługę *File And Printer Sharing For Microsoft Networks* (Udostępnianie plików i drukarek w sieci Microsoft Networks), nazywaną również usługą serwera, tak aby klienci programu *Client For Microsoft Networks* (nazywanego także usługą stacji roboczej) mogli w sieci uzyskiwać dostęp do danego foldera i jego podfolderów. Z pewnością każdy administrator udostępniał folder za pomocą programu *Windows Explorer* (Eksplorator Windows) — kliknięcie foldera prawym przyciskiem myszy, wybranie polecenia *Sharing And Security* (Udostępnianie i zabezpieczenia), a następnie opcji **Share This Folder** (Udostępnij ten folder).

Jednakże zakładka *Sharing* (Udostępnianie) znajdująca się w oknie dialogowym właściwości foldera dostępna jest tylko, jeśli zasób jest udostępniany podczas sesji przy użyciu logowania interakcyjnego lub za pomocą usług terminalowych. Dla systemu *zdalnego* nie jest możliwe udostępnienie foldera za pomocą programu Windows Explorer. Z tego powodu, analiza tworzenia, właściwości, konfiguracji oraz zarządzania foldera udostępnionego będzie przeprowadzana przy użyciu przystawki *Shared Folders* (Foldery udostępnione), która może być wykorzystywana zarówno dla lokalnego, jak i dla zdalnego systemu.

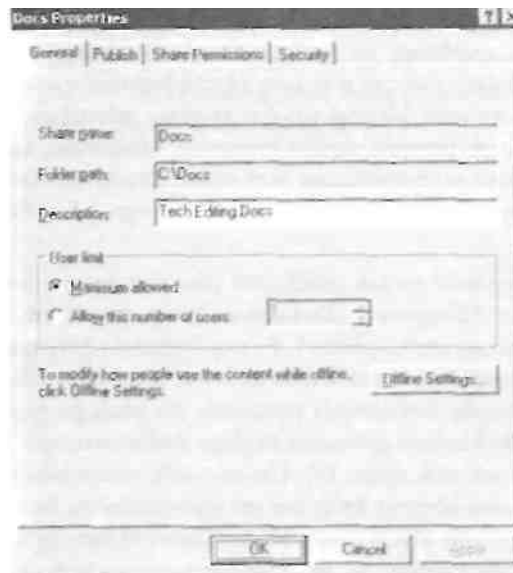
Przystawkę *Shared Folders* (Foldery udostępnione) można uruchomić jako element niestandardowej konsoli MMC, jako część konsoli *Computer Management* (Zarządzanie komputerem) lub jako część konsoli *File Server Management* (Zarządzanie serwerem plików). Po uruchomieniu przystawki, warto zwrócić uwagę, że niektóre foldery administracyjne systemu Windows Server 2003 są już udostępnione (ustawienia domyślne). Te współdzielone zasoby umożliwiają połączenie do katalogu systemu (najczęściej jest to C:\Windows), jak również do katalogu głównego każdego dysku twardego. W nazwie tych zasobów udostępnionych umieszczany jest znak dolara (\$). Umieszczenie znaku dolara na końcu nazwy powoduje, że zasób ten staje się *udziałem ukrytym*, który nie jest wyświetlany na listach przeglądarek, można natomiast dołączyć się do niego przy użyciu nazwy UNC (*Universal Naming Convention*) w postaci `\\servername\sharename$`. Do udostępnionego zasobu administracyjnego mogą dołączyć się jedynie administratorzy.

Aby udostępnić folder komputera, należy dołączyć się do komputera za pomocą przystawki **5/Wl Folders** (Foldery udostępnione) poprzez kliknięcie prawym przyciskiem myszy węzła głównego przystawki i wybranie polecenia **Connect To Another Computer** (Podłącz do innego komputera). Po wskazaniu w przystawce komputera, należy kliknąć węzeł **Shares** (Udziały) i z menu skrótów lub z menu **Action** (Akcja) wybrać polecenie **New Share** (Nowy udział). Najważniejsze strony kreatora udostępniania foldera określające ustawienia udziałów **to**:

- **Strona Folder Path (Ścieżka foldera)** W oknie tym wpisywana jest ścieżka foldera dla *lokalnej napędu dysku*. Jeśli więc folder umieszczony jest na napędzie D serwera, ścieżka do tego foldera ma postać D:\nazwa foldera.
- **Strona Name (Nazwa), Description (Opis) i Settings (Ustawienia)** W oknie tym wpisywani jest nazwa udziału. Jeśli w sieci używane są programy klienckie niskiego poziomu (jak na przykład dla systemu DOS), należy pamiętać, aby zachować konwencję nazewnictwa 8.3 pozwalającą starszym programom uzyskiwać dostęp do tych zasobów. Nazwa udziału będzie tworzyła nazw[^] UNC zasobu w postaci \\nazwa_serwera\nazwa_udzialu. Dodanie znaku dolara na końcu nazwy powoduje, że zasób ten będzie udziałem ukrytym. Inaczej niż w przypadku wbudowanych udziałów administracyjnych, do ręcznie utworzonych udziałów mogą przyłączać się użytkownicy, a ograniczeniem jest jedynie posiadanie odpowiednich uprawnień.
- **Strona Permissions (Uprawnienia)** Na tej stronie określone są uprawnienia do danego udziału.

Zarządzanie folderem udostępnionym

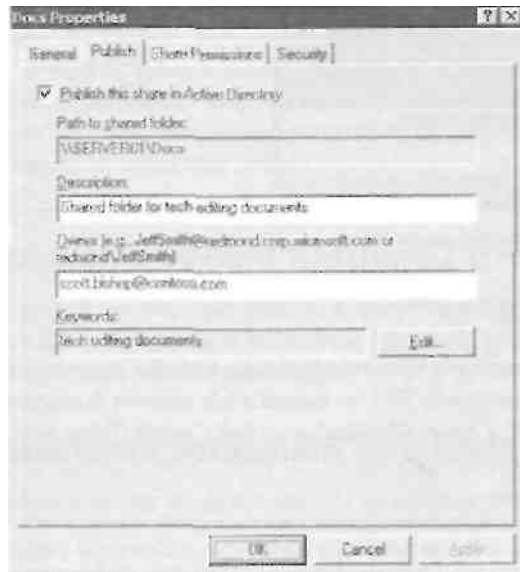
W węźle *Shares* (Udziały) przystawki *Shared Folders* wyświetlana jest lista wszystkich udziałów danego komputera oraz dla każdego udziału udostępnione jest menu kontekstowe, za pomocą którego można zakończyć udostępnianie foldera, otworzyć udział w oknie programu Windows Explorer lub skonfigurować właściwości udziału. Wszystkie właściwości, które były określane w oknach programu *Shm A Folder Wizard* (Kreator udostępniania foldera), można modyfikować w oknie dialogowym *Properties* (Właściwości) danego udziału. Na rysunku 6-1 przedstawione zostało omawiane okno dialogowe.



Rysunek 6-1 Zakładka General (Ogólne) foldera udostępnionego

W oknie *Properties* (Właściwości) umieszczone zostały następujące zakładki:

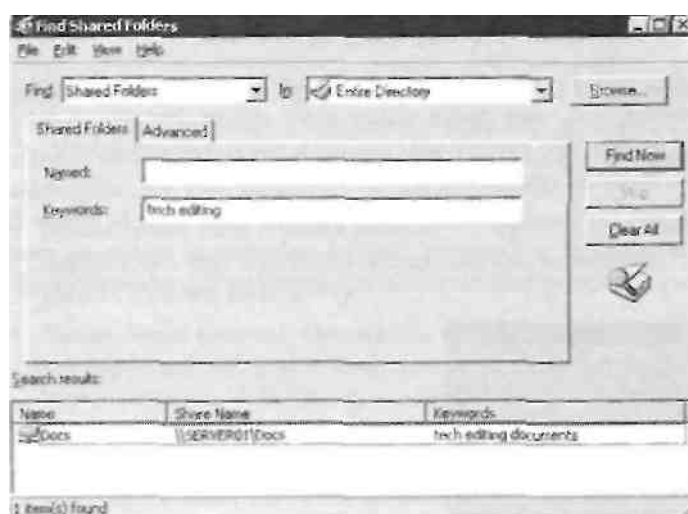
- **General (Ogólne)** Pierwsza zakładka umożliwia dostęp do nazwy udziału, ścieżki foldera, opisu, liczby jednoczesnych połączeń oraz ustawień dla plików trybu offline. Nie można modyfikować nazwy udziału oraz ścieżki foldera. Aby zmienić nazwę udziału, należy najpierw zakończyć udostępnianie foldera, a następnie utworzyć udział nadając mu nową nazwę.
- **Publish (Publikowanie)** Jeśli zaznaczona zostanie opcja **Publish This Share In Active Directory** (Publikuj ten udział w usłudze Active Directory), tak jak pokazane to zostało na rysunku 6-2, w usłudze Active Directory utworzony zostanie obiekt reprezentujący ten udostępniony folder.



Rysunek 6-2 Zakładka *Publish* (Publikowanie) foldera udostępnionego

We właściwościach obiektu możliwe jest określanie opisu i słów kluczowych. Dzięki temu, za pomocą okna dialogowego *Find Users, Contacts and Groups* (Wyszukaj użytkowników, kontakty i grupy), administrator może zlokalizować folder udostępniony bazując na jego opisie lub słowie kluczowym. W tym oknie dialogowym można również z menu rozwijanego wybrać opcję **Shared Folders** (Foldery udostępnione), co przekształca je w okno *Find Shared Folders* (Znajdowanie: Foldery udostępnione), tak jak przedstawione to zostało na rysunku 6-3.

- **Share Permissions (Uprawnienia do udziału)** Zakładka ta umożliwia konfigurowanie uprawnień do udziału.
- **Security (Zabezpieczenia)** Zakładka ta umożliwia skonfigurowanie uprawnień NTFS dla folderu.



Rysunek 6-3 Wyszukiwanie foldera udostępnionego

Konfigurowanie uprawnień udziału

W tabeli 6-1 przedstawiona została lista dostępnych uprawnień udziału. Choć uprawnienia udziału nie są tak szczegółowo określone, jak uprawnienia NTFS, to można z ich pomocą konfigurować trzy podstawowe rodzaje dostępu: *Read* (Odczyt), *Change* (Zmiana) oraz *Full Control* (Pełna kontrola).

Tabela 6-1. Uprawnienia udziału

Uprawnienia	Opis
Read (Odczyt)	Użytkownicy mogą wyświetlić nazwy folderów, nazwy plików, dane plików oraz atrybuty. Użytkownicy mogą również uruchamiać pliki programów i uzyskiwać dostęp do podfolderów foldera udostępnionego. Użytkownicy mogą tworzyć foldery, dodawać pliki do folderów, zmieniać dane plików, dodawać dane do plików, zmieniać atrybuty plików, usuwać foldery i pliki oraz wykonywać czynności dopuszczone dla uprawnień Odczyt. Użytkownicy mogą zmieniać uprawnienia plików, stać się właścicielem plików oraz wykonywać czynności dopuszczone dla uprawnień Zmiana.
Change (Zmiana)	
Full Control (Pełna kontrola)	

Można zezwalać lub odmawiać przydzielania uprawnień do udziału. Efektywny zestaw uprawnień udziału jest sumą uprawnień *Allow* (Zezwalaj) przydzielonych użytkownikowi i grupom, do których użytkownik należy. Na przykład, jeśli użytkownik jest członkiem grupy mającej uprawnienia *Read* (Odczyt) oraz jest też członkiem innej grupy mającej uprawnienia *Change* (Zmiana), to uprawnienia czynne określone będą jako Zmiana. Trzeba jednak pamiętać, że odmowa uprawnień (*Deny*) unieważnia uprawnienie *Allow* (Zezwalaj). Tak więc, jeśli użytkownik jest członkiem grupy, która ma uprawnienia do odczytu oraz jest członkiem innej grupy, dla której odmówiono uprawnień *Full Control* (Pełna kontrola), to użytkownik nie będzie mógł odczytać plików i folderów tego udziału.

Uprawnienia udziału definiują *maksymalne* uprawnienia czynne dla wszystkich plików i folderów umieszczonych poniżej foldera udostępnionego. Uprawnienia do poszczególnych plików czy folderów mogą być jeszcze bardziej ograniczane poprzez uprawnienia NTFS, uprawnienia nie mogą być jednak rozszerzane. Inaczej mówiąc, dostęp użytkownika do pliku lub foldera jest zestawem najsłabszych uprawnień wynikających z uprawnień czynnych do udziału i uprawnień NTFS do zasobu. Jeśli chcemy utworzyć grupę mającą pełną kontrolę do foldera i grupa ta ma pełne uprawnienia przydzielone poprzez uprawnienia NTFS, natomiast uprawnienia udziału są domyślne (grupa Wszyscy, zezwalaj na odczyt) lub nawet uprawnienia udziału określone zostały jako Zmiana, to i tak pełne uprawnienia NTFS zostaną ograniczone przez uprawnienia udziału. Mechanizm ten oznacza, że uprawnienia udziału tworzą dodatkową warstwę złożoności zarządzania dostępem do zasobu i jest to jeden z powodów, dla których często w przedsiębiorstwach określane są pełne uprawnienia do udziałów (Wszyscy: Zezwalaj na pełną kontrolę), a do zabezpieczeń folderów lub plików używane są jedynie uprawnienia NTFS. Informacje zamieszczone w poniższej sekcji „Uprawnienia udziału widziane z trzech perspektyw” są źródłem dodatkowej wiedzy, wychodzącej poza zaplanowany dla tego rozdziału zakres dyskusji dotyczącej uprawnień udziału.

Uprawnienia udziału widziane z trzech perspektyw

Ważną sprawą jest ocena perspektyw, z których wynika podejście do uprawnień udziałów przyjęte w rzeczywistych implementacjach przez firmę Microsoft, podejście przyjęte przez zadania egzaminacyjne oraz przez zasoby takie jak niniejsza książka.

Ograniczenia uprawnień do udziału

Uprawnienia udziału mogą być istotnie ograniczane, przy uwzględnieniu następującego podziału:

- **Zakres** Uprawnienia do udziału stosują się tylko do dostępu w sieci za pośrednictwem programów Client for Microsoft Networks (Klient sieci Microsoft Networks). Nie stosują się natomiast do określania dostępu lokalnego bądź poprzez usługi terminalowe dla plików lub folderów czy innych typów dostępu do sieci, takich jak protokoły Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Telnet itp.
- **Replikacja** Uprawnienia do udziału nie są replikowane poprzez usługi replikacji plików FRS.
- **Sprężystość** Uprawnienia do udziału nie są dołączane do wolumenów kopii zapasowych i odtwarzania.
- **Nietrwałość** Uprawnienia do udziału znikają, jeśli folder udostępniony zmieni nazwę lub zostanie przesunięty.
- **Brak dokładnej kontroli** Uprawnienia do udziału nie mają charakteru szczegółowego, stosują się do wszystkich plików i folderów umieszczonych poniżej udziału. Nie można rozszerzać dostępu do foldera lub pliku umieszczonego poniżej udziału, a także nie można ograniczać tego dostępu bez włączenia uprawnień NTFS.
- **Inspekcja** Nie można konfigurować inspekcji w oparciu o uprawnienia do udziału.
- **„Wszędzie dobrze, gdzie nas nie ma”** System wyposażony jest w uprawnienia NTFS, które umożliwiają dobrą i bezpieczną kontrolę dostępu do plików i folderów. Uprawnienia NTFS replikują się,

ciąg dalszy na następnej stronie

ciąg dalszy ze strony poprzedniej

dołączane są do wolumenów kopii zapasowych i odtwarzania, mogą być poddawane inspekcji oraz umożliwiają niezwykle elastyczne i proste zarządzanie. I dlatego organizacje opierają kontrole dostępu do zasobów na uprawnieniach NTFS.

- **Złożoność** Jeśli stosowane są zarówno uprawnienia do udziału, jak i NTFS, najsłabsze uprawnienia stają się uprawnieniami czynnymi. Stanowi to podniesienie poziomu złożoności analizy uprawnień czynnych i rozwiązywania problemów dotyczących dostępu do plików.

Praktyczne wykorzystywanie uprawnień do udziałów

Ze względu na swoje ograniczenia, z uprawnień do udziału korzysta się rzadko, najczęściej wtedy, gdy wykorzystywane są wolumeny FAT lub FAT32, które nie obsługują uprawnień NTFS. Inaczej mówiąc, „praktyka” zaleca stosowanie reguły — skonfigurowanie pełnych uprawnień do udziału dla grupy Everyone (Wszyscy) oraz blokowanie udostępnionych folderów i ich podfolderów za pomocą uprawnień NTFS.

Zawężenie uprawnień do udziału wprowadzone przez firmę Microsoft

Przed wprowadzeniem systemu Windows XP, domyślne uprawnienia do udziału były następujące Everyone: Allow Full Control (Wszyscy: Zezwalaj na pełną kontrolę). Korzystanie w praktyce z takich ustawień domyślnych było oczywiste: administratorzy nie zmieniali uprawnień udziału, ale bezpośrednio przechodzili do konfigurowania uprawnień NTFS. W systemie Windows Server 2003 domyślne ustawienia uprawnień do udziału są inne: Everyone: Allow Read (Wszyscy: Zezwalaj na odczyt) oraz Administrators: Allow Full Control (Administratorzy: Zezwalaj na pełną kontrolę). Jest to problematyczne, ponieważ dla wszystkich użytkowników, poza administratorami, cały udostępniony folder może być jedynie odczytywany.

Firma Microsoft wprowadziła te zmiany mając na uwadze szlachetny cel: poprawę bezpieczeństwa poprzez ograniczenie uprawnień domyślnych przydzielonych podczas tworzenia udziału. Wielu administratorów, po utworzeniu foldera udostępnionego, zapominało włączyć uprawnienia NTFS lub robiło to za późno, przez co uprawnienia były zbyt mało restrykcyjne. Nowe ustawienia domyślne do udostępnionych zasobów zezwalające tylko na odczyt pozwalają administratorom unikać takich problemów. Niestety większość organizacji, ze względu na ograniczenia uprawnień do udziałów, unika ich stosowania, a zamiast tego, konfiguracja zabezpieczeń opierana jest na uprawnieniach NTFS. Obecnie administratorzy muszą pamiętać, aby przydzielać pełną kontrolę dla udziałów (Wszyscy: Zezwalaj na pełną kontrolę), co pozwoli powrócić do stosowania dobrej praktyki wprowadzonej wcześniej w przedsiębiorstwie.

Zadania certyfikujące

Jest to trzecia perspektywa dotycząca uprawnień udziałów, czyli zadania certyfikujące. Pomimo, że uprawnienia do udziałów są najczęściej wprowadzane w ścisłym związku z zasadami przedsiębiorstwa (Wszyscy: Zezwalaj na pełną kontrolę), to fakt, że uprawnienia mogą chociaż przez jeden dzień odbiegać od tych ustawień oraz że dane mogą być przechowywane na wolumenach FAT lub FAT32 (dla których

ciąg dalszy na następnej stronie

ciąg dalszy ze strony poprzedniej

uprawnienia udziału są jedyną opcją kontroli dostępu) oznacza, że należy dobrze opanować zagadnienia uprawnień udziałów, aby wykonać zadania egzaminów MCSA i MCSE. Szczególnie ważne są przykłady, w których do zasobu stosowane są zarówno uprawnienia udziałów, jak i uprawnienia NTFS. W takich przypadkach, w momencie uzyskiwania dostępu do zasobu przez usługę Client For Microsoft Networks (Klient sieci Microsoft Networks), zestaw najsłabszych uprawnień staje się uprawnieniami czynnymi tego zasobu.

Tak więc warto zwrócić uwagę na uprawnienia do udziałów i na występujące pomiędzy nimi niuanse. Należy znać sposoby oceny uprawnień czynnych w połączeniu z uprawnieniami NTFS. Dopiero następnie konfigurować udostępnione zasoby zgodnie z zasadami przedsiębiorstwa, które prawdopodobnie będą inne (Wszyscy: Zezwalaj na pełną kontrolę) niż domyślne ustawienia uprawnień do udziałów systemu Windows Server 2003-

Zarządzanie sesjami użytkownika i otwartymi plikami

Czasami zdarza się, że serwer musi zostać wyłączony ze względu na konserwację, wykonywanie kopii zapasowych lub wykonywanie innych zadań wymagających odłączenia użytkowników oraz zamknięcia otwartych bądź zablokowanych plików. W każdej z tych sytuacji używana będzie przystawka *Shared Folders* (Foldery udostępnione).

Węzeł *Sessions* (Sesje) przystawki *Shared Folders* (Foldery udostępnione) umożliwia monitorowanie liczby użytkowników przyłączonych do konkretnego serwera oraz jeśli zachodzi taka potrzeba, umożliwia odłączanie użytkowników od serwera. Węzeł *Open Files* (Otwarte pliki) dla pojedynczego serwera wyświetla listę wszystkich otwartych i zablokowanych plików oraz pozwala zamknąć jeden otwarty plik i odłączyć wszystkie otwarte pliki.

Przed wykonaniem którejkolwiek z podanych czynności warto powiadomić użytkownika, że zostanie odłączony, dzięki czemu użytkownik będzie miał czas na zapisanie swoich opracowywanych informacji. Wiadomość można wysłać klikając prawym przyciskiem myszy węzeł *Shares* (Udziały). Wiadomości są wysyłane za pośrednictwem usługi *Messenger Service* (Posłaniec), przy czym używana jest nazwa komputera, a nie nazwa użytkownika. Ustawienia domyślne systemu Windows Server 2003 określają, że usługa *Messenger* (Posłaniec) jest wyłączona. Usługa *Messenger* musi zostać uruchomiona automatycznie lub ręcznie, zanim z komputera zostanie wysłana wiadomość konsoli.

Zadanie kontrolne: Konfiguracja folderów udostępnionych

W zadaniu tym zostanie skonfigurowany folder udostępniony oraz zostaną zmodyfikowane właściwości udziału. Następnie przeprowadzona zostanie próba przyłączenia się do tego udziału i symulacja procedury wykonywanej przed wyłączeniem serwera.

Ćwiczenie 1: Udostępnianie foldera

1. Na dysku C utwórz folder nazwany Docs. W tym momencie *nie* musi on być udostępniany.
2. Otwórz stronę programu *Manage Your Server* (Zarządzanie serwerem) znajdującego się w grupie programów *Administrative Tools* (Narzędzia administracyjne).

3. W kategorii *File Server* (Serwer plików) kliknij opcję **Manage This File Server** (Zarządzaj tym serwerem plików). Jeśli serwer nie był skonfigurowany jako serwer plików, dodaj tę rolę lub uruchom konsolę **File Server Management** (Zarządzanie serwerem plików) zgodnie z poniższą wskazówką.



Wskazówka Konsola File Server Management (Zarządzanie serwerem plików) jest bardzo przydatnym narzędziem i warto utworzyć skrót pozwalający na szybszy dostęp do konsoli. Ścieżka do konsoli jest następująca: %SystemRoot%\System32 \Filesrv.msc.

4. Zaznacz węzeł **Shares** (Udziały).
5. Z listy zadań okna szczegółów wybierz polecenie **Add A Shared Folder** (Dodaj nowy folder). Tę samą czynność można wykonać wybierając odpowiednie polecenie w menu **Action** (Akcja) lub w menu skrótów.
6. Wyświetlone zostanie okno programu *Share A Folder Wizard* (Kreator udostępniania foldera). Kliknij przycisk **Next** (Dalej).
7. Wpisz ścieżkę **c:\docs**, a następnie kliknij przycisk **Next** (Dalej).
8. Zaakceptuj domyślną nazwę udziału — docs i kliknij przycisk **Next** (Dalej).
- 9- Na stronie *Permissions* (Uprawnienia) kliknij opcję **Use Gustom Share And Folder Permissions** (Użyj niestandardowych uprawnień udziału i foldera), a następnie kliknij przycisk *Customize* (Dostosuj).
10. Kliknij pole wyboru **Allow Fuli Control** (Zezwalaj na pełną kontrolę), a następnie kliknij przycisk **OK**.
11. Kliknij kolejno przyciski **Finish** (Zakończ) i **Close** (Zamknij).

Ćwiczenie 2: Łączenie się z folderem udostępnionym

1. W konsoli *File Senier Management* (Zarządzanie serwerem plików) kliknij węzeł **Sessions** (Sesje). Jeśli w węźle wyświetlane są jakiekolwiek sesje, kliknij polecenie **Disconnect AU Sessions** (Rozłącz wszystkie sesje) (wybrane z listy) zadań, a następnie, w celu potwierdzenia, kliknij przycisk **Yes** (Tak).
2. W menu **Start** wybierz polecenie **Run** (Uruchom). Wpisz nazwę UNC foldera udostępnionego **\\server01\docs** i kliknij przycisk **OK**.
Używając nazwy UNC zamiast ścieżki fizycznej, takiej jak **c:\docs**, tworzone jest połączenie sieci do foldera udostępnionego, dokładnie tak jak sobie życzył użytkownik.
- 3- W konsoli *File Senier Management* (Zarządzanie serwerem plików) kliknij węzeł **Sessions** (Sesje). Warto zwrócić uwagę, że użytkownik wymieniony jest na liście jako obsługujący sesję połączenia z serwerem. Być może, aby zmiany zostały uwidocznione, trzeba będzie poprzez naciśnięcie przycisku klawiatury **F5** odświeżyć konsolę. 4. Kliknij węzeł **Open Files** (Otwarte pliki). Należy zwrócić uwagę, że użytkownik jest wymieniony na liście i że otworzył plik **c:\docs**.

Ćwiczenie 3: Symulacja przygotowań do wyłączenia serwera

1. W konsoli *File Semer Management* (Zarządzanie serwerem plików) kliknij prawym przyciskiem myszy węzeł **Shares** (Udziały). W menu **AU Tasks** (Wszystkie zadania) wybierz polecenie **Send Console Message** (Wyślij komunikat konsoli).



Wskazówka Usługa Messenger (Posłaniec) musi być uruchomiona na komputerach odbierających wiadomość. Ponieważ nikt nie oczekuje, że na konsoli serwera ktokolwiek będzie logował się w trybie interaktywnym, usługa Messenger (Posłaniec) jest domyślnie wyłączona. Aby wysłać w ćwiczeniu wiadomość do samego siebie, należy za pomocą konsoli Services (Usługi), skonfigurować usługę Messenger (Posłaniec) tak, aby była uruchamiana automatycznie lub ręcznie, a następnie uruchomić usługę.

2. Wpisz komunikat informujący, że serwer zostanie wyłączony i w związku z tym użytkownik powinien zapisać swoją pracę.
3. Kliknij przycisk **Send** (Wyślij).
Jeśli jest dostępny dodatkowy system, sytuację można zasymulować bardziej realistycznie łącząc się do udostępnionego foldera docs i wysyłając komunikat do systemu.
4. Kliknij węzeł **Open Files** (Otwarte pliki).
- 5- Zaznacz plik c:\docs, który jest otwarty poprzez połączenie do udostępnionego foldera.
6. Zamknij otwarty plik. W tym celu stosuje się odpowiednie polecenia menu **Action** (Akcja) lub menu skrótów.
7. Zaznacz węzeł **Sessions** (Sesje).
8. Na liście zadań kliknij polecenie **Disconnect All Sessions** (Rozłącz wszystkie sesje). Teraz moż. na wyłączyć serwer.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Które z wymienionych poniżej narzędzi umożliwia administrację udziału na serwerze zdalnym? Zaznacz wszystkie właściwe odpowiedzi.
 - a. Przystawka *ShareclFolders* (Foldery udostępnione).
 - b. Program Windows Explorer (Eksplorator Windows) uruchomiony na komputerze lokalnym i przyłączony do udziału serwera zdalnego lub do ukrytego, udostępnionego napędu.
 - c. Program Windows Explorer (Eksplorator Windows) uruchomiony na komputerze zdalnym za pośrednictwem sesji programu *TerminalServices* (Usługi terminalowe) lub *Remote Desktop* (Pulpit zdalny).
 - d. Konsola *File Server Management* (Zarządzanie serwerem plików).
2. Na wolumenie FAT32 został udostępniony folder. Grupa Project Managers ma uprawnienia *Allow Full Control* (Zezwalaj na pełną kontrolę). Grupa Project Engineers ma uprawnienia *Allow Read* (Zezwalaj na odczyt). Julie należy do grupy Project Engineers. Po awansie, Julie została dodana do grupy Project Managers. Jakie są jej uprawnienia czynne do foldera?

3. Na wolumenie NTFS udostępniony został folder, a domyślne uprawnienia nie zostały zmienione. Grupa Project Managers ma uprawnienia NTFS *Allow Full Control* (Zezwalaj na pełną kontrolę). Julie, która należy do grupy Project Managers nie potrafi w folderze utworzyć pliku. Dlaczego Julie nie może tworzyć plików?

Podsumowanie lekcji

- Program *Windows Explorer* (Eksplorator Windows) może być używany jedynie do konfigurowania udziałów na wolumenie lokalnym. Oznacza to, że aby zarządzać udziałami za pomocą programu Eksplorator Windows, użytkownik musi zalogować się w serwerze lokalnie (interakcyjnie) lub za pomocą programu *Remote Desktop* (usługi terminalowe).
- Przystawka *Shared Folders* (Foldery udostępnione) umożliwia zarządzanie udziałami komputera lokalnego lub zdalnego.
- Ukryte udziały (udziały, które nie są wyświetlane na listach przeglądarek) tworzone są przez dodanie na końcu nazwy udziału znaku dolara (\$). Aby połączyć się udziałem, należy zastosować formę! nazwy UNC: \\nazwa_serwera\nazwa_udziału\$.
- Uprawnienia udziałów definiują maksymalne uprawnienia czynne dla wszystkich plików i folderów dostępnych dla połączenia programu *Client for Microsoft Networks* (Klient sieci Microsoft Networks).
- Uprawnienia udziału nie dotyczą dostępu lokalnego (interakcyjnego), usług terminalowych, programu IIS lub innych typów dostępu.

Lekcja 2: Konfigurowanie uprawnień systemu plików

Serwery systemu Windows poprzez NTFS obsługują dokładną kontrolę dostępu do poszczególnych plików i folderów. Uprawnienia dostępu do zasobu są przechowywane w postaci wpisów kontroli dostępu (ACE) listy ACL, która jest częścią opisu zabezpieczeń każdego zasobu. Jeśli użytkownik próbuje uzyskać dostęp do zasobu, żeton dostępu użytkownika, zawierający identyfikatory zabezpieczeń SID konta użytkownika i kont grup, jest porównywany pod kątem zgodności z identyfikatorami SID we wpisach ACE list ACL. Ten proces *uwierzytelnienia* nie zmienił się zasadniczo od wprowadzenia systemu Windows NT. Natomiast szczegóły implementacji uwierzytelnienia, narzędzia zarządzania i specyfika konfigurowania dostępu do zasobów są różne w każdej wersji systemu Windows.

Niniejsza lekcja omawia nowe cechy kontroli dostępu systemu Windows Server 2003. Opisane zostaną sposoby wykorzystywania edytora ACL do zarządzania szablonami uprawnień, dziedziczeniem, uprawnieniami specjalnymi oraz oceny uprawnień efektywnych użytkownika lub grupy.

Materiały omówione podczas lekcji pozwalają na

- Konfigurowanie uprawnień za pomocą edytora ACL systemu Windows Server 2003
- Zarządzanie dziedziczeniem uprawnień ACL
- Określanie uprawnień czynnych
- Sprawdzanie uprawnień czynnych
- Zmianę właściciela plików i folderów
- Przenoszenie własności plików i folderów

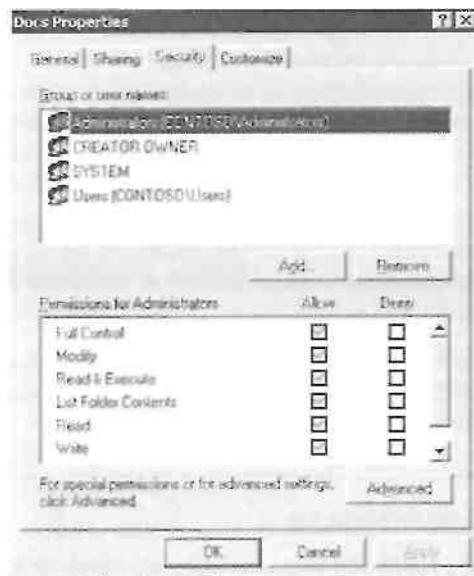
Szacunkowy czas lekcji: 30 minut

Konfigurowanie uprawnień

Program *Windows Explorer* (Eksplorator Windows) jest najczęściej używanym narzędziem rozpoczynającym zarządzanie uprawnieniami dostępu do zasobów, zarówno na wolumenach lokalnych, jak i serwerach zdalnych. Inaczej niż dla folderów udostępnionych, Eksplorator Windows może być zdalnie i lokalnie używany do konfigurowania uprawnień.

Edytor listy ACL (Access Control List)

Tak jak we wcześniejszych wersjach systemu Windows, zabezpieczenia dla plików i folderów mogą być konfigurowane na dowolnym wolumenie NTFS. W tym celu należy prawym przyciskiem myszy kliknąć zasób i wybrać polecenie **Properties** (Właściwości) lub **Sharing And Security** (Udostępnianie i zabezpieczenia), a następnie kliknąć zakładkę **Security** (Zabezpieczenia). Wyświetlony interfejs nazywany jest różnie: okno dialogowe *Permissions* (Uprawnienia), okno dialogowe *Security Settings* (Ustawienia zabezpieczeń), zakładka *Security* (Zabezpieczenia) lub edytor ACL. Jakakolwiek nazwa zostanie użyta, okno wygląda tak samo. Na rysunku 6-4 został przedstawiony przykładowy widok zakładki *Security* (Zabezpieczenia) w oknie dialogowym *Properties* (Właściwości) dla zasobu Docs.

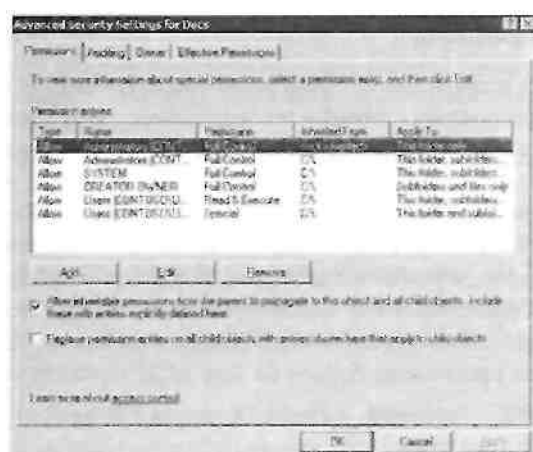


Rysunek 6-4 Edytor ACL w oknie dialogowym *Properties (Właściwości)* dla zasobu *Docs*

Przed wersją systemu Windows 2000 uprawnienia były dość uproszczone. Firma Microsoft dla wersji Windows 2000 (i późniejszych) wprowadziła znacznie bardziej elastyczną i silniejszą kontrolę dostępu do zasobów. Silniejsze narzędzie jest również bardziej złożone. Obecnie edytor ACL ma trzy okna dialogowe, a w każdym z nich obsługiwane są inne i ważne funkcje.

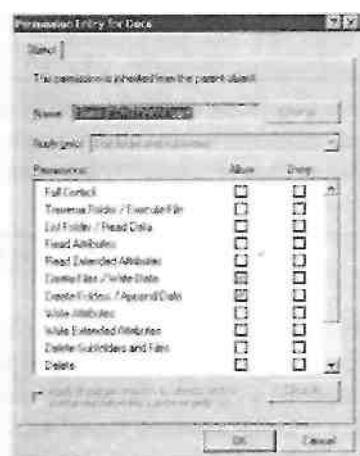
Pierwsze okno dialogowe udostępnia ogólny przegląd ustawień zabezpieczeń i uprawnień zasobu. Umożliwia zaznaczenie każdego konta, dla którego zdefiniowany został dostęp i przeglądanie szablonu uprawnień przydzielonych dla danego użytkownika, grupy bądź komputera. Każdy szablon uprawnia pokazany w tym oknie dialogowym stanowi zestaw uprawnień, które razem umożliwiają konfigurowanie poziomu dostępu. Na przykład, aby zezwolić użytkownikowi odczytać plik, wymagane jest określenie kilku jednostkowych uprawnień. Złożoność tego procesu została ukryta, a użytkownik po prostu zaznacza szablon uprawnień *Allow: Read & Execute* (Zezwalaj: Zapis i wykonanie), a system Windows w tle ustawia odpowiednie uprawnienia do pliku i foldera.

Aby przeglądać szczegółowo listę ACL, należy kliknąć przycisk **Advanced** (Zaawansowane). Uruchomione zostanie drugie okno dialogowe edytora ACL — *Advanced Security Settings For Docs* (Zaawansowane ustawienia zabezpieczeń dla Docs). Okno to pokazane zostało na rysunku 6-5. Umieszczona tu została lista określonych wpisów kontroli dostępu, które zostały przypisane do pliku lub foldera. Lista jest najbliższym przybliżeniem, dostępnym w interfejsie użytkownika, rzeczywistych informacji przechowywanych na liście ACL. Inne okna dialogowe umożliwiają konfigurowanie inspekcji, zarządzanie własnością i sprawdzanie uprawnień czynnych.



Rysunek 6-5 Okno dialogowe *Advanced Security Settings* (Zaawansowane ustawienia zabezpieczeń; edytora ACL)

Po zaznaczeniu uprawnienia na liście *Permission Entries* (Wpisy uprawnień) i kliknięciu przycisku *Edit* (Edytuj), wyświetlone zostanie trzecie okno dialogowe edytora ACL. Okno to, *Permission Entry For Docs* (Wpis uprawnień dla Docs), pokazane zostało na rysunku 6-6. Zawiera listę szczegółowych, pojedynczych uprawnień i stanowi pewnego rodzaju kompromis pomiędzy wpisami uprawnień drugiego okna dialogowego (lista wpisów uprawnień) a pierwszym oknem dialogowym (lista uprawnień użytkownika).



Rysunek 6-6 Okno dialogowe *Permission Entry* (Wpis uprawnień) edytora ACL

- C\ **Wskazówka egzaminacyjna** Przystawka Shared Folders (Foldery udostępnione) udostępnia edytor ACL. Należy otworzyć okno właściwości foldera udostępnionego i kliknąć zakładkę Security (Zabezpieczenia).

Dodawanie i usuwanie wpisów uprawnień

Dla każdego podmiotu zabezpieczeń można zezwalać lub zabraniać przydziału uprawnień. W systemie Windows Server 2003 występują następujące podmioty zabezpieczeń: użytkownicy, grupy, komputery oraz specjalna klasa obiektu InetOrgPerson (opisana w specyfikacji RFC 2798), która jest używana do reprezentowania użytkowników w pewnych sytuacjach dotyczących katalogów różnych platform. Aby dodać uprawnienie, należy kliknąć przycisk **Add** (Dodaj) na pierwszym lub drugim oknie dialogowym edytora ACL. Okno dialogowe *Select User, Computer Or Group* (Wybór użytkownika, komputera lub grupy) umożliwia znalezienie odpowiedniego podmiotu zabezpieczeń. Następnie należy wybrać właściwe uprawnienie. W stosunku do poprzednich wersji systemu Windows interfejs nieznacznie się różni, a te niewielkie zmiany nie przeszkadzają doświadczonemu administratorowi w szybkim opanowaniu programu. Aby usunąć konkretne uprawnienia dodane do listy ACL, wystarczy zaznaczyć je na liście i kliknąć przycisk **Remove** (Usuń).

Modyfikowanie uprawnień

Uprawnienie może być modyfikowane w oknie dialogowym zakładki *Security* (Zabezpieczenia) poprzez zaznaczanie lub usuwanie zaznaczenia pól wyboru *Allow* (Zezwalaj) lub *Deny* (Odmawiaj), przez co zastosowany zostanie odpowiedni szablon uprawnień.

Jeśli kontrola powinna być dokładniejsza, należy kliknąć przycisk **Advanced** (Zaawansowane), zaznaczyć uprawnienie i kliknąć przycisk **Edit** (Edytuj). Edytowane mogą być pojedyncze uprawnienia. Dziedziczenie uprawnień omówione zostanie w dalszej części lekcji.

W oknie dialogowym *Permission Entry For Docs* (Wpisy uprawnień dla Docs), pokazanym na rysunku 6-6, można modyfikować uprawnienia oraz za pomocą listy rozwijanej *Apply Onto* (Zastosuj do) określać zakres dziedziczenia uprawnień.



Uwaga Istotną sprawą jest zrozumienie wpływu zmian dokonywanych w omawianym oknie dialogowym. Z jednej strony dobrze, że firma Microsoft umożliwiła szczegółową kontrolę, ale z drugiej strony zwiększenie liczby kontrolowanych elementów powoduje skomplikowanie operacji i zwiększone możliwości popełnienia błędów.

Nowe podmioty zabezpieczeń

W systemie Windows Server 2003, inaczej niż dla Windows NT 4, istnieje możliwość dodawania *komputerów* lub grup komputerów do listy ACL, dzięki czemu zwiększyła się elastyczność konfigurowania dostępu do zasobów. Obecnie można kontrolować dostęp do zasobu w oparciu o komputer klienta, bez względu na to, który użytkownik uzyskuje dostęp. Przykładowo, może zachodzić potrzeba udostępnienia komputera w holu biura, ale trzeba zapobiec, aby na tym komputerze, podczas przerwy na lunch, menedżer nie mógł uzyskać dostępu do ważnych informacji. Dzięki dodaniu komputera do list ACL i odmowie uprawnień dostępu, menedżer, który uzyskuje dostęp do ważnych informacji na swoim pulpicie, nie uzyska dostępu do tych na komputerze w holu biura.

System Windows Server 2003 umożliwia również zarządzanie dostępem do zasobów w oparciu o typ logowania. Do listy ACL można dodawać konta specjalne — *Interactive* (Interakcyjni), *Network* (Sieć) oraz *Terminal Server User* (Użytkownicy serwera terminali). Tożsamość *Interactive* (Interakcyjni) reprezentuje użytkowników, którzy do konsoli zalogowali się lokalnie. Grupa *Terminal Server User*

(Użytkownicy serwera terminali) to użytkownicy, którzy przyłączyli się za pomocą pulpitu zdalnego lub usług terminalowych. Grupa *Network* (Sieć) reprezentuje połączenia sieci, na przykład program *Client for Microsoft Networks* (Klient sieci Microsoft Networks) systemu Windows.

Szablony uprawnień oraz uprawnienia specjalne

Szablony uprawnień, wyświetlone na zakładce *Security* (Zabezpieczenia) pierwszego okna dialogowego są zestawami uprawnień specjalnych, które są dokładnie pokazane w trzecim oknie dialogowym — *Permissions Entry For Docs* (Wpisy uprawnień dla Docs). Znaczenie większości szablonów i uprawnień specjalnych łatwo określić na podstawie ich nazwy, a z kolei omówienie niektórych pozycji wykracza poza zaplanowany zakres niniejszej książki. Poniżej zostało wymienionych kilka pozycji, które są warte odnotowania:

- **Read & Execute (Odczyt i wykonanie)** Ten szablon uprawnień jest wystarczający dla użytkowników, którzy mają otwierać oraz odczytywać pliki i foldery. Uprawnienia *Read & Execute* (Odczyt i wykonanie) umożliwiają także użytkownikowi skopiowanie zasobu, przy założeniu, że mają uprawnieni?, do zapisu w folderze bądź na nośniku docelowym. W systemie Windows brak uprawnień zabraniających kopiowania. Funkcjonalność taka będzie dostępna po wprowadzeniu w systemach Windows technologii Digital Rights Management.
- **Write and Modify (Zapis i modyfikowanie)** Zastosowany do foldera szablon uprawnień *Write* (Zapis) umożliwia użytkownikom tworzenie nowych plików bądź folderów, natomiast zastosowany do pliku, umożliwia modyfikowanie zawartości pliku, jak również jego atrybutów (ukryty, systemowy, tylko do odczytu) oraz atrybutów rozszerzonych (zdefiniowanych przez aplikację „odpowiedzialną” za dany dokument). Szablon *Modify* (Modyfikowanie) umożliwia usuwanie obiektu.
- **Change Permissions (Zmiana uprawnień)** Po doraźnym zmodyfikowaniu list ACL można zdziwić się sprawdzając, kto może modyfikować uprawnienia. Pierwsza odpowiedź dotyczy właściciela zasobu. Własność zasobu zostanie omówiona w dalszej części tej lekcji. Druga odpowiedź wiąże się z faktem, że każdy użytkownik, który ma uprawnienie czynne pozwalające zmieniać uprawnienia (*Change Permission*), może modyfikować listę ACL zasobu. Uprawnienie *Change Permission* (Zmiana uprawnień) musi być zarządzane przy użyciu trzeciego okna dialogowego edytora ACL. Uprawnienie to jest również dołączone do szablonu uprawnień *Full Control* (Pełna kontrola).

Dziedziczenie

System Windows Server 2003 obsługuje dziedziczenie uprawnień, co po prostu oznacza, że uprawnienia zastosowane do foldera będą się również stosowały do plików i folderów znajdujących się poniżej danego foldera (dotyczy ustawień domyślnych). Dowolne zmiany nadrzędnej listy ACL będą miały podobny wpływ na całą zawartość tego foldera. Dziedziczenie umożliwia skupienie administracji w jednym punkcie, czyli zarządzanie jedną listą ACL danej gałęzi lub zasobów znajdujących się poniżej danego foldera.

Mechanizm dziedziczenia

Dziedziczenie jest wynikiem dwóch cech deskryptora zabezpieczeń zasobu. Po pierwsze, uprawnienia mogą być dziedziczone (ustawienia domyślne). Tak jak przedstawiono to na rysunku 6-5, uprawnienie *Allow I 'sers to Read & Execute* (Zezwalaj użytkownikom na odczyt i wykonanie) jest dodatkowo określone w polu *Apply to* (Zastosuj dla: Ten folder, podfoldery i pliki). Jednakże te ustawienia same

nie są wystarczające, aby zadziałało dziedziczenie. Dodatkowo wymagane jest, aby podczas tworzenia nowego obiektu nie zostało zmienione domyślne zaznaczenie pola wyboru *Allow Inheritable Permissions From The Parent To Propagate To This Object...* (Zezwalaj na propagowanie dziedziczenia uprawnień z obiektu nadrzędnego do tego obiektu..).

Tak więc nowo utworzony plik lub folder będzie dziedziczył uprawnienia po obiekcie nadrzędnym, a także każda zmiana w obiekcie nadrzędnym będzie miała wpływ na podrzędne pliki i foldery. Warto zapoznać się z tym dwuetapowym wprowadzaniem dziedziczenia, ponieważ stanowi ono dwa różne sposoby zarządzania dziedziczeniem: z punktu widzenia obiektu nadrzędnego oraz z punktu widzenia obiektu podrzędnego.

W każdym oknie dialogowym edytora ACL dziedziczenie uprawnień jest różnic wyświetlane. W pierwszym i trzecim oknie dialogowym, zakładka *Security* (Zabezpieczenia) oraz *Permissions Entry For Docs* (Wpisy uprawnień dla Docs) dziedziczone uprawnienia pokazywane są jako nieaktywne zaznaczenia (przyciemnione), dla odróżnienia ich od uprawnień przydzielanych do zasobu bezpośrednio (nazywane uprawnieniami „wyraźnymi”). W drugim oknie dialogowym - *Advanced Security Settings* (Zaawansowane ustawienia zabezpieczeń) — program pokazuje dla każdego uprawnienia, na podstawie którego foldera uprawnienie jest dziedziczone.

Unieważnianie dziedziczenia

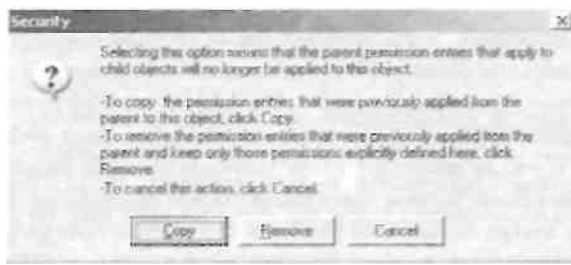
Dziedziczenie umożliwia konfigurowanie uprawnień w najwyższym punkcie drzewa foldera. Takie początkowe uprawnienia oraz ich zmiany będą propagowane do wszystkich plików i folderów tego drzewa, których domyślna konfiguracja umożliwia dziedziczenie.

Czasami jednak zachodzi potrzeba zmodyfikowania uprawnień podfolderów lub plików tak, aby użytkownicy lub grupy uzyskiwali dodatkowy dostęp, a czasem, aby dostęp ten był bardziej ograniczony. Uprawnienia dziedziczone nie mogą być usuwane z listy ACL. Można natomiast unieważnić dziedziczone uprawnienie przez przydzielenie uprawnienia bezpośredniego. Alternatywnym rozwiązaniem jest zablokowanie dziedziczenia i utworzenie całej bezpośredniej listy ACL.

Aby unieważnić dziedziczone uprawnienia poprzez ich zastąpienie uprawnieniami bezpośrednimi, wystarczy po prostu zaznaczyć pole wyboru odpowiedniego uprawnienia. Na przykład, jeśli folder dziedziczy uprawnienie *Allow Read* (Zezwalaj na odczyt) przydzielone do grupy Sales Rcps i jeśli dla grupy Sales Rcps należy zabronić tego dostępu do foldera, wystarczy zaznaczyć pole wyboru *Deny Read* (Odmawiaj odczytu).

Aby unieważnić wszystkie dziedziczone uprawnienia, należy dla zasobów otworzyć okno dialogowe *Advanced Security Settings* (Zaawansowane ustawienia zabezpieczeń) i usunąć zaznaczenie opcji *Allow Inheritable Permissions From The Parent To Propagate To This Object...* (Zezwalaj na propagowanie dziedziczenia uprawnień z obiektu nadrzędnego do tego obiektu..). Zablokowane zostanie dziedziczenie wszystkich uprawnień pochodzących z obiektu nadrzędnego. Następnie trzeba skonfigurować dostęp do zasobu poprzez przydzielenie wystarczających uprawnień bezpośrednich.

Aby ułatwić tworzenie uprawnień bezpośrednich w liście ACL, podczas blokowania dziedziczenia system Windows przedstawia użytkownikowi dwie możliwości. Użytkownik może skopiować lub usunąć wpisy uprawnień. Odpowiednie okno dialogowe przedstawione zostało na rysunku 6-7.



Rysunek 6-7 Kopiowanie lub usuwanie

wpisów uprawnień

Kopiowanie tworzy uprawnienia bezpośrednie identyczne z odziedziczonymi uprawnieniami. Następnie można usunąć konkretne wpisy uprawnienia, jeśli nie mają dotyczyć danego zasobu. Po uruchomieniu funkcji *Remove* (Usuń) lista ACL będzie pusta i będzie można do niej dodawać wpisy uprawnień. Taki sam rezultat uzyskuje się po umieszczeniu na liście ACL uprawnień bezpośrednich. Tak więc, kwestią jest raczej, czy łatwiej będzie rozpocząć określanie uprawnień od zera, czyli od pustej listy ACL, czy rozpocząć od skopiowania dziedziczonych uprawnień i zmodyfikować listę do wymaganego kształtu. Jeśli nowa lista ACL jest istotnie różna od listy dziedziczonych uprawnień, lepiej uruchomić funkcję *Remove* (Usuń). Jeśli natomiast nowa lista ACL różni się niewiele, bardziej wydajne będzie jej skopiowanie.

Dziedziczenie blokowane jest poprzez usunięcie zaznaczenia opcji *AUow Inheritable Permissions* (Zezwalaj na dziedziczenie uprawnień). W takim przypadku każdy dostęp do zasobu jest zarządzany przez uprawnienia bezpośrednie przydzielone do tego pliku lub foldera. Żadna zmiana listy ACL foldera nadrzędnego *nie* będzie miała wpływu na dany zasób. Pomimo, że uprawnienia obiektu nadrzędnego mogą być dziedziczone, obiekt podrzędny ich nie dziedziczy. Blokowanie dziedziczenia należy stosować ostrożnie, ponieważ komplikuje to zarządzanie, sprawdzanie i rozwiązywanie problemów związanych z dostępem do zasobu.

Ponowna instalacja dziedziczenia

Istnieją dwa sposoby ponownej instalacji dziedziczenia: z punktu widzenia zasobu podrzędnego lub z punktu widzenia foldera nadrzędnego. Rezultaty różnią się nieznacznie. Potrzeba ponownego włączenia dziedziczenia dla zasobu może mieć miejsce, jeśli dziedziczenie zostało zablokowane przypadkowo lub jeśli zmieniły się potrzeby przedsiębiorstwa. W takim przypadku wystarczy po prostu w oknie dialogowym *AdvancedSecurity Settings* (Zaawansowane ustawienia zabezpieczeń) ponownie zaznaczyć opcję **AUow Inheritable Permissions** (Zezwalaj na dziedziczenie uprawnień). Uprawnienia dziedziczone po obiekcie nadrzędnym nic mają wpływu na zasób. Pozostają wszystkie uprawnienia bezpośrednie przydzielone do zasobu. Wynikowa lista ACL jest połączeniem uprawnień bezpośrednich, które mogą być usuwane oraz odziedziczonych uprawnień. Z tego względu, niektóre odziedziczone uprawnienia mogą nie być uwidaczniane w pierwszym i trzecim oknie dialogowym edytora ACL. Na przykład, jeśli zasób ma uprawnienie bezpośrednie *Allows Sales Reps Read & Execute* (Zezwalaj grupie Sales Reps na odczyt i wykonanie), a folder nadrzędny ma takie same uprawnienie, to po zezwoleniu dziedziczenia dla obiektu podrzędnego, w rezultacie obiekt podrzędny będzie miał *zarówno* dziedziczone, jak i bezpośrednie uprawnienia. Odpowiednie zaznaczenia będą widoczne w pierwszym i trzecim oknie dialogowym. W interfejsie uprawnienia bezpośrednie przesłaniają uprawnienia dziedziczone. Jednak w rzeczywistości odziedziczone uprawnienia są przedstawiane, o czym można się przekonać przeglądając drugie okno dialogowe - *AdvancedSecurity Settings* (Zaawansowane ustawienia zabezpieczeń).

Druga metoda ponownej instalacji dziedziczenia przeprowadzana jest w obiekcie nadrzędnym. Dla danego foldera, w oknie dialogowym *Advanced Security Settings* (Zaawansowane ustawienia zabezpieczeń) należy zaznaczyć pole wyboru *Replace Permission Entries On AU Chi/J Objects With Entries Shown Here That Apply To Child Objects* (Zamień wpisy uprawnienia na wszystkich obiektach podrzędnych na wpisy tutaj pokazane, stosowane do obiektów podrzędnych). W rezultacie wszystkie listy ACL podfolderów i plików zostaną usunięte. Zastosowane zostaną uprawnienia obiektu nadrzędnego. Działania przypominają więc metodę wyburzenia starego domu i zbudowanie w tym miejscu nowego budynku. Po użyciu tej opcji, inaczej niż podczas ponownej instalacji dziedziczenia dla obiektów podrzędnych, zostaje usunięte każde uprawnienie bezpośrednie zastosowane do podfolderów i plików. Ponieważ dziedziczenie zostało odtworzone, każda zmiana listy ACL foldera nadrzędnego jest propagowana do podfolderów i plików. Od tego momentu, dla podfolderów i plików możliwe jest określanie nowych uprawnień bezpośrednich. Po zastosowaniu opcja *Replace Permissions* (Zastąp uprawnienia) spełniła swoje zadanie, a wprowadzone uprawnienia obiektu nadrzędnego będzie można modyfikować.

Uprawnienia czynne

Często zdarza się, że użytkownicy należą do kilku grup, a grupy te mają przydzielony różny poziom dostępu do zasobów. Jeśli lista ACL zawiera wiele wpisów, użytkownik musi mieć możliwość oceny uprawnień, które zostały mu przydzielone na podstawie jego członkostwa w grupach. Uprawnienia wynikowe nazywane są *uprawnieniami czynnymi*.



Wskazówka egzaminacyjna Uprawnienia czynne są częstym zadaniem egzaminacyjnym w większości obowiązkowych egzaminów dotyczących systemu Microsoft Windows Ser/er 2003, jak również w przypadku innych egzaminów dotyczących przykładowo projektowania. Warto zwrócić szczególną uwagę na informacje i zagadnienia omawiane w ćwiczeniach praktycznych dotyczące uprawnień czynnych, aby być pewnym doskonałego opanowania tego tematu.

Określanie uprawnień czynnych

Poniżej wymienione zostały reguły pozwalające określić uprawnienia czynne:

- **Uprawnienia plików unieważniają uprawnienia folderów.** W zasadzie nie jest to reguła, ale w dokumentacji jest często w ten sposób przedstawiana i warto ją omówić. Każdy zasób obsługuje listę ACL. Jedynie lista ACL odpowiedzialna jest za określanie dostępu do zasobu. Pomimo, że na liście ACL mogą pojawiać się wpisy dziedziczone po obiekcie nadrzędnym, to są jednak wpisami listy ACL danego zasobu. Określając dostęp, podsystem zabezpieczeń nie sprawdza uprawnień foldera nadrzędnego. Tak więc reguła ta mogłaby brzmieć: Znaczenie ma jedynie lista ACL danego zasobu.
- **Uprawnienia zezwalające sumują się.** Dla danego użytkownika, poziom dostępu do zasobu może być określany przez uprawnienia przydzielone do grup, do których użytkownik należy. Uprawnienia *Allow* (Zezwalaj) przydzielone w żetonie zabezpieczeń użytkownika do dowolnego obiektu użytkownika, grupy bądź identyfikatorów ID komputera będą stosowane do tego użytkownika. Tak więc uprawnienia czynne są sumą wszystkich uprawnień *Allow* (Zezwalaj). Jeśli grupa Sales Repsmado foldera uprawnienia *Allow Read & Execute* oraz *Write* (Zezwalaj na Odczyt i wykonanie oraz Zapis), zaś dla grupy Sales Managers dopuszczone zostały uprawnienia *Read & Execute* oraz *Delete* (Odczyt i wykonanie oraz Usuwanie), to użytkownik, który należy do obu grup, będzie

niał uprawnienia czynne równoważne z szablonem uprawnień *Modify: Read & Execute, Write* oraz *Delete*. • **Odmowa uprawnień ma pierwszeństwo w stosunku do zezwoleń.** Odmowa uprawnienia unieważnia wpis dotyczący zezwolenia dostępu. Rozszerzając przykład zamieszczony powyżej, jeśli dla grupy Temporary Employees odmówiono uprawnienia *Read* (Odczyt) i jeśli użytkownik należy do grup Sales Reps oraz Temporary Employees, to nie będzie mógł odczytać foldera.



Informacja Zalecaną praktyką jest ograniczanie stosowania odmowy uprawnień, a zamiast tego zezwalanie na minimalne uprawnienia, które pozwalają wykonywać zadania. Odmowa uprawnień komplikuje dodatkowo administrację list ACL i powinna być stosowana tylko wtedy, kiedy jest to absolutnie konieczne, aby odmówić dostępu użytkownikom, którzy uprawnienia do zasobu mają przydzielone poprzez członkostwo w innych grupach.



Wskazówka egzaminacyjna Jeśli użytkownik nie może uzyskać dostępu do zasobu ze względu na odmowę uprawnień, a dostęp ten jest potrzebny, należy usunąć odmowę uprawnień lub usunąć użytkownika z grupy, do której odmowa uprawnień została zastosowana. Jeśli natomiast odmowa uprawnień jest dziedziczona, udostępnienie zasobu można zrealizować poprzez dodanie uprawnienia bezpośredniego Allow (Zezwalaj).

- **Uprawnienia bezpośrednie mają pierwszeństwo nad uprawnieniami dziedziczonymi.** Wpis uprawnienia, który został bezpośrednio zdefiniowany dla zasobu unieważnia sprzeczny wpis uprawnienia dziedziczonego. Działanie takie wynika z podstawowych założeń projektu: Folder nadrzędny określa „regułę” dzięki temu, że działa dziedziczenie. Obiekt podrzędny może wymagać dostępu, który nie jest zgodny z regułą i dlatego uprawnienie jest dodawane bezpośrednio do listy ACL obiektu podrzędnego. Uprawnienie bezpośrednie ma pierwszeństwo.

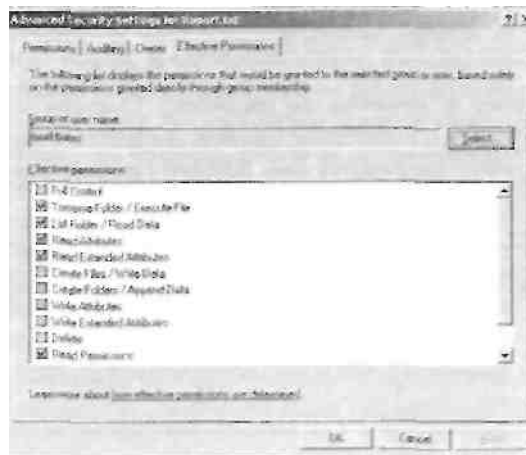


Wskazówka egzaminacyjna Działanie omawianej reguły powoduje, że *bezpośrednie uprawnienie zezwalające (Allow)* unieważnia *dziedziczone uprawnienie zabraniające (Deny)*.

Sprawdzanie uprawnień czynnych

Umożliwienie kontrolowania jednostkowych uprawnień i dziedziczenia obsługiwanego w systemie plików NTFS komplikuje zarządzanie tymi uprawnieniami. Stosując te wszystkie uprawnienia do użytkowników i grup nasuwa się pytanie: w jaki sposób dla użytkownika określić rzeczywiste uprawnienia i poziom dostępu do zasobów.

Firma Microsoft opracowała długo oczekiwane narzędzie ułatwiające udzielenie odpowiedzi na powyższe pytanie. Przedstawiona na rysunku 6-8 zakładka *Effective Permissions* (Czynne uprawnienia) znajdująca się w oknie dialogowym *Advanced Security Settings* (Zaawansowane ustawienia zabezpieczeń), umożliwia z dobrym przybliżeniem określenie dla użytkownika wynikowych uprawnień dostępu do zasobu.



Rysunek 6-8 Zakładka *Effective Permissions* (Czynne uprawnienia) w oknie dialogowym *Advanced Security Settings* (Zaawansowane ustawienia zabezpieczeń)

Aby użyć programu *Effective Permissions* (Czynne uprawnienia), należy kliknąć przycisk *Select* (Wybierz) i określić użytkownika, grupę lub wbudowane konto, które będzie analizowane. Następnie system Windows Server 2003 wygeneruje listę uprawnień czynnych. Lista ta jest jedynie przybliżeniem i nie uwzględnia uprawnień do udostępnionego zasobu określonego wewnątrz konta, a także nie sprawdza specjalnego członkostwa konta, takiego jak:

- Anonymous Logon (Logowanie anonimowe)
- Bacch(Wsad)
- Creator Group (Grupa twórców)
- Dialup
- Enterprise Domain Controllers (Kontrolery domeny przedsiębiorstw)
- Interactive (Interaktywny)
- Network (Sieć)
- Proxy
- Restricted (Z ograniczeniami)
- Remote Interactive Logon (Zdalny)
- Service (Usługa)
- System
- Terminal Server User (Użytkownik serwera terminali)
- Other Organization (Inna organizacja)
- This Organization (Ta organizacja)

Lista ACL może zawierać wpisy dla kont grup *Network* (Sieć) lub *Interactive* (Interaktywny). Dzięki temu, użytkownik w zależności od sposobu zalogowania się (interakcyjnie czy poprzez sieć) uzyskuje różny poziom dostępu do zasobów. Ponieważ podczas sprawdzania uprawnień czynnych użytkownik nie jest zalogowany w systemie, pomijane są uprawnienia związane ze sposobem logowania. Aby ocena

uprawnień była precyzyjna, należy przeprowadzić jeszcze dodatkowy krok, w którym sprawdzone zostaną uprawnienia dla kont specjalnych bądź wbudowanych, takich jak *Interactive* (Interaktywny) lub *Network* (Sieć).

Właściciel zasobu

W systemie Windows Server 2003 określony został specjalny podmiot zabezpieczeń nazwany *Creator Owner* (Twórca-właściciel) oraz wpis w deskrytorze zabezpieczeń zasobu, który definiuje właściciela obiektu. Aby w pełni zrozumieć zagadnienia zarządzania i rozwiązywania problemów związanych z uprawnieniami zasobów, należy zapoznać się z tymi dwoma elementami obrazu zabezpieczeń.

Twórca właściciel

Jeśli użytkownik tworzy plik lub folder (jest to możliwe, jeśli dla użytkownika dopuszczone zostały odpowiednie uprawnienia *Create Files/Write Data* (Tworzenie plików/Zapis danych) lub *Create Folders/Append Data* (Tworzenie plików/ Dodawanie danych)), użytkownik staje się twórcą i początkowym właścicielem tego zasobu. Każde uprawnienie foldera nadrzędnego przydzielone do konta specjalnego *Creator Owner* (Twórca-właściciel) zostaje bezpośrednio przydzielone do tego użytkownika.

Jako przykład założono, że folder umożliwia użytkownikom tworzenie plików, czyli zezwala na uprawnienia *Create Files/Write Data* (Tworzenie plików/Zapis danych) oraz że uprawnienia foldera zezwalają użytkownikom na: *Read & Execute* oraz *Creator Owner Full Control* (Odczyt i wykonanie oraz Twórca właściciel — Pełna kontrola). Ten zestaw uprawnień będzie umożliwiał Marii utworzenie pliku. Maria, jako twórca pliku będzie miała pełną kontrolę nad tym plikiem. Ta również może utworzyć plik i również będzie miała pełną kontrolę nad swoim plikiem. Jednak każda z nich może jedynie odczytywać pliki utworzone przez drugą. Tia mogłaby jednak zmienić listę ACL pliku, który utworzyła, ponieważ w szablonie uprawnień *Full Control* (Pełna kontrola) dołączone są uprawnienia *Change Permission* (Zmiana uprawnień).

Własność

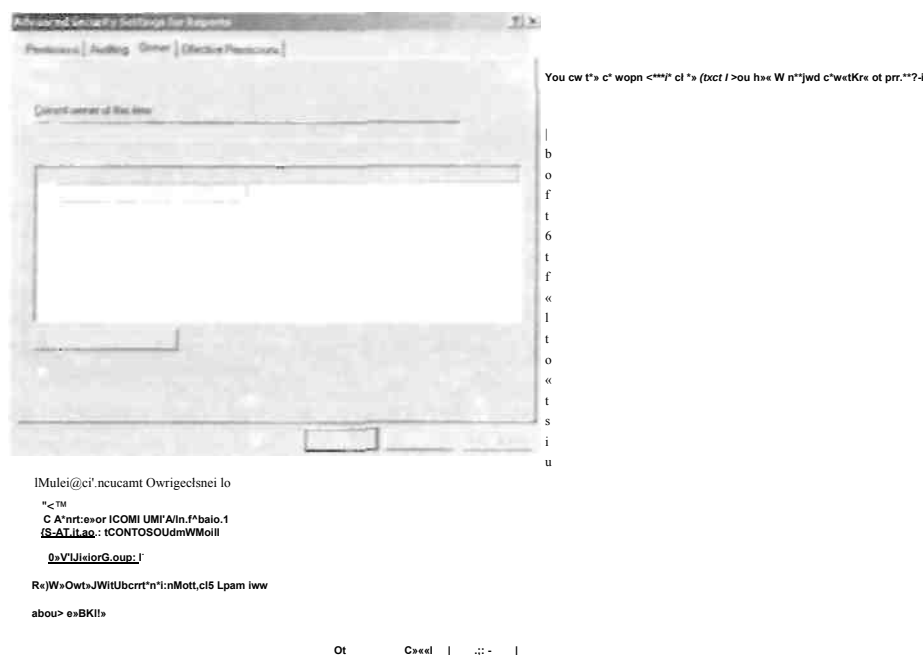
Jeśli z jakichkolwiek powodów Tia zmodyfikowała listę ACL i samej sobie odmówiła uprawnień *Full Control* (Pełna kontrola), będzie mogła nadal zmieniać listę ACL, ponieważ właściciel obiektu zawsze może modyfikować listę ACL swojego obiektu. Takie podejście uniemożliwia użytkownikom permanentne zablokowanie swoich własnych plików lub folderów.

Zalecaną praktyką jest zarządzanie własnością obiektów tak, aby właściciel obiektu był prawidłowo zdefiniowany. Zarządzanie możliwe jest tylko częściowo, ponieważ właściciele mogą modyfikować listy ACL swoich obiektów, a także dlatego, że nowsze technologie, takie jak przydział dysku, do obliczania przestrzeni dyskowej używanej przez poszczególnych użytkowników wykorzystują atrybut „własność”. Zarządzanie własnością obiektów w wersjach wcześniejszych niż Windows Server 2003 było bardzo niewygodne. System Windows Server 2003 został wyposażony w wartościowe narzędzie ułatwiające przenoszenie własności.

Właściciel obiektu jest określany w deskrytorze zabezpieczeń obiektu. Użytkownik, który utworzył plik lub folder jest początkowym jego właścicielem. Inny użytkownik może przejąć lub przypisać własność obiektu przy zastosowaniu następujących procesów:

- **Administratorzy mogą przejmować własność.** Użytkownik, który należy do grupy administratorów systemu lub któremu przydzielone zostało prawo użytkownika *Take Ownership* (Przejmij na własność) może przejść na własność dowolny obiekt systemu.

Aby przejść na własność zasób, należy w oknie dialogowym *Advanced Security Settings* (Zaawansowane ustawienia zabezpieczeń) kliknąć zakładkę **Owner** (Właściciel). Widok zakładki przedstawiony został na rysunku 6-9. Następnie należy wybrać z listy konto użytkownika, zaznaczyć pole wyboru **Replace Owner On Subcontainers And Objects** (Zamień właściciela dla podkontenerów i obiektów) oraz kliknąć przycisk **Apply** (Zastosuj).



Rysunek 6-9 Zakładka *Owner* (Właściciel) w oknie dialogowym *Advanced Security Setting* (Zaawansowane ustawienia zabezpieczeń)

- **Użytkownicy mogą przejąć własność, jeśli przydzielone zostało im prawo *Take Ownership* (Przejmij na własność).** Specjalne uprawnienie *Take Ownership* (Przejmij na własność) może być przydzielane dowolnej grupie bądź użytkownikowi. Użytkownicy mający te uprawnienia mogą przejmować na własność zasób, a następnie, jako właściciele, mogą modyfikować listę ACL, aby definiować wymagane uprawnienia.
- **Administratorzy mogą ułatwiać przenoszenie własności.** Administrator może przejąć własność dowolnego pliku lub foldera. Następnie, jako właściciel, administrator może zmienić uprawnienia do zasobu, przydzielając nowemu użytkownikowi prawo *Allow Take Ownership* (Zezwalaj: Przejmij na własność). Użytkownik ten może teraz przejąć na własność dany zasób.
- **Uprawnienia *Restore Files And Directories* (Odtwarzanie plików i katalogów) umożliwiają zmianę własności.** Użytkownik, który ma uprawnienia *Restore Files And Directories* (Odtwarzanie plików i katalogów) może jednemu użytkownikowi zabrać własność pliku i przydzielić ją innemu użytkownikowi. Mając takie uprawnienia, wystarczy kliknąć opcję **Other Users Or Groups** (Inni użytkownicy lub grupy), a następnie wskazać nowego właściciela. Jest to nowa funkcja systemu Windows Server 2003 i umożliwia administratorom bądź operatorom kopii zapasowych zarządzanie i przenoszenie własności zasobu bez interwencji użytkownika.

adanie kontrolne: Konfigurowanie uprawnień systemu plików

W zadaniu tym edytor ACL będzie wykorzystywany do zabezpieczania zasobów, sprawdzania uprawnień czynnych oraz do przenoszenia własności plików. Należy sprawdzić, czy skonfigurowane zostały obiekty użytkowników i grup opisane w sekcji „Wymagania”.

Ćwiczenie 1: Konfigurowanie uprawnień NTFS

1. Otwórz folder `c:\docs` utworzony w zadaniu kontrolnym podczas lekcji 1.
2. Utwórz folder nazwany Project 101.
3. Otwórz edytor ACL poprzez kliknięcie prawym przyciskiem myszy foldera Project 101, wybranie polecenia **Properties** (Właściwości), a następnie kliknięcie zakładki **Security** (Zabezpieczenia).
4. Skonfiguruj folder tak, aby dostęp do niego był zgodny z opisem zamieszczonym w poniższej tabeli. Zadanie to wymaga rozważenia oraz skonfigurowania dziedziczenia i uprawnień dla grup.

Podmiot zabezpieczeń	Dostęp
Administratorzy	Full Control (Pełna kontrola)
Użytkownicy grupy Project 101 Team	Mogą odczytywać dane, dodawać pliki i foldery oraz mają pełną kontrolę nad utworzonymi przez siebie plikami i folderami.
Grupa Managers	Członkowie tej grupy mogą odczytywać i modyfikować wszystkie pliki, ale nie mogą usuwać plików, których nie utworzyli. Menedżerowie powinni mieć pełną kontrolę nad utworzonymi przez siebie plikami i folderami.
Grupa System	Usługi uruchomione za pomocą konta tej grupy powinny mieć pełną kontrolę.

Po zakończeniu konfigurowania uprawnień należy kliknąć przycisk **Apply** (Zastosuj), a następnie kliknąć przycisk **Advanced** (Zaawansowane), aby porównać ustawienia pokazane w oknie dialogowym *Advanced Security Settings* (Zaawansowane ustawienia zabezpieczeń) z ustawieniami pokazanymi na rysunku 6-10.

Aby skonfigurować te uprawnienia, trzeba wyłączyć dziedziczenie. W przeciwnym razie wszyscy użytkownicy, a nie tylko należący do grupy Project 101, będą mogli odczytywać pliki foldera Project 101. Folder nadrzędny `c:\docs` przekazuje uprawnienie *Users: Allow Read & Execute* (Użytkownicy: Zezwalaj na odczyt i wykonanie). Jedynym sposobem odmowy tego dostępu jest usunięcie zaznaczenia opcji *Allow Inheritable Permissions From The Parent...* (Zezwalaj na propagowanie dziedziczonych uprawnień z obiektu nadrzędnego...). Warto zauważyć, że wymagania nie określają konieczności odmowy prawa odczytu dla członków grupy *Users* (Użytkownicy), ale również wprost nie zostało powiedziane, że uprawnienie to (odczyt) jest wymagane. Prawo odczytu nie zostanie przydzielone ze względu na stosowanie zalecanej zasady przydzielania jedynie minimum wymaganych uprawnień.

Po zablokowaniu dziedziczenia, okno dialogowe *Advanced Security Settings* (Zaawansowane ustawienia zabezpieczeń) powinno wyglądać tak, jak przedstawia to rysunek 6-10.



Rysunek 6-10 Zakładka Permissions (Uprawnienia) okna dialogowego Advanced Security Setting (Zaawansowane ustawienia zabezpieczeń)

Opcja zezwalająca na dziedziczenie została zablokowana, więc wszystkie uprawnienia wyświetlane są jako <nic dziedziczono. Pełną kontrolę mają członkowie grup *Administrators* (Administratora'), *System* oraz *Creator Owner* (Twórca właściciel). Należy pamiętać, że jeśli grupa *Creator Owner* (Twórca-właściciel) ma pełną kontrolę, użytkownik, który utworzył plik lub folder, ma pełną kontrolę nad tym zasobem. Grupa Project 101 została zaznaczona jako posiadająca specjalne wpisy uprawnień. Po zaznaczeniu tej pozycji i kliknięciu polecenia **View/Edit** (Przeglądaj/Edytuj) można zobaczyć uprawnienia przydzielone grupie Project 101 (uprawnienia przedstawione zostały na rysunku 6-11).



Rysunek 6-11 Specjalne uprawnienia grupy Project 101

Grupa Managers ma uprawnienia: *Read, Write, Read&Execute* (Zezwalaj: Odczyt, Zapis, Odczyt i wykonanie). Szablon ten pozwala również utworzyć pliki i foldery oraz, podobnie jak dla członków grupy Project 101, jeśli członek grupy Managers tworzy zasób, do tego zasobu przydzielane są dla niego uprawnienia *Creator Owner* (Twórca właściciel). Ten zestaw uprawnień *nie* pozwala członkom grupy

Managers usuwać plików innych użytkowników. Warto zapamiętać, że szablon uprawnień *Modify* (Modyfikowanie), który nie został przydzielony, zawiera uprawnienie *Delete* (Usuwanie).

Ćwiczenie 2: Stosowanie uprawnień odmowy

1. Została wynajęta grupa dostawców. Dla dostawców, wszystkie konta użytkowników umieszczone zostały w grupie Project Contractors i nie należą do żadnej innej grupy domeny. Co należy zrobić, aby uniemożliwić dostawcom dostęp do foldera Project 101, który był zabezpieczany w poprzednim ćwiczeniu?

Nic. Ponieważ dostawcy nie należą do żadnej innej grupy domeny, nie mają uprawnień przydzielanych przez aktualną listę ACL, która mogłaby zezwolić na dostęp do zasobu. Dlatego nie zachodzi konieczność odmowy uprawnień.

2. Załóżmy, że pewne konta użytkowników, takie jak konto Scott Bishop, należą do obu grup Project Contractors oraz Engincers. Co należy zrobić, aby uniemożliwić dostęp dla dostawców?

W tym przypadku trzeba odmówić uprawnień (Deny) dla grupy Project Contractors. Ponieważ grupa ta otrzymała uprawnienia Allow (Zezwalaj) przydzielone innym grupom, muszą one zostać unieważnione przez odmowę uprawnień (Deny).

3. Skonfiguruj folder tak, aby dla grupy Project Contractors następowała odmowa uprawnień Full Control (Pełna kontrola).

Ćwiczenie 3: Uprawnienia czynne

1. Dla foldera Project 101, otwórz okno dialogowe Advanced Security Settings (Zaawansowane ustawienia zabezpieczeń) - uruchomienie okna właściwości foldera, kliknięcie zakładki Security (Zabezpieczenia), a następnie kliknięcie przycisku Advanced (Zaawansowane).
2. Kliknij zakładkę Effective Permissions (Czynne uprawnienia).
3. Wybierz każdego z wymienionych poniżej użytkowników i sprawdź jego uprawnienia.

Użytkownik Czynne uprawnienia

Scott Bishop	Brak uprawnień
Danielle Tiedt	Traverse Folder/Execute File (Przechodzenie przez folder/ Wykonywanie pliku) List Folder/Read Data (Wyświetlanie zawartości foldera/Odczyt danych) Read Attributes (Odczyt atrybutów) Read Extended Attributes (Odczyt atrybutów rozszerzonych) Create Files/Write Data (Tworzenie plików/Zapis danych) Create Folders/Append Data (Tworzenie folderów/Dołączanie danych) Read Permissions (Odczyt uprawnień)
Lorrin Smith-Bates	Traverse Folder/Execute File (Przechodzenie przez folder/ Wykonywanie pliku) List Folder/Read Data (Wyświetlanie zawartości foldera/Odczyt danych) Read Attributes (Odczyt atrybutów) Read Extended Attributes (Odczyt atrybutów rozszerzonych) Create Files/Write Data (Tworzenie plików/Zapis danych) Create Folders/Append Data (Tworzenie folderów/Dołączanie danych)

ciąg dalszy na następnej stronie

ciąg dalszy ze strony poprzedniej

Użytkownik Czynne uprawnienia

Lorrin Smidv Write Attributes (Zapis atrybutów)

Bates (*ceL*) Write Extended Attributes (Zapis atrybutów rozszerzonych)
Read Permissions (Odczyt uprawnień)

Jeśli wymienione powyżej uprawnienia nie zgadzają się z listą uprawnień utworzoną podczas ćwiczenia, oznacza to, że na liście uprawnień pojawił się błąd (w tym przypadku należy powrócić do ćwiczenia 1 i 2) lub błąd występuje w definicji członkostwa grup (w takim przypadku należy powrócić do sekcji „Wymagania” znajdujące się na początku rozdziału). Należy wprowadzić korekty, aż uzyskana zostanie zgodność list uprawnień.

Ćwiczenie 4: Własność

1. Zaloguj się jako Danielle Tiedt.
2. Otwórz folder udostępniony przyłączając się do foldera \\Server01\Docs.
3. Otwórz folder Project 101 i utwórz w nim plik tekstowy nazwany **Report**.
4. Dla pliku Report, otwórz okno dialogowe Adva.nc.ed Security Settings (Zaawansowane ustawienia zabezpieczeń).
5. Sprawdź, czy wszystkie uprawnienia są dziedziczone po folderze nadrzędnym. Jakie występują różnice w listach ACL pomiędzy tym obiektem a folderem Project 101?
Folder Project 101 przydziela uprawnienia *Full Control* (Pełna kontrola) dla grupy *Creator Owner* (Twórca właściciel). Plik Report przydziela uprawnienia *Full Control* (Pełna kontrola) dla użytkownika Danielle. Jeśli Danielle utworzy plik, jej identyfikatorowi SID zostaną przypisane uprawnienia przydzielone specjalnej grupie *Creator Owner* (Twórca właściciel). Oprócz tego, uprawnienie grupy Project 101 Team do tworzenia plików i folderów (*Create Files* oraz *Create Folders*) jest uprawnieniem foldera i nie występuje na liście ACL pliku Report.
6. Zaloguj się jako administrator.
7. Dla pliku Report otwórz okno dialogowe *Advanced Security Settings* (Zaawansowane ustawienia zabezpieczeń).
8. Kliknij zakładkę **Owner** (Właściciel).
9. Sprawdź, czy Danielle jest na liście aktualnych właścicieli.
10. Zaznacz swoje konto użytkownika i kliknij przycisk **Apply** (Zastosuj). Administrator stał się teraz właścicielem obiektu.
11. Użytkownik posiadający uprawnienie *Restore Files And Directories* (Odtwarzanie plików i katalogów) może przekazywać własność obiektu innemu użytkownikowi. Kliknij opcję **Other Users Or Group** (Inni użytkownicy lub grupy) i zaznacz użytkownika Lorrin Smith-Bates. Po wyświetleniu konta Lorrin na liście **Change Owner To** (Zmień właściciela na:), zaznacz je i kliknij przycisk **Apply** (Zastosuj).
12. Sprawdź, czy użytkownik Lorrin jest nowym właścicielem pliku Report.
- 13- Czy użytkownik Lorrin ma obecnie pełną kontrolę nad obiektem? Dlaczego tak lub dlaczego nie? Czy użytkownik Danielle zachował pełną kontrolę lub jego uprawnienia zostały zmienione? Sprawdź to za pomocą zakładki *Effective Permissions* (Czynne uprawnienia).

Użytkownik Lorrin nie ma pełnej kontroli, a jedynie uprawnienia *Modiyy* (Modyfikowanie). Lorrin jest członkiem grupy Managers, która takie uprawnienia posiada. Uprawnienia *Fuli Control* (Pełna kontrola) są przypisane grupie *Creator Owner* (Twórca właściciel) i przydzielane użytkownikowi jedynie wtedy, gdy tworzy obiekt.



Informacja Zmiana właściciela, po utworzeniu obiektu, nie modyfikuje w żaden sposób listy ACL

>P> Nowy właściciel lub dowolny użytkownik mający uprawnienia Allow Change Permissions (Zezwalaj: Zmiana uprawnień) może jednak modyfikować listę ACL i określać odpowiedni dla siebie poziom dostępu do zasobu.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Jakie są minimalne uprawnienia NTFS umożliwiające użytkownikowi otwieranie dokumentów i uruchamianie programów przechowywanych w udostępnionym folderze?
 - a. Fuli Control (Pełna kontrola)
 - b. Modify (Modyfikowanie)
 - c. Write (Zapis)
 - d. Read & Execute (Odczyt i wykonanie)
 - e. List Folder Contents (Wyświetlanie zawartości foldera)
2. Użytkownik Bill nie może uzyskać dostępu do planu wydziału. Po otwarciu zakładki Security (Zabezpieczenia) dla tego zasobu okazało się, że wszystkie uprawnienia do dokumentu dziedziczone są po folderze nadrzędnym. Grupie, do której należy Bill, odmówiono uprawnień Read (Odczyt). Która z poniższych metod umożliwi dostęp do planu wydziału dla użytkownika Bill?
 - a. Zmodyfikowanie uprawnień foldera nadrzędnego poprzez dodanie uprawnienia BilkAllow Fuli Control (Bill: Zezwalaj na pełną kontrolę).
 - b. Zmodyfikowanie uprawnień foldera nadrzędnego poprzez dodanie uprawnienia BilhAllow Read (Bill: Zezwalaj na odczyt).
 - c. Zmodyfikowanie uprawnień dokumentu „plan” poprzez dodanie uprawnienia BilliAllow Read (Bill: Zezwalaj na odczyt).
 - d. Zmodyfikowanie uprawnień dokumentu „plan” poprzez usunięcie uprawnienia Allow Inheritable Permissions (Zezwalaj na dziedziczenie uprawnień), wybranie polecenia Copy (Kopiuj) i usunięcia odmowy uprawnień (Deny).
 - e. Zmodyfikowanie uprawnień dokumentu „plan” poprzez usunięcie uprawnienia Allow Inheritable Permissions (Zezwalaj na dziedziczenie uprawnień), wybranie polecenia Copy (Kopiuj) i dodanie uprawnienia BilkAllow Fuli Control (Bill: Zezwalaj na pełną kontrolę).
 - f. Usunięcie użytkownika Bill z grupy, której odmówiono uprawnień (Deny).

3. Użytkownik Bill dzwonił ponownie informując, że w dalszym ciągu nie może uzyskać dostępu do planu wydziału. Administrator użył narzędzia Effective Permissions (Czynne uprawnienia), zaznaczył konto użytkownika Bill i okazało się, że Bill posiada wystarczające uprawnienia. Czym można wyjaśnić rozbieżność pomiędzy wynikami programu Effective Permissions (Czynne uprawnienia) a informacjami podanymi przez użytkownika?

Podsumowanie lekcji

- Uprawnienia NTFS mogą być skonfigurowane za pomocą edytora ACL. Edytor ma trzy okna dialogowe: zakładka *Security* (Zabezpieczenia), *Advanced Security Settings* (Zaawansowane ustawienia zabezpieczeń) oraz *Permission Entry For* (Wpisy uprawnień dla).
- Uprawnień można odmawiać lub można na nie zezwalać. Uprawnienia mogą być bezpośrednie lub dziedziczone. Odmowa (*Deny*) uprawnienia ma pierwszeństwo nad zezwoleniem (*Allow*) uprawnienia. Podobnie, uprawnienia bezpośrednie mają pierwszeństwo nad uprawnieniami dziedziczonymi. W rezultacie, bezpośrednie uprawnienie *Allow* (Zezwalaj) unieważnia dziedziczone uprawnienie *Deny* (Odmawiaj).
- Dziedziczenie umożliwia administratorom zarządzanie uprawnieniami w pojedynczym folderze nadrzędnym, który zawiera pliki i foldery, dla których obowiązują te same wymagania związane z dostępem do zasobu. Ustawienia domyślne określają, że lista ACL nowego obiektu zawiera uprawnienie zezwalające na dziedziczenie po folderze nadrzędnym.
- Istnieje kilka metod zmiany wyników działania dziedziczenia uprawnień. Można zmodyfikować uprawnienia pierwotne (obiektu nadrzędnego) i zezwolić, żeby nowe uprawnienia były dziedziczone przez obiekt. Można określać uprawnienia bezpośrednie obiektu (uprawnienia takie mają pierwszeństwo nad uprawnieniami dziedziczonymi) lub można dla obiektu zablokować dziedziczenie i skonfigurować listę ACL używając do definiowania dostępu uprawnień bezpośrednich.
- Zakładka *Effective Permissions* (Czynne uprawnienia) w oknie dialogowym *Advanced Security Settings* (Zaawansowane ustawienia zabezpieczeń) jest przydatnym narzędziem umożliwiającym dla użytkowników lub grup określenie przybliżonego poziomu dostępu do zasobu. Narzędzie analizuje uprawnienia konta, jak również uprawnienia grup, do których dane konto należy.
- Właściciel obiektu może w dowolnym momencie modyfikować listę ACL tego obiektu. Użytkownik, który ma uprawnienie *Take Ownership* (Przejmij na własność) może stać się właścicielem obiektu. Administratorzy mogą stać się właścicielami dowolnego obiektu systemu. Konta grup *Administrators*, *Backup Operators* (Operatorzy kopii zapasowych) oraz inne konta, którym przydzielone zostało prawo *Restore Files And Directories* (Odtwarzanie plików i katalogów) mogą zmienić właściciela pliku lub foldera i cechę tę przypisywać innemu użytkownikowi lub grupie.

Lekcja 3: Inspekcja dostępu systemu plików

Wiele organizacji poddaje inspekcji dostęp systemu plików, aby uzyskać pogląd na poziom wykorzystania zasobów oraz potencjalne luki w zabezpieczeniach. Windows Server 2003 obsługuje inspekcję pojedynczych elementów systemu bazując na kontach użytkowników lub grup oraz specyficznych działaniach realizowanych przez te konta. Aby skonfigurować inspekcję, należy wykonać trzy kroki: określić ustawienia inspekcji, włączyć zasadę inspekcji oraz sprawdzić zdarzenia zarejestrowane w dzienniku zabezpieczeń. Niniejsza lekcja omawia te procesy i doradza, w jaki sposób skutecznie przeprowadzać inspekcję tak, aby spełnić wymagania przedsiębiorstwa i jednocześnie nie „utonać” analizując przeróżne wpisy dziennika zdarzeń.

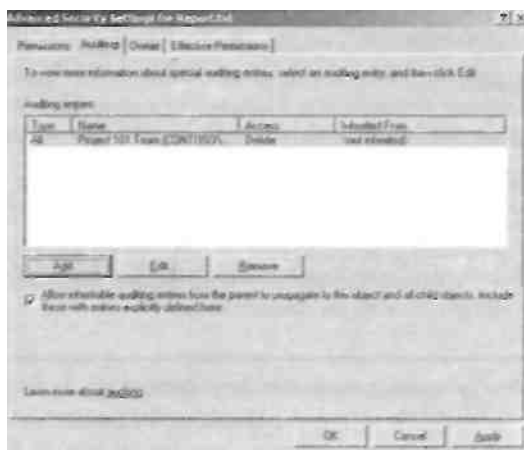
Materiały omówione podczas lekcji pozwalają na

- Konfigurowanie ustawień inspekcji dla pliku lub foldera
- Włączanie inspekcji dla serwera autonomicznego lub grupy serwerów
- Analiza zdarzeń inspekcji zarejestrowanych w dzienniku Security (Zabezpieczenia)

Szacunkowy czas lekcji: 20 minut

Konfigurowanie zdarzeń inspekcji

Aby zdefiniować działania, które mają być monitorowane bądź śledzone, należy dla pliku lub foldera skonfigurować ustawienia inspekcji w oknie dialogowym *Advanced Security Settings* (Zaawansowane ustawienia zabezpieczeń). Zakładka *Auditing* (Inspekcja), pokazana na rysunku 6-12, wygląda bardzo podobnie do zakładki *Permissions* (Uprawnienia). Jedynie, zamiast wpisów uprawnień, dodawane są wpisy dotyczące inspekcji.



Rysunek 6-12 Zakładka *Auditing* (Inspekcja) okna dialogowego *Advanced Security Settings* (Zaawansowane ustawienia zabezpieczeń)

W celu poddania inspekcji użytkownika, grupę lub komputer, należy kliknąć przycisk Add (Dodaj). Następnie, w oknie dialogowym *AuditingEntry* (Wpis inspekcji), pokazanym na rysunku 6-13, należy wskazać uprawnienie używane do inspekcji.



Rysunek 6-13 Okno dialogowe *Auditing Entry* (Wpis inspekcji)

Można rejestrować udane, nieudane lub obie próby dostępu do zasobu przy użyciu każdego pojedynczego uprawnienia, które zostało przypisane do danego obiektu.

Dla wymienionych poniżej zdarzeń można rejestrować udane próby (sukcesy):

- Rejestrowanie dostępu do zasobu w celu tworzenia raportu i rozliczeń.
- Monitorowanie dostępu, który wskazuje, że użytkownicy przeprowadzają działania inne niż dla nich zaplanowane, co wskazuje, że ich uprawnienia są zbyt silne.
- Rozpoznawanie dostępu, który dla danego konta jest poza zakresem jego funkcji, co może oznaczać, że konto użytkownika jest używane przez włamywacza.

Inspekcja nieudanych prób dostępu umożliwia:

- Monitorowanie złośliwych prób dostępu do zasobu, dla których nastąpiła odmowa dostępu.
- Rozpoznawanie nieudanych prób dostępu do pliku lub foldera, do których użytkownik powinien uzyskać dostęp. Sytuacja taka wskazuje, że uprawnienia nie są wystarczające do wykonywania powierzonych zadań.

Ustawienia inspekcji, podobnie jak uprawnienia, podlegają regułom dziedziczenia. Dziedziczenie ustawień inspekcji jest stosowane do obiektów, które zezwalają na dziedziczenie.



Informacja Dzienniki inspekcji dość szybko zwiększają swoje rozmiary i dlatego regułą dla inspekcji powinno być konfigurowanie absolutnie minimalnych ustawień pozwalających zrealizować zadania w przedsiębiorstwie. Określenie dla inspekcji rejestrowania udanych i nieudanych zdarzeń dla często używanego foldera i dla grupy Everyone (Wszyscy), a także dla wszystkich uprawnień będzie generować ogromną liczbę wpisów dziennika inspekcji, co będzie miało wpływ na wydajność serwera i może również uniemożliwić wyszukanie określonych zdarzeń poddanych inspekcji.

Włączanie inspekcji

Samo skonfigurowanie wpisów deskryptora zabezpieczeń pliku bądź foldera nie włącza jeszcze inspekcji. Inspekcja włączana jest za pośrednictwem zasady. Po włączeniu inspekcji, podsystem zabezpieczeń zaczyna sprawdzać ustawienia inspekcji i rejestrować dostępy określone przez te ustawienia.

Zasada inspekcji może zostać włączona na serwerze autonomicznym za pomocą konsoli *Local Security Policy* (Lokalna zasada zabezpieczeń), a na kontrolerze domeny za pomocą konsoli *Domain Controller Security Policy* (Zasada zabezpieczeń kontrolera domeny). Należy wybrać węzeł **Audit Policy** (Zasada inspekcji) znajdujący się poniżej węzła **Local Policies** (Zasady lokalne) i dwukrotnie kliknąć zasadę **Audit Object Access** (Przeprowadź inspekcję dostępu do obiektu). Należy zaznaczyć opcję **Deny These Policy Settings** (Definiuj następujące ustawienia zasad), a następnie zaznaczyć, czy włączona będzie inspekcja dla „sukcesu”, dla „niepowodzenia” czy dla obu tych zdarzeń.



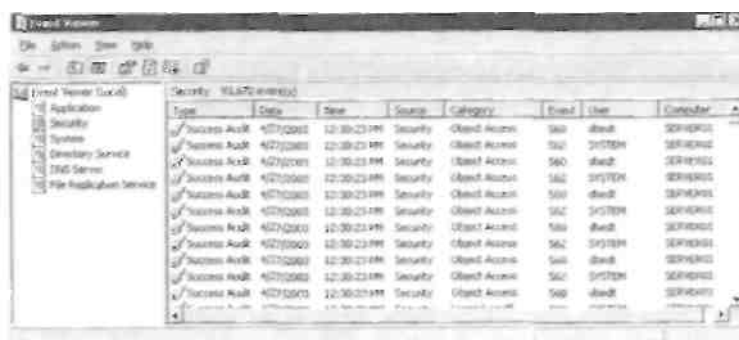
Informacja Warto zapamiętać, że dostęp, który jest poddany inspekcji i protokolowany, jest połączeniem wpisów inspekcji dotyczących określonego foldera bądź pliku oraz ustawień zasady inspekcji (Audit Policy). Jeśli wpis inspekcji określa rejestrowanie niepowodzeń, a zasada włączyła jedynie rejestrowanie udanych prób, to dziennik inspekcji pozostanie pusty.

Za pomocą obiektu GPO (Active Directory Group Policy Objects), inspekcję można także włączyć dla kilku komputerów. Węzeł *Audit Policy* (Zasada inspekcji) można znaleźć rozwijając kolejno węzły *Computer Configuration* (Konfiguracja komputera), *Windows Settings* (Ustawienia systemu Windows), *Security Settings* (Ustawienia zabezpieczeń), *Local Policies* (Zasady lokalne). Podobnie jak dla wszystkich zasad grupy, komputery, do których stosuje się zasadę, określone są przez definicję zakresu zasady. Jeśli przykładowo zasada powiązana zostanie z jednostką organizacyjną Servers i włączona zostanie inspekcja, to wszystkie obiekty komputerów tej jednostki poddane zostaną inspekcji dostępu do zasobów, zgodnie z wpisami inspekcji dotyczącymi plików i folderów dla danego systemu.

Analiza dziennika zabezpieczeń

Po skonfigurowaniu dla plików i folderów wpisów inspekcji oraz po włączeniu inspekcji za pomocą zasady lokalnej lub zasady grupy, system rozpoczyna rejestrować dostępy, zgodnie z wpisami inspekcji. Wyniki można przeglądać i analizować za pomocą programu *Event Viewer* (Podgląd zdarzeń), w którym należy wybrać dziennik *Security* (Zabezpieczenia) tak, jak to zostało pokazane na rysunku 6-14.

Jak łatwo zauważyć, dziennik *Security* (Zabezpieczenia) może zawierać dużo wpisów, w zależności od typu wykonywanej inspekcji. Zdarzenia można sortować, aby ułatwić sobie rozpoznawanie zdarzeń dostępu do obiektu. W tym celu należy kliknąć nagłówek kolumny *Category* (Kategoria) i zlokalizować zdarzenia *Object Access* (Dostęp do obiektu).



Rysunek 6-14 Dziennik Security (Zabezpieczenia) programu Event Viewer (Podgląd zdarzeń)

Sortowanie jest tylko pewną pomocą podczas „przekopywania się” przez zaprotokołowane zdarzenia. Lepsze rezultaty można uzyskać stosując filtrowanie zdarzeń dziennika za pomocą polecenia **Filter** (Filtr) znajdującego się w menu **View** (Widok) lub poprzez wybranie zakładki **Security** (Zabezpieczenia), następnie polecenia **Properties** (Właściwości) z menu **Action** (Akcja) bądź z menu skrótów, a na koniec wybranie zakładki **Filter** (Filtr). Zakładka **Filter** (Filtr) umożliwia określenie kryteriów wyszukiwania, jak na przykład typ zdarzenia, kategoria, źródło, przedział czasu, użytkownik czy komputer. Rysunek 6-15 ilustruje przykład filtra zastosowanego przy rozpoznawaniu zdarzeń inspekcji dotyczących dostępu do określonych danych.



Rysunek 6-15 Zakładka Filter (Filtr)

Ostatecznie, istnieje również możliwość wyeksportowania dziennika **Security** (Zabezpieczenia) poprzez wybranie z menu kontekstowego polecenia **Save Log File As** (Zapisz plik dziennika jako). Plik w macierzystym formacie dziennika zdarzeń ma rozszerzenie .cvt. Za pomocą programu *Event Vieioer* (Podgląd zdarzeń) plik może być otwierany w innych systemach. Alternatywna metoda to zapisanie pliku w formatach, w których wartości rozdzielane są przecinkami lub znakami tabulacji. Plik w takim

formacie może być otwierany przez szereg narzędzi analizy, w tym przez program Microsoft Excel. W programie Excel można oczywiście stosować filtry, aby wyszukać bardziej specyficzne informacje, jak na przykład dla danego zdarzenia zawartość pola *Description* (Opis).

Zadanie kontrolne: Inspekcja systemu plików

W zadaniu tym zostanie przeprowadzona konfiguracja ustawień inspekcji, dla dostępu do obiektu włączone zostaną zasady inspekcji oraz w dzienniku zabezpieczeń wyszukane zostaną specyficzne zdarzenia. Typowym zadaniem administratora przedsiębiorstwa jest monitorowanie usuwania plików przechowywanych w ważnych folderach, dzięki czemu mamy pewność, że jedynie odpowiedni użytkownicy usuwają pliki.

Ćwiczenie 1: Konfigurowanie ustawień inspekcji

1. Zaloguj się jako Administrator.
2. Otwórz okno dialogowe *Advanced Security Settings* (Zaawansowane ustawienia zabezpieczeń) dla foldera C:\Docs\Project 101.
3. Kliknij zakładkę **Auditing** (Inspekcja).
4. Dodaj wpis inspekcji, który pozwala śledzić grupę Project 101 Team. Określ, że monitorowane mają być działania dotyczące uprawnienia **Delete** (Usuń) zakończone zarówno powodzeniem, jak i niepowodzeniem.

Ćwiczenie 2: Włączenie zasady inspekcji

Ponieważ administrator zalogował się do kontrolera domeny, do włączenia inspekcji używana będzie konsola *Domain Controller Security Policy* (Zasada zabezpieczeń kontrolera domeny). Na serwerze autonomicznym byłaby używana zasada *Local Security Policy* (Lokalna zasada zabezpieczeń). Do włączania inspekcji można również stosować obiekty GPO.

1. Otwórz konsolę **Domain Controller Security Policy** (Zasada zabezpieczeń kontrolera domeny) znajdującą się w folderze **Administrative Tools** (Narzędzia administracyjne).
2. Rozwiń węzeł **Local Policies** (Zasady lokalne) i wybierz Zasadę inspekcji.
- 3- Dwukrotnie kliknij zasadę **Audit Object Access** (Przeprowadź inspekcję dostępu do obiektu).
4. Zaznacz pole wyboru **Define These Policy Settings** (Definiuj następujące ustawienia zasad)
5. Włącz inspekcję zarówno dla wpisów dotyczących powodzenia, jak i niepowodzenia wykonywanych operacji.
6. Kliknij przycisk OK, a następnie zamknij konsolę.
7. Aby odświeżyć zasadę i upewnić się, że zastosowane zostały wszystkie ustawienia, otwórz okno wiersza poleceń i wpisz komendę **gpupdate**.

Ćwiczenie 3: Generowanie zdarzeń inspekcji

1. Zaloguj się jako Danielle Tiedt.
2. Przyłącz się do foldera \\ServerO 1 \Docs\Project 101.
3. Usuń plik tekstowy Report.

Ćwiczenie 4: Analiza dziennika zabezpieczeń

1. Zaloguj się jako administrator.
2. Otwórz program **Event Viewer** (Podgląd zdarzeń) znajdujący się w folderze **Administrative Tools** (Narzędzia administracyjne).
3. Wybierz dziennik **Security** (Zabezpieczenia).
4. Jakiego typu zdarzeń został zarejestrowany w dzienniku *Security* (Zabezpieczenia)? Czy tylko zdarzenia typu *Object Access* (Dostęp do obiektu)? Jakiego inne typy zdarzeń zostały zarejestrowane? Warto zapamiętać, że zasady mogą włączyć inspekcję dla wielu czynności związanych z bezpieczeństwem, wliczając w to dostęp do usługi katalogowej, zarządzanie kontem, logowanie itp.
5. Aby zawęzić zakres wyszukiwania zdarzeń dziennika, z menu View (Widok) wybierz polecenie **Filter (Filtr)**.
6. Skonfiguruj filtr tak, aby zakres został maksymalnie zawężony. Co wiadomo o zdarzeniach, które próbujemy wyszukać? Wiadomo, że inspekcja dotyczyła „powodzenia” oraz „niepowodzenia”, że kategoria zdarzeń to *Object Access* (Dostęp do obiektu) oraz że zdarzenia miały miejsce w dniu dzisiejszym. Poprawność wykonanych czynności można sprawdzić porównując z ekranem przedstawionym na rysunku 6-15.
7. Kliknij przycisk **Apply** (Zastosuj).
8. Czy istnieje prostszy sposób wyszukiwania zdarzenia związanego z usunięciem pliku Report przez użytkownika Danielle? Otwórz zdarzenie i sprawdź informacje tam umieszczone. Opis zdarzenia identyfikuje użytkownika, plik oraz czynność. Można więc nie filtrować zawartości opisu za pomocą programu *Event Viewer* (Podgląd zdarzeń), lecz wyeksportować plik i przeprowadzić jego analizę innymi narzędziami, jak na przykład za pomocą programu Microsoft Excel.
9. (Opcjonalne) Jeśli masz dostęp do programu Microsoft Excel, kliknij prawym przyciskiem myszy węzeł dziennika **Security** (Zabezpieczenia) i wybierz polecenie **Save Log File As** (Zapisz plik dziennika jako). Wpisz nazwę dla pliku oraz wybierz typ pliku *Comma-Delimited* (wartości rozdzielane przecinkami). Otwórz plik za pomocą programu Excel.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Które z wymienionych niżej czynności muszą być przeprowadzone, aby wygenerowany został dziennik rejestrujący dostęp do zasobu (dla pliku lub foldera)? Wybierz wszystkie właściwe odpowiedzi.
 - a. Skonfigurowanie uprawnień NTFS, które pozwalają kontu grupy System przeprowadzać inspekcję dostępu do zasobu.
 - b. Skonfigurowanie wpisów inspekcji określających typ dostępu poddanego inspekcji.
 - c. Włączenie zasady Audit Privilege Use (Przeprowadź inspekcję użycia uprawnień).
 - d. Włączenie zasady Audit Object Access (Przeprowadź inspekcję dostępu do obiektu).

2. Które z wymienionych poniżej kryteriów są prawidłowymi kryteriami nitrowania dziennika zabezpieczeń pozwalającymi zidentyfikować określone zdarzenia związane z dostępem do plików i folderów? Wybierz wszystkie właściwe odpowiedzi.
 - a. Data zdarzenia
 - b. Użytkownik, który spowodował powstanie zdarzenia
 - c. Typ dostępu do obiektu, który wygenerował zdarzenie
 - d. Inspekcja „powodzenia” lub „niepowodzenia”
3. Aby uzyskać dostęp do serwera Sever01, użytkownicy firmy Contoso Ltd. korzystają z aplikacji Microsoft Office. Zadaniem administratora jest monitorowanie serwera Server01 tak, aby uprawnienia te nie były zbyt restrykcyjne i użytkownicy nie mieli problemów z uzyskaniem swoich przydziałów. Który dziennik oraz który typ zdarzenia rejestruje informacje potrzebne administratorowi?
 - a. Dziennik Application (Aplikacja); Zdarzenie — Sukces
 - b. Dziennik Application (Aplikacja); Zdarzenie — Niepowodzenie
 - c. Dziennik Security (Zabezpieczenia); Zdarzenie — Sukces
 - d. Dziennik Security (Zabezpieczenia); Zdarzenie — Niepowodzenie
 - e. Dziennik System; Zdarzenie — Sukces
 - f. Dziennik System; Zdarzenie - Niepowodzenie

Podsumowanie lekcji

- Wpisy inspekcji są przechowywane w deskrytorze zabezpieczeń plików lub folderów wolumenów NTFS. Są konfigurowane przy użyciu programu Windows Explorer (Eksplorator Windows), za pomocą okna dialogowego Advanced Security Settings (Zaawansowane ustawienia zabezpieczeń) we właściwościach danego pliku bądź foldera.
- Same wpisy inspekcji nie powodują generowania dzienników inspekcji. Musi być jeszcze włączona zasada Audit Object Access (Przeprowadź inspekcję dostępu do obiektu) będąca częścią zasady Local Security Policy (Lokalna zasada zabezpieczeń), Domain Controller Security Policy (Zasada zabezpieczeń kontrolera domeny) lub obiektu GPO.
- Dziennik Security (Zabezpieczenia) można przeglądać w przystawce Event Viewer (Podgląd zdarzeń). Dziennik umożliwia zlokalizowanie i analizę zdarzeń związanych z dostępem do obiektu.

Lekcja 4: Administracja Internet Information Services (Internetowe usługi informacyjne)

W lekcji 1 omówione zostały zagadnienia dotyczące udostępniania foldera tak, aby użytkownicy korzystający z programu *Client For Microsoft Networks* (Klient sieci Microsoft Networks) mogli uzyskać dostęp do serwera, na którym uruchomione są usługi *File And Print Sharing For Microsoft Networks* (Udostępnianie plików i drukarek w sieciach Microsoft Networks). Jest to jednak tylko jeden ze sposobów uzyskiwania dostępu do potrzebnych plików i folderów. Istnieje także możliwość uzyskiwania dostępu za pośrednictwem technologii sieci Internet, takich jak usługi FTP bądź Web (HTTP).

Niniejsza lekcja omawia sposoby konfigurowania i zarządzania usługami IIS. Opisane zostanie jak skonfigurować strony sieci Web czy usługi FTP, katalogi wirtualne oraz zabezpieczenia programu IIS.

Materiały omówione podczas lekcji pozwalają na

- Instalowanie programu IIS
- Konfigurowanie stron Web oraz FTP
- Konfigurowanie strony domyślnych danych sieci Web
- Tworzenie katalogu wirtualnego sieci Web
- Modyfikowanie ustawień uwierzytelnienia i zabezpieczeń usługi IIS

Szacunkowy czas lekcji: 20 minut

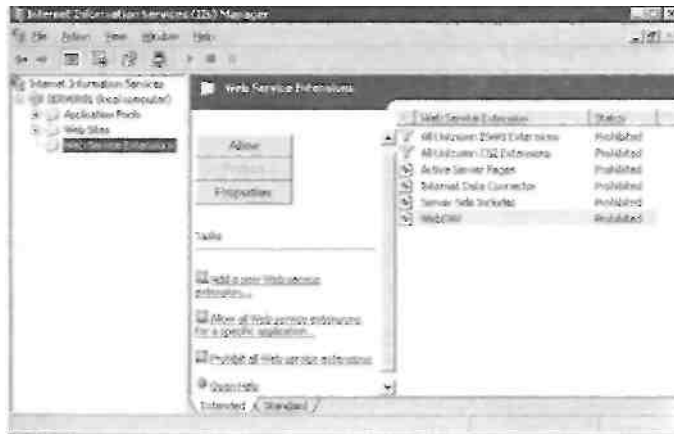
Instalowanie programu IIS 6.0

W celu zmniejszenia ryzyka ataku na system Windows Server 2003, usługi IIS nie są domyślnie instalowane. Usługi te należy zainstalować za pomocą programu **Add/Remove Windows Components Wizard** (Kreator składników systemu Windows) uruchamianego w module **Add Or Remove Programs** (Dodaj lub usuń programy) programu **Control Panel** (Panel sterowania). Po zaznaczeniu pozycji **Application Server** (Serwer aplikacji), należy kliknąć przycisk **Details** (Szczegóły), a następnie zaznaczyć opcję **Internet Information Services (IIS)** [Internetowe usługi informacyjne (IIS)]. Użytkownik może wybierać komponenty, z których zbudowana zostanie usługa IIS, ale jeśli nie są mu **dokładnie** znane role poszczególnych elementów usługi IIS, nie powinien usuwać żadnych składników domyślnych. Można natomiast dodać niektóre składniki, takie jak ASP.NET, FTP czy *FrontPage Server Extensions* (Rozszerzenie serwera FrontPage).

Administracja środowiska sieci Web

Po zainstalowaniu usług IIS, utworzona zostanie domyślna strona sieci Web, dzięki czemu wprowadzenie i nie środowiska Web staje się szybkie i proste. Użytkownik może modyfikować to środowisko zgodnie ze swoimi wymaganiami. System Windows Server 2003 został wyposażony w narzędzia potrzebne do administrowania usługami i witrynami programu IIS.

Po zakończeniu instalacji, użytkownik może uruchomić konsolę **Internet Information Services (IIS) Manager** (Menedżer internetowych usług informacyjnych) umieszczoną w grupie programów Administrative Tools (Narzędzia administracyjne). Domyślne ustawienia określają, że program IIS może obsługiwać jedynie dane statyczne. Aby włączyć obsługę danych dynamicznych, należy zaznaczyć węzeł Web Service Extensions (Rozszerzenia usługi Web). Zgodnie z rysunkiem 6-16, wszystkie rozszerzenia są zabronione. Należy zaznaczyć odpowiednie rozszerzenie i kliknąć przycisk **Allow** (Zezwalaj).



Rysunek 6-16 Przystawka Internet Information Services (IIS) Manager (Menedżer internetowych usług informacyjnych)

Podczas uzyskiwania przez klienta dostępu do zasobu za pośrednictwem programu IIS, mają miejsce następujące podstawowe procesy:

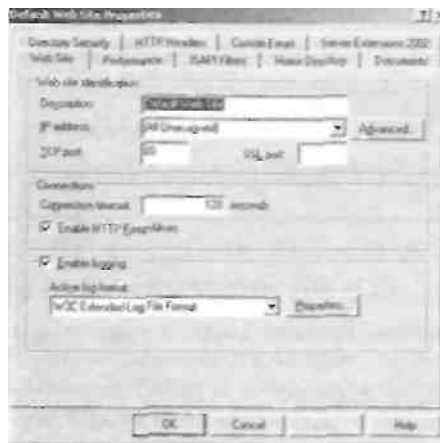
- Wprowadzany przez klienta adres URL (Universal Resource Locator) może mieć następujące formy:
 - » http://ldns.domena.nazwalkatalog_wirtualny/strona.htm lub
 - » ftp://ldns.domena.nazwalkatalog_wirtualny
- Usługa DNS (Domain Name Service) zamienia nazwę na adres IP i odsyła wynik (adres) do klienta
- Klient łączy się z adresem IP serwera przy użyciu portu charakterystycznego dla usługi (najczęściej dla HTTP jest port 80, a dla FTP port 21)
- Adres URL nie przedstawia fizycznej ścieżki do zasobu na serwerze, ale ścieżkę wirtualną. Serwer przekształca żądanie przychodzące tworząc ścieżkę fizyczną i odpowiednie zasoby dla klienta. Na przykład, serwer może wyświetlić listę plików foldera dla klienta FTP lub może przedstawić stronę główną dla klienta HTTP.
- Proces może być chroniony za pomocą uwierzytelnienia (poświadczenia takie jak nazwa użytkownika i hasło) oraz zezwoleń (kontrola dostępu realizowana poprzez uprawnienia).

Proces ten można prześledzić otwierając przeglądarkę i wpisując adres <http://server01>. Serwer wygeneruje stronę „W przygotowaniu”.

Konfigurowanie oraz zarządzanie witrynami Web i FTP

Instalacja programu IIS konfiguruje pojedynczą witrynę sieci Web — Default Web Site (Domyślna witryna sieci Web). Chociaż usługi IIS, w zależności od konfiguracji sprzętu serwera, mogą utrzymywać tysiące lub setki tysięcy witryn, domyślna witryna sieci Web dobrze nadaje się do omówienia funkcjonalności i administracji witryn Web programu IIS. Witryna ta jest dostępna w przeglądarce pod adresem URL: <http://server01.contoso.com>. Wyświetlany tekst informuje, że jest to „strona w przygotowaniu”.

Warto zapamiętać, że żądanie przeglądarki przestane do serwera sieci Web jest kierowane do adresu IP serwera, który został określony przez system DNS na podstawie adresu. Żądanie zawiera adres URL, który często zawiera jedynie nazwę witryny (na przykład: www.microsoft.com). W jaki sposób serwer generuje stronę główną? Jeśli przeanalizujemy zakładkę Web Site (Witryna sieci Web) znajdującą się w oknie Default Web Site Properties (Właściwości domyślnej witryny sieci Web), to można zauważyć, że witryna jest przypisana do grupy adresów All Unassigned IP (Wszystkie nieprzypisane) dla portu 80 (rysunek 6-17). W ten sposób żądanie przeglądarki trafia do portu 80 serwera, który rozpoznaje żądanie i rozpoczyna obsługę domyślnej witryny sieci Web.



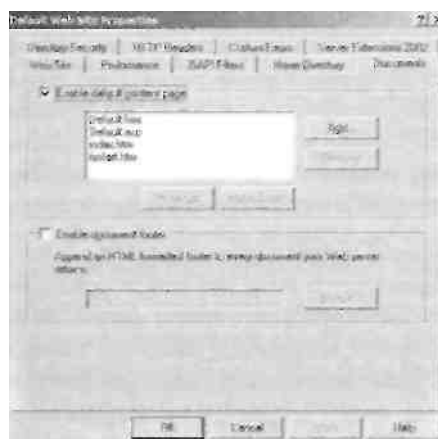
Rysunek 6-17 Zakładka Web Site (Witryna sieci Web) okna dialogowego Default Web Site Properties (Właściwości domyślnej witryny sieci Web)

Następne pytanie dotyczy określenia, które informacje powinny być obsługiwane. Jeśli adres URL zawiera jedynie nazwę witryny (na przykład www.microsoft.com lub server01.contoso.com), to witryna będzie wyświetlała informacje na podstawie katalogu macierzystego. Zakładka Home Directory (Katalog macierzysty), zgodnie z widokiem przedstawionym na rysunku 6-18, wyświetla ścieżkę fizyczną katalogu macierzystego (najczęściej jest to c:\inetpub\wwwroot).



Rysunek 6-18 Zakładka Home Directory (Katalog domowy) okna dialogowego Default Web Site Properties dialog box (Właściwości domyślnej witryny sieci Web)

Który dokładnie plik jest przesyłany do klienta? Plik ten jest określany na zakładce Documents (Dokumenty) pokazanej na rysunku 6-19. Program IIS wyszukuje plik zgodnie z kolejnością przedstawioną na liście. Natychmiast po znalezieniu w ścieżce lokalnej katalogu macierzystego pliku zgodnego z nazwą umieszczoną na liście plików strona zostaje przesłana do klienta, a serwer przerywa dalsze wyszukiwanie. Jeśli plik taki nie został znaleziony, program IIS wyświetla komunikat o błędzie — 404—File Not Found (404 Plik nie został znaleziony) informujący klienta, że żądana strona nie została znaleziona.



Rysunek 6-19 Zakładka Documents (Dokumenty) okna dialogowego Default Web Site Properties (Właściwości domyślnej witryny sieci Web)

W przeglądarce może być wpisany specyficzny adres URL, na przykład <http://server01.contoso.com/contactinfo.htm>. W takim przypadku informacje dla tej konkretnej strony pobierane są z katalogu macierzystego, a jeśli nie można ich znaleźć, zwracany jest błąd 404.

Aby utworzyć witrynę sieci Web, należy prawym przyciskiem myszy kliknąć węzeł **Web Sites** (Witryny sieci Web) i wybrać polecenie **New Web Site** (Nowa witryna sieci Web) lub w programie Manager IIS

kliknąć istniejącą witrynę sieci Web. Aby skonfigurować witrynę, należy otworzyć okno jej właściwości. Można skonfigurować adres IP witryny. Jeśli serwer ma kilka adresów IP, każdy adres IP reprezentuje oddzielną witrynę sieci Web. Kilka witryn może być również obsługiwanych przy użyciu innego portu dla każdej z nich lub przy użyciu nagłówków hosta. Omówienie tych opcji leży poza zakresem materiału przewidzianego dla tej książki. Istnieje również możliwość skonfigurowania ścieżki do katalogu, który jest używany jako katalog macierzysty, a także można modyfikować listę lub kolejność dokumentów, które będą pobierane jako zawartość domyślna strony.

Adres URL może także zawierać bardziej złożoną ścieżkę informacji, jak na przykład <http://www.microsoft.com/windowsserver2003/>. Taki adres URL nie żąda specyficznej strony — na końcu adresu brak rozszerzenia, na przykład .htm bądź .asp. Żądanie takie pobiera informacje z katalogu „windowsserver2003”. Serwer traktuje ten dodatkowy element adresu URL jak katalog wirtualny. Folder zawierający pliki, dla których odniesieniem jest nazwa „windowsserver2003”, może znajdować się w dowolnym miejscu, a nawet nie musi znajdować się na serwerze IIS.

Aby utworzyć katalog wirtualny, należy kliknąć prawym przyciskiem myszy witrynę sieci Web i wybrać polecenie **New Virtual Directory** (Nowy katalog wirtualny). Kreator poprosi o wprowadzenie nazwy zastępczej (alias), która stanie się nazwą foldera używaną w adresie URL oraz o określenie ścieżki fizycznej do zasobu, który może znajdować się na wolumenie lokalnym lub serwerze zdalnym.



Wskazówka egzaminacyjna Katalog wirtualny sieci Web można również utworzyć na dysku NTFS. W tym celu wystarczy kliknąć prawym przyciskiem myszy dany folder, wybrać polecenie Properties (Właściwości), a następnie kliknąć zakładkę Web Sharing (Udostępnianie w sieci Web).

Witryny FTP działają i są administrowane podobnie jak witryny sieci Web. Program IIS instaluje jedną witrynę FTP — Default FTP Site (Domyślna witryna FTP) i konfiguruje ją tak, aby odpowiadała na wszystkie żądania przychodzące FTP (wszystkie nieprzypisane adresy, port 21). Witryna FTP odpowiada klientowi przysyłając listę plików katalogu określonego na zakładce Home Directory (Katalog macierzysty). Witryny FTP mogą również zawierać katalogi wirtualne i tak na przykład w odpowiedzi na żądanie <ftp://lserver01.contoso.com/pub>, mogą zostać przesłane zasoby serwera innego niż <ftp://lserver01.contoso.com/vendor-uploads>. Adresy i witryny FTP nie używają domyślnych dokumentów.

Rozbudowane serwery IIS mogą utrzymywać dziesiątki tysięcy witryn o indywidualnych ustawieniach każdej z nich. Utrata wszystkich informacji konfiguracyjnych może być bardzo dokuczliwa, a trzeba pamiętać, że typowe kopie zapasowe systemu plików umożliwiają odtworzenie danych, ale konfiguracje są gubione. Aby utworzyć kopię zapasową lub odtworzyć konfigurację usługi IIS, należy zapisać lub odtworzyć *metabaze danych*, czyli dokument XML (Extensible Markup Language), który jest używany do przechowywania ustawień. W tym celu, w programie Manager IIS należy prawym przyciskiem myszy kliknąć węzeł serwera i z menu AU **Tasks** (Wszystkie zadania) wybrać polecenie **Backup/ Restore Configuration** (Wykonaj kopię zapasową/Odtwórz konfigurację).



Zobacz także Dodatkowe informacje o programie IIS można znaleźć w książce *Vademecum administratora Microsoft IIS 6.0* (APN Promise, 2003).

Ochrona plików w programie IIS

Zabezpieczenia plików, do których dostęp uzyskiwany jest za pośrednictwem usług IIS, można podzielić na kilka kategorii: uwierzytelnienie, zezwolenia bazujące na uprawnieniach NTFS oraz uprawnieniach IIS. Uwierzytelnienie jest procesem sprawdzania tożsamości przy użyciu nazwy użytkownika i hasła. Domyślne ustawienia określają, że wszystkie żądania skierowane do programu IIS są obsługiwane przez bezosobowego użytkownika, którego konto ma postać `IUSR_nazwakomputera`. Zanim możliwe będzie udostępnianie zasobów tylko określonym użytkownikom, należy utworzyć domenę lub konta użytkowników lokalnych i wymagać wyższego poziomu niż domyślne uwierzytelnienie anonimowe.

Konfigurowanie metod uwierzytelniania'

Na zakładce *Directory Security* (Zabezpieczenia katalogów) serwera, witryny sieci Web (lub FTP), katalogu wirtualnego lub pliku można skonfigurować następujące metody zabezpieczeń:

Opcje uwierzytelnienia sieci Web

- **Uwierzytelnienie anonimowe** Użytkownicy mogą uzyskać dostęp do publicznych obszarów witryny sieci Web bez konieczności podawania nazwy i hasła użytkownika.
- **Uwierzytelnienie podstawowe** Wymagane jest, aby użytkownicy mieli konta użytkownika (lokalne lub w domenie). Poświadczenia przesyłane są zwykłym tekstem.
- **Uwierzytelnienie szyfrowane** Charakteryzuje się taką samą funkcjonalnością, jak w przypadku uwierzytelnienia podstawowego, z tą różnicą, że zapewniony jest wyższy poziom bezpieczeństwa podczas przesyłania w sieci poświadczeń tożsamości użytkownika. Uwierzytelnienie szyfrowane opiera się na protokole HTTP 1.1.
- **Zaawansowane uwierzytelnienie szyfrowane** Działa tylko wtedy, jeśli konto użytkownika jest częścią usługi Active Directory. Metoda gromadzi poświadczenia tożsamości użytkownika i przechowuje je na kontrolerze domeny. Zaawansowane uwierzytelnienie szyfrowane wymaga, aby użytkownik stosował przeglądarkę Internet Explorer w wersji 5 lub późniejszej oraz protokół HTTP 1.1.
- **Zintegrowane uwierzytelnienie systemu Windows** Metoda gromadzi informacje za pomocą chronionej postaci uwierzytelnienia (czasami nazywana metodą uwierzytelnienia Windows NT Challenge/Response), w której nazwa użytkownika oraz hasło, zanim zostaną przesłane w sieci, są kodowane przy pomocy metody mieszania.
- **Certyfikat uwierzytelnienia** Metoda dodaje warstwę zabezpieczeń SSL (Secure Sockets Layer) poprzez wprowadzenie certyfikatów klienta, serwera lub obu stron. Opcja ta jest dostępna jedynie, jeśli usługi certyfikatów (Certificate Services) zostały zainstalowane i skonfigurowane.
- **Uwierzytelnienie usługi Passport w sieci .NET** Metoda ta udostępnia usługę pojedynczego rejestrowania poprzez SSL, przekierowania HTTP, pliki cookies, Microsoft JScript oraz silne szyfrowanie kluczem symetrycznym.

Opcje uwierzytelnienia FTP

- **Uwierzytelnienie anonimowe FTP** Użytkownicy mogą uzyskać dostęp do publicznych obszarów witryny FTP bez konieczności podawania nazwy i hasła użytkownika.
- **Uwierzytelnienie podstawowe FTP** Metoda wymaga, aby użytkownicy logowali się za pomocą nazwy użytkownika i hasła zgodnego z ważnym kontem użytkownika w systemie Windows.

Definiowanie dostępu do zasobu przy pomocy uprawnień

Po skonfigurowaniu uwierzytelnienia, do plików i folderów należy przypisać uprawnienia. Typową metodą definiowania dostępu do zasobów za pośrednictwem usług IIS jest korzystanie z uprawnień NTFS. Uprawnienia NTFS definiują dostęp do zasobu bez względu na sposób uzyskiwania do niego dostępu, ponieważ uprawnienia są przypisane do pliku lub foldera.

Program IIS definiuje również uprawnienia katalogów wirtualnych i witryn. Pomimo, że uprawnienia NTFS określają konkretny poziom dostępu dla istniejących kont użytkowników i grup systemu Windows, uprawnienia zabezpieczeń katalogów skonfigurowane dla witryn lub katalogów wirtualnych stosowane są do *wszystkich* użytkowników i grup. W tabeli 6-2 zostały szczegółowo przedstawione poziomy uprawnień sieci Web:

Tabela 6-2. Uprawnienia katalogu usług IIS

Uprawnienie	Opis
Read (Odczyt) Ustawienie domyślne	Użytkownicy mogą przeglądać dane i właściwości plików
Write (Zapis)	Użytkownicy mogą zmieniać dane i właściwości plików
Script Source Access (Dostęp do źródła skryptu)	Użytkownicy mają dostęp do kodu źródłowego plików, takich jak skrypt) aplikacji ASP (Active Server Pages). Opcja ta jest dostępna tylko wtedy, jeśli przydzielone zostały uprawnienia Read (Odczyt) lub Write (Zapis). Użytkownicy mogą uzyskać dostęp do plików źródłowych. Jeśli przydzielone zostało uprawnienie Read (Odczyt), kod źródła może być tylko czytany. Jeśli natomiast przydzielone zostało uprawnienie Write (Zapis), to kod źródła może być również modyfikowany. Trzeba zdawać sobie sprawę, że zezwalając użytkownikom na odczyt i zapis kodu źródłowego, istotnie zmniejszamy bezpieczeństwo serwera.
Directory browsing (Przeglądanie katalogów)	Użytkownicy mogą przeglądać listy plików i kolekcji

Uprawnienia Execute (Wykonaj) kontrolują poziom bezpieczeństwa wykonania skryptu i zostały opisane w tabeli 6-3.

Tabela 6-3. Uprawnienia wykonywania aplikacji

Uprawnienie	Opis
None (Brak)	Ustawienie takie uniemożliwia uruchomienie programu bądź skryptu.
Scripts only (Tylko skrypty)	Ustawienie takie umożliwia jedynie uruchomienie skryptu w danym katalogu, bez uprawnień do uruchamiania innych kodów wykonywalnych. Ustawienie jest bardziej bezpieczne niż Scripts and Executables (Skrypty i pliki wykonywalne), ponieważ aplikacja może być uruchomiona tylko w katalogu.
Scripts and Executables (Skrypty i pliki wykonywalne)	Ustawienie umożliwia uruchomienie aplikacji w danym katalogu, przy czym możliwe są odniesienia są do plików wykonywalnych (.dll oraz .exe).



Wskazówka egzaminacyjna Jeśli określone zostały zarówno uprawnienia usługi IIS, jak i systemu plików NTFS, uprawnienia czynne to te, które są bardziej restrykcyjne.

Zadanie kontrolne: Administracja programu MS

W zadaniu tym zostaną zainstalowane usługi IIS oraz skonfigurowana nowa witryna sieci Web i katalog wirtualny.

Ćwiczenie 1: Instalacja programu IIS

1. W programie **Control Panel** (Panel sterowania) otwórz moduł **Add Or Remove Programs** (Dodaj lub usuń programy) i kliknij przycisk **Add/Remove Windows Components** (Dodaj/Usuń składniki systemu Windows).
2. Zaznacz opcje **Application Server** (Serwer aplikacji) i kliknij przycisk **Details** (Szczegóły).
3. Zaznacz opcję **Internet Information Services (IIS)** (Internetowe usługi informacyjne) i kliknij przycisk **Details** (Szczegóły).
4. Sprawdź, czy zaznaczone są opcje **Common Files**, usługi **File Transfer Protocol (FTP) Service** oraz **World Wide Web Service**, a także **Internet Information Services Manager** (Menedżer internetowych usług informacyjnych). Jest to lista elementów wymaganych do zainstalowania programu IIS.
5. Zakończ instalację.

Ćwiczenie 2: Przygotowanie przykładowych danych sieci Web

1. Utwórz folder na dysku C:\ nazwany ContosoCorp.
2. Otwórz program Notepad (Notatnik) i utwórz plik zawierający tekst „Welcome to Contoso.” Zapisz plik jako: „**C:\ContosoCorp\Default.htm**”. Upewnij się, że nazwa została objęta znakami cudzysłowu.
3. Utwórz drugi plik zawierający tekst „This is the site for Project 101.” Zapisz plik jako: „**C:\VDocs\Project 101\Default.htm**”. Upewnij się, że nazwa została objęta znakami cudzysłowu.

Ćwiczenie 3: Tworzenie witryny sieci Web

1. Otwórz przystawkę **Internet Information Services (IIS) Manager** (Menedżer internetowych usług informacyjnych) znajdującą się w grupie programów **Administrative Tools** (Narzędzia administracyjne).
2. Prawym przyciskiem myszy kliknij węzeł **Default Web Site** (Domyślna witryna sieci Web) i wybierz polecenie **Stop** (Zatrzymaj).
3. Kliknij prawym przyciskiem myszy węzeł **Web Sites** (Witryny sieci Web) i wybierz polecenie **New Web Site** (Nowa witryna sieci Web).
4. Nadaj witrynie nazwę **Contoso** i określ ścieżkę jako **C:\ContosoCorp**. Wszystkie inne ustawienia domyślne mogą pozostać niezmienione.

Ćwiczenie 4: Tworzenie chronionego katalogu wirtualnego

1. Prawym przyciskiem myszy kliknij witrynę Contoso i wybierz polecenie New Virtual Directory (Nowy katalog wirtualny).
2. Wprowadź w polu **Alias** **ProjectOI**, a polu **Path** (Ścieżka) C:\Docs\Project 101.
3. Otwórz okno właściwości dla katalogu wirtualnego **ProjectOI**
4. Kliknij zakładkę **Directory Security** (Zabezpieczenia katalogów).
5. W ramce *Authentication and Access Control* (Uwierzytelnienia i kontrola dostępu) kliknij przycisk **Edit** (Edytuj).
6. Usuń zaznaczenie opcji umożliwiającej dostęp anonimowy. Od tego momentu uzyskanie dostępu do plików będzie realizowane poprzez ważne konto użytkownika. Kliknij dwukrotnie przycisk OK
7. Otwórz przeglądarkę Internet Explorer i wpisz adres <http://server01.contoso.com>. Powinna zostać wyświetlona strona zawierająca tekst „Welcome To Contoso”.
8. Wpisz adres URL <http://server01.contoso.com/Project01>. Użytkownik zostanie poproszony o podanie poświadczeń tożsamości. Zaloguj się jako Scott Bishop. Po zalogowaniu wyświetlona zostanie strona główna ProjectOI.
9. Zmień uprawnienia dokumentu C:\Docs\Project 101\Dcfault.htm tak, aby tylko administratorzy mogli odczytywać dokument.
10. Zamknij i ponownie otwórz przeglądarkę Internet Explorer. Przyłącz się do <http://server01.contoso.com/Project01> i zaloguj jako Administrator. Strona powinna zostać wyświetlona.
11. Zamknij i ponownie otwórz przeglądarkę Internet Explorer. Przyłącz się do tego samego adresu URL jako Scott Bishop. Powinna zostać wyświetlona strona informująca o odmowie dostępu -Access Denied error (401- Unauthorized).

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Na serwerze Server01, w usłudze IIS administrator konfiguruje witrynę sieci Web. Nazwa domeny sieci Internet witryny to adatum.com, a katalog główny witryny to C:\Web\Adatum. Jaki adres URL powinien wpisać użytkownik Internetu, aby uzyskać dostęp do plików katalogu głównego tej witryny?
 - a. <http://server01.web.adatum>
 - b. <http://web.adatum.com/server01>
 - c. <http://server01.adatum/home>
 - d. <http://server01.adatum.com>
2. Dane intranetu przedsiębiorstwa są aktualnie przechowywane na dysku D: serwera IIS. Podjęta została decyzja, że dział HR będzie dostarczał informacje dotyczące firmy ze swojego serwera oraz że adres URL pozwalający uzyskać te informacje powinien mieć postać: <http://intranet.contoso.com/hr>. Co należy skonfigurować?

- a. Nową witrynę sieci Web
 - b. Nową witrynę FTP
 - c. Katalog wirtualny z pliku
 - d. Katalog wirtualny
- 3- Administrator chce zapewnić najwyższy poziom zabezpieczeń intranetu przedsiębiorstwa bez wykorzystywania infrastruktury usługi certyfikatów. Celem jest udostępnienie uwierzytelnienia, które jest dla użytkowników oczywiste i zabezpiecza zasoby intranetu ograniczając dostęp dla kont istniejących w usłudze Active Directory. Wszyscy użytkownicy znajdują się w sieci chronionej ścianą ogniową (firewall) przedsiębiorstwa. Którą metodę uwierzytelnienia należy wybrać?
- a. Anonymous Access (Dostęp anonimowy)
 - b. Basic Authentication (Uwierzytelnienie podstawowe)
 - c. Digest Authentication (Uwierzytelnienie szyfrowane)
 - d. Integrated Windows Authentication (Zintegrowane uwierzytelnienie systemu Windows)

Podsumowanie lekcji

- Usługi IIS nie są instalowane domyślnie. Instaluje się je przy użyciu m dułu Windows Components Wizard (Kreator składników systemu Windows) w programie Add Or Rcmove Programs (Dodaj lub usuń programy).
- Katalog główny witryny sieci Web lub FTP jest lokalizacją fizyczną zasobów obsługiwanych przez tę witrynę.
- Katalog wirtualny jest zastępczą lokalizacją i ścieżką, która wskazuje serwerowi IIS położenie zasobów. Adres URL ma postać http://lserwer.dns.nazwalkatalog_wirtualny. Zasoby mogą być umieszczone na wolumenie lokalnym lub serwerze zdalnym.
- Usługi IIS obsługują kilka poziomów uwierzytelnienia. Domyślnie wybrany jest poziom Anonymous Authentication (Uwierzytelnienie anonimowe), który umożliwia każdemu przyłączonemu użytkownikowi dostęp do obszarów publicznych witryny. Jeśli potrzebne jest zwiększenie bezpieczeństwa, można stosować poziom Integrated Windows Authentication (Zintegrowane uwierzytelnienie systemu Windows), który pozwala przydzielać uprawnienia NTFS do zasobów.
- Dostęp do zasobów serwera IIS na wolumenie NTFS jest kontrolowany przez listy ACL, dokładnie w ten sam sposób, w jaki dostęp do zasobu uzyskiwał program Client For Microsoft Networks (Klient sieci Microsoft Networks).
- W programie IIS określone są uprawnienia do katalogu i aplikacji. Jeśli jednocześnie stosowane są uprawnienia IIS oraz NTFS, uprawnieniami czynnymi stają się uprawnienia, które są bardziej restrykcyjne.

Zadanie praktyczne



Informacja Poniższe zadanie praktyczne zostało opracowane jako przygotowanie i uzupełnienie sekcji „Rozwiązywanie problemów”. Zalecane jest, aby student przeprowadził oba ćwiczenia, nabywając tym samym jak najwięcej umiejętności dotyczących zabezpieczeń systemu plików Windows Server 2003. Przed przeprowadzeniem ćwiczeń należy zainstalować serwer IIS (zobacz Lekcja 4, ćwiczenie 1) oraz utworzyć grupę i konta użytkowników zgodnie z informacjami podanymi na początku rozdziału w sekcji „Wymagania”.

Firma Contoso, Ltd. chce skonfigurować witrynę intranetu przedstawiającą nowe wiadomości dotyczące firmy i poszczególnych jej działów. Wywołanie witryny powinno być proste zarówno dla pracowników, jak i dla menedżerów, którzy są odpowiedzialni za aktualizację dokumentów. Do przeglądania intranetu wszyscy pracownicy używają najnowszej wersji przeglądarki internetowej - Internet Explorer. Do tworzenia stron sieci Web menedżerowie będą wykorzystywać inne narzędzia.

Ćwiczenie 1: Tworzenie folderów udostępnionych i przykładowych danych sieci Web



Informacja Metod tworzenia folderów udostępnionych jest, rzecz jasna, kilka. W poniższym przykładzie należy stosować metodę opisaną w ćwiczeniu.

1. Otwórz okno wiersza poleceń.
2. Wpisz następujące polecenia:

```
md c:\ContosoIntranetNews
net share News=c:\ContosoIntranetNews
```
3. Otwórz program Notepad (Notatnik) i utwórz plik zawierający tekst „Contoso Company News.” Zapisz plik jako „C:\ContosoIntranetNews\Default.htm”. Należy upewnić się, że nazwa pliku została objęta znakami cudzysłowu.
4. Dodaj następujące uprawnienie do foldera C:\ContosoIntranetNews:
Managers: Allow Modify
5. W oknie dialogowym *Properties* (Właściwości) dla foldera C:\ContosoIntranetNews kliknij zakładkę **Web Sharing** (Udostępnianie w sieci Web).
6. Z listy rozwijanej *Share On* (Udostępnij na) wybierz **Contoso**. Jeśli nie zostały wykonane ćwiczenia lekcji 4, nie została utworzona witryna **Contoso Web**. W takim przypadku zamiast niej wybierz domyślną witrynę sieci Web (Default Web Site). Kliknij opcję **Share This Folder** (Udostępnij ten folder) i wpisz w polu alias **News**. Uprawnienia domyślne są odpowiednie. Kliknij przycisk OK

Ćwiczenie 2: Optymalizacja dostępu do sieci intranet

W ćwiczeniu tym będzie sprawdzane funkcjonowanie intranetu i optymalizacja jego wykorzystania. 1.

Otwórz przeglądarkę Internet Explorer i wpisz adres URL: <http://server01.contoso.com/News>.

2. Będziesz poproszony o podanie poświadczenia tożsamości. Zarejestruj się jako Administrator. Powinna zostać wyświetlona strona Company News.
3. Zamknij przeglądarkę Internet Explorer.
Wymagane przedstawianie tożsamości wynika z tego, że dla witryny Company News nie umożliwiono dostępu anonimowego. Podczas tworzenia katalogu wirtualnego za pomocą zakładki *Web Sharing* (Udostępnianie w sieci Web) domyślne ustawienia określają, że dostęp anonimowy jest wyłączony.
4. Przy użyciu menedżera programu IIS otwórz okno właściwości katalogu wirtualnego News.
5. Kliknij zakładkę *Directory Security* (Zabezpieczenia katalogów), a następnie, w ramce *Authentication and Access Control* (Uwierzytelnienie i kontrola dostępu) kliknij przycisk **Edit** (Edytuj).
6. Włącz dostęp anonimowy.
7. Powtórz kroki od 1 do 3, aby sprawdzić działanie po wprowadzeniu zmian.

Ćwiczenie 3: Sprawdzenie, czy członkowie grupy Managers mogą modyfikować dane publikowane w intranecie



Informacja Dla zasymulowania zarządzania zdalnego danymi sieci intranet ważne jest korzystanie ze ścieżki UNC do folderów i plików zgodnych z podanymi poprzednio instrukcjami. Nie należy używać ścieżki lokalnej.

1. Wyloguj się z serwera Server01, a następnie ponownie zaloguj jako użytkownik Lorrin Smith-Bates, który jest członkiem grupy Managers.
2. Otwórz program Notepad (Notatnik) i utwórz dokument zawierający tekst „Good News Contoso!” Zapisz dokument jako **„Wserver01\news\goodnews.htm”**. Upewnij się, że nazwa objęta została znakami cudzysłowu oraz że dla foldera News używana jest ścieżka UNC, a nie ścieżka lokalna.
- 3- Czy mogłeś zapisać plik?
Jeśli instrukcje niniejszego Zadania praktycznego zostały dokładnie wykonane, pliku nie powinno się udać zapisać. W sekcji „Rozwiązywanie problemów” będzie kontynuowane rozpoznawanie i rozwiązywanie napotkanego problemu.

Rozwiązywanie problemów



Informacja Poniższa sekcja jest kontynuacją czynności przeprowadzanych w sekcji „Zadanie kontrolne”. Zaleca się przeprowadzenie obu ćwiczeń praktycznych, co pozwala lepiej opanować umiejętności związane z systemem zabezpieczeń Windows Server 2003.

Do przeprowadzenia tego zadania trzeba zainstalować serwer IIS (zobacz Lekcja 4, ćwiczenie I) oraz należy utworzyć konta grup i użytkowników zgodnie z opisem zamieszczonym na początku rozdziału w sekcji „Wymagania”. Należy również przeprowadzić co najmniej jedno ćwiczenie w sekcji „Zadanie kontrolne”.

Lorin Smith-Bates dzwoni do działu wsparcia technicznego informując, że nie może zapisać dokumentów w intranetowym folderze News. Strona sieci Web została utworzona za pomocą programu Notepad (Notatnik), a błąd wystąpił przy próbie zapisania pliku w folderze `\\server01\News\goodnews.htm`.

Folder znajduje się w ścieżce `C:\ContosoIntranet\News` i jest udostępniany jako News. Folder skonfigurowany jest jako katalog wirtualny News witryny Contoso Web. Odebrany komunikat o Wędie informuje o odmowie dostępu (Access Denied). Na jego podstawie można wnioskować, że komputer prawdopodobnie połączył się z serwerem, ale brak odpowiednich uprawnień uniemożliwił zapis pliku.

Aby wykonać poniższą procedurę rozwiązywania problemu, zaloguj się na serwerze Server01 jako administrator.

Krok 1: Sprawdzenie członkostwa grupy

Pomimo pewności, że Lorin jest członkiem grupy Managers oraz że grupa Managers dla foldera `C:\ContosoIntranet\News` ma przyznane uprawnienia Modify (Modyfikowanie), należy sprawdzić te założenia. W jaki sposób sprawdzić członkostwo grupy użytkownika Lorin?

Członkostwo grupy danego użytkownika można wyświetlić za pomocą polecenia Dsget omawianego w rozdziale 3. Otwórz okno wiersza poleceń i wpisz komendę:

```
dsget user "CN=Lorin Smith-Bates,OU=Employees,DC=Contoso,DC=com" -
memberof -expand
```

Powinny zostać wyświetlone grupy pokazane poniżej, jak również inne grupy, w zależności od tego, które ćwiczenia zostały przeprowadzone.

```
"CN=Managers,OU=Security Groups,DC=contoso,DC=com"
"CN^Project 101 Team,OU=Security Groups,DC=contoso,DC=com"
"CN=Domain Users,CN=Users, DC=contoso,DC=com" 'CN=Print
Operators,CN=Builtin,DC=contoso,DC=com"
"CN=Users.CN=Builtin,DC=contoso,DC=com"
```

W jaki sposób sprawdzić, do której grupy należy Lorin? Otwórz konsolę Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) i w oknie dialogowym Properties (Właściwości) użytkownika Lorin przeanalizuj zakładkę Member Of (Członek grupy).

Krok 2: Sprawdzenie uprawnień czynnych

Należy sprawdzić uprawnienia przypisane do foldera C:\ContosoIntranetNews. Na zakładce Security oraz w oknach dialogowych Advanced Security Settings (Zaawansowane ustawienia zabezpieczeń) powinno być uwidocznione, że grupie Managers przydzielone zostały uprawnienia Modify (Modyfikowanie).

W oknie dialogowym Advanced Security Settings (Zaawansowane ustawienia zabezpieczeń) należy kliknąć zakładkę Effective Permissions (Czynne uprawnienia) i zaznaczając konto użytkownika Lorrin, sprawdzić jego uprawnienia czynne. Wymienione uprawnienia pozwalają na tworzenie plików i zapis danych w folderach.

Krok 3: Ocena sytuacji

Jeśli uprawnienia czynne użytkownika Lorrin umożliwiają tworzenie plików i zapis danych, dlaczego pojawia się komunikat o odmowie dostępu? W znalezieniu rozwiązania pomocne może być przejrzanie sekcji Podsumowanie lekcji (po lekcjach 1 oraz 4).

Problem może dotyczyć innych uprawnień przydzielonych do foldera C:\ContosoIntranetNews. Uprawnienia udziału oraz uprawnienia sieci Web lub katalogów wirtualnych określają maksymalne dopuszczalne uprawnienia dotyczące dostępu. Tak więc, jeśli jedno z tych uprawnień jest zbyt restrykcyjne, użytkownik Lorrin nie będzie mógł w pełni korzystać z przydzielonych uprawnień NTFS: Al Iow Modify (Zezwalaj na modyfikowanie).

Podczas zapisywania strony sieci Web w programie Notatnik, użytkownik był połączony z serwerem zdalnie. Na podstawie poniższej listy należy rozpoznać używane usługi i programy klienta:

- FTP Publishing Service (Usługa publikowania FTP)
- Worldwide Web Publishing Service (Usługa publikowania WWW)
- Telnet Service (Usługa telnet)
- File and Printer Sharing For Microsoft Networks (Udostępnianie plików i drukowania w sieciach Microsoft Networks)
- - Internet browser client (Klient przeglądarki sieci Internet)
- FTP client (Klient FTP)
- Telnet client (Klient Telnet)
- Client For Microsoft Networks (Klient sieci Microsoft Networks)

Do połączenia się z usługą File and Printer Sharing (Udostępnianie plików i drukarek) na serwerze Server01, użytkownik Lorrin korzysta z usługi Client For Microsoft Networks (Klient sieci Microsoft Networks). Można przekonać się o tym sprawdzając ścieżkę zdefiniowaną przez użytkownika do zapisywania pliku: \\Wserver01\News\goodnews.htm. Jest to ścieżka UNC, używana do połączeń w sieci Microsoft.

Wiedząc o tym, można wyeliminować przyczyny problemu związane z uprawnieniami przypisanymi do witryny Web lub katalogu wirtualnego — uprawnienia te dotyczą jedynie połączeń klienta sieci Web do usługi tej sieci.

Pozostaje więc tylko jedna możliwa przyczyna problemu: uprawnienia udziału. Domyślne uprawnienia udziału w systemie Windows Server 2003 przydzielają grupie Everyone (Wszyscy) jedynie

uprawnienie Read (Odczyt). Ponieważ uprawnienia udziału definiują maksymalne dopuszczalne uprawnienia, będą one unieważniać uprawnienia NTFS przypisane do foldera: Allow Modify (Zezwalaj na modyfikowanie).

Krok 4: Rozwiązanie problemu

Należy zmodyfikować uprawnienia do foldera C:\ContosoIntranetNews tak, aby grupa Everyone (Wszyscy) miała uprawnienia Full Control (Pełna kontrola).

Wymagania przedsiębiorstwa dotyczące nowej witryny intranetu są takie, aby użytkownicy mogli jedynie odczytywać dokumenty. Domyślne uprawnienia NTFS pozwalają użytkownikom tworzyć pliki i foldery, a następnie, jako ich właściciele, mogą oni wykonywać na tych plikach dowolne operacje.

Należy zablokować uprawnienia NTFS dla foldera tak, aby członkowie grupy Users mieli uprawnienia Read & Execute (Odczyt i wykonanie) bez uprawnień specjalnych - Create Files/Write Data (Tworzenie plików/Zapis danych), Create Folders/Append Data (Tworzenie folderów/Dodłączanie danych).

Wykonane operacje można sprawdzić logując się jako Scott Bishop. Użytkownik ten powinien widzieć folder <http://server01.contoso.com/News>. Po połączeniu z folderem Wserver01\News, użytkownik Scott *nie* powinien mieć możliwości utworzenia nowego pliku lub modyfikowania istniejącego.

Następnie należy zalogować się jako użytkownik Lorrin. Użytkownik Lorrin również powinien mieć możliwość przeglądania witryny News w intranecie, ale powinien także mieć możliwość tworzenia i modyfikowania plików udziału Wserver01\News. Użytkownik powinien mieć możliwość utworzenia dokumentu wiadomości zgodnie z opisem w ćwiczeniu 3 Zadania praktycznego, a następnie dokument ten powinien być dla niego dostępny pod adresem <http://server01.contoso.com/News/goodnews.htm>.

Podsumowanie rozdziału

- System Windows Server 2003 został wyposażony w nowe konsole i przystawki służące do zarządzania folderami udostępnionymi, zasadę inspekcji oraz usługi IIS. Do zarządzania listami ACL w dalszym ciągu jest używany program Windows Explorer (Eksplorator Windows), jak również stosować można przystawkę Shared Folder (Foldery udostępnione), chociaż edytor ACL jest narzędziem o znacznie większych możliwościach.
- Uprawnienia NTFS można przyznawać lub odmawiać ich przydzielenia. Uprawnienia mogą być przydzielane bezpośrednio lub mogą być dziedziczone. Uprawnienie Deny (Odmawiaj) ma pierwszeństwo w stosunku do uprawnienia Allow (Zezwalaj). Podobnie, uprawnienie bezpośrednie ma pierwszeństwo w stosunku do uprawnienia dziedziczonego. W rezultacie takiego podejścia, bezpośrednie uprawnienie Allow (Zezwalaj) unieważni dziedziczone uprawnienie Deny (Odmawiaj).
- Dostęp określony przez uprawnienia NTFS może być bardziej ograniczany przez uprawnienia udziału oraz przez uprawnienia usług IIS, witryn Web, wirtualnych katalogów i dokumentów. Jeśli jednocześnie stosowane są dwa rodzaje uprawnień, jak uprawnienia udziału i uprawnienia NTFS, uprawnieniami czynnymi stają się uprawnienia, które są bardziej restrykcyjne.
- Deskryptor zabezpieczeń pliku lub foldera zawiera również informacje o właścicielu obiektu. Właściciel, jak również każdy użytkownik posiadający uprawnienia Allow Change (Zezwalaj na zmiany), może modyfikować listę ACL. Użytkownik, który ma uprawnienie Allow Take Ownership (Zezwalaj Przejęcie na własność), może przejąć obiekt na własność lub własność obiektu może być przekazywana użytkownikom przez dowolnego użytkownika, który posiada prawo Restore Files And Directories (Odtwarzanie plików i katalogów).
- Deskryptor zabezpieczeń zawiera między innymi wpisy inspekcji. Jeśli włączona jest zasada inspekcji, na podstawie tych wpisów system rejestruje określone typy dostępu dla wybranych użytkowników lub grup.

Informacje dla zdających egzamin

Przed przystąpieniem do egzaminu, należy zapoznać się z przedstawionymi poniżej najważniejszymi faktami i pojęciami, aby określić, które tematy wymagają pogłębienia. Należy powrócić do lekcji, aby osiągnąć większą wprawę oraz przejrzeć działy znajdujące się w części 2 — „Materiały dodatkowe”. Informacje tu zawarte kierują do materiałów uzupełniających tematy objęte zadaniami egzaminacyjnymi.

Najważniejsze fakty

- Należy zapoznać się z narzędziami używanymi do konfigurowania folderów udostępnionych, uprawnień NTFS, inspekcji oraz usługi IIS. Trzeba poświęcić trochę czasu analizie właściwości konfigurowanych w każdej przystawce oraz roli tych właściwości w zarządzaniu plikami i folderami.
- Należy dobrze opanować określanie uprawnień czynnych i zapoznać się z oddziaływaniem bezpośrednich, dziedziczonych, zezwalających oraz odmawiających uprawnień na użytkowników, grupy, komputery oraz rodzaje logowania, takie jak interakcyjne czy poprzez sieć.

- Trzeba wiedzieć, jakie trzy etapy są wymagane do skonfigurowania inspekcji oraz jaką metodę stosować do określania typu inspekcji (powodzenie lub niepowodzenie) tak, aby osiągnąć zamierzony cel.
- Należy zdobyć doświadczenie i umiejętności konfigurowania witryn sieci Web oraz katalogów wirtualnych. Jeśli czytelnikowi brak doświadczeń związanych z działaniem programu IIS, powinien zapoznać się z zadaniem kontrolnym lekcji 4 i zadaniami praktycznymi oraz sekcją Rozwiązywanie problemów.

Najważniejsze pojęcia

Udział ukryty Folder udostępniony staje się folderem ukrytym poprzez umieszczenie na końcu jego nazwy znaku dolara \$. Połączenie do foldera jest możliwe przy użyciu nazwy UNC (na przykład \\server01\docs\$), natomiast udział ukryty nie jest pokazywany na listach przeglądarek. W systemie Windows Server 2003 utworzone są ukryte udziały administracyjne, takie jak Admin\$, Print\$ oraz udział ukryty każdego katalogu głównego wolumenu. Dostęp do ukrytych udziałów administracyjnych mogą mieć jedynie administratorzy.

Dziedziczenie Domyślne ustawienia określają, że uprawnienia przydzielone do foldera stosowane są również do jego podfolderów i plików, a pliki i foldery są tak skonfigurowane, aby zezwalać na dziedziczenie uprawnień po folderach lub wolumenach nadrzędnych, dzięki czemu informacje o ustawieniach umieszczane są w ich listach ACL. W ten sposób uprawnienia przydzielone do foldera wyższego poziomu przekazywane są do jego zawartości.

Uprawnienia czynne Uprawnienia mogą dotyczyć odmowy lub zezwolenia, mogą być dziedziczone lub przydzielane bezpośrednio. Mogą być przydzielane do jednego lub wielu użytkowników, komputerów bądź grup. Uprawnienia czynne to uprawnienia wynikowe, określające dla podmiotu zabezpieczeń rzeczywisty poziom dostępu.

Własność Każdy plik lub folder NTFS obsługuje właściwość definiującą podmiot zabezpieczeń, który posiada (jest jego właścicielem) dany zasób. Właściciel może w dowolnym momencie modyfikować listę ACL obiektu, co oznacza, że obiekt nic może być dla niego zamknięty. Obiekt można przejmować na własność lub własność obiektu może być przekazywana. W tym celu wymagane są odpowiednio uprawnienia Take Ownership (Przejmij na własność) i Restore Files And Directories (Odtwarzanie plików i katalogów).

Konta specjalne: Creator Owner (Twórca właściciel), Network (Sieć) oraz Interactive (Interaktywny)

Wymienione podmioty zabezpieczeń są dynamiczne i prezentują relacje między użytkownikiem a zasobem. Kiedy użytkownik tworzy plik lub folder, staje się twórcą i właścicielem (Creator Owner) tego zasobu, a wszystkie uprawnienia dziedziczone po folderze lub wolumenie nadrzędnym przypisane do grupy Creator Owner zostaną bezpośrednio przypisane do użytkownika nowego obiektu grupy Network (Sieć) oraz Interactive (Interaktywny), można powiedzieć, reprezentują stan połączenia użytkownika, określają, czy użytkownik przyłączył się do zasobu za pomocą klienta zdalnego, czy zalogował się w trybie interakcyjnym.

Zasada inspekcji dostępu do obiektu Zasada ta jest częścią lokalnej zasady zabezpieczeń (Local Security Policy) autonomicznego systemu Windows Server 2003 lub obiektów GPO (Group Policy Objects) i określa, czy dostęp do plików, folderów i drukarek ma być rejestrowany w dzienniku Security (Zabezpieczenia). Po włączeniu tej zasady typy protokolowanych operacji są określane na podstawie wpisów inspekcji (Auditing Entries) każdego obiektu.

Katalog wirtualny Katalog wirtualny jest obiektem usługi IIS, który powoduje, że folder dowolnego lokalnego lub zdalnego wolumenu traktowany jest jak podfolder witryny Web.

Pytania i odpowiedzi

185 Pytania do lekcji 1

1. Które z wymienionych poniżej narzędzi umożliwia administrację udziału na serwerze zdalnym? Zaznacz wszystkie właściwe odpowiedzi.
 - a. Przystawka Shared Folders (Foldery udostępnione).
 - b. Program Windows Explorer (Eksplorator Windows) uruchomiony na komputerze lokalnym i przyłączony do udziału serwera zdalnego lub do ukrytego, udostępnionego napędu.
 - c. Program Windows Explorer (Eksplorator Windows) uruchomiony na komputerze zdalnym za pośrednictwem sesji programu Terminal Services (Usługi terminalowe) lub Remote Desktop (Pulpit zdalny).
 - d. Konsola File Server Management (Zarządzanie serwerem plików).

Prawidłowa odpowiedź to a, c, oraz d. Program Windows Explorer (Eksplorator Windows) może być używany jedynie do administrowania udziałami lokalnymi. Aby za pomocą programu Windows Explorer zarządzać udziałami serwera zdalnego, trzeba uruchomić zdalną sesję pulpitu serwera i w niej uruchomić program Windows Explorer. Lepszym i częściej używanym narzędziem jest przystawka Shared Folders (Foldery udostępnione), która umieszczona jest w konsoli File Server Management (Zarządzanie serwerem plików).

2. Na wolumenie FAT32 został udostępniony folder. Grupa Project Managers ma uprawnienia Allow Full Control (Zezwalaj na pełną kontrolę). Grupa Project Engineers ma uprawnienia Allow Read (Zezwalaj na odczyt). Julie należy do grupy Project Engineers. Po awansie, Julie została dodana do grupy Project Managers. Jakie są jej uprawnienia czynne do foldera?

Full Control (Pełna kontrola)

3. Na wolumenie NTFS udostępniony został folder, a domyślne uprawnienia nie zostały zmienione. Grupa Project Managers ma uprawnienia NTFS Allow Full Control (Zezwalaj na pełną kontrolę). Julie, która należy do grupy Project Managers nie potrafi w folderze utworzyć pliku. Dlaczego Julie nie może tworzyć plików?

Domyślne uprawnienia udziału w systemie Windows Server 2003 to Everyone: Allow Read (Wszyscy: Zezwalaj na odczyt). Uprawnienia udziału określają maksymalne uprawnienia czynne dla plików i folderów tego udziału. Uprawnienia udziału ograniczają uprawnienia NTFS: pełna kontrola. Aby rozwiązać ten problem, należy zmodyfikować uprawnienia udziału tak, aby przydzielały grupie Project Managers co najmniej prawo Change (Zmiana).

203 Pytania do lekcji 2

1. Jakie są minimalne uprawnienia NTFS umożliwiające użytkownikowi otwieranie dokumentów i uruchamianie programów przechowywanych w udostępnionym folderze?
 - a. Full Control (Pełna kontrola)
 - b. Modify (Modyfikowanie)

- c. Write (Zapis)
- d. Read & Execute (Odczyt i wykonanie)
- e. List Folder Contents (Wyświetlanie zawartości foldera)

Prawidłowa odpowiedź to d.

2. Użytkownik Bill nie może uzyskać dostępu do planu wydziału. Po otwarciu zakładki Security (Zabezpieczenia) dla tego zasobu okazało się, że wszystkie uprawnienia do dokumentu dziedziczone są po folderze nadrzędnym. Grupie, do której należy Bill, odmówiono uprawnień Read (Odczyt). Która z poniższych metod umożliwi dostęp do planu wydziału dla użytkownika Bill?
- a. Zmodyfikowanie uprawnień foldera nadrzędnego poprzez dodanie uprawnienia BillrAllow Full Control (Bill: Zezwalaj na pełną kontrolę).
 - b. Zmodyfikowanie uprawnień foldera nadrzędnego poprzez dodanie uprawnienia BillrAllow Read (Bill: Zezwalaj na odczyt).
 - c. Zmodyfikowanie uprawnień dokumentu „plan” poprzez dodanie uprawnienia Bill:Allow Read (Bill: Zezwalaj na odczyt).
 - d. Zmodyfikowanie uprawnień dokumentu „plan” poprzez usunięcie uprawnienia Allow Inheritable Permissions (Zezwalaj na dziedziczenie uprawnień), wybranie polecenia Copy (Kopiuj) i usunięcia odmowy uprawnień (Deny).
 - e. Zmodyfikowanie uprawnień dokumentu „plan” poprzez usunięcie uprawnienia Allow Inheritable Permissions (Zezwalaj na dziedziczenie uprawnień), wybranie polecenia Copy (Kopiuj) i dodanie uprawnienia BilkAllow Full Control (Bill: Zezwalaj na pełną kontrolę).
 - f. Usunięcie użytkownika Bill z grupy, której odmówiono uprawnień (Deny).

Prawidłowe odpowiedzi to c, d oraz f.

3. Użytkownik Bill dzwonił ponownie informując, że w dalszym ciągu nie może uzyskać dostępu do planu wydziału. Administrator użył narzędzia Effective Permissions (Czynne uprawnienia), zaznaczył konto użytkownika Bill i okazało się, że Bill posiada wystarczające uprawnienia. Czym można wyjaśnić rozbieżność pomiędzy wynikami programu Effective Permissions (Czynne uprawnienia) a informacjami podanymi przez użytkownika?

Za pomocą narzędzia Effective Permissions (Uprawnienia czynne) można tylko uzyskać informacje o przybliżonym poziomie dostępu użytkownika. Istnieje możliwość, że wpis uprawnienia zabraniającego dostępu został przydzielony do kont związanych z typem logowania, takich jak Interactive (Interaktywny) lub Network (Sieć). Uprawnienia grup logowania nie są sprawdzane przez program Effective Permissions (Uprawnienia czynne). Inną możliwością jest taka, że użytkownik nie zalogował się jako Domain Admin (Administrator domeny) i przez to nie mógł odczytać wszystkich informacji o członkostwie w grupach, co mogło być przyczyną rozbieżności raportu uprawnień.

210 Pytania do lekcji 3

1. Które z wymienionych czynności muszą być przeprowadzone, aby wygenerowany został dziennik rejestrujący dostęp do zasobu (dla pliku lub foldera)? Wybierz wszystkie właściwe odpowiedzi.
- a. Skonfigurowanie uprawnień NTFS, które umożliwiają kontu grupy System przeprowadzać inspekcję dostępu do zasobu.
 - b. Skonfigurowanie wpisów inspekcji określających typ dostępu poddanego inspekcji.

- c. Włączenie zasady Audit Privilege Use (Przeprowadź inspekcję użycia uprawnień).
 - d. Włączenie zasady Audit Object Access (Przeprowadź inspekcję dostępu do obiektu).
- Prawidłowe odpowiedzi to b oraz d.
2. Które z wymienionych kryteriów są prawidłowymi kryteriami filtrowania dziennika zabezpieczeń pozwalającymi zidentyfikować określone zdarzenia związane z dostępem do plików i folderów? Wybierz wszystkie właściwe odpowiedzi.
- a. Data zdarzenia
 - b. Użytkownik, który spowodował powstanie zdarzenia
 - c. Typ dostępu do obiektu, który wygenerował zdarzenie
 - d. Inspekcja „powodzenia” lub „niepowodzenia”
- Prawidłowe odpowiedzi to a, b oraz d.
3. Aby uzyskać dostęp do serwera Sever01, użytkownicy firmy Contoso Ltd. korzystają z aplikacji Microsoft Office. Zadaniem administratora jest monitorowanie serwera Server01 tak, aby uprawnienia te nie były zbyt restrykcyjne i użytkownicy nie mieli problemów z uzyskaniem swoich przydziałów. Który dziennik oraz który typ zdarzenia rejestruje informacje potrzebne administratorowi?
- a. Dziennik Application (Aplikacja); Zdarzenie — Sukces
 - b. Dziennik Application (Aplikacja); Zdarzenie — Niepowodzenie
 - c. Dziennik Security (Zabezpieczenia); Zdarzenie — Sukces
 - d. Dziennik Security (Zabezpieczenia); Zdarzenie — Niepowodzenie
 - e. Dziennik System; Zdarzenie — Sukces
 - f. Dziennik System; Zdarzenie — Niepowodzenie

Prawidłowe odpowiedzi to d.

Pytania do lekcji 4

- 1. Na serwerze Server01, w usłudze IIS administrator konfiguruje witrynę sieci Web. Nazwa domeny sieci Internet witryny to adatum.com, a katalog główny witryny to C:\Web\Adatum. Jaki adres URL powinien wpisać użytkownik Internetu, aby uzyskać dostęp do plików katalogu głównego tej witryny?
 - a. <http://server01.web.adatum>
 - b. <http://web.adatum.com/server01>
 - c. <http://server01.adatum/home>
 - d. <http://server01.adatum.com>

Prawidłowa odpowiedź to d.
- 2. Dane intranetu przedsiębiorstwa są aktualnie przechowywane na dysku D: serwera IIS. Podjęta została decyzja, że dział HR będzie dostarczał informacje dotyczące firmy ze swojego serwera oraz że adres URL pozwalający uzyskać te informacje powinien mieć postać: <http://intranet.contoso.com/hr>. Co należy skonfigurować?
 - a. Nową witrynę sieci Web

- b. Nową witrynę FTP
- c. Katalog wirtualny z plikami
- d. Katalog wirtualny

Prawidłowa odpowiedź to d.

3. Administrator chce zapewnić najwyższy poziom zabezpieczeń sieci intranet dla przedsiębiorstwa bez wykorzystywania infrastruktury usługi certyfikatów. Celem jest udostępnienie uwierzytelnienia, które jest dla użytkowników oczywiste i zabezpiecza intranet ograniczając dostęp jedynie do kont istniejących w usłudze Active Directory. Wszyscy użytkownicy znajdują się w sieci chronionej ścianą ogniową (firewall) przedsiębiorstwa. Którą metodę uwierzytelnienia należy wybrać?

- a. Anonymous Access (Dostęp anonimowy)
- b. Basic Authentication (Uwierzytelnienie podstawowe)
- c. Digest Authentication (Uwierzytelnienie szyfrowane)
- d. Integrated Windows Authentication (Zintegrowane uwierzytelnienie systemu Windows)

Prawidłowa odpowiedź to d.

7 Tworzenie kopii zapasowych danych



Zadania egzaminacyjne omawiane w tym rozdziale:

- Zarządzanie procedurami tworzenia kopii zapasowych
 - » Sprawdzanie poprawności wykonania kopii zapasowej »
- Zarządzanie urządzeniami tworzenia kopii zapasowej
- Konfigurowanie zabezpieczeń operacji tworzenia kopii zapasowych
- Harmonogram tworzenia kopii zapasowych
- Odtwarzanie danych na podstawie kopii zapasowej

Cele rozdziału

Administrator włożył wiele pracy, aby zbudować i skonfigurować najlepiej dostosowane środowisko serwera. Sam serwer został wyposażony w niezawodny podsystem dyskowy RAID, właściwie zastosowane zostały uprawnienia udziałów, serwer został zabezpieczony odpowiednimi zasadami, a także umieszczony został w miejscu fizycznie uniemożliwiającym nieautoryzowany dostęp. Pomimo tych wszystkich zabezpieczeń, administrator stanął przed koniecznością odtworzenia systemu i jego danych, ponieważ poprzedniej nocy włączył się zraszac przeciwpożarowy i rano serwery były pełne wody.

Do jednych z najważniejszych zadań administratora sieci należy tworzenie i obsługa procedur związanych z zapisywaniem kopii zapasowych oraz z odtwarzaniem na ich podstawie danych systemu. System Microsoft Windows Server 2003 został wyposażony w sprawne i elastyczne narzędzia pozwalające tworzyć kopie zapasowe danych przechowywanych lokalnie i zdalnie. Narzędzia te umożliwiają kopiowanie otwartych i zablokowanych plików oraz tworzenie harmonogramu wykonywania kopii w okresach niskiego poziomu wykorzystania systemu, jak na przykład w nocy.

W niniejszym rozdziale omówiony został interfejs graficzny (GUI) programu Ntbackup oraz funkcjonalność wiersza poleceń dotycząca ochrony plików danych. Przedstawione zostały sposoby budowania sprawnego systemu zarządzania tworzeniem kopii zapasowych i obsługą nośników danych oraz sposoby odtwarzania danych w zależności od różnych sytuacji. Podkreślono znaczenie usługi VSS (Volume Shadow Copy Service) umożliwiającej szybsze odtwarzanie danych. W dalszej części rozdziału ponownie omawiany jest program Ntbackup w kontekście zagadnień odtwarzania systemu operacyjnego.

Lekcje rozdziału:

- Lekcja 1: Podstawy tworzenia kopii zapasowych.....235
- Lekcja 2: Przywracanie danych 246
- Lekcja 3: Zaawansowane funkcje tworzenia kopii zapasowych i przywracania danych.....251

Wymagania

Przeprowadzenie ćwiczeń praktycznych zamieszczonych w niniejszym rozdziale wymaga przygotowania następujących elementów:

- Przystawka Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory)
- System Windows Server 2003 (Standard lub Enterprise). Serwer powinien być nazwany Server01 i skonfigurowany jako kontroler domeny w domenie contoso.com

Lekcja 1: Podstawy tworzenia kopii zapasowych

Podstawą każdej procedury tworzenia kopii zapasowych jest narzędzie, za pomocą którego kopie te są tworzone oraz harmonogram tych prac. System Windows Server 2003 wyposażony został w efektywne i elastyczne narzędzie nazwane Ntbackup. Program Ntbackup obsługuje wiele funkcji, w które wyposażone zostały inne tego typu narzędzia, wliczając w to harmonogram tworzenia kopii zapasowych oraz ściśle współdziałanie z usługą VSS i systemem RSM (*RemOvable Storage Management*). Niniejsza lekcja opisuje koncepcje i procedury związane z zagadnieniami tworzenia kopii zapasowych danych tak, aby zasady planowania i tworzenia kopii realizowanych za pomocą programu Ntbackup były jak najbardziej zrozumiałe.

Materiały omówione podczas lekcji pozwalają na

- Tworzenie kopii zapasowych danych komputera zdalnego lub lokalnego
- Zapoznanie się z typami kopii zapasowych
- Planowanie strategii tworzenia kopii zapasowych w oparciu o połączenie zwykłych i różnicowych kopii zapasowych

Szacunkowy czas lekcji: 20 minut

Zapoznanie z programem Backup Utility (Kopia zapasowa)

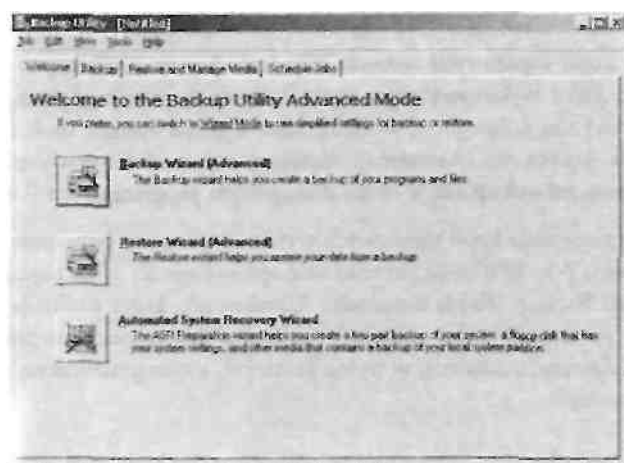
Program narzędziowy tworzenia kopii zapasowych systemu Windows Server 2003, często nazywany Ntbackup zgodnie z nazwą jego pliku wykonywalnego, może być uruchamiany poprzez kliknięcie polecenia Backup (Kopia zapasowa) znajdującego się w menu Start - grupa System Tools (Narzędzia systemowe) w grupie programów Accessories (Akcesoria). Alternatywna metoda uruchomienia programu polega na wpisaniu polecenia **ntbackup.exe** w oknie dialogowym programu Run (Uruchom).

Pierwsze uruchomienie narzędzia tworzenia kopii zapasowych wywołuje program typu kreator, tak jak to zostało przedstawione na rysunku 7-1. W niniejszym rozdziale opisane zostały tylko najczęściej używane moduły interfejsu programu Backup (Kopia zapasowa). Użytkownik, który preferuje używanie typowego programu narzędziowego zamiast trybu „kreator”, może zmienić zaznaczenie pola wyboru **Always Start In Wizard Mode** (Zawsze uruchamiaj w trybie kreatora), a następnie kliknąć polecenie **Advanced Mode** (tryb zaawansowany).



Rysunek 7-1 Kreator tworzenia kopii zapasowych lub przywracania

Zgodnie z przedstawionym na rysunku 7-2 ekranem powitalnym, użytkownik programu może wybrać tryb ręcznego tworzenia kopii zapasowych, czyli zakładkę **Backup** (Kopia zapasowa), lub program **Backup Wizard** (Kreator kopii zapasowych). Użytkownik może również definiować harmonogram automatycznie realizowanych zadań tworzenia kopii zapasowych. Program *Backup Utility* jest także używany do ręcznego odtwarzania danych - zakładka *Restore And Manage Media* (Przywracanie i zarządzanie nośnikiem). Te same zadania można realizować stosując program *Restore Wizard* (Kreator przywracania). W dalszej części rozdziału zostanie omówiony program *Automated System Recovery Wizard* (Kreator automatycznego odzyskiwania systemu).



Rysunek 7-2 Zakładka Welcome (Zapraszamy) programu Backup Utility (Kopia zapasowa)

Zagadnienia opisywane w niniejszej lekcji dotyczą planowania i wykonywania kopii zapasowych. Podczas lekcji omawiane są możliwości programu w oparciu o funkcje zakładki *Backup* (Kopia zapasowa) pokazanej na rysunku 7-2, a nie modułu *Backup Wizard* (Kreator kopii zapasowych).



Rysunek 7-3 Zakładka Backup (Kopia zapasowa)

Wybór plików dodawanych do kopii zapasowej

Zakładka *Backup* pozwala wybrać pliki lub foldery, które zostaną zarchiwizowane. Poszczególne pozycje mogą znajdować się na wolumenach lokalnych lub w folderach sieci. Jeśli wybrany zostanie cały folder, zaznaczenie wyświetlane jest za pomocą niebieskiego znacznika. Jeśli natomiast wybranych zostanie tylko kilka pozycji foldera, folder ten zaznaczany jest za pomocą przyciemnionego znacznika.

Aby zarchiwizować pliki lub foldery komputera zdalnego, należy wybrać poszczególne pozycje mapowanego napędu lub rozwinąć węzeł *My Network Places* (Moje miejsca sieciowe). Ten drugi sposób jest równoważny z użyciem nazwy UNC, takiej jak `\\Server01\Nazwa_udziału\Ścieżka_zasobu`. Pomimo, że zaznaczanie plików i folderów za pomocą modułu *My Network Places* jest mało efektywne (aby znaleźć pliki, trzeba poruszać się pomiędzy wieloma poziomami interfejsu), to metoda ma jedną zaletę - mapowanie napędów zmienia się znacznie rzadziej niż nazwy UNC.

Wskazówka Zbiór wybranych plików i folderów może zostać zapisany przy użyciu polecenia *Save Selections* (Zapisz wybrane), które znajduje się w menu *Job* (Zadanie). Zbiór ten można później pobrać za pomocą polecenia *Load Selections* (Załaduj wybrane), co znacznie oszczędza czas potrzebny do ponownego utworzenia zestawu plików.

Wybór miejsca docelowego kopii zapasowej

System Windows Server 2003 umożliwia tworzenie zadania kopii zapasowej na różnych rodzajach nośników: napędy taśm, dyski wymienne takie jak Iomega Jaz oraz co najważniejsze, bezpośrednio do pliku na wolumenie dyskowym. Jeśli miejscem docelowym jest taśma, wyspecyfikowana nazwa musi zgadzać się z nazwą taśmy, która została zamontowana w napędzie taśmy.

Jeśli kopia zapasowa jest tworzona bezpośrednio do pliku, program *Backup Utility* (Kopia zapasowa) w określonej lokalizacji utworzy plik o rozszerzeniu `.bkf`. Plik może być przechowywany w lokalnym lub zdalnym folderze. Administratorzy często używają programu *Backup Utility* do zarchiwizowania plików na poszczególnych serwerach, a dopiero potem gromadzą te pliki na serwerze centralnym, gdzie

zostają przeniesione na media wymienne. Do zrealizowania takiego sposobu archiwizowania danych, miejsce docelowe kopii zapasowej jest konfigurowane jako nazwa UNC pojedynczej lokalizacji serwera centralnego lub jako plik lokalny poszczególnych serwerów, który jest następnie kopiowany do lokalizacji centralnej.

Warto zwrócić uwagę na dwa istotne ograniczenia programu *Backup Utility* (Kopia zapasowa). Po pierwsze podczas zapisu nie są obsługiwane formaty DVD i CD. Aby ominąć to ograniczenie, trzeba najpierw utworzyć plik kopii zapasowej, a dopiero potem zapisać go na dysku CD lub DVD. Po drugie, archiwizowanie do dowolnego miejsca przeznaczenia *za wyjątkiem* pliku wymaga, aby nośnik docelowy był umieszczony w urządzeniu przyłączonym fizycznie do systemu. Oznacza to, że nie można archiwizować danych na taśmie, która jest przyłączona serwera zdalnego.

Określanie strategii tworzenia kopii zapasowych

Po wybraniu plików, które zostaną zarchiwizowane oraz po określeniu miejsca docelowego kopii zapasowej, należy dokonać jeszcze co najmniej jednego istotnego wyboru. Po kliknięciu przycisku Start Backup (Rozpocznij), a następnie przycisku Advanced (Zaawansowane) uruchomione zostanie okno dialogowe *AdvancedBackup Options* (Zaawansowane opcje kopii zapasowej), które umożliwia określenie rodzaju kopii zapasowej. Typ kopii zapasowej zależy od tego, czy wybrane pliki będą w rzeczywistości kopiowane na nośnik docelowy.

Każdy rodzaj kopii zapasowej zależy w ten czy inny sposób od atrybutu obsługiwanego przez każdy plik archiwalny. Atrybut archiwalny (A) pliku jest flagą ustawianą, jeśli plik został tworzony lub zmieniony. W celu zmniejszenia rozmiaru i czasu trwania zadań archiwizacji, większość typów kopii zapasowych przenosi na nośnik tylko te pliki, które mają ustawiony atrybut archiwalny. Większość pomyłek dotyczących atrybutu archiwalny wynika z terminologii. Można często usłyszeć „Plik został oznaczony jako: przeznaczony do zarchiwizowania”, co tak naprawdę oznacza, że atrybut archiwalny został *wyzerowany* w wyniku działania konkretnego zadania związanego z tworzeniem kopii zapasowej. W trakcie następnego zadania plik ten nie będzie przenoszony na nośnik. Z kolei, jeśli plik zostanie zmodyfikowany, atrybut archiwalny zostanie ponownie ustawiony, a plik zostanie przeniesiony podczas tworzenia kolejnej kopii zapasowej.



Wskazówka egzaminacyjna Po zapoznaniu się z typami kopii zapasowych, należy prześledzić, w jaki sposób atrybut archiwalny jest używany i traktowany przez każdy typ kopii zapasowej. Warto zapoznać się z zaletami i wadami każdego typu kopii zapasowej oraz w jaki sposób można w pełni odtworzyć strukturę danych w oparciu o wprowadzone procedury archiwizacyjne.

Normalna kopia zapasowa

Wszystkie zaznaczone pliki i foldery są archiwizowane. Atrybut archiwalny jest zerowany. Normalna kopia zapasowa nie używa atrybutu archiwalny do określania, które pliki należy zarchiwizować - wszystkie wybrane pozycje zostaną przeniesione na nośnik docelowy. Wszystkie procedury tworzenia kopii zapasowej rozpoczynają się od normalnej kopii zapasowej, która archiwizując wszystkie pliki i tworzy podstawę danego zadania.

Spośród innych typów kopii zapasowej, wykonanie normalnej kopii zapasowej pochłania najwięcej czasu oraz wymaga największej pojemności urządzeń pamięciowych. Jednakże, normalna kopia zapasowa jest

najbardziej wydajnym rodzajem archiwizacji w kontekście przywracania systemu, ponieważ generuje pełną kopię zapasową. Nie zachodzi potrzeba odtwarzania wielu zadań. Normalne kopie zapasowe zerują atrybut archiwalny wszystkich wybranych plików.

Przyrostowa kopia zapasowa

Tworzona jest kopia zapasowa wybranych plików, dla których ustawiony jest atrybut archiwalny. Atrybut archiwalny jest zerowany. Wybrane pliki, które mają ustawioną flagę archiwalny zostają przeniesione do medium docelowego, a flaga zostaje wyczyszczona. Jeśli przeprowadzana jest przyrostowa kopia zapasowa dzień po wykonaniu normalnej kopii zapasowej, zadanie będzie zawierało jedynie pliki, które zostały utworzone lub zmienione w ciągu ostatniego dnia. Podobnie, jeśli następnego dnia wykonywana jest kolejna kopia przyrostowa, zadanie będzie zawierało jedynie te pliki, które zostały utworzone bądź zmienione w ciągu tego dnia.

Przyrostowa kopia zapasowa jest najszybszym i zajmującym najmniej miejsca rodzajem kopii zapasowych. Jest jednak mniej wygodną metodą podczas odtwarzania, ponieważ odtwarzać trzeba normalną kopię zapasową, a następnie w kolejności tworzenia, każdą cząstkową kopię przyrostową.

Różnicowa kopia zapasowa

Tworzona jest kopia zapasowa wybranych plików, dla których ustawiony jest atrybut archiwalny. Atrybut archiwalny nie jest zerowany. Ponieważ różnicowa kopia zapasowa używa atrybutu archiwalny, zadanie zawierać będzie jedynie pliki, które zostały utworzone lub zmienione od momentu wykonania ostatniej normalnej lub przyrostowej kopii zapasowej. Różnicowa kopia zapasowa nie zeruje atrybutu archiwalny i dlatego, jeśli wykonywana jest taka kopia dwa dni z rzędu, drugie zadanie będzie zawierało wszystkie pliki pierwszej kopii, jak również wszystkie pliki, które zostały utworzone lub zmienione w trakcie drugiego dnia. W rezultacie różnicowa kopia najczęściej jest większa i jej tworzenie trwa dłużej niż kopii przyrostowej, ale jest mniejsza niż normalna kopia zapasowa.

Podczas odtwarzania, różnicowa kopia zapasowa jest znacznie bardziej wydajna niż kopia przyrostowa. Do pełnego odtworzenia systemu potrzebne będzie odtworzenie normalnej kopii zapasowej oraz i ostatniej kopii różnicowej.

Kopia

Wszystkie wybrane pliki i foldery zostają zarchiwizowane. Kopia nie używa i nie zeruje atrybutu archiwalny. Kopia nie jest używana do wykonywania typowych lub planowanych kopii zapasowych. Metoda ta jest przydatna do przenoszenia danych pomiędzy systemami lub do tworzenia archiwalnej kopii danych bez przerywania standardowych procedur tworzenia kopii zapasowych.

Codzienna kopia zapasowa

Tworzona jest kopia zapasowa wszystkich plików i folderów zmienionych w ciągu określonego dnia. Lista plików powstaje w oparciu o datę modyfikacji. Atrybut archiwalny nie jest używany i nie jest zerowany. Jeśli zachodzi potrzeba utworzenia kopii wszystkich plików i folderów, które w ciągu dnia zostały zmienione bez uwzględniania harmonogramu tworzenia kopii zapasowych, należy zastosować codzienną kopię zapasową.

Łączenie różnych typów kopii zapasowych

Tworzona co noc normalna kopia zapasowa zapewnia, że następnego dnia, na jej podstawie, można będzie odtworzyć dane serwera używając pojedynczego zadania. Jednak kopia taka pochłania zbyt dużo czasu i może kończyć się dopiero rano, kolidując z typowymi godzinami pracy. Aby powstała optymalna metoda wykonywania kopii zapasowej, należy rozważyć czas trwania oraz rozmiar kopii zapasowej, jak również czas potrzebny do odtworzenia systemu po awarii. Najczęściej stosowane są dwa rozwiązania:

- **Normalne i różnicowe kopie zapasowe** W niedzielę wykonywana jest normalna kopia zapasowa, a od poniedziałku do piątku kopia różnicowa. Różnicowe kopie nie zerują atrybutu archiwalny, co oznacza, że każda kopia zawiera wszystkie zmiany powstałe od niedzieli. Jeśli dane zostaną uszkodzone w piątek, do odbudowania systemu potrzebne będzie odtworzenie normalnej kopii zapasowej z niedzieli oraz różnicowej kopii zapasowej z czwartku. Podczas tworzenia kopii, metoda ta wymaga więcej czasu, w szczególności, jeśli dane zmieniają się często. Jest jednak prostsza i szybsza podczas odtwarzania, ponieważ zestaw plików kopii zapasowej przechowywany jest na mniejszych dyskach bądź taśmach.
- **Normalne i przyrostowe kopie zapasowe** W niedzielę wykonywana jest normalna kopia zapasowa, a od poniedziałku do piątku przyrostowa kopia. Przyrostowa kopia zapasowa zeruje atrybut archiwalny, co oznacza, że każda kopia zawiera jedynie te pliki, które zostały zmienione od momentu wykonania poprzedniej kopii zapasowej. Jeśli dane uległy zniszczeniu w piątek, do odbudowania systemu potrzebne będzie odtworzenie normalnej kopii zapasowej z niedzieli oraz każdej przyrostowej kopii zapasowej od poniedziałku do piątku. Metoda ta podczas tworzenia kopii zapasowych wymaga mniej czasu, natomiast znacznie więcej podczas odtwarzania systemu.

Zadanie kontrolne: Wykonywanie różnicowej kopii zapasowej

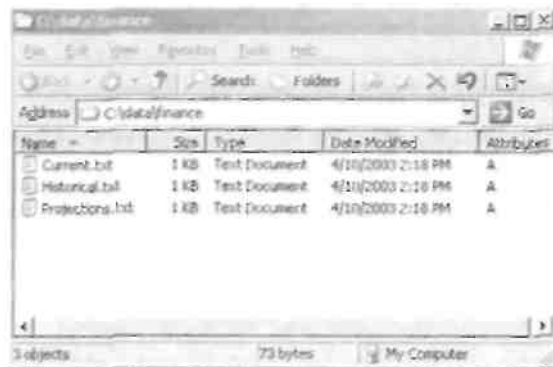
W ćwiczeniu tym zostanie utworzonych kilka zadań kopii zapasowych i zostanie przeanalizowana rola atrybutu archiwalny.

Ćwiczenie 1: Tworzenie przykładowych danych

1. Otwórz program Notepad (Notatnik) i utwórz plik tekstowy o zawartości przedstawionej poniżej. Wpisz uważnie wszystkie wiersze.

```
md c:\0ata
net share data=C:\Data
md c:\Data\Finance
cd c:\data\Finance
echo Historical Financial Data > Historical.txt
echo Current Financials > Current.txt
echo Budget > Budget.txt
echo Financial Projections > Projections.txt
```
2. Zapisz plik jako c:\createfiles.bat. Nazwa powinna być objęta znakami cudzysłowu.
3. Otwórz okno wiersza poleceń i wpisz `cd a\`.
4. Wprowadź polecenie `creatcfiles.bat`.

- 5- Otwórz program Windows Explorer (Eksplorator Windows) i przejdź do katalogu **c:\data\finance**. Na monitorze powinien zostać wyświetlony następujący ekran:



6. Jeśli kolumna *Attributes* (Atrybuty) nie jest widoczna, kliknij prawym przyciskiem myszy nagłówek *Date Modified* (Data modyfikacji) i z menu kontekstowego wybierz opcję **Attributes** (Atrybuty). Atrybut archiwalny zostanie wyświetlony.



Informacja Pozostaw otwarte okno programu Windows Explorer (Eksplorator Windows) dla katalogu **C:\Data\Finance**. W trakcie tego ćwiczenia okno to będzie jeszcze wykorzystywane.

Ćwiczenie 2: Wykonanie normalnej kopii zapasowej

- Otwórz program **Backup Utility** (Kopia zapasowa) uruchamiając program **Ntbackup.exe** z wiersza poleceń lub wybierając polecenie **Backup** (Kopia zapasowa) w menu **Start** (Akcesoria/Narzędzia systemowe).
- Usuń zaznaczenie pola wyboru **Always Start In Wizard Mode** (Zawsze uruchamiaj w trybie kreatora).
- Kliknij odniesienie **Advanced Mode** (Tryb zaawansowany).
- Wybiera zakładkę **Backup** (Kopia zapasowa).
- Rozwiń kolejno węzeł **My Computer** (Mój komputer), dysk C i katalog **Data** tak, aby można było zaznaczyć folder **Finance**.

Folder **Finance** oznaczony jest za pomocą niebieskiego znacznika, informującego, że wykonana powinna być pełna kopia zapasowa całego foldera. Jego folder nadrzędny oznaczony jest przyciemnionym znacznikiem, co oznacza wykonywanie kopii części foldera. Dowolny plik *dodany* do foldera **Finance** zostanie dołączony do kopii zapasowej, natomiast pliki dodane do foldera **Data** nie będą dołączane do kopii zapasowej.

- W menu **Job** (Zadanie) wybierz polecenie **Save Selections** (Zapisz wybory).
- Zapisz wybory jako **Finance Backup.bks**.
- W polu **Backup Media Or Filename** (Nośnik kopii zapasowej lub nazwa pliku) wpisz **c:\backup-normal.bkf**.



Informacja W środowisku pracy będą prawdopodobnie wykorzystywane wymienne nośniki kopii zapasowych, ale w zadaniach kontrolnych tej lekcji, dla zachowania minimalnych wymagań sprzętowych, do tworzenia kopii zapasowych i ich odtwarzania wykorzystywane będą pliki lokalne. Jeśli czytelnik ma dostęp do napędu taśmy, śmiało może zmodyfikować ćwiczenie.

9. Kliknij przycisk **Start Backup** (Rozpocznij), a następnie **Advanced** (Zaawansowane).
10. Sprawdź, czy jako typ kopii zapasowej zaznaczony został typ **Normal** (Normalna) na liście rozwijanej *Backup Type* (Typ kopii zapasowych), a następnie kliknij przycisk OK.
11. Zaznacz opcję **Replace The Data On The Media With This Backup** (Zastąp dane na nośniku tą kopią zapasową), a następnie kliknij przycisk **Start Backup** (Rozpocznij wykonywanie kopii zapasowej).
12. Obserwuj okno dialogowe *Backup Progress* (Postęp wykonywania kopii zapasowej). Po zakończeniu kliknij przycisk **Report** (Raport).
13. Przeanalizuj raport. W raporcie nie powinny występować komunikaty o błędach.
14. Zamknij raport i program *Backup Utility* (Kopia zapasowa)
Warto zauważyć, że w programie Windows Explorer (Eksplorator Windows) w kolumnie *Atrybuta* (Atrybuty) nie jest już pokazywany atrybut archiwalny.

Ćwiczenie 3: Wykonanie różnicowej kopii zapasowej

1. Otwórz plik C:\Data\Finance\Current.txt i dodaj do niego pewien tekst. Zapisz i zamknij plik.
2. Sprawdź folder C:\Data\Finance w programie Windows Explorer. Przy których plikach wyświetlany jest atrybut archiwalny?
Zmieniony został jeden plik.
3. Otwórz program **Backup Utility** (Kopia zapasowa) i kliknij zakładkę **Backup** (Kopia zapasowa).
4. W menu **Job** (Zadania) wybierz polecenie **Load Selections** (Załaduj wybory) i wskaż wybór **Finance Backup**.
5. W ramce *Backup Media Or Filename* (Nośnik kopii zapasowej lub nazwa pliku) wpisz c:\backup-diff-davl .bkf.
6. Kliknij przycisk **Start Backup** (Rozpocznij).
7. Kliknij przycisk **Advanced** (Zaawansowane) i zaznacz, że tworzona będzie różnicowa kopia zapasowa (*Differentiated*).
8. Uruchom tworzenie kopii zapasowej, a po zakończeniu sprawdź, czy w trakcie jej tworzenia nie wystąpiły błędy.
9. Zamknij program *Backup Utility* (Kopia zapasowa).
10. Sprawdź folder w programie Windows Explorer. Przy których plikach wyświetlany jest atrybut archiwalny?
Plik Current.txt jest wciąż oznaczony jako plik przeznaczony do archiwizacji.
11. Otwórz plik **Budget** i zmodyfikuj go. Zapisz i zamknij plik. Sprawdź, czy ustawiony jest jego atrybut archiwalny.

12. Powtórz kroki procedury od punktu 3 do 9 budując zadanie tworzenia kopii zapasowej w lokalizacji: **c:\backup-diff-day2.bkf**. Należy przeanalizować raport tworzenia kopii zapasowej. Ile plików zostało skopiowanych w tym zadaniu?

Dwa.

Ćwiczenie 4: Wykonanie przyrostowej kopii zapasowej

1. Otwórz program **Backup Utility** (Kopia zapasowa) i kliknij zakładkę **Backup** (Kopia zapasowa).
2. W menu **Job** (Zadanie) wybierz polecenie **Load Selections** (Załaduj wybory), aby pobrać wybór **Finance Backup**.
3. W ramce *Backup Media Or Filename* (Nośnik kopii zapasowej lub nazwa pliku) wpisz **c:\backup-inc-day2.bkf**.
4. Kliknij przycisk **Start Backup** (Rozpocznij)
- 5- Kliknij przycisk **Advanced** (Zaawansowane) i zaznacz, że tworzona będzie przyrostowa kopia zapasowa (*Incremental*).
6. Uruchom tworzenie kopii zapasowej, a po zakończeniu sprawdź, czy w trakcie jej tworzenia nie wystąpiły błędy.
7. Zamknij program *Backup Utility* (Kopia zapasowa).
8. Sprawdź folder w programie Windows Explorer. Przy których plikach wyświetlany jest atrybut archiwalny?
Brak takich plików.
9. Otwórz plik **Projections** i zmodyfikuj go. Zapisz i zamknij plik. W programie Windows Explorer przy tym pliku powinien być wyświetlany atrybut archiwalny.
10. Powtórz kroki procedury od punktu 1 do 8 budując zadanie tworzenia kopii zapasowej w lokalizacji: **c:\backup-inc-day3.bkf**.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec rozdziału.

1. Która Z poniższych lokalizacji *nie* może być używana do tworzenia kopii zapasowych w systemie Windows Server 2003?
 - a. Lokalny napęd taśmy
 - b. Lokalny napęd dysków CD-RW
 - c. Lokalny dysk twardy
 - d. Folder udostępniony serwera zdalnego
 - e. Lokalny napęd dysku DVD+R
 - f. Lokalny dysk wymienialny
 - g. Napęd taśmy serwera zdalnego

MCSE Training Kit: Egzamin 70-290

2. Każdego wieczoru administrator wykonuje kopię zapasową serwera plików systemu Windows Server 2003. Wykonywana jest ręczna, normalna kopia zapasowa. Administrator chce zaplanować wykonywanie kopii zapasowych każdego wieczoru przez następne dwa tygodnie. Za pomocą którego typu kopii zapasowej zadanie to zostanie najszybciej zrealizowane?
- Normal (Normalna)
 - Differential (Różnicowa)
 - Incremental (Przyrostowa)
 - Copy (Kopia)
- 3- Każdego wieczoru administrator wykonuje kopię zapasową serwera plików systemu Windows Server 2003. Wykonywana jest ręczna, normalna kopia zapasowa. Administrator chce zaplanować wykonywanie kopii zapasowych każdego wieczoru przez następne dwa tygodnie. Przy użyciu którego typu kopii zapasowej odtworzenie danych będzie najprostsze?
- Normal (Normalna)
 - Differential (Różnicowa)
 - Incremental (Przyrostowa)
 - Daily (Codzienna)
4. Każdego wieczoru administrator wykonuje kopię zapasową serwera plików systemu Windows Server 2003. Wykonywana jest normalna kopia zapasowa. Następnego wieczoru administrator zastanawia się, który typ kopii zapasowych powinien być używany: kopia różnicowa czy przyrostowa. Czy dla tych typów występują różnice w szybkości tworzenia kopii i wielkości plików archiwizacyjnych? Jeśli następnego dnia serwer ulegnie awarii, czy wystąpią różnice wydajności podczas odtwarzania danych?
5. Należy przejrzeć kroki procedury przeprowadzanej w Zadaniu kontrolnym i przewidzieć zawartość następujących zadań tworzenia kopii zapasowych:
- » backup-normal.bkf
 - » backup-diff-day1.bkf
 - » backup-diff-day2.bkf
 - » backup-inc-day2.bkf
 - » backup-inc-day3.bkf
- Czy zawartości kopii zapasowych backup-diff-day2 oraz backup-inc-day2 będą się między sobą różniły?



Informacja Odpowiedzi znajdują się w dziale „Pytania i odpowiedzi” na końcu lekcji. Student powinien jednak sprawdzić swoje przewidywania wykonując Zadanie kontrolne zamieszczone w lekcji 2.

Podsumowanie lekcji

- Programy Backup Utility (Kopia zapasowa) i Ntbackup umożliwiają tworzenie kopii zapasowych oraz odtwarzanie danych przy użyciu folderów zdalnych i lokalnych.
- Kopia zapasowa może być tworzona w plikach lokalnych, na napędach taśmowych, nośnikach wymiennych lub folderach udostępnionych serwerów zdalnych. Kopia zapasowa nie może być tworzona przy użyciu napędów CD lub DVD.
- Normalna kopia zapasowa jest pełną kopią wszystkich wybranych plików i folderów. Jest zawsze punktem początkowym każdej metody tworzenia kopii zapasowych.
- Przyrostowa kopia zapasowa kopiuje wybrane pliki, które zostały zmodyfikowane od momentu utworzenia ostatniej normalnej lub przyrostowej kopii zapasowej. Obie metody, normalna i przyrostowa, zerują atrybut „archiwalny”.
- Różnicowa kopia zapasowa kopiuje wybrane pliki, które zostały zmodyfikowane od momentu wykonania ostatniej normalnej lub przyrostowej kopii zapasowej. Różnicowa kopia zapasowa *nie* zeruje atrybutu „archiwalny”.
- Najczęściej używanymi typami kopii zapasowych są „kopia” oraz „codzienna”. Typ Kopia kopiuje wszystkie wybrane pliki, natomiast typ Codzienna kopiuje pliki zmodyfikowane w dniu, którego data została wyspecyfikowana. Obie metody nie zerują atrybutu „archiwalny” i dlatego mogą być używane do przechwycenia danych kopii zapasowej lub do ich transferu bez wpływu na harmonogram normalnych kopii zapasowych.

Lekcja 2: Odtwarzanie danych

Wraz z wyborem strategii wykonywania kopii zapasowych należy utworzyć i sprawdzić procedury przywracania, aby upewnić się, że osoby obsługujące te procedury będą posiadały odpowiednie umiejętności potrzebne podczas odtwarzania danych. Niniejsza lekcja omawia procesy i opcje związane z przywracaniem danych, dostępne w programie *Backup Utility* (Kopia zapasowa).

Materiały omówione podczas lekcji pozwalają na

- Odtworzenie danych w lokalizacji oryginalnej lub innym folderze
- Skonfigurowanie opcji przywracania

Szacunkowy czas lekcji: 10 minut

Przywracanie danych przy użyciu programu Backup Utility

Odtwarzanie danych jest prostą procedurą. Po uruchomieniu programu *Backup Utility* (Kopia zapasowa) i kliknięciu zakładki *Restore And Manage Media* (Przywracanie i zarządzanie nośnikiem) użytkownik może wybrać odpowiedni zestaw kopii zapasowej, który zostanie odtworzony. Rysunek 7-4 przedstawia omawianą zakładkę. Następnie system Windows Server 2003 sprawdza katalog kopii zapasowej oraz wyświetli pliki i foldery, które znajdują się w wybranym zestawie. Do odtwarzania użytkownik może wybrać określone pliki lub foldery. Podobnie jak przy zaznaczaniu plików kopii zapasowej, niebieski znacznik wskazuje, że plik lub folder będzie odtworzony w całości, natomiast znacznik przyciemniony oznacza, że odtworzone zostaną tylko niektóre pozycje wybranego foldera.



Rysunek 7-4 Zakładka *Restore And Manage Media* (Przywracanie i zarządzanie nośnikiem) w programie *Backup Utility* (Kopia zapasowa)

Użytkownik będzie także poproszony o określenie lokalizacji, w której pliki i foldery zostaną odtworzone. Do dyspozycji są trzy możliwości:

- **Lokalizacja oryginalna** Pliki i foldery zostaną odtworzone w lokalizacji, z której zostały skopiowane podczas tworzenia kopii zapasowych. Struktura foldera oryginalnego zostanie zachowana lub jeśli foldery zostały usunięte, będzie odtworzona.
- **Lokalizacja alternatywna** Pliki i foldery zostaną odtworzone w folderze, który został wyspecyfikowany w polu Alternate Location (Lokalizacja alternatywna). Struktura foldera oryginalnego zostaje zachowana i odtworzona poniżej wybranego foldera, który staje się równoważnikiem katalogu głównego (wolumenu) dla odtwarzanych danych. I tak na przykład, jeśli kopia zapasowa foldera C:\Data\Finance będzie odtwarzana w folderze C:\Restore, folder Finance będzie znajdował się w C:\Restore\Data\Finance.
- **Pojedynczy folder** Pliki odtworzone zostaną w określonym przez użytkownika folderze, przy czym nie zostaje zachowana struktura foldera kopii zapasowej. Wszystkie pliki zostaną odtworzone w pojedynczym folderze.

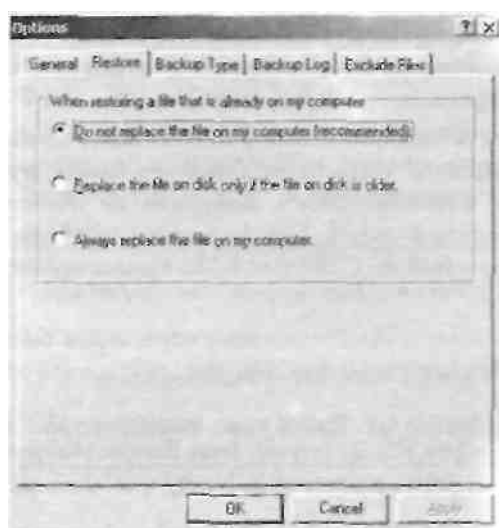
Po wybraniu plików i lokalizacji odtwarzania należy kliknąć przycisk **Start Restore** (Rozpocznij przywracanie). Kliknięcie przycisku OK rozpoczyna proces przywracania. Należy sprawdzić, czy w trakcie odtwarzania nie wystąpiły błędy.

Opcje przywracania

System Windows Server 2003 został wyposażony w szereg opcji definiujących sposób obsługi plików podczas odtwarzania w lokalizacji docelowej. Opisane poniżej opcje znajdują się w oknie *Options* (Opcje) na zakładce *Restore* (Przywracanie). Okno Opcje pokazane na rysunku 7-5 uruchamiane jest w menu *Tools* (Narzędzia) programu *Backup Utility* (Kopia zapasowa).

- **Do Not Replace The File On My Computer (Nie zamieniaj pliku na tym komputerze).** Jest to opcja domyślna, która powoduje, że program przywracania pomija pliki, które już znajdują się w lokalizacji docelowej. Opcja używana jest najczęściej w sytuacji, kiedy w lokalizacji przywracania zostały usunięte tylko niektóre pliki i na podstawie kopii zapasowej brakujące pliki zostaną odtworzone.
- **Replace Ute File On Disk Only If Ite File On Disk Is Older (Zmień plik na dysku tylko wtedy, gdy plik na dysku jest starszy).** Zaznaczenie tej opcji powoduje, że proces przywracania będzie zastępował istniejące pliki, z wyjątkiem tych plików, które są nowsze niż pliki kopii zapasowych. Dla tej metody założono, że plik w lokalizacji docelowej jest nowszy niż plik kopii zapasowej i tym samym prawdopodobnie zawiera informacje, które nie powinny zostać zastąpione starszymi danymi.
- **Always Replace TJte File On My Computer (Zawsze zmieniaj plik na tym komputerze).** Zaznaczenie tej opcji powoduje, że wszystkie pliki zostaną zastąpione przez pliki kopii zapasowych, bez względu na to, czy są nowsze czy starsze niż pliki kopii zapasowej. Dane, które zostały zmodyfikowane od momentu utworzenia ostatniej kopii zapasowej, zostaną utracone. Wszystkie pliki, które *nie* były umieszczone w kopii zapasowej pozostaną niezmienione.

Po wybraniu plików przywracania i opcji dla tego procesu oraz miejsca docelowego, należy kliknąć przycisk **Start Restore** (Rozpocznij przywracania), a następnie potwierdzić wykonanie funkcji. Wyświetlone zostanie okno dialogowe *Start Restore* (Rozpoczęcie przywracania).



Rysunek 7-5 *Opcje zakładki Restore (Przywracanie)*

Po potwierdzeniu wykonania operacji przywracania należy skonfigurować, w jaki sposób operacje te będą traktować opcje zabezpieczeń plików kopii zapasowych. W tym celu należy w oknie dialogowym *Confirm Restore* (Potwierdzenie przywracania) kliknąć przycisk **Advanced** (Zaawansowane) i wybrać opcję **Restore Security** (Przywróć zabezpieczenia). Jeśli dane są archiwizowane i odtwarzane przy użyciu wolumenu NTFS, to ustawienie domyślne będzie odtwarzać uprawnienia, ustawienia inspekcji oraz informacje o właścicielu. Usunięcie zaznaczenia tej opcji spowoduje odtworzenie danych bez ich deskryptora zabezpieczeń, a wszystkie przywracane pliki będą dziedziczyć uprawnienia po docelowym wolumenie lub folderze przywracania.

Zadanie kontrolne: Przywracanie danych

W zadaniu tym sprawdzone zostaną procedury tworzenia kopii zapasowej i odtwarzania danych za pomocą wspólnej metody: przywracanie do lokalizacji testowej.

Ćwiczenie 1: Sprawdzenie procedur tworzenia kopii zapasowych i przywracania danych

Dla sprawdzenia procedur kopiowania i odtwarzania danych wielu administratorów przeprowadza próbne odtworzenie zestawu kopii zapasowej. Dzięki temu nie zostaną zniszczone aktualnie wykorzystywane dane, ponieważ dane nie są odtwarzane w oryginalnej lokalizacji, ale w innym folderze. W środowisku pracy, sprawdzenie powinno dotyczyć przywracania danych na serwerze zapasowym, dzięki czemu można mieć pewność, że urządzenia kopii zapasowych (takie jak napęd taśmy) są prawidłowo zainstalowane na serwerze, który w razie awarii serwera głównego przejmuje jego funkcje. W tym celu należy wykonać następujące czynności:

1. Otwórz program **Backup Utility** (Kopia zapasowa).
2. Kliknij zakładkę **Restore And Manage Media** (Przywracanie i zarządzanie nośnikiem).
3. Kliknij znak plus, aby rozwinąć plik.

4. Kliknij znak plus, aby rozwinąć plik **Backup-normal.bkf**.
5. Kliknij pole wyboru, aby zaznaczyć C:.
6. Rozwiń kolejno C:, **Data** oraz **Finance**. Warto zwrócić uwagę, że zaznaczenie foldera C: spowodowało zaznaczenie jego folderów i plików podrzędnych.
- 7- Na liście rozwijanej *Restore Files To* (Przywróć pliki do) zaznacz opcję **Alternate Location** (Lokalizacja alternatywna).
8. W polu *Alternate Location* (Lokalizacja alternatywna) wpisz **C:\TestRestore**.
9. Klikni przycisk **Start Restore** (Rozpocznij przywracanie)
10. W oknie dialogowym *Confirm Restore* (Potwierdzenie przywracania) kliknij przycisk OK.
11. Po zakończeniu zadania kliknij przycisk **Report** i sprawdź dziennik operacji przywracania.
12. Otwórz folder **C:\TestRestore** i sprawdź, czy prawidłowo została odtworzona struktura foldera i jego pliki.
13. Powtórz kroki procedury od punktu 1 do 10, aby odtworzyć plik **backup-diff-day2.bkf**. Po zakończeniu przejdź do punktu 14, aby przeanalizować raport zadania.
14. Po zakończeniu zadania, kliknij przycisk **Report** (Raport) i sprawdź dziennik operacji przywracania. Jeśli przypadkowo zamknięte zostało okno statusu, można w menu **Tools** (Narzędzia) wybrać polecenie **Report** (Raport), następnie wybrać najnowszy plik raportu i kliknąć przycisk **View** (Widok).
15. Sprawdź raport dla ostatniej operacji przywracania. Ile plików zostało odtworzonych?
Żaden.
Dlaczego?
Odpowiedź związana jest z opcjami przywracania.
16. W menu **Tools** (Narzędzia) wybierz polecenie **Options** (Opcje) i kliknij zakładkę **Restore** (Przywracanie). Teraz można rozpoznać problem. Konfiguracja domyślna kopii zapasowej nie zastępuje plików komputera. Dlatego kopia różnicowa, która zawiera pliki aktualizowane po wykonaniu ostatniej normalnej kopii zapasowej, nie została poprawnie przywrócona.
- 17- Wybierz opcję **Always Replace The File On My Computer** (Zawsze zamieniaj plik na tym komputerze).
18. Powtórz operację przywracania dla pliku **backup-diff-day2.bkf**. W raporcie powinno być zaznaczone, że odtworzone zostały dwa pliki.
19. W ten sposób sprawdzone zostały procedury tworzenia kopii zapasowych i przywracania danych, wliczając w to konieczność zmodyfikowania opcji przywracania. Usuń folder **C:\TestRestore**.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Użytkownik przypadkowo usunął dane dokumentu programu Microsoft Word i zapisał dokument, przez co trwale zmienił oryginalny plik. Poprzedniego wieczoru wykonana została normalna kopia zapasowa. Która opcja przywracania powinna zostać zastosowana?

- a. Do Not Replace The File On My Computer (Nie zamieniaj pliku na tym komputerze).
 - b. Replace The File On Disk Only If The File On Disk Is Older (Zamień plik na dysku tylko wtedy, gdy plik na dysku jest starszy).
 - c. Always Replace The File On My Computer (Zawsze zamieniaj plik na tym komputerze).
2. Dyrektor wrócił z delegacji. Przed wyjazdem skopiował pliki z foldera sieciowego na dysk twardy swojego komputera. Folder jest współużytkowany przez inne osoby, które zmieniły pliki tego foldera w czasie jego nieobecności. Dyrektor po powrocie przeniósł swoją kopię plików do foldera udostępnionego w sieci, przez co zaktualizował pliki zmianami poczynionymi podczas delegacji, ale również zastąpił wszystkie pliki, które były modyfikowane przez innych współpracowników. Ci ostatni nie byli zadowoleni, że ich pliki zostały zastąpione wersjami plików aktualnych przed wyjazdem dyrektora. Na szczęście poprzedniego wieczoru wykonana została normalna kopia zapasowa. Która opcja przywracania powinna zostać zastosowana?
- a. Do Not Replace The File On My Computer (Nie zamieniaj pliku na tym komputerze).
 - b. Replace The File On Disk Only If The File On Disk Is Older (Zamień plik na dysku tylko wtedy, gdy plik na dysku jest starszy).
 - c. Always Replace The File On My Computer (Zawsze zamieniaj plik na tym komputerze).
3. Administrator chce sprawdzić procedury przywracania na serwerze, ale chce również uniknąć wpływu przeprowadzania tych procedur na kopie zapasowe aktualnie wykorzystywanych w przedsiębiorstwie danych. Która lokalizacja powinna być użyta podczas próbnego przywracania danych?
- a. Original location (Lokalizacja oryginalna)
 - b. Alternate location (Lokalizacja alternatywna)
 - c. Single folder (Pojedynczy folder)

Podsumowanie lekcji

- Program Backup Utility (Kopia zapasowa) umożliwia również odtwarzanie danych na podstawie utworzonej kopii zapasowej.
- Podczas przywracania brakujących plików lub folderów jako lokalizacja przywracania najczęściej wybierana jest opcja Original Location (Lokalizacja oryginalna).
- Podczas procedur testowych, jako lokalizacja przywracania najczęściej wybierana jest opcja Alternate Location (Lokalizacja alternatywna), dzięki czemu procedury te nie mają wpływu na oryginalne kopie zarchiwizowanych plików i folderów.
- Podczas przywracania różnicowych lub przyrostowych kopii zapasowych, po odtworzeniu normalnej kopii zapasowej, należy zaznaczyć opcję przywracania Always Replace The File On My Computer (Zawsze zamieniaj plik na tym komputerze).
- Podczas przywracania folderów, z których usunięta została część plików, a pozostałe są niezmienione, należy zaznaczyć opcję przywracania Do Not Replace The File On My Computer (Nie zamieniaj pliku na tym komputerze) lub Replace The File On Disk Only If The File On Disk Is Older (Zamień plik na dysku tylko wtedy, gdy plik na dysku jest starszy).

Lekcja 3: Zaawansowane funkcje tworzenia kopii zapasowych i przywracania danych

Po zapoznaniu się z planowaniem archiwizacji oraz po sprawdzeniu procedur tworzenia kopii zapasowych i odtwarzania danych warto dokładniej przeanalizować procesy tak, aby operacje tworzenia kopii zapasowych były automatyczne, bardziej elastyczne, a być może prostsze. Niniejsza lekcja omawia technologie leżące u podstaw archiwizowania danych, takie jak VSC oraz RSM i opisuje opcje potrzebne do tworzenia skryptów oraz harmonogramu operacji związanych z wykonywaniem kopii zapasowych. Podkreślone zostanie znaczenie nowej funkcji *Shadow Copies Of Shared Folders* (Kopiowanie w tle folderów udostępnionych), która umożliwia użytkownikom, w typowych przypadkach utraty danych, odtworzenie plików bez udziału administratora.

Materiały omówione podczas lekcji pozwalają na

- Konfigurowanie członkostwa użytkowników, które umożliwia wykonywanie operacji tworzenia kopii zapasowych i przywracania danych
- Zarządzanie taśmowymi nośnikami kopii zapasowych
- Wykaz zestawów kopii zapasowych
- Konfigurowanie opcji tworzenia kopii zapasowych
- Wykonywanie kopii zapasowych przy użyciu komend wiersza poleceń
- Harmonogram zadań wykonywania kopii zapasowych
- Konfigurowanie i korzystanie z funkcji *Shadow Copies Of Shared Folders* (Kopiowanie w tle folderów udostępnionych)

Szacunkowy czas lekcji: 30 minut

Omówienie usługi VSS

System Windows Server 2003 został wyposażony w usługę VSS, nazywaną również „snap backup”. Funkcja VSS umożliwia tworzenie kopii zapasowych baz danych oraz innych plików, które są otwarte lub zablokowane przez operatora lub funkcje systemu. Kopiowanie w tle umożliwia aplikacjom zapis danych na wolumenach podczas wykonywania operacji tworzenia kopii zapasowych, a administratorom pozwala na wykonywanie kopii zapasowych w dowolnym momencie, bez konieczności blokowania użytkowników lub ryzyka pomijania otwartych plików.

Pomimo, że usługa VSS jest ważnym ulepszeniem funkcjonalności tworzenia kopii zapasowych w systemie Windows Server 2003, to jednak zaleca się wykonywanie kopii zapasowych w okresach niewielkiego obciążenia systemu. Jeśli używane są aplikacje, które inaczej obsługują konsystencję pamięci w momencie otwarcia plików, może to wpłynąć na konsystencję plików ich kopii zapasowych. W przypadku ważnych aplikacji lub dla aplikacji takich jak Microsoft SQL Server, które są wyposażone we własne funkcje tworzenia kopii zapasowych, należy sprawdzić w dokumentacji, jakie są dla nich zalecane procedury archiwizacyjne.

Zabezpieczenia dla procesów tworzenia kopii zapasowych

Aby utworzyć kopię zapasową pliku, użytkownik musi mieć prawo *Backup Files And Directom I* (Tworzenie kopii zapasowych plików i katalogów) lub uprawnienia NTFS *Read* (Odczyt). Podobnie, I aby odtworzyć plik, użytkownik musi mieć prawo *Restore Files And Directories* (Przywracanie plików I i katalogów) lub uprawnienia NTFS *Write* (Zapis) do docelowego miejsca przeznaczenia. Uprawnienia te są przydzielone do grupy *Administrators* (Administratorzy) oraz do grupy *Backup Operators* (Operatorzy kopii zapasowych). Tak więc minimalne wymagane uprawnienia dla użytkownika, grupy bądź usługi mogą zostać przydzielone poprzez ich umieszczenie w grupie serwera *Backup Operators*.

Użytkownicy, którzy mają prawo *Restore Files And Directories* (Przywracanie plików i katalogów) mogą podczas odtwarzania usuwać z pliku uprawnienia NTFS. W systemie Windows Server 2003 użytkownicy ci mogą dodatkowo przenosić własność pliku pomiędzy użytkownikami.

Dlatego istotną sprawą jest kontrola członkostwa w grupie *Backup Operators* oraz fizyczne zabezpieczenie taśm kopii zapasowych. „Zgubiona” taśma kopii zapasowych sprawia, że odtworzenie i dostęp do ważnych informacji przez intruza staje się łatwe.

Zarządzanie nośnikami

Program Backup Utility (Kopia zapasowa) systemu Windows Server 2003 współdziała ściśle z usługami RSM. Usługi RSM zostały opracowane do obsługi automatycznych bibliotek taśmowych i dysków CD-ROM, obsługują żądania dostępu do nośnika przychodzące z innych usług lub aplikacji oraz zapewniają, że nośniki są prawidłowo zamontowane i załadowane.

Usługa RSM jest również używana do współpracy z urządzeniami obsługującymi pojedyncze nośniki, takie jak ręcznie ładowany napęd taśmy, napęd CD-ROM bądź dysk Iomega Jaz. W przypadku napędów obsługujących pojedyncze nośniki, usługa RSM śledzi nośnik przy pomocy jego etykiety lub numeru seryjnego. Stosowanie usługi RSM powoduje, że nawet w systemie archiwizacji o napędach obsługujących pojedyncze nośniki każda taśma musi mieć swoją unikatową etykietę.

Pula nośników

Program *Backup Utility* (Kopia zapasowa) systemu Windows Server 2003 obsługuje taśmy przy pomocy usługi RSM wykorzystując *pulę nośników*, co zostało pokazane na rysunku 7-6.



Rysunek 7-6 Pula nośników

W odniesieniu do kopii zapasowych rozróżniane są cztery pule nośników:

- **Nierozpoznane** Nośnik taśmowy zupełnie pusty lub o nieznanym formacie umieszczany jest w puli nośników nierozpoznanych, dopóki nie zostanie sformatowany.
- **Wolne** Pula nośników wolnych zawiera nośniki taśmowe nowo sformatowane, jak również taśmy, które zostały specjalnie oznaczone przez administratora jako wolne. Nośniki wolne przechodzą do puli nośników kopii zapasowych po zapisaniu na nich plików kopii zapasowej.
- **Kopii zapasowej** Pula ta zawiera nośniki, które zostały zapisane przez program *Backup Utility* (Kopia zapasowa). Program *Backup Utility* będzie zapisywał kopie jedynie na nośnikach puli nośników wolnych (i będzie oznaczał taśmy nazwą wpisaną przez użytkownika uruchamiającego zadanie tworzenia kopii zapasowych) lub będzie zapisywał na nośnikach znajdujących się w puli nośników kopii zapasowej, które zostały wyspecyfikowane poprzez podanie nazwy.
- **Importu** Pula nośników importu zawiera nośniki taśmowe, które nie są skatalogowane na lokalnym dysku. Skatalogowanie takiej taśmy przesuwają do puli nośników kopii zapasowej.

Zarządzanie taśmami i pulami nośników

W połączeniu z procedurami wykonywania kopii zapasowych i rotacji nośników, zachodzi konieczność zarządzania taśmami pul nośników. W tym celu, w programie *Backup Utility* (Kopia zapasowa) na stronie *Restore And Manage Media* (Przywracanie i zarządzanie nośnikami) udostępnione zostały następujące funkcje:

- **Formatowanie taśmy** Kliknij taśmę prawym przyciskiem myszy i wybierz polecenie **Format**. Formatowanie nie jest bezpieczną metodą usunięcia zawartości taśmy. Jeśli ze względów bezpieczeństwa czy prawnych zachodzi potrzeba wymazania taśmy, należy użyć odpowiedniego programu narzędziowego innych producentów. Formatowanie przygotowuje taśmę i przesuwa ją do puli taśm wolnych. Jednak nie wszystkie napędy obsługują formatowanie.
- **Naciąg taśmy** Kliknij taśmę prawym przyciskiem myszy i wybierz polecenie **Retension** (Naciąg). Nie wszystkie napędy obsługują ponowne naciąganie taśmy.
- **Oznaczanie taśmy jako taśmy wolnej** Kliknij taśmę prawym przyciskiem myszy i wybierz polecenie **Mark As Free** (Oznacz jako wolne). Czynność ta przesuwa taśmę do puli nośników wolnych. Zawartość taśmy *nie* zostaje zmaszana. Jeśli ze względów prawnych, zachodzi potrzeba wymazania taśmy, należy użyć odpowiedniego programu narzędziowego innych producentów

Wykazy

Podczas tworzenia przez program *Backup Utility* (Kopia zapasowa) zestawu kopii, program tworzy także wykaz, w którym umieszczona zostaje lista plików i folderów danego zestawu kopii zapasowej. Wykaz ten jest przechowywany na dysku serwera (wykaz lokalny lub na dysku) oraz na samym nośniku (wykaz na nośniku). Wykaz lokalny ułatwia szybkie wyszukanie plików i folderów potrzebnych przy odtwarzaniu. Program *Backup Utility* może wyświetlić wykaz natychmiast, zamiast ładować wykaz z najczęściej znacznie wolniejszego nośnika kopii zapasowych. Wykaz na nośniku ma istotne znaczenie wtedy, gdy wykaz lokalny został uszkodzony lub jeśli pliki są przekazywane do innego systemu. W tych przypadkach, system Windows odtwarza wykaz lokalny na podstawie wykazu umieszczonego na nośniku.

W programie *Backup Utility* (Kopia zapasowa) na stronie *Restore And Manage Media* (Przywracam; i zarządzanie nośnikami) udostępnione zostały następujące funkcje pozwalające zarządzać wykazami

- Usuwanie wykazu Kliknij prawym przyciskiem myszy zestaw kopii zapasowej i wybierz polecenie* Delete Catalog (Usuń wykaz), jeśli taśma została zgubiona bądź uszkodzona lub jeśli pliki przetrzebione są do innego systemu i nie wymagają już wykazu lokalnego. Omawiane polecenie nie dowala wykazu na nośniku.
- Wykaz Taśma innego systemu, która nie jest skatalogowana na komputerze lokalnym, umiata-B czana jest w puli nośników importu. Kliknij prawym przyciskiem myszy nośnik i wybierz polecenie Catalog (Wykaz). System Windows wygeneruje wykaz lokalny na podstawie taśmy lub pliku. Czyn-1 ność ta nie tworzy ani nie modyfikuje wykazu na nośniku.



Wskazówka Jeśli dysponujemy wszystkimi taśmami zestawu kopii zapasowych oraz jeśli taśmy te nie są zniszczone bądź uszkodzone, należy otworzyć okno dialogowe Options (Opcje) i na zakładce General (Ogólne) wybrać opcję Use The Catalogs On The Media To Speed Up Building Restore Catalogs On Disk (Użyj wykazów na nośniku w celu przyspieszenia tworzenia wykazów przywracania na dysku). I Jeśli brak którejkolwiek z taśm zestawu kopii zapasowej lub jeśli taśma jest zniszczona bądź uszkodzona, należy usunąć zaznaczenie tej opcji. Działanie takie zapewni, że wykaz jest pełny i aktualny, chociaż utworzenie wykazu może wymagać dużo czasu.

Opcje kopii zapasowych

Opcje kopii zapasowych są określane w oknie *Options* (Opcje), które uruchamiane jest w menu W I (Narzędzia). Wiele z tych opcji konfiguruje ustawienia domyślne używane przez program *Backup Utility* oraz przez narzędzie wiersza poleceń — program Ntbackup. Ustawienia te mogą być unieważniane przez opcje konkretnego zadania.

Opcje ogólne

Na zakładce *General* (Ogólne) okna dialogowego *Options* (Opcje) umieszczone zostały następujące ustawienia:

- Compute Selection Information Before Backup And Restore Operations (Oblicz informacje | o zaznaczonych elementach przed rozpoczęciem wykonywania kopii zapasowych lub operacji przywracania) Program, przed rozpoczęciem operacji, ocenia liczbę plików i bajtów, które będą kopiowane lub odtwarzane.
- Use The Catalogs On The Media To Speed Up Building Restore Catalogs On Disk (Użyj wykazów na nośniku w celu przyspieszenia tworzenia wykazów przywracania na dysku) Jeśli dla taśmy system nie ma wykazu lokalnego, opcja ta pozwala utworzyć taki wykaz na podstawie wykazu na nośniku. Jednakże, jeśli brak taśmy zawierającej wykaz na nośniku lub jeśli nośnik zestawu jest uszkodzony, należy usunąć zaznaczenie tej opcji, a system będzie przeglądał cały zestaw kopii zapasowej (lub część zestawu, która jest dostępna), w celu utworzenia wykazu lokalnego. Jeśli zestaw kopii zapasowych jest duży, operacja taka może trwać kilka godzin.
- Verify Data After The Backup Completes (Weryfikuj dane po wykonaniu kopii zapasowej) System porównuje zawartość nośnika kopii zapasowej z oryginalnym plikiem i protokołuje różnice. Opcja ta, rzecz jasna, znacząco wydłuża czas wymagany do zakończenia operacji wykonywania kopii zapasowych. Występowanie rozbieżności jest prawdopodobne, jeśli dane zmieniają się często

podczas tworzenia kopii zapasowych lub weryfikacji. Nie jest zalecane weryfikowanie kopii zapasowych systemu ze względu na liczbę zmian stale występujących w plikach systemowych. Tak długo, jak taśmy są zmieniane i wycofywane z użycia przed ich zniszczeniem, nie zachodzi potrzeba weryfikowania danych.

- **Backup The Contents Of Mounted Drives (Wykonaj kopię zawartości zainstalowanych dysków)** Zainstalowany napęd jest wolumenem napędu, który zamiast przypisania do napędu litery, został przypisany do foldera innej przestrzeni nazw wolumenu. Jeśli opcja ta nie została zaznaczona, wykonana zostanie jedynie kopia informacji o ścieżce do foldera zainstalowanego wolumenu, natomiast zawartość nie zostanie skopiowana. Zaznaczenie tej opcji powoduje, że wykonywana jest również kopia zapasowa zawartości zainstalowanych wolumenów. Tworzenie kopii zapasowych punktów montowania jest poprawne, jednakże, jeśli jednocześnie tworzona jest kopia zapasowa zainstalowanego punktu i napędu, zestaw kopii zapasowej zostanie powielony.

Jeśli najpierw wykonywana jest kopia zapasowa do pliku, a następnie plik ten zapisywany jest na innym nośniku, należy *usunąć zaznaczenie* wymienionych poniżej opcji. Jeśli natomiast najpierw wykonywana jest kopia zapasowa na taśmę lub inny nośnik obsługiwany przez usługę Removable Storage (Magazyn wymienny), należy *zaznaczyć* wymienione poniżej opcje.

- **Show Alert Message When I Start the Backup Utility And Removable Storage Is Not Running** (Pokaż komunikat alertu, gdy narzędzie Kopia zapasowa jest uruchomione, a Magazyn wymienny nie działa).
- **Show Alert Message When I Start The Backup Utility And Trierę Is Recognizable Media Available** (Pokaż komunikat alertu, gdy narzędzie Kopia zapasowa jest uruchomione i dostępny jest rozpoznawalny nośnik).
- **Show Alert Message When New Media Is Inserted** (Pokaż komunikat alertu, gdy zostanie włożony nowy nośnik).
- **Always Allow Use Of Recognizable Media Without Prompting** (Zawsze zezwalaj na użycie rozpoznawalnego nośnika bez monitorowania).



Wskazówka Opcja Always Allow Use Of Recognizable Media Without Prompting (Zawsze zezwalaj na użycie rozpoznawalnego nośnika bez monitorowania) może być wybrana, jeśli lokalny napęd taśmy używany jest jedynie do wykonywania kopii zapasowych, a nie przez usługę Remote Storage (Magazyn wymienny) lub przez inne funkcje. Opcja ta eliminuje konieczność znajdowania wolnego nośnika za pomocą węzła Removable Storage (Magazyn wymienny) w konsoli Computer Management (Zarządzanie komputerem).

Protokołowanie operacji wykonywania kopii zapasowych

W oknie dialogowym *Options* (Opcje) umieszczona jest zakładka nazwana *Backup Log* (Dziennik kopii zapasowej). Rejestrowanie ostrzega przed problemami, które mogą zagrażać wykonaniu kopii zapasowych i dlatego warto również zastanowić się nad sposobami protokołowania przy opracowywaniu ogólnego planu działania związanego z wykonywaniem kopii zapasowych. Tworzenie szczegółowego dziennika to rejestracja każdego pliku i ścieżki kopii zapasowych, ale prawdopodobnie przyczyną przeoczenia problemów będzie właśnie rozmiar dziennika. Dlatego zaleca się stosowanie skróconych dzienników i jest to również opcja domyślna. Skrócone dzienniki odnotowują jedynie pominięte pliki oraz błędy.

System będzie zapisywał 10 dzienników kopii zapasowych na ścieżce %UserProfile%\Local Settings\Application Data\Microsoft\Windows NT\Ntbackup\Data. Ścieżki tej ani liczby dzienników nie można zmieniać zanim nie zostanie zastąpiony najstarszy dziennik. Można oczywiście dołączyć tę ścieżkę do kopii zapasowej i tym samym zarchiwizować stare dzienniki.

Wykluczanie plików

Zakładka *Exclude Files* (Wykluczanie plików) okna dialogowego *Options* (Opcje) umożliwia określenie rozszerzeń i poszczególnych plików, które powinny zostać pominięte podczas wykonywania kopii zapasowych. Domyślne ustawienia określają, że program *Backup Utility* (Kopia zapasowa) pomija plik stronicowania, pliki tymczasowe, bufor klienta, folder Debug, bazę danych i pliki usługi FRS (File Replication Service), jak również inne lokalne dzienniki i bazy danych.

Wykluczanie może bazować na tym, kto jest właścicielem plików. W ramce *Files Excluded For All Users* (Wykluczone pliki dla wszystkich użytkowników) należy kliknąć przycisk **Add New** (Dodaj nowy). Jeśli użytkownik chce wykluczyć jedynie pliki, które należą do niego, powinien kliknąć przycisk **Add New** (Dodaj nowy) w ramce **Files Excluded For User <username>** (Wykluczone pliki dla użytkownika <nazwa_użytkownika>). Jeśli zachodzi potrzeba wykluczenia plików w oparciu o zarejestrowany typ pliku lub w oparciu o rozszerzenie, należy zastosować niestandardową maskę pliku (*Custom File Mask*). Ostatnią możliwością ograniczania plików wykluczanych jest wyspecyfikowanie foldera lub dysku twardego za pomocą opcji *Applies To Path* (Zastosuj do ścieżki) oraz *Applies To All Subfolders* (Zastosuj do wszystkich podfolderów).

Zaawansowane opcje kopii zapasowych

Po wybraniu plików kopii zapasowej oraz po kliknięciu przycisku **Start Backup** (Rozpocznij wykonywanie kopii zapasowej), istnieje możliwość skonfigurowania dodatkowych opcji, specyficznych dla konkretnego zadania. W tym celu należy kliknąć przycisk **Advanced** (Zaawansowane), a najważniejsze ustawienia tego okna to:

- **Verify Data After Backup (Weryfikuj dane po wykonaniu kopii zapasowej)** Ustawienie to zastępuje ustawienia domyślne znajdujące się w oknie dialogowym Backup Options (Opcje kopii zapasowej).
- **If Possible, Compress The Backup Data To Save Space (Jeżeli to możliwe, kompresuj dane kopii zapasowej, aby zaoszczędzić miejsce)** Zaznaczenie tej opcji powoduje kompresowanie danych w celu zaoszczędzenia przestrzeni nośnika kopii zapasowej. Opcja nie jest aktywna, jeśli napęd taśmy nie obsługuje kompresji.
- **Disable Volume Shadow Copy (Wyłącz kopiowanie woluminów w tle)** Usługa VSS umożliwia tworzenie kopii zapasowych otwartych i zablokowanych plików. Zaznaczenie tej opcji powoduje, że otwarte lub używane pliki mogą zostać pominięte.

Polecenie Ntbackup

Polecenie Ntbackup umożliwia w systemie Windows Server 2003 utworzenie skryptu zadań wykonywania kopii zapasowych. Polecenie ma następującą składnię:

```
Ntbackup backup {"ścieżka dla kopii zapasowej" lub "@plik wyboru.bks") /  
j "Nazwa zadania" opcje
```

Pierwszym przełącznikiem polecenia jest *backup*, który określa tryb polecenia — w wierszu poleceń nie można wybrać trybu przywracania. Po tym przełączniku znajduje się parametr, który określa, co będzie archiwizowane. Użytkownik może wyspecyfikować rzeczywistą ścieżkę do foldera lokalnego, udział w sieci lub plik, który ma zostać skopiowany. Inną możliwością jest wskazanie ścieżki do pliku wyboru kopii zapasowej (plik.bks) za pomocą składni @plik_wyboru.bks. Symbol (@) musi poprzedzać nazwę pliku wyboru kopii zapasowej. Plik wyboru zawiera informacje o plikach i folderach, na podstawie których utworzona zostanie kopia zapasowa. Plik musi zostać utworzony za pomocą graficznego interfejsu użytkownika (GUI) programu Backup Utility (Kopia zapasowa).

Trzeci przełącznik, /J „Nazwa_zadania” definiuje opisową nazwę zadania, która jest następnie wykorzystywana w raporcie kopii zapasowej.

Następnie można stosować bardzo długą listę przełączników, które zostały poniżej pogrupowane w oparciu o typ zadania wykonywanych kopii zapasowych.

Wykonywanie kopii zapasowej do pliku

Należy użyć przełącznika

/F „Nazwa_pliku”

gdzie Nazwa_pliku jest ścieżką dysku logicznego i nazwą pliku. Razem z tym przełącznikiem, nie można używać przełączników: /T /P /IG.

Poniższy przykład polecenia spowoduje utworzenie w pliku lokalnym napędu E kopii zapasowej udziału zdalnego Data, znajdującego się na serwerze Server01:

```
ntbackup backup "Wserver01\Data" /O "Backup of Server01 Data folder" /F "E:\Backup.bkf"
```

Dołączanie do pliku lub taśmy

Aby wykonać operację dołączania, należy użyć przełącznika:

/A

Jeśli kopia jest dołączana do taśmy, a nie do pliku, razem z tym przełącznikiem należy użyć przełącznika /G lub /T. Przełączniki /N lub /P nie mogą być stosowane.

Poniższy przykład polecenia spowoduje utworzenie kopii zapasowej udziału zdalnego Profiles znajdującego się na serwerze Server02 oraz dołączenie zestawu do zadania utworzonego w poprzednim przykładzie:

```
ntbackup backup "Wserver02\Profiles" /J "Backup of Server 02 Profiles folder" /F  
"E:\Backup.bkf" /A
```

Tworzenie kopii zapasowej na nowej taśmie bądź w nowym pliku lub zastępowanie zawartości istniejącej taśmy

Należy użyć następującego przełącznika:

/N „Nazwa_nośnika”

gdzie Nazwa_nośnika jest nazwą nadawaną nowej taśmie. Razem z tym przełącznikiem nie można używać przełącznika /A.

Tworzenie kopii zapasowej na nowej taśmie

Należy użyć następującego przełącznika:

/P „Nazwa_puli”

gdzie Nazwa_puli określa pulę nośników zawierającą nośnik kopii zapasowej. Jest to najczęściej jedna z pul zbioru pul nośników kopii zapasowych, takich jak 4-milimetrowe taśmy DDS. Razem z przełącznikiem /P nie wolno używać przełączników /A, /IG, /F lub /T.

Poniższy przykład polecenia spowoduje utworzenie na napędzie taśmy kopii zapasowej plików i folderów wymienionych w pliku wyboru kopii zapasowej c:\backup.bks:

```
ntbackup backup @c:\backup.bks /j "Backup Job 101" /n "Command Linę Backup Job" /p "4mm DDS"
```

Tworzenie kopii zapasowej na istniejącej taśmie

Aby określić taśmę, która będzie używana w operacjach dołączania lub zastępowania, należy użyć przełącznika /T lub /G razem z przełącznikiem /A (dołączanie) lub /N (zastępowanie). Z przełącznikami /T lub /G nie można stosować przełącznika /R.

Aby określić taśmę wskazując jej nazwę, należy użyć przełącznika /T, który ma następującą składnię:

/T „Nazwa_taśmy”

gdzie Nazwa_taśmy specyfikuje zarejestrowaną taśmę puli nośników.

Aby wykonać kopię zapasową w oparciu o plik wyboru i dołączyć ją do taśmy utworzonej w poprzednim przykładzie, należy użyć następującej komendy wiersza poleceń:

```
ntbackup backup @c:\backup.bks /j "Backup Job 102" /a /t "Command Linę Backup Job"
```

Aby określić taśmę wskazując jej identyfikator GUID, a nie jej nazwę, należy użyć przełącznika /G zgodnie z poniższą składnią:

/G „Nazwa_GUID”

gdzie Nazwa_GUID określa zarejestrowaną taśmę puli nośników.

Opcje zadania

Poniżej wymienione zostały przełączniki, za pomocą których można określać dodatkowe opcje dla każdego typu zadania opisanego powyżej:

- **/M {BackupType}** Określa typ kopii zapasowej. Typy kopii zapasowych to: normalna, kopia, różnicowa, przyrostowa oraz codzienna.
- **/D {„SetDescription”}** Określa etykietę zestawu kopii zapasowej.
- **/V:{yes | no}** Sprawdza dane po zakończeniu tworzenia kopii zapasowej.
- **/R:{yes | no}** Ogranicza dostęp do taśmy dla właścicieli lub członków grupy Administratorzy.
- **/L:{f | s | n}** Określa typ pliku dziennika: f=full (szczegółowy), s=summary (podsumowanie), n=none (plik dziennika nie jest tworzony).

/RS:{yes | no} Wykonuje kopie zapasową poddanych migracji plików danych znajdujących się w Magazynie wymiennym.



Wskazówka Opcja /RS wiersza poleceń nie jest wymagana do wykonywania kopii zapasowych lokalnej bazy danych Magazynu wymiennego, która zawiera pliki zastępcze Magazynu zdalnego (Remote Storage). Podczas wykonywania kopii zapasowej foldera %systemroot% program Backup (Kopia zapasowa) automatycznie wykonuje również kopię zapasową bazy danych Magazynu wymiennego.

- /HC:{on | off} Używa kompresji sprzętowej, jeśli ta jest dostępna dla napędu taśmy.
- /SNAP:{on | off} Określa, czy podczas wykonywania kopii zapasowych powinna być używana usługa Volume Shadow Copy (Kopiowanie wolumenów w tle)

Harmonogram zadań wykonywania kopii zapasowych

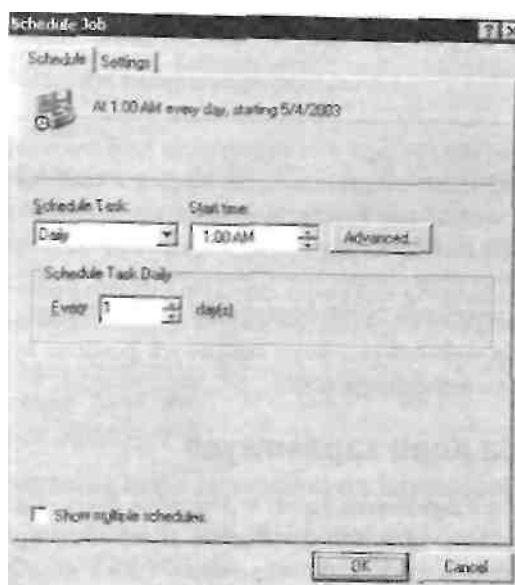
Aby określić harmonogram wykonywania kopii zapasowych, należy w programie *Backup Utility* (Kopia zapasowa) utworzyć zadanie, a następnie kliknąć przycisk **Start Backup** (Rozpocznij wykonywanie kopii zapasowej) i skonfigurować zaawansowane opcje kopii zapasowych. Po ich skonfigurowaniu należy kliknąć przycisk **Schedule** (Harmonogram) i w oknie dialogowym *Set Account Information* (Ustawianie informacji o koncie) wpisać nazwę użytkownika i hasło konta używanego przez zadanie wykonywania kopii zapasowej.



Alert bezpieczeństwa Zaleca się tworzenie kont dla każdej usługi, a nie uruchamianie usług za pomocą konta grupy System. Nie należy konfigurować uruchamiania usługi za pośrednictwem konta grupy User (Użytkownik) lub Administrator. Zmiana hasła konta User (Użytkownik) wymusza modyfikowanie ustawień hasła dla wszystkich usług, które do uruchomienia korzystały z tego konta. Konto zadania tworzenia kopii zapasowych powinno należeć do grupy Backup Operators (Operatorzy kopii zapasowej).

W oknie dialogowym *Scheduled Job Options* (Opcje zaplanowanego zadania), należy wpisać nazwę zadania i kliknąć przycisk **Properties** (Właściwości). Wyświetlone zostanie okno *Schedule Job* (Planowanie zadania) pokazane na rysunku 7-7. Umożliwia ono określenie daty i godziny zadania oraz okresu powtarzania operacji. Za pomocą przycisku **Advanced** (Zaawansowane) można skonfigurować dodatkowe ustawienia harmonogramu, w tym zakres daty wykonywania zadania. Zakładka *Settings* (Ustawienia) okna dialogowego *Schedule Job* (Planowanie zadania) umożliwia udoskonalanie zadania, na przykład można określić, żeby zadanie było wykonywane tylko w okresach bezczynności komputera.

«. iiamiiig r\u: egzamin /u-2ao



Rysunek 7-7 O&wo dialogowe *Schedule Job* (Planowanie zadania)

Po zaplanowaniu zadania istnieje możliwość modyfikowania harmonogramu. W tym celu, w programie *Backup Utility* należy kliknąć zakładkę **Schedule Jobs** (Planowanie zadań). Zadania umieszczane są w oknie kalendarza. Aby otworzyć okno harmonogramu zadania, wystarczy kliknąć wybrane zadanie. Dodawanie zadania kopii zapasowej można również zrealizować klikając przycisk **Addjob** (Dodaj zadanie) na zakładce *Schedule Jobs* (Planowanie zadania). Uruchomiony zostanie kreator kopii zapasowych, za pomocą którego można wybierać pliki kopii zapasowej oraz określać niektóre właściwości zadania. Wielu administratorów uważa, że tworzenie zadania kopii zapasowych bezpośrednio \ na zakładce *Backup* (Kopia zapasowa) jest wygodniejsze niż klikanie przycisku **Start Backup** (Rozpocznij wykonywanie kopii zapasowej), a następnie przycisku **Schedule** (Harmonogram), tak jak zostało to opisane powyżej.

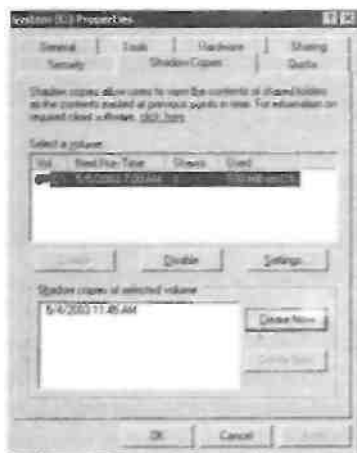
Kopiowanie w tle folderów udostępnionych

System Windows Server 2003 obsługuje inny sposób szybkiego przywracania uszkodzonych plików i folderów, zarówno dla administratorów, jak i dla użytkowników. Wykorzystując usługę VSS system Windows Server 2003 automatycznie buforuje kopie plików, które zostały zmodyfikowane. Jeśli użytkownik usunie plik, zastąpi bądź wykona na nim niezaplanowane operacje, to istnieje prosty sposób przywrócenia poprzedniej wersji pliku. Jest wartościowa właściwość, ale nie została pomyślana, aby zastąpić wykonywanie kopii zapasowych. Została zaprojektowana, aby ułatwić szybkie odtworzenie danych, wynikające z prostych, codziennych problemów, a nie będące konsekwencją dużych strat danych powstałych na przykład wskutek awarii.

Włączanie i konfigurowanie kopiowania w tle

Funkcja *Shadow Copies* (Kopiowanie w tle) dla folderów udostępnionych nie jest włączana w sposób domyślny. Aby włączyć tę funkcję, należy w programie Windows Explorer lub w przystawce *Disk Management* (Zarządzanie dyskami) otworzyć okno dialogowe *Properties* (Właściwości) napędu danego

wolumenu. Na zakładce *Shadow Copies* (Kopie w tle), pokazanej na rysunku 7-8, wybrać wolumen i kliknąć przycisk **Enable** (Włącz). Po włączeniu, wszystkie foldery udostępnione tego wolumenu będą kopiowane w tle. Na wolumenie nie można wybierać pojedynczych udziałów. Klikając przycisk **Create Now** (Utwórz teraz) można ręcznie zainicjować kopiowanie w tle.



Rysunek 7-8 Zakładka *Shadow Copies* (Kopie w tle) okna dialogowego *Properties* wolumenu

Uwaga Jeśli kliknięty zostanie przycisk **Disable** (Wyłącz), spowoduje to usunięcie wszystkich kopii, które zostały utworzone za pomocą usługi VSS. Należy dokładnie rozważyć, czy trzeba wyłączyć usługę VSS dla wolumenu, czy może lepiej będzie zmodyfikować harmonogram tak, aby zapobiec tworzeniu nowych kopii w tle.

Domyślne ustawienia określają, że serwer wykonuje kopie udostępnionych folderów o 7 rano oraz w południe, od poniedziałku do piątku. Dla bufora kopiowania w de zarezerwowanych zostało 10% przestrzeni dysku, na którym znajduje się udostępniony folder.

Poniżej wymienione zostały ustawienia, które mogą być modyfikowane. Opcje dostępne są po kliknięciu przycisku **Settings** (Ustawienia) na zakładce *Shadow Copies* (Kopie w tle).

- **Storage volume (Wolumin magazynu)** Aby poprawić wydajność (nie dotyczy zwiększenia redundancji systemu), można przenieść magazyn kopiowania w de na inny wolumen. Czynność tę należy wykonać, kiedy kopie nie zostały jeszcze utworzone. Jeśli kopie już istnieją, a użytkownik chce zmienić wolumen magazynu, musi usunąć wszystkie kopie istniejące na tym wolumenie, a dopiero potem zmienić wolumen magazynu.
- **Details (Szczegóły)** To okno dialogowe zawiera listę przechowywanych kopii oraz statystyki dotyczące ich wykorzystania.
- **Storage limits (Limity magazynu)** Najmniejsza wartość, jaką można określić, to 100 MB. Jeśli podczas kopiowania w tle zabraknie pamięci, system usuwa starsze wersje plików, aby nowe wersje mogły zostać skopiowane. Prawidłowa konfiguracja tego ustawienia zależy od całkowitej wielkości folderów udostępnionych wolumenu, na którym włączona została funkcja kopiowania w tle, od częstotliwości modyfikowania plików, ich rozmiarów oraz od liczby poprzednich kopii, które mają

zostać zachowane. Maksymalnie mogą być przechowywane 63 kolejne wersje każdego pliku zaoM najstarsza wersja zostanie usunięta z magazynu.

- **Schedule (Harmonogram)** Można skonfigurować harmonogram tak, aby odzwierciedlał sposób pracy użytkowników systemu, zapewniając dostępność odpowiedniej liczby poprzednich wersji plików bez przedwczesnego zapełnienia magazynu i tym samym usuwania najstarszych wersji. Warto zapamiętać, że podczas wykonywania kopii w tle, zostaną skopiowane wszystkie pliki zmodyfikowane od momentu wykonania poprzedniej kopii. Jeśli plik został kilka razy zaktualizowany: w okresie pomiędzy wykonywaniem kolejnych kopii, jego tymczasowe wersje nie będą dostępne.

Wykorzystanie kopiowania w tle

Kopiowanie w tle folderów udostępnionych umożliwia dostęp do poprzednich wersji plików, które zostały zapisane w buforze serwera zgodnie z określonym harmonogramem. Dzięki temu można:

- Odtworzyć pliki, które zostały przypadkowo usunięte
- Odtworzyć pliki, które zostały przypadkowo zastąpione innymi
- Podczas pracy porównywać wersje plików

Aby uzyskać dostęp do poprzednich wersji, należy kliknąć właściwości pliku lub foldera, a następnie kliknąć zakładkę **Previous Versions** (Poprzednie wersje) pokazaną na rysunku 7-9.



Rysunek 7-9 Zakładka *Previous Versions* (Poprzednie wersje) zasobu udostępnionego

Strona *Previous Versions* (Poprzednie wersje) nie jest dostępna, jeśli na serwerze nie została włączona funkcja *Shadow Copies* (Kopiowanie w tle) lub jeśli na serwerze brak poprzednich wersji plików. Zakładka nie będzie również dostępna, jeśli nie został w systemie zainstalowany klient funkcji kopiowania w tle. W systemie Windows Server 2003 plik ten znajduje się w folderze %Systemroot%\System32\Clients\1wclient\x86. Plik instalatora systemu Windows (.msi) może być instalowany za pomocą zasady grupy, SMS lub wiadomości poczty elektronicznej. Strona *Previous Versions* (Poprzednie wersje) jest dostępna tylko przy przeglądaniu właściwości pliku poprzez folder udostępniony (na stacji klienta). Jeśli plik przechowywany jest na lokalnym dysku twardym, zakładka *Previous Versions* nie będzie widoczna,

Zadanie praktyczne

Administrator został poproszony, aby skonfigurował procedurę wykonywania kopii zapasowych i udostępnionego działu finansowego. Kopie zapasowe powinny być wykonywane automatycznie we wczesnych i godzinach porannych, jako że użytkownicy na różnych zmianach pracują od 4:00 do 24:00. od poniedziałku do piątku. Pliki foldera są często modyfikowane - około połowa plików zmieniana jest raz w tygodniu, a pozostała część plików codziennie. Wiadomo również, że czas wyłączenia serwera jest bardzo kosztowny dla firmy i dlatego przywracanie plików po jego awarii musi odbywać się w możliwie krótkim czasie.

1. Wiedząc, że wiele plików modyfikowanych jest codziennie oraz że odtwarzanie danych musi trwać jak najkrócej, jaki typ kopii zapasowej powinien być uruchamiany w godzinach nocnych?

Rozpatrywane powinno być wykonanie normalnej kopii zapasowej. Ponieważ w folderze udostępnionym jest wiele plików, które zmieniają się codziennie, korzystanie z przyrostowej lub różnicowej kopii zapasowej w porównaniu do normalnej kopii przyniesie zysk mniejszy niż 50%. Jedną podczas przywracania normalna kopia zapasowa jest najszybsza, ponieważ zawiera wszystkie pliki potrzebne do odtworzenia.

2. Administrator skonfigurował zadanie wykonywania normalnej codziennej kopii zapasowej uruchamianej o 24:00, po zakończeniu pracy ostatniej zmiany. Niestety okazało się, że realizacja zadania kopii zapasowej nie kończy się przed 4:00 rano, a o tej porze pracę rozpoczyna poranna zmiana. W jaki sposób należy zmodyfikować wykonywanie kopii zapasowej?

Należy utworzyć normalną kopię zapasową na koniec tygodnia, być może w niedzielę, a w tygodniu, w godzinach nocnych, należy tworzyć różnicowe kopie zapasowe. Można stosować zarówno różnicową, jak i przyrostową kopię zapasową, ale podczas przywracania danych kopia różnicowa jest szybsza, jako że ostatnia kopia różnicowa zawiera wszystkie pliki zmodyfikowane od momentu wykonania normalnej kopii zapasowej.

Ćwiczenie 1: Tworzenie przykładowych danych

1. Otwórz ikonę **My Computer** (Mój komputer) oraz napęd C.
2. Usuń folder Data. Użytkownik zostanie poproszony o potwierdzenie wykonania tej czynności oraz poinformowany, że jest to folder udostępniony, a jego usunięcie spowoduje usunięcie udostępnionego zasobu. Aby kontynuować, należy potwierdzić zrozumienie treści ostrzeżenia.
3. Otwórz okno wiersza poleceń i wpisz `cd a\`.
4. Wpisz polecenie **createfiles.bat**.



Informacja Jeśli podczas lekcji 1, w ćwiczeniu 1, nie został utworzony plik `createfiles.bat`, należy wykonać czynności opisane w punktach od 1 do 3 (ćwiczenie 1), aby utworzyć odpowiedni skrypt

Ćwiczenie 2: Harmonogram zadania kopii zapasowej

Należy skonfigurować i utworzyć harmonogram wykonywania opisanych poniżej zadań kopii zapasowych. Pomocą podczas realizacji tych zadań mogą być instrukcje zamieszczone w Zadaniach kontrolnych lekcji 1 i 3-

Zadanie kontrolne: Zaawansowane funkcje wykonywania kopii zapasowych i przywracania danych

W zadaniu tym tworzony będzie harmonogram zadań kopii zapasowych, wykonywana będzie kopia zapasowa przy użyciu komend wiersza poleceń oraz skonfigurowana i zastosowana zostanie funkcja *Shadow Copies* (Kopie w tle) folderów udostępnionych.

Ćwiczenie 1: Harmonogram zadań wykonywania kopii zapasowych

1. Otwórz program **Backup Utility** (Kopia zapasowa) i kliknij zakładkę **Backup** (Kopia zapasowa).
2. W menu **Job** (Zadanie) kliknij polecenie **Load selection** (Załaduj wybory) i wybierz zests **Finance Backup**.
3. W polu *Backup Media Or File Name* (Nośnik kopii zapasowej lub nazwa pliku) wpisz:
C:\Backup-Everyday.bkf.
4. Kliknij przycisk **Start Backup** (Rozpocznij).
5. Kliknij przycisk **Advanced** (Zaawansowane) i wybierz typ kopii zapasowej: **Incremental** (Przyrostowa). Kliknij przycisk OK.
6. Kliknij przycisk **Schedule** (Harmonogram).
7. W oknie dialogowym *Set Account Information* (Ustawianie informacji o koncie) wpisz swoje hasła i kliknij przycisk OK.
8. Nazwij zadanie **Daily Incremental Backup**.
9. Kliknij przycisk **Properties** (Właściwości). Skonfiguruj zadanie, aby było uruchamiane codziennie. Określ czas o dwie minuty późniejszy niż bieżąca godzina tak, aby można było zaobserwować działanie zadania.
10. Zakończ konfigurowanie harmonogramu. Program poprosi ponownie o wprowadzenie hasła.
11. Zamknij program *Backup Utility* (Kopia zapasowa).
12. W programie Windows Explorer otwórz napęd C i poczekaj dwie minuty. Zadanie kopii zapasowej powinno zostać wyświetlone.
- 13. Otwórz program *Backup Utility*, w menu Tools (Narzędzia) wybierz polecenie **Report** (Raport) i przejrzyj dziennik ostatniego zadania kopii zapasowej, aby potwierdzić status zadania. Jeśli zadany plik nie został zmodyfikowany, to podczas wykonywania kopii zapasowej, żaden plik nie został skopiowany.
14. W przypadku nieprawidłowej pracy zadania należy otworzyć program *Event Viewer* (Podgląd zdarzeń) znajdujący się w folderze *Administrative Tools* (Narzędzia administracyjne) i w celu rozpoznania przyczyny awarii przeanalizować dziennik aplikacji.

Ćwiczenie 2: Uruchamianie wykonywania kopii zapasowych w wierszu poleceń

Jednym z łatwiejszych sposobów określenia prawidłowości stosowania przełączników poleceń tworzenia kopii zapasowych jest zbudowanie harmonogramu kopii zapasowej takiej, jak w ćwiczeniu 1 i sprawdzenie, czy polecenie utworzyło zaplanowane zadanie.

1. Otwórz program *Backup Utility* (Kopia zapasowa) i kliknij zakładkę **Schedule Jobs**.
2. W kalendarzu kliknij ikonę reprezentującą zaplanowane zadanie.

3. Kliknij przycisk **Properties** (Właściwości).
4. Zaznacz polecenie wpisane w polu *Run* (Uruchom) i aby je skopiować, naciśnij CTRL+C.
5. Kliknij przycisk **Cancel** (Anuluj), aby zamknąć okno dialogowe *Schedule Jobs* (Planowanie zadań), a następnie zamknij program *Backup Utility* (Kopia zapasowa).
6. Otwórz okno wiersza poleceń.
7. Kliknij menu okna (ikona w lewym górnym rogu okna wiersza poleceń) i w menu **Edit** (Edytuj) wybierz opcję **Paste** (Wklej). Polecenie programu Ntbackup wraz z wszystkimi przełącznikami zostało wklejone do wiersza poleceń. Naciśnij ENTER. Zadanie kopii zapasowej zostanie wykonane.

Wskazówka Zaleca się, aby na tym etapie usunąć zaplanowane zadanie kopii zapasowej wykonywanej w tym Zadaniu kontrolnym. Dodatkowe planowanie zadań przeprowadzane będzie w Zadaniu praktycznym i łatwiej będzie je realizować, jeśli harmonogram jest pusty. W programie Backup Utility (Kopia zapasowa) kliknij zakładkę *Schedule Jobs* (Planowanie zadań), a następnie w kalendarzu kliknij ikonę zaplanowanego zadania. Kliknij przycisk **Delete** (Usuń).

Ćwiczenie 3: Włączanie usługi kopiowania w tle

1. Upewnij się, czy folder C:\Data został udostępniony i czy uprawnienia udziału zezwalają na pełną kontrolę członkom grupy Wszyscy (Everyone Full Control).
2. Otwórz ikonę **My Computer** (Mój komputer).
3. Kliknij prawym przyciskiem myszy napęd C i wybierz opcję **Properties** (Właściwości).
4. Kliknij zakładkę **Shadow Copies** (Kopie w tle).
5. Wybierz wolumen C i kliknij przycisk **Enable** (Włącz).
6. Wyświetlony zostanie komunikat. Aby kontynuować, kliknij przycisk **Yes** (Tak).

Ćwiczenie 4: Symulowanie zmian plików sieciowych

1. Otwórz folder C:\Data\Finance, a w nim otwórz plik **Current.txt**. Zmodyfikuj zawartość pliku, a następnie zapisz i zamknij plik.
2. Usuń plik C:\Data\Finance\Projections.txt.

Ćwiczenie 5: Przywracanie plików za pomocą funkcji Previous Versions (Poprzednie wersje)

1. Otwórz udostępnione dane klikając kolejno menu **Start**, polecenie **Run** (Uruchom), a następnie wpisując \\server01\data.

Informacja Stosowanie nazwy UNC, a nie ścieżki lokalnej, ma podstawowe znaczenie. Zakładka Previous Versions (Poprzednie wersje) jest dostępna tylko, jeśli połączenie do foldera udostępnionego realizowane jest poprzez sieć.

2. Otwórz folder **Finance**.
3. Kliknij prawym przyciskiem myszy plik **Current.txt** i wybierz polecenie **Properties** (Właściwości).
4. Wybierz zakładkę **Previous Versions** (Poprzednie wersje).

5. Zaznacz poprzednią wersję pliku Current.txt.
6. Kliknij przycisk **Copy** (Kopiuj), zaznacz folder Desktop jako miejsce docelowe, a następnie kliknij I ponownie przycisk **Copy** (Kopiuj).
7. Kliknij przycisk OK, aby zamknąć okno dialogowe **Properties** (Właściwości).
8. Otwórz plik Current.txt umieszczony na pulpicie. Jest to wersja pliku bez modyfikacji wykonanych I w ćwiczeniu 4.
9. Wróć do udziału \\Server01\Data. Na tym etapie nie otwieraj foldera Finance.
10. Aby odtworzyć usunięty plik Projections.txt, kliknij prawym przyciskiem myszy folder Finance, a następnie wybierz polecenie **Properties** (Właściwości).
11. Wybierz zakładkę **Previous Versions** (Poprzednie wersje).
12. Zaznacz poprzednią wersję foldera Finance i kliknij przycisk **View** (Widok).
W otwartym oknie wyświetlona zostanie zawartość foldera taka, jaka była w momencie tworzenia kopii (za pomocą funkcji kopiowania w tle).
- 13- Kliknij prawym przyciskiem myszy plik Projections.txt i wybierz polecenie **Copy** (Kopiuj).
14. Przejdź do widoku, w którym pokazany jest bieżący folder **Wserver01\data**.
15. Otwórz folder **Finance**.
16. Do tego foldera wklej plik Projections.txt. Została odtworzona poprzednia wersja pliku Projections.txt.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Użytkownik Scott Bishop ma duże uprawnienia w lokalizacji zdalnej, która liczy 20 użytkowników. W siedzibie tej wykorzystywany jest system Windows Server 2003, w oparciu o który zbudowane zostały serwery plików i drukowania. W systemie został zainstalowany napęd taśmy. Ponieważ w siedzibie na pełny etat nie jest zatrudniony administrator, zdecydowano, że uprawnienia potrzebne do wykonywania kopii zapasowych i przywracania systemu przydzielone zostaną użytkownikowi Scott. Jednakże należy przydzielić tylko te uprawnienia, które są niezbędne do wykonywania kopii zapasowych i odtwarzania danych. Jaka jest zalecana praktyka udostępniania użytkownikowi Scott niezbędnych uprawnień tak, aby mógł wykonywać powierzone zadanie?
2. Napisz polecenie umożliwiające wykonanie pełnej kopii zapasowej foldera C:\Data\Finance do pliku nazwanego Backup.bkf w udostępnionym folderze Backup serwera Server02. Nazwa zadania kopii zapasowych powinna brzmieć „Backup of Finance Folder”. Następnie napisz to polecenie tak, aby umożliwiło wykonanie przyrostowej kopii zapasowej oraz dołączenie zestawu kopii do tego samego pliku i z tą samą nazwą zadania kopii zapasowej.

3. Użytkownik usunął plik w udostępnionym folderze serwera. Użytkownik otworzył okno właściwości foldera. W oknie tym nie była wyświetlana zakładka Previous Versions (Poprzednie wersje). Co mogłoby być tego przyczyną? Wybierz wszystkie właściwe odpowiedzi.
- Dla foldera nie została włączona funkcja Shadow Copy (Kopie w de).
 - Dla wolumenu nie została włączona funkcja Shadow Copy (Kopie w de).
 - Użytkownik nie ma uprawnień do przeglądania bufora usługi Shadow Copy (Kopie w tle).
 - Program klienta usługi Shadow Copy (kopie w tle) nie został zainstalowany na komputerze użytkownika.
 - Folder został umieszczony na wolumenie FAT.

Podsumowanie lekcji

- Używanie programu Backup Utility (Kopia zapasowa) lub innego tego typu programu narzędziowego wymaga uprawnień potrzebnych do wykonywania kopii zapasowych i przywracania danych. Domyślne ustawienia określają, że uprawnienia takie mają grupy Backup Operators (Operatorzy kopii zapasowych) oraz Administratorzy.
- Okno dialogowe Options (Opcje) umożliwia skonfigurowanie ustawień na zakładkach General (Ogólne), Backup (Kopia zapasowa) oraz Restore (Przywracanie). Wiele z tych ustawień staje się ustawieniami domyślnymi określającymi działanie programów Backup Utility (Kopia zapasowa) oraz Ntbackup, o ile nie zostaną zastąpione opcjami związanymi z zadaniem, które zostały zdefiniowane w oknie dialogowym Advanced Backup Options (Zaawansowane opcje kopii zapasowych) lub określone za pomocą przełączników komend wiersza poleceń.
- Polecenie Ntbackup wraz z pełnym zestawem przełączników umożliwia uruchomienie zadania kopii zapasowej w oknie wiersza poleceń lub na podstawie pliku wsadowego.
- Dla zadań wykonywania kopii zapasowych można określać harmonogram automatycznego i regularnego ich uruchamiania w okresach małego wykorzystania systemu.
- Usługa VSS (Volume Shadow Copy Service) umożliwia użytkownikowi dostęp do poprzednich wersji plików i folderów udostępnionych w sieci. Dzięki dostępowi do poprzednich wersji, użytkownik może odtworzyć usunięte bądź uszkodzone pliki lub może porównywać wersje plików.

Zadanie praktyczne

Administrator został poproszony, aby skonfigurował procedurę wykonywania kopii zapasowych foldera udostępnionego działu finansowego. Kopie zapasowe powinny być wykonywane automatycznie we wczesnych godzinach porannych, jako że użytkownicy na różnych zmianach pracują od 4:00 do 24:00. od poniedziałku do piątku. Pliki foldera są często modyfikowane - około połowa plików zmieniana jest raz w tygodniu, a pozostała część plików codziennie. Wiadomo również, że czas wyłączenia serwera jest bardzo kosztowny dla firmy i dlatego przywracanie plików po jego awarii musi odbywać się w możliwie krótkim czasie.

1. Wiedząc, że wiele plików modyfikowanych jest codziennie oraz że odtwarzanie danych musi trwać jak najkrócej, jaki typ kopii zapasowej powinien być uruchamiany w godzinach nocnych?

Rozpatrywane powinno być wykonanie normalnej kopii zapasowej. Ponieważ w folderze udostępnionym jest wiele plików, które zmieniają się codziennie, korzystanie z przyrostowej lub różnicowej kopii zapasowej w porównaniu do normalnej kopii przyniesie zysk mniejszy niż 50%. Jednak podczas przywracania normalna kopia zapasowa jest najszybsza, ponieważ zawiera wszystkie pliki potrzebne do odtworzenia.

2. Administrator skonfigurował zadanie wykonywania normalnej codziennej kopii zapasowej uruchamianej o 24:00, po zakończeniu pracy ostatniej zmiany. Niestety okazało się, że realizacja zadania kopii zapasowej nie kończy się przed 4:00 rano, a o tej porze prace rozpoczyna poranna zmiana. W jaki sposób należy zmodyfikować wykonywanie kopii zapasowej?

Należy utworzyć normalną kopię zapasową na koniec tygodnia, być może w niedzielę, a w tygodniu, w godzinach nocnych, należy tworzyć różnicowe kopie zapasowe. Można stosować zarówno różnicową, jak i przyrostową kopię zapasową, ale podczas przywracania danych kopia różnicowa jest szybsza, jako że ostatnia kopia różnicowa zawiera wszystkie pliki zmodyfikowane od momentu wykonania normalnej kopii zapasowej.

Ćwiczenie 1: Tworzenie przykładowych danych

1. Otwórz ikonę **My Computer** (Mój komputer) oraz napęd C.
2. Usuń folder Data. Użytkownik zostanie poproszony o potwierdzenie wykonania tej czynności oraz poinformowany, że jest to folder udostępniony, a jego usunięcie spowoduje usunięcie udostępnionego zasobu. Aby kontynuować, należy potwierdzić zrozumienie treści ostrzeżenia.
- 3- Otwórz okno wiersza poleceń i wpisz `cd c\`.
4. Wpisz polecenie **createfiles.bat**.

Informacja Jeśli podczas lekcji 1, w ćwiczeniu 1, nie został utworzony plik `createfiles.bat`, należy wykonać czynności opisane w punktach od 1 do 3 (ćwiczenie 1), aby utworzyć odpowiedni skrypt

Ćwiczenie 2: Harmonogram zadania kopii zapasowej

Należy skonfigurować i utworzyć harmonogram wykonywania opisanych poniżej zadań kopii zapasowych. Pomocą podczas realizacji tych zadań mogą być instrukcje zamieszczone w Zadaniach kontrolnych lekcji 1 i 3.

- Zadanie wykonania normalnej kopii zapasowej archiwizującej folder C:\Data\Finance w pliku nazwanym C:\BackupFinance.bkf (zastępowanie nośnika). Kopia wykonywana jest każdej niedzieli o godzinie 21:00.
- Zadanie wykonania różnicowej kopii zapasowej archiwizującej ten sam folder, w tym samym pliku (dołączanie do nośnika). Kopia powinna być wykonywana o 00:15 od wtorku do soboty (czyli w nocy od poniedziałku do piątku).

Ćwiczenie 3: Symulowanie wykonywania zaplanowanych zadań

Zamiast czekać do niedzieli, aż w nocy automatycznie rozpocznie się wykonywanie zadania kopii zapasowej, można wykonać zadanie w oknie wiersza poleceń.

1. Otwórz program *Backup Utility* (Kopia zapasowa).
2. Kliknij zakładkę **Schedule Jobs** (Planowanie zadań).
3. W kalendarzu kliknij ikonę zadania reprezentującego normalną kopię zapasową wykonywaną w niedzielę w nocy.
4. Kliknij przycisk **Properties** (Właściwości).
5. Zaznacz polecenie znajdujące się w polu *Run* (Uruchom) i aby je skopiować, naciśnij CTRL+C.
6. Naciśnij przycisk **Cancel** (Anuluj), aby zamknąć okno dialogowe *Schedule* (Harmonogram), a następnie zamknij program *Backup Utility* (Kopia zapasowa).
7. Otwórz okno wiersza poleceń.
8. Kliknij menu okna (ikona w lewym górnym rogu okna wiersza poleceń) i w menu **Edit** (Edytuj) wybierz opcję **Paste** (Wklej). Polecenie programu Ntbackup wraz z wszystkimi przełącznikami zostało wklejone do wiersza poleceń. Naciśnij ENTER. Zostanie wykonane zadanie kopii zapasowej.
9. Otwórz i zmodyfikuj plik C:\Data\Finance\Projections.txt. Zapisz i zamknij plik.
10. Powtórz procedurę od punktu 1 do 8, uruchamiając zadanie *różnicowej* kopii zapasowej, której wykonanie zaplanowane zostało na porę nocną.

Ćwiczenie 4: Sprawdzenie procedury

1. Otwórz program *Backup Utility* (Kopia zapasowa).
2. W menu **Tools** (Narzędzia) kliknij polecenie **Report** (Raport).
3. Otwórz dwa ostatnie raporty kopii zapasowych i sprawdź, czy zadania zostały poprawnie wykonane. Normalna kopia zapasowa powinna zawierać skopiowane cztery pliki. Różnicowa kopia zapasowa powinna składać się tylko z jednego pliku.
4. Przeprowadź odtwarzanie plików do foldera nazwanego C:\TestRestore. Najpierw należy przywrócić normalną kopię zapasową, a następnie różnicową. Pomocne mogą być informacje podane w Zadaniu kontrolnym zamieszczonym w lekcji 2.

Uwaga Warto zapamiętać, że przed odtworzeniem zadania różnicowego, należy skonfigurować opcje zakładki *Restore* (Przywracanie) tak, aby pliki były zawsze zastępowane. Zakładka uruchamiana jest za pomocą polecenia *Options* (Opcje) w menu *Tools* (Narzędzia). Być może również trzeba będzie skatalogować plik, aby widoczne były wszystkie zawarte w nim zestawy kopii zapasowych.

Rozwiązywanie problemów

O 13:00 we wtorek użytkownik działu finansowego powiadomił administratora, że przypadkowo usunął pliki foldera Finance. Administrator jest pewny, że wprowadzona procedura wykonywania kopii zapasowych pozwoli odzyskać usunięte pliki. Jednakże należy zapewnić, aby pliki zmodyfikowane w dniu dzisiejszym nie zostały zastąpione przez pliki kopii zapasowej utworzonej w nocy.

W ćwiczeniu tym należy zasymulować działania, które zasymulują opisane zdarzenia, a następnie odtworzą brakujące pliki.

Ćwiczenie 1: Zasymulowanie sytuacji utraty danych

1. Otwórz folder C:\Data\Finance.
2. Otwórz i zmodyfikuj plik Current.txt. Zapisz i zamknij plik.
3. Otwórz i zmodyfikuj plik Budget file. Zapisz i zamknij plik.
4. Usuń pliki Historical.net oraz Projections.txt.

Ćwiczenie 2: Zaplanowanie procedury przywracania

Należy przejrzeć metodę wykonywania kopii zapasowych wprowadzoną w Zadaniu praktycznym: normalna kopia zapasowa wykonywana nocą w niedzielę oraz różnicowa kopia zapasowa wykonywana codziennie nocą (poza sobotą i niedzielą).

1. W jaki sposób należy przeprowadzić odzyskiwanie brakujących danych?

Normalna kopia zapasowa zawiera wszystkie wybrane pliki. Jest podstawą do rozpoczęcia procedur przywracania brakujących danych. Różnicowa kopia zapasowa zawiera wszystkie pliki zmodyfikowane od momentu wykonania ostatniej normalnej kopii zapasowej. Po odtworzeniu normalnej kopii zapasowej, należy odtworzyć ostatnią kopie różnicową. Należy jednak pamiętać, że niektóre pliki zostały zmodyfikowane już po wykonaniu ostatniej różnicowej kopii zapasowej.

2. W jaki sposób zapobiec zastępowaniu tych nowszych plików, plikami znajdującymi się w zestawie kopii zapasowej?

W oknie dialogowym Options (Opcje) została umieszczona zakładka Restore Options (Opcje przywracania), za pomocą której można definiować sposób zapisu plików zestawu kopii zapasowej w miejscu docelowym. Należy określić, aby program Backup Utility (Kopia zapasowa) zastępował pliki jedynie wtedy, kiedy pliki na dysku są starsze niż pliki zestawu kopii zapasowej. Dzięki temu nowsze pliki pozostaną niezmienione.

Ćwiczenie 3: Przywracanie danych

1. Otwórz program Backup Utility (Kopia zapasowa).
2. W menu Tools (Narzędzia) wybierz polecenie Options (Opcje).
3. Kliknij zakładkę Restore (Przywracanie).
4. Skonfiguruj funkcję przywracania tak, aby nowsze pliki pozostawały niezmienione — przez zaznaczenie opcji Replace The File On Disk Only If The File On Disk Is Older (Zmień plik na dysku tylko wtedy, gdy plik na dysku jest starszy), a następnie zamknij okno dialogowe Options (Opcje).
5. Wybierz nośnik kopii zapasowej, który zawiera normalną i różnicową kopie zapasową.

6. Przywróć normalną kopię zapasową w jej lokalizacji oryginalnej.
7. Przywróć różnicową kopię zapasową w jej lokalizacji oryginalnej.
8. Otwórz pliki Current oraz Budget. Ponieważ pliki te są nowsze niż pliki znajdujące się w zestawie kopii zapasowej, a także dzięki odpowiednim ustawieniom przywracania, powinna to być wersja plików zmodyfikowanych podczas realizacji Zadania praktycznego.

Podsumowanie rozdziału

- Używanie programu Backup Utility (Kopia zapasowa) lub innego tego typu programu narzędziowego wymaga uprawnień potrzebnych do wykonywania kopii zapasowych i przywracania danych. Domyślne ustawienia określają, że uprawnienia takie mają grupy Backup Operators (Operatorzy kopii zapasowych) oraz Administratorzy.
- Programy Backup Utility (Kopia zapasowa) i Ntbackup umożliwiają tworzenie kopii zapasowych oraz odtwarzanie danych przy użyciu folderów zdalnych i lokalnych. Kopia zapasowa nie może być tworzona przy użyciu napędów CD lub DVD.
- Procedura tworzenia kopii zapasowych najczęściej rozpoczyna się od wykonania normalnej kopii zapasowej, po czym regularnie wykonywane są różnicowe lub przyrostowe kopie. Zadania przyrostowych kopii zapasowych tworzą kopie najszybciej, natomiast kopie różnicowe są szybsze podczas operacji przywracania. Zadania mogą zostać tak zaplanowane, aby wykonywane były w okresach niskiego poziomu wykorzystania systemu.
- Typ kopii zapasowych: Kopia oraz Codzienna mogą być używane do przechwytywania plików bez wpływu na realizację zaplanowanych zadań kopii zapasowych.
- Program Backup Utility (Kopia zapasowa) umożliwia odtworzenie danych kopii zapasowych w ich oryginalnej lub innej lokalizacji. Odtwarzanie w innej lokalizacji jest przydatne do przetestowania i sprawdzenia procedur przywracania. Ustawienia zamieszczone na zakładce Restore (Przywracanie) okna dialogowego Options (Opcje) umożliwiają kontrolę tego, które pliki zostaną odtworzone podczas wykonywania procedur przywracania.
- Polecenie Ntbackup wraz z pełnym zestawem przełączników umożliwia uruchomienie zadania kopii zapasowej w oknie wiersza poleceń lub na podstawie pliku wsadowego.
- Usługa VSS (Volume Shadow Copy Service) umożliwia użytkownikowi dostęp do poprzednich wersji plików i folderów udostępnionych zasobów sieci. Dzięki dostępowi do poprzednich wersji, użytkownik może odtworzyć usunięte bądź uszkodzone pliki lub może porównywać wersje plików.

Informacje dla zdających egzamin

Przed przystąpieniem do egzaminu, należy zapoznać się z przedstawionymi poniżej najważniejszymi faktami i pojęciami, aby określić które tematy wymagają pogłębienia. Należy powrócić do lekcji, aby osiągnąć większą wprawę oraz przejrzeć działy znajdujące się w części 2 — „Materiały dodatkowe”. Informacje tu zawarte kierują do materiałów uzupełniających tematy objęte zadaniami egzaminacyjnymi.

Najważniejsze fakty

- Znajomość praw i członkostwa grup wymaganych do wykonywania kopii zapasowych lub operacji przywracania.
- Tworzenie procedur tworzenia kopii zapasowych w oparciu o wymagania dotyczące czasu potrzebnego na wykonanie kopii oraz szybkości wykonywania operacji przywracania danych.
- Znajomość sposobów przywracania danych w różnych warunkach, w tym dla całkowitej lub częściowej utraty danych. Analiza brakujących danych w odniesieniu do harmonogramu wykonywania kopii zapasowych umożliwiającą określenie, jaki zestaw kopii zapasowych musi zostać odtworzony. Połączenie wiedzy związanej z zalecaną kolejnością przywracania kopii zapasowych i związanej z metodami zastępowania istniejących na dysku plików.
- Tworzenie harmonogramu zadań kopii zapasowych i konfigurowanie opcji dotyczących ich wykonywania.
- Włączanie kopiowania w tle folderów udostępnionych oraz przywracanie danych za pomocą zakładki Previous Versions (Poprzenie kopie) znajdującej się w oknie dialogowym Properties (Właściwości) foldera.

Najważniejsze pojęcia

Kopia, codzienna, różnicowa, przyrostowa oraz normalna kopia zapasowa Pięć rodzajów kopii zapasowych, które przy użyciu określonych kryteriów mogą być stosowane do wyboru plików kopii. *Kopia* oraz *normalna kopia zapasowa* kopiuje wszystkie pliki. *Codzienna kopia zapasowa* archiwizuje wszystkie pliki zmodyfikowane w danym dniu. *Kopia różnicowa* i *przyrostowa* zapisuje pliki, dla których ustawiony został atrybut archiwalny. *Kopia normalna i przyrostowa* zerują ustawienie atrybutu archiwalny.

Atrybut archiwalny Atrybut ten jest ustawiany w momencie tworzenia lub modyfikowania pliku. *Kopia różnicowa* i *przyrostowa* zapisuje pliki, dla których ustawiony został atrybut archiwalny. *Kopia przyrostowa* zeruje ustawienie atrybut archiwalny.

Usługa VSS (Volume Shadow Copy Service) Cecha systemu Windows Server 2003 umożliwiającą tworzenie kopii zapasowych otwartych lub zablokowanych plików.

Pule nośników: nierozpoznanych, importu, wolnych, kopii zapasowych Są to cztery kategorie nośników wymiennych. Program Ntbackup wykonuje kopię zapasową jedynie na nośnikach znajdujących się w puli wolnych nośników lub w puli nośników kopii zapasowych.

Kopie w tle folderów udostępnionych Cecha systemu Windows Server 2003, którą należy skonfigurować na serwerze i stacji klienta oraz która umożliwia użytkownikom pobieranie poprzednich wersji plików bez udziału administratora-

Pytania i odpowiedzi

243 Pytania do lekcji 1

1. Która z poniższych lokalizacji **nie** może być używana do tworzenia kopii zapasowych w systemie Windows Server 2003?
 - a. Lokalny napęd taśmy
 - b. Lokalny napęd dysków CD-RW
 - c. Lokalny dysk twardy
 - d. Folder udostępniony serwera zdalnego
 - e. Lokalny napęd dysku DVD+R
 - f. Lokalny dysk wymienialny
 - g. Napęd taśmy serwera <-v.. Inego

Prawidłowe odpowiedzi to b, e oraz g.

2. Każdego wieczoru administrator wykonuje kopię zapasową serwera plików systemu Windows Server 2003. Wykonywana jest ręczna, normalna kopia zapasowa. Administrator chce zaplanować wykonywanie kopii zapasowych każdego wieczoru przez następne dwa tygodnie. Za pomocą którego typu kopii zapasowej zadanie to zostanie najszybciej zrealizowane??
 - a. Normal (Normalna)
 - b. Differential (Różnicowa)
 - c. Incremental (Przyrostowa)
 - d. Copy (Kopia)

Prawidłowa odpowiedź to c.

3. Każdego wieczoru administrator wykonuje kopię zapasową serwera plików systemu Windows Server 2003. Wykonywana jest ręczna, normalna kopia zapasowa. Administrator chce zaplanować wykonywanie kopii zapasowych każdego wieczoru przez następne dwa tygodnie. Przy użyciu którego typu kopii zapasowej odtworzenie danych będzie najprostsze?
 - a. Normal (Normalna)
 - b. Differential (Różnicowa)
 - c. Incremental (Przyrostowa)
 - d. Daily (Codzienna)

Prawidłowa odpowiedź to a.

4. Każdego wieczoru administrator wykonuje kopię zapasową serwera plików systemu Windows Server 2003. Wykonywana jest normalna kopia zapasowa. Następnego wieczoru administrator zastanawia się, który typ kopii zapasowych powinien być używany: kopia różnicowa czy przyrostowa. Czy dla tych typów występują różnice w szybkości tworzenia kopii i wielkości plików archiwizacyjnych? Jeśli następnego dnia serwer ulegnie awarii, czy wystąpią różnice wydajności podczas odtwarzania danych?

Następnego wieczoru można użyć dowolnego rodzaju kopii. Normalna kopia zapasowa zeruje ustawienie atrybutu archiwalny. Obie kopie, różnicowa i przyrostowa, będą kopiowały wszystkie

m,uac iraining mi: egzamin lu-^au

pliki utworzone lub zmodyfikowane w ciągu dnia drugiego. Dlatego zawartość obu kopii będzie taka sama i tym samym, trzeciego dnia, nie będzie różnic podczas operacji przywracania. Trzeciego dnia należy odtworzyć normalną kopie zapasową, a następnie kopię utworzoną wieczorem dnia | poprzedniego.

Jednakże, przyrostowa i różnicowa kopie zapasowe inaczej obsługują atrybut archiwalny: kopie I przyrostowa zeruje ustawienie atrybutu, natomiast kopie różnicowa je pozostawia. Tak więc, | *następne* kopie zapasowe będą się już różniły. Druga przyrostowa kopie zapasowa będzie kopiować jedynie pliki utworzone lub zmodyfikowane od momentu wykonania pierwszej kopii przyrostowej. Natomiast druga kopie różnicowa będzie zawierać wszystkie pliki utworzone lub zmodyfikowane od momentu wykonania normalnej kopii zapasowej, to znaczy, będzie zawierać wszystkie pliki, które już zostały skopiowane przez pierwszą kopie różnicową. 5. Należy przejrzeć kroki procedury przeprowadzanej w Zadaniu kontrolnym i przewidzieć zawartość następujących zadań tworzenia kopii zapasowych:

- backup-normal.bkf
- backup-diff-day1 .bkf
- backup-diff-day2.bkf
- backup-i nc-day2. bkf
- backup-inc-day3.bkf

Czy zawartości kopii zapasowych backup-diff-day2 oraz backup-inc-day2 będą się między sobą różniły?

- » backup-normal.bkf: Historical, Current, Budget oraz Projections
- » backup-diff-day1.bkf: Current
- » backup-diff-day2.bkf: Current oraz Budget
- » backup-inc-day2.bkf: Current oraz Budget
- » backup-inc-day3.bkf: Projections

Kopie zapasowe backup-diff-day2 oraz backup-inc-day2 będą takie same. Obie kopie będą zapisywać pliki, dla których ustawiony został atrybut archiwalny. Ponieważ normalna kopie zapasowa została utworzona w pierwszym dniu, wszystkie zmodyfikowane od tego momentu pliki będą miały ustawiony atrybut archiwalny.

Pytania do lekcji 2

1. Użytkownik przypadkowo usunął dane dokumentu programu Microsoft Word i zapisał dokument, przez co trwale zmienił oryginalny plik. Poprzedniego wieczoru wykonana została normalna kopie zapasowa. Która opcja przywracania powinna zostać zastosowana?

- a. Do Not Replace The File On My Computer (Nie zamieniaj pliku na tym komputerze).
- b. Replace The File On Disk Only If The File On Disk Is Older (Zamień plik na dysku tylko wtedy, gdy plik na dysku jest starszy).
- c. Always Replace The File On My Computer (Zawsze zamieniaj plik na tym komputerze).

Prawidłowa odpowiedź to c. Plik istnieje na serwerze, lecz został uszkodzony. Należy zastąpić ten plik jego kopią zapasową.

2. Dyrektor wrócił z delegacji. Przed wyjazdem skopiował pliki z foldera sieciowego na dysk twardy swojego komputera. Folder jest współużytkowany przez inne osoby, które zmieniły pliki tego foldera w czasie jego nieobecności. Dyrektor po powrocie przeniósł swoją kopię plików do foldera udostępnionego w sieci, przez co zaktualizował pliki zmianami poczynionymi podczas delegacji, ale również zastąpił wszystkie pliki, które były modyfikowane przez innych współpracowników. Ci ostatni nie byli „szczęśliwi”, że ich pliki zostały zastąpione wersjami plików aktualnych przed wyjazdem dyrektora. Na szczęście poprzedniego wieczoru wykonana została normalna kopia zapasowa. Która opcja przywracania powinna zostać zastosowana?
- Do Not Replace The File On My Computer (Nie zamieniaj pliku na tym komputerze).
 - Replace The File On Disk Only If The File On Disk Is Older (Zamień plik na dysku tylko wtedy, gdy plik na dysku jest starszy).
 - Always Replace The File On My Computer (Zawsze zamieniaj plik na tym komputerze).
- Prawidłowa odpowiedź to b. Zaznaczenie tej opcji nie spowoduje zastąpienia plików, które zostały zmienione przez dyrektora podczas jego nieobecności w biurze. Pliki te są nowsze niż pliki zawarte w kopii zapasowej. Jednakże, dzięki tej opcji zastąpione zostaną inne, starsze wersje plików dyrektora, które zostały przez niego skopiowane do sieci.

Wskazówka Użytkownicy powinni zapoznać się z funkcją Cifline Files (Pliki trybu offline), która pozwala zapobiec tego rodzaju, rzadko spotykanym „katastrofom”. Funkcja Offline Files (Pliki trybu offline) synchronizuje tylko zmienione pliki, tak więc tylko zaktualizowane przez dyrektora pliki zostałyby skopiowane do sieci, natomiast pozostałe pliki dyrektora pozostałyby niezmienione.

3. Administrator chce sprawdzić procedury przywracania na serwerze, ale chce również uniknąć wpływu przeprowadzania tych procedur na kopie zapasowe aktualnie wykorzystywanych w przedsiębiorstwie danych. Która lokalizacja powinna być użyta podczas próbnego przywracania danych?
- Original location (Lokalizacja oryginalna)
 - Alternate location (Lokalizacja alternatywna)
 - Single folder (Pojedynczy folder)
- Prawidłowa odpowiedź to b. Przywracanie w innej lokalizacji będzie odtwarzać strukturę i pliki foldera w postaci, w jakiej zostały skopiowane. Będzie więc możliwe porównanie zawartości docelowej z oryginalną i sprawdzenie poprawności procedury przywracania danych.

Pytania do lekcji 3

1. Użytkownik Scott Bishop ma duże uprawnienia w lokalizacji zdalnej, która liczy 20 użytkowników. W siedzibie tej wykorzystywany jest system Windows Server 2003, w oparciu o który zbudowane zostały serwery plików i drukowania. W systemie został zainstalowany napęd taśmy. Ponieważ w siedzibie na pełny etat nie jest zatrudniony administrator, zdecydowano, że uprawnienia potrzebne do wykonywania kopii zapasowych i przywracania systemu przydzielone zostaną użytkownikowi Scott. Jednakże należy przydzielić tylko te uprawnienia, które są niezbędne do wykonywania kopii zapasowych i odtwarzania danych. Jaka jest zalecana praktyka udostępniania użytkownikowi Scott niezbędnych uprawnień tak, aby mógł wykonywać powierzone zadanie?

Użytkownik Scott powinien być członkiem grupy Backup Operators (Operatorzy kopii zapasowych). Ustawienia domyślne określają, że grupa ta ma uprawnienia pozwalające wykonywać kopie zapasowe oraz odtwarzać dane folderów i plików.

2. Napisz polecenie umożliwiający wykonanie pełnej kopii zapasowej foldera C:\Data\Financ do pliku nazwanego Backup.bkf w udostępnionym folderze Backup serwera Server02. Nazwa zadania kopii zapasowych powinna brzmieć „Backup of Finance Folder”. Następnie napisz to polecenie tak, aby umożliwiała wykonanie przyrostowej kopii zapasowej oraz dołączenie zestawu kopii do tego samego pliku i z tą samą nazwą zadania kopii zapasowej.

```
ntbackup backup "c:\data\finance" /J "Backup of Finance Folder" /F "W
server02
\backup\backup.bkf"
ntbackup backup "c:\data\finance" /J "Backup of Finance Folder" /F "W
server01
\backup\backup.bkf" /a /m incremental
```

- 3- Użytkownik usunął plik w udostępnionym folderze serwera. Użytkownik otworzył okno właściwości foldera. W oknie tym nie była wyświetlana zakładka Previous Versions (Poprzednie wersje). Co mogłoby być tego przyczyną? Wybierz wszystkie właściwe odpowiedzi.
- a. Dla foldera nie została włączona funkcja Shadow Copy (Kopie w tle).
 - b. Dla wolumenu nie została włączona funkcja Shadow Copy (Kopie w tle).
 - c. Użytkownik nie ma uprawnień do przeglądania bufora usługi Shadow Copy (Kopie w tle).
 - d. Program klienta usługi Shadow Copy (kopie w tle) nie został zainstalowany na komputerze użytkownika.
 - e. Folder został umieszczony na woluminie FAT.

Prawidłowe odpowiedzi to b oraz d. Funkcja Shadow Copy (Kopie w tle) jest włączana dla wolumenu, a nie dla foldera. Po włączeniu funkcji Shadow Copy (Kopie w tle), każdy użytkownik (wymagane zainstalowanie programu klienta) będzie mógł używać zakładkę Previous Versions (Poprzednie wersje) dla "modyfikowanych plików lub folderów". Funkcja Shadow Copy (Kopie w tle) jest obsługiwana na woluminach FAT oraz NTFS.

Drukarki

Zadania egzaminacyjne omawiane w tym rozdziale:

- Monitorowanie kolejek drukowania.
- Monitorowanie serwerów plików i wydruku. Omawiane narzędzia co: Task Manager (Menedżer zadań), Event Viewer (Podgląd zdarzeń) oraz System Monitor (Monitor systemu).

Cele rozdziału

Do typowych zadań administratora zawsze należą zagadnienia dotyczące drukarek. Zadaniom takim jak testowanie i instalowanie nowych drukarek, rozwiązywanie problemów drukowania lub zabezpieczania czy monitorowanie wykorzystania drukarek trzeba poświęcić mniej więcej tyle samo czasu, co w przypadku zadań związanych z dostępem do plików i folderów.

System Microsoft Windows Server 2003 został wyposażony w zestaw funkcji obsługujących w przedsiębiorstwie usługi druku. Niniejszy rozdział omawia ustawienia i konfiguracje drukarek systemu Windows Server 2003, współdziałanie drukarek i usługi katalogowej Active Directory, przyłączanie klientów drukarek sieciowych oraz monitorowanie usług drukowania i rozwiązywanie problemów usług drukowania. Opisane zostaną sposoby zarządzania lokalnymi, sieciowymi oraz internetowymi drukarkami, a także, w jaki sposób elastycznie i jednocześnie zachowując odpowiedni poziom bezpieczeństwa, konfigurować drukarki.

Lekcje w tym rozdziale:

- Lekcja 1: Instalowanie i konfigurowanie drukarek..... 279
- Lekcja 2; Zaawansowana konfiguracja i zarządzanie drukarkami..... 291
- Lekcja 3: Konserwacja, monitorowanie i usuwanie problemów związanych z drukarkami 304

Wymagania

W niniejszym rozdziale przedstawione zostały zagadnienia związane z administracją drukarek systemu Windows Server 2003. Opracowując zestaw szkoleniowy przyjęto założenie, że student ma co najmniej 18-miesięczne doświadczenia dotyczące wykorzystywania usługi Active Directory i konsoli MMC (Microsoft Management Console). Ze względu jednak na to, że wielu administratorów pracowało w innych niż system Windows Server 2003 środowiskach, takich jak na przykład Novell NetWare oraz ze względu na niewielkie zmiany w terminologii dotyczącej drukarek, pierwsza lekcja rozdziału omawia podstawy konfiguracji drukarek. Dwie następne lekcje, oparte o te podstawy, przygotowują do bardziej zaawansowanej administracji, obsługi, monitorowania oraz rozwiązywania problemów drukarek wykorzystywanych w środowisku systemu Windows Server 2003.

Z pewnością, podczas przeprowadzania ćwiczeń pomocne byłoby posiadanie drukarki i dwóch komputerów (system Windows Server 2003 oraz system klienta Windows XP lub Windows 2000 Professional), ale zadania są tak pomyślane, że można je zakończyć mając tylko jeden komputer. W tym celu należy przygotować:

- System Windows Server 2003 (Standard or Enterprise). Serwer powinien nazywać się Server01 i być kontrolerem domeny w domenie contoso.com
- Jednostkę organizacyjną pierwszego poziomu nazwaną Security Groups
- Konsolę Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) lub niestandardową konsolę zawierającą przystawkę Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory).

Lekcja 1: Instalowanie i konfigurowanie drukarek

System Windows Server 2003 udostępnia sprawne, bezpieczne i elastyczne usługi drukowania. System Windows Server 2003 może być używany do zarządzania drukarkami przyłączonymi lokalnie lub poprzez sieć i umożliwia wykorzystywanie tych drukarek przez aplikacje uruchomione lokalnie na serwerze Windows 2003 lub przez użytkowników dowolnych platform, wliczając w to poprzednie wersje Windows, jak również systemy Netware, UNIX lub Apple Macintosh. Niniejsza lekcja omawia podstawowe pojęcia, terminologię oraz umiejętności dotyczące konfigurowania drukarek w systemie Windows Server 2003.

Materiały omówione podczas lekcji pozwalają na

- Zapoznanie się z modelem i terminologią używaną w środowisku drukowania systemu Windows
- Instalowanie drukarek logicznych na serwerach wydruku dla drukarek przyłączonych poprzez sieć
- Przygotowanie serwera wydruku do obsługi klientów, w tym komputerów wykorzystujących poprzednie wersje systemu Windows
- Przyłączenie klienta drukarki do drukarki logicznej serwera wydruku
- Zarządzanie zadaniami drukowania

Szacunkowy czas lekcji: 15 minut

Omówienie modelu drukarki systemu Windows Server 2003

System Windows Server 2003, a także poprzednie wersje Windows, obsługują dwa typy drukarek:

- **Drukarki przyłączone lokalnie** Są to drukarki przyłączone do portu fizycznego serwera wydruku. Najczęściej jest to port USB (Universal Serial Bus) lub port równoległy.
- **Drukarki sieciowe** Są to drukarki przyłączone do sieci, a nie do portu fizycznego. Drukarka sieciowa jest węzłem sieci. Serwer wydruku komunikuje się z drukarką przy użyciu protokołu sieciowego, takiego jak TCP/IP (Transmission Control Protocol/Internet Protocol).

Na serwerze wydruku każdy typ drukarki jest przedstawiany jako drukarka logiczna. *Drukarka logiczna* określa cechy i zachowanie drukarki. Można powiedzieć, że drukarka logiczna zawiera sterownik drukarki, jej ustawienia, domyślne ustawienia wydruku oraz inne właściwości kontrolujące sposób przetwarzania i wysyłania zadania wydruku do wybranej drukarki. Taka wirtualizacja drukarki umożliwia niezwykle elastyczność i pomysłowość w konfigurowaniu usług drukowania.



Informacja Poprzednie wersje systemów Windows oraz poprzednie wersje dokumentacji w odniesieniu do drukarki używały pojęcia „urządzenie drukujące”, a w odniesieniu do drukarki logicznej stosowały pojęcie „drukarka”.

Istnieją dwa sposoby zainstalowania drukarek sieciowych. Jeden z nich polega na zainstalowaniu drukarek logicznych na wszystkich komputerach, a następnie na przyłączeniu tych drukarek logicznych bezpośrednio do drukarki sieciowej. W takim modelu brak serwera wydruku, każdy komputer obsługuje swoje własne ustawienia, przetwarzanie i kolejkę wydruku. Jeśli użytkownik sprawdza kolejkę wydruku, widzi tylko zadania, które sam wysłał do drukarki. Użytkownik nie ma możliwości sprawdzenia, jak zadania zostały wysłane do drukarki przez innych użytkowników. Oprócz tego, komunikaty o błędach wyświetlone zostaną jedynie na komputerze, który wysłał zadanie aktualnie drukowane. Warto także zwrócić uwagę, że wszystkie zadania wydruku są przetwarzane na komputerze lokalnym użytkownika, zamiast przekazywania ich do serwera wydruku i obciążenia komputera lokalnego.

Ze względu na te istotne wady, najbardziej typową konfiguracją drukarek przedsiębiorstw jest moduł trójelementowy, składający się z drukarki fizycznej, drukarki logicznej obsługiwanej przez serwer wydruku oraz klientów wydruku przyłączonych do drukarki logicznej serwera. Niniejsza lekcja opisuje jedynie tę strukturę, chociaż można również znaleźć informacje o pojęciach i umiejętnościach związanych z innymi konfiguracjami drukarek.

Poniżej wymienione zostały zalety drukowania przy użyciu serwera wydruku:

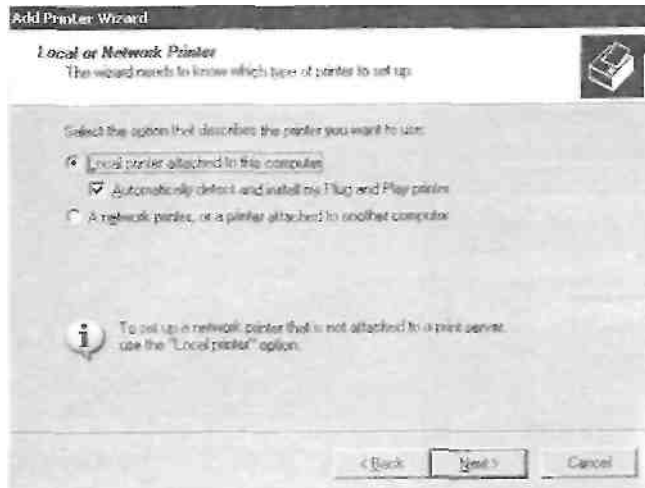
- Drukarka logiczna serwera wydruku określa ustawienia drukarki i zarządza sterownikami drukarki. I
- Drukarka logiczna tworzy pojedynczą kolejkę wydruku, która jest widoczna na wszystkich komputerach klientów, dzięki czemu użytkownicy wiedzą, jak w danym momencie wykorzystywana jest drukarka przez innych jej użytkowników.
- Komunikaty o błędach, takie jak brak papieru czy zakleszczenie papieru, są widoczne dla wszystkich klientów, dzięki czemu wszyscy użytkownicy mają informacje o aktualnym stanie drukarki.
- Poprzez przekazanie przetwarzania zadania wydruku do serwera zmniejszone zostaje, czasami w stopniu istotnym, obciążenie większości aplikacji i sterowników drukarek, dzięki czemu skrócony zostaje czas odpowiedzi komputera klienta. Inaczej mówiąc, jeśli użytkownik kliknie polecenie Print (Drukuj), jego zadanie zostanie szybko przesłane do serwera wydruku, a użytkownik może kontynuować swoją pracę w czasie, kiedy serwer wydruku przetwarza zadania.
- Zostały scentralizowane funkcje zabezpieczeń, inspekcji, monitorowania i protokolowania.

Instalowanie drukarki w systemie Windows Server 2003

Najczęściej drukarki są obsługiwane przy użyciu foldera *Printers And Faxes* (Drukarki i faksy), który łączy w sobie możliwości obsługi zarówno drukarek, jak i faksów. Program *AddPrinter Wizard* (Kreator dodawania drukarki) pomaga skonfigurować urządzenie. Poniżej wymienione zostały najważniejsze parametry, które użytkownik musi określić podczas instalowania drukarki:

- **Drukarka lokalna lub sieciowa** Na rysunku 8-1 przedstawiona została omawiana strona programu *Add Printer Wizard* (Kreator dodawania drukarki). Podczas konfigurowania drukarki w systemie Windows Server 2003 warto zwrócić uwagę, że pojęcia drukarka lokalna i drukarka sieciowa mają trochę inne znaczenie niż można by oczekiwać. *Drukarka lokalna* jest drukarką logiczną obsługującą drukarki przyłączone bezpośrednio do serwera lub obsługującą autonomiczne drukarki sieciowe. Zaznaczenie opcji *LocalPrinter Attached To This Computer* (Drukarka lokalna podłączona do tego komputera) powoduje, że serwer udostępni tę drukarkę innym klientom sieci. Natomiast *drukarka sieciowa* jest drukarką logiczną skojarzoną z drukarką, która jest bezpośrednio podłączona do innego komputera lub przyłączona do drukarki zarządzanej przez inny serwer wydruku. Interfejs

użytkownika może wprowadzać w błąd i dlatego warto pamiętać, że w typowych instalacjach serwera wydruku, serwer wydruku będzie obsługiwał drukarki lokalne (czy to bezpośrednio przyłączone do komputera czy to drukarki sieciowe), natomiast stacje robocze tworzą drukarki sieciowe podłączone do udostępnionych drukarek logicznych serwera.



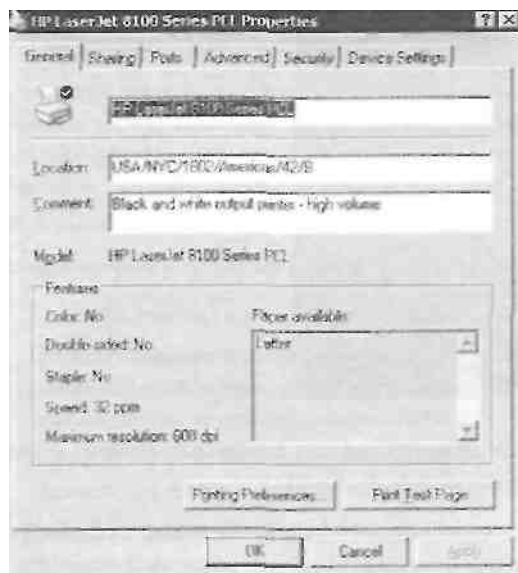
Rysunek 8-1 Strona *Local Or Network Printer* (Drukarka lokalna lub sieciowa) w programie *Add Printer Wizard* (Kreator dodawania drukarki)

- **Wybór portu drukarki** Podczas tworzenia drukarki lokalnej na serwerze wydruku, program *Add Printer Wizard* (Kreator dodawania drukarki) wymaga określenia portu, do którego drukarka zostanie przyłączona. Jeśli port taki istnieje, na przykład port LPT1 lub port sieci określany przez adres IP, należy wybrać ten port z listy rozwijanej *Use The Following Port* (Użyj następującego portu). Jeśli natomiast skonfigurowana jest drukarka logiczna dla drukarki sieciowej, dla której port nie został utworzony, należy kliknąć opcję **Create A New Port** (Utwórz nowy port), zaznaczyć opcję **Standard TCP/IP Port**, a następnie kliknąć przycisk **Next** (Dalej). Wyświetlone zostanie okno *Add Standard TCP/IP Printer Port Wizard* (Kreator dodawania standardowego portu TCP/IP). Po kliknięciu przycisku **Next** (Dalej), użytkownik wprowadza adres IP lub nazwę DNS drukarki. Po dodaniu portu następuje powrót do programu *Add Printer Wizard* (Kreator dodawania drukarki).
- **Instalowanie oprogramowania drukarki** Jeśli funkcja „Plug and Play” automatycznie nie wykryła i nie zainstalowała prawidłowo drukarki, użytkownik może wybrać drukarkę z listy podzielonej według producentów drukarek. Jeśli natomiast dany model drukarki nie został na tej liście umieszczony, należy kliknąć przycisk **Have Disk** (Z dysku) i zainstalować drukarkę na podstawie dostarczonych przez producenta sterowników.
- **Nazwa drukarki oraz nazwa udziału** Pomimo, że system Windows Server 2003 obsługuje długie nazwy drukarek oraz nazwy udziałów zawierające spacje i znaki specjalne, to zaleca się tworzenie prostych i krótkich nazw. Cała nazwa kwalifikowana zawierająca nazwę serwera (na przykład \\Server01\PSSCRIPT) nie powinna być dłuższa niż 32 znaki.

Utworzona nazwa drukarki i nazwa udziału są używane w wielu miejscach interfejsu użytkownika systemu Windows. Chociaż nazwa udziału może różnić się od nazwy drukarki, celem unikania pomyłek w wielu przedsiębiorstwach stosowane są takie same oznaczenia.

Konfigurowanie właściwości drukarki

Po zainstalowaniu drukarki logicznej, użytkownik może skonfigurować szereg właściwości. Czynności przeprowadzane są w oknie dialogowym *Properties* (Właściwości) drukarki, takim jak pokazane na rysunku 8-2. Zakładka *General* (Ogólne) pozwala określić nazwę drukarki, lokalizację, wpisać komentarze. Początkowe wpisy tych pól powstały w oparciu o informacje wprowadzone w programie (*Printer Wizard* (Kreator dodawania drukarki)).

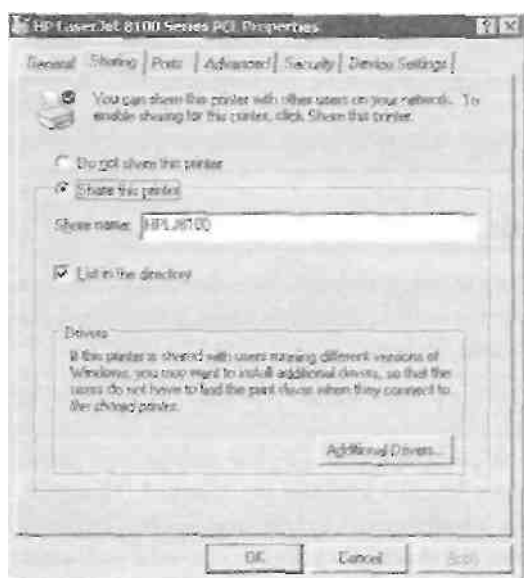


Rysunek 8-2 Zakładka *General* (Ogólne) okna dialogowego *Properties* (Właściwości) drukarki

Zakładka *Sharing* (Udostępnianie), pokazana na rysunku 8-3, umożliwia zdefiniowanie, czy drukarka lokalna ma być udostępniana innym klientom sieci oraz czy drukarka ma być umieszczona w usłudze Active Directory (ustawienie domyślne dla udostępnionych drukarek), dzięki czemu użytkownicy będą mogli łatwo wyszukać i przyłączyć drukarki.



Informacja Za pomocą zakładki *Sharing* (Udostępnianie) można zakończyć udostępnianie drukarki. Jeśli na przykład trzeba drukarkę przełączyć w tryb offline, funkcja ta uniemożliwia próby uzyskania dostępu do drukarki.



Rysunek 8-3 Zakładka *Sharing* (Udostępnianie) okna dialogowego *Properties* (Właściwości) drukarki

Podczas konfigurowania drukarki, system Windows Server 2003 umieszcza na serwerze wydruku sterowniki, które obsługują drukarkę na komputerach klientów działających pod kontrolą systemów Windows Server 2003, Windows XP oraz Windows 2000. Sterowniki drukarek są zależne od platformy. Jeśli inne, niż wymienione powyżej, platformy będą podłączane do udostępnionych drukarek logicznych, na serwerze należy zainstalować odpowiednie sterowniki tak, aby po przyłączeniu klient takiego systemu Windows automatycznie pobierał sterownik. W przeciwnym razie, administrator będzie stale proszony o dostarczenie odpowiednich sterowników dla poszczególnych użytkowników sieci.

Na zakładce *Sharing* (Udostępnianie) okna dialogowego (Właściwości) należy kliknąć przycisk **Additional Drivers** (Dodatkowe sterowniki), aby na serwerze wydruku zainstalowane zostały sterowniki komputerów działających pod kontrolą systemów starszych niż Windows 2000. Po zaznaczeniu opcji dotyczącej poprzednich wersji systemu Windows, serwer poprosi o wskazanie lokalizacji odpowiednich dla danej platformy i drukarek sterowników. Sterowniki te dostarcza producent, a czasami są dostępne na oryginalnych dyskach systemu Windows.

Dzięki zainstalowaniu na serwerze sterowników dla klientów wszystkich platform, dystrybucja sterowników jest uproszczona i scentralizowana. Klienci komputerów systemów Windows NT, Windows 2000, Windows XP oraz Windows Server 2003 pobierają sterownik, kiedy pierwszy raz podłączają udostępnioną drukarkę. Program klienta tych systemów sprawdza, czy używana jest aktualna wersja sterownika, a jeśli nie, pobiera ją z serwera wydruku. Administrator musi jedynie aktualizować sterowniki na serwerze wydruku. Programy klienta komputerów systemu Windows 95 lub Windows 98 nie weryfikują sterowników i dla tych systemów administrator musi ręcznie aktualizować sterowniki drukarek.

Inne właściwości drukarek są omawiane w dalszej części rozdziału.



Wskazówka Dostęp do innych folderów drukarek na serwerach można uzyskać przeszukując sieć lub wybierając w menu Start polecenie Run (Uruchom), w którym należy wpisać lnazwa serwera. Następnie znalezione na innych serwerach foldery *Printer and Faxes* (Drukarki i faksy) można przeciągnąć do swojego foldera, dzięki czemu uzyskuje się łatwy dostęp do zarządzanych drukarek zdalnych.

Podłączanie klientów do drukarek

Drukarki, które na serwerze wydruku zostały skonfigurowane jako drukarki logiczne, mogą być udostępniane dla innych systemów w sieci. Systemy te będą również wymagały skonfigurowania drukarek logicznych, które będą reprezentowały drukarki sieciowe.

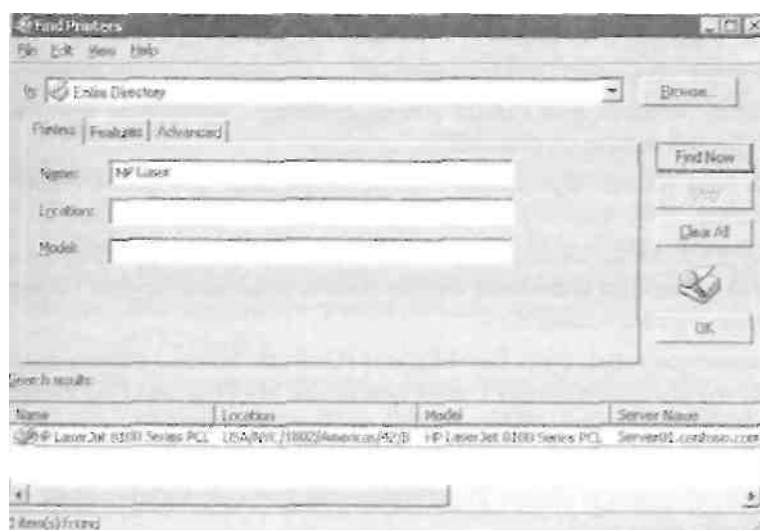
Konfigurowanie programu klienta druku można przeprowadzać kilkoma sposobami, na przykład przy użyciu programu *Add Printer Wizard* (Kreator dodawania drukarki), który jest uruchamiany w folderze *Printers And Faxes* (Drukarki i faksy) lub za pomocą typowego okna dialogowego prawie wszystkich aplikacji firmy Microsoft, w tym programów Internet Explorer czy Notepad (Notatnik). Na stronie *Local or Network Printer* (Drukarka lokalna lub sieciowa) należy wybrać opcję **A Network Printer Or A Printer Attached To Another Computer** (Drukarka sieciowa lub drukarka podłączona do innego komputera). Aby podać nazwę drukarki, można przeszukać usługę Active Directory, wpisać jej nazwę UNC (Universal Naming Convention), na przykład `\\Server\Printersharename` bądź wpisać jej adres URL (Uniform Resource Locator) lub wyszukać drukarkę za pomocą przycisku **Browse** (Przeglądaj),

Jednym z szybszych sposobów skonfigurowania programów klienta jest wyszukanie drukarki w usłudze Active Directory. W tym celu na stronie *Specify A Printer* (Określanie drukarki) w programie *Add Printer Wizard* (Kreator dodawania drukarki), należy wybrać opcję **Find A Printer In The Directory** (Znajdź drukarkę w katalogu), a następnie kliknąć przycisk **Next** (Dalej). Wyświetlone zostanie okno dialogowe *Find Printers* (Znajdowanie: Drukarki), pokazane na rysunku 8-4. W oknie tym można określić kryteria wyszukiwania takie jak nazwa drukarki, lokalizacja, model i właściwości. W wielu filtrach można stosować symbole wieloznaczne. Po kliknięciu przycisku **Find Now** (Znajdź teraz) wyświetlone zostaną wyniki wyszukiwania. Należy zaznaczyć drukarkę i kliknąć przycisk OK. Następnie program *Add Printer Wizard* poprowadzi użytkownika przez pozostałe etapy konfiguracji.



Informacja Wyniki wyszukiwania można zapisać wybierając w menu File (Plik) polecenie *Save Search* (Zapisz wyszukiwanie). Administrator może utworzyć i zapisać niestandardowe wyszukiwania na komputerze użytkowników, umożliwiając im łatwe zlokalizowanie drukarek używanych w przedsiębiorstwie na podstawie przygotowanego zbioru.

Drukarka logiczna zawiera sterowniki, ustawienia oraz kolejkę druku dla drukarek przyłączonych do wybranych portów. Dwukrotne kliknięcie drukarki w folderze *Printers And Faxes* (Drukarki i faksy) powoduje wyświetlenie zadań kolejki drukarki. Kliknięcie prawym przyciskiem myszy dowolnego zadania pozwala na zatrzymanie, wznowienie, anulowanie oraz ponowne uruchomienie zadania. W menu *Printer* (Drukarka) użytkownik może zatrzymać lub anulować wszystkie wydruki, uzyskać dostęp do właściwości drukarki, ustawić drukarkę jako drukarkę domyślną lub wprowadzić drukarkę w tryb offline. Możliwości wykonywania przez użytkownika opisanych czynności zależą, rzecz jasna, od jego uprawnień zapisanych na liście ACL drukarki.



Rysunek 8-4 Okno dialogowe *Find Printers* (Znajdowanie: Drukarki)

Do skonfigurowania klienta wydruku w systemach Windows Server 2003 lub Windows XP można używać alternatywnej metody opisanej za pomocą poniższej procedury:

1. Kliknij menu **Start** i wybierz polecenie **Search** (Wyszukaj).
2. W oknie *Search Companion* (Wyniki wyszukiwania) kliknij kolejno polecenie **Other Search Options** (Inne opcje wyszukiwania), **Printers, Computers, Or People** (Drukarki, komputery lub osoby), a na koniec **A Printer On The Network** (Drukarka w sieci).
3. Wyświetlone zostanie okno dialogowe *Find Printers* (Znajdowanie: Drukarki), które umożliwia wyszukiwanie drukarek przy użyciu rozmaitych kryteriów.
4. Po zdefiniowaniu odpowiednich kryteriów kliknij przycisk **Find Now** (Znajdź teraz).

Zadanie kontrolne: Instalowanie i konfigurowanie drukarki

W zadaniu tym na serwerze wydruku konfigurowana będzie drukarka logiczna oraz symulowane będzie podłączenie klienta do drukarki udostępnionej. Następnie do drukarki zostanie wysłane zadanie wydruku.

Aby przeprowadzić przedstawione ćwiczenia, nie trzeba dysponować drukarką przyłączoną do serwera Server01 lub do sieci ani drugim komputerem działającym jako Identyfikator druku. Jednakże, jeśli dodatkowe elementy są dostępne, zaleca się wykonanie ćwiczeń przy użyciu dodatkowych urządzeń.

Ćwiczenie 1: Dodawanie drukarki lokalnej i konfigurowanie udostępniania drukarki

W ćwiczeniu tym, do dodania drukarki logicznej do serwera Server01, używany będzie program Add Printer Wizard (Kreator dodawania drukarki). Drukarka zostanie podłączona do drukarki sieciowej HP LaserJet 8100 o adresie IP 10.0.0.51- Prawdziwa drukarka nie jest potrzebna, aby zakończyć ćwiczenie.

MCSE Training Kit Egzamin 70-290

1. Zaloguj się do serwera Server01 jako administrator.
2. Otwórz folder *Printers And Faxes* (Drukarki i faksy).
3. Dwukrotnie kliknij polecenie **Add Printer** (Dodaj drukarkę). Wyświetlone zostanie okno *AM Printer Wizard* (Kreator dodawania drukarki).
4. Kliknij przycisk **Next** (Dalej). Wyświetlona zostanie strona *Local Or Network Printer* (Drukarka lokalna lub sieciowa).

Użytkownik powinien określić lokalizację drukarki. Pomimo, że drukarka jest przyłączona do sieci, drukarka logiczna obsługująca tę drukarkę zostanie dodana do serwera Server01 i dlatego drukarka traktowana jest jak drukarka lokalna.
5. Sprawdź, czy zaznaczona została opcja **Local Printer** (Drukarka lokalna) oraz czy usunięte zostało zaznaczenie pola wyboru **Automatically Detect And Install My Plug And Play Printer** (Automatycznie wykryj i zainstaluj moją drukarkę typu Plug and Play). Opcji tej nie powinno się zaznaczać, ponieważ skonfigurowana jest fikcyjna drukarka. Kliknij przycisk **Next** (Dalej).
6. Wyświetlona zostanie strona *A Printer Port* (Wybieranie portu drukarki). Kliknij opcję **Create A New Port** (Utwórz nowy port).
7. Na liście rozwijanej *Type Of Port* (Typ portu) zaznacz opcję **Standard TCP/IP Port**.

Typy portów inne niż porty lokalne stają się dostępne w zależności od zainstalowania protokołów sieci. W przypadku zainstalowania tylko protokołu TCP/IP, widoczny będzie tylko port bazujący na tym protokole.
8. Kliknij przycisk **Next** (Dalej). Wyświetlone zostanie okno programu *Add Standard TCP/IP Printer Port Wizard* (Kreator dodawania standardowego portu TCP/IP).
9. Kliknij przycisk **Next** (Dalej).
10. Wpisz adres IP: **10.0.0.51** i zaakceptuj domyślną nazwę portu: **IP_10.0.0.51-**
11. Kliknij przycisk **Next** (Dalej).

Urządzenie drukujące w rzeczywistości nie jest przyłączone do sieci przy użyciu wyspecyfikowanego adresu i fakt ten jest przyczyną pewnego opóźnienia występującego w tym momencie w programie konfiguracji. Opóźnienie wynika z tego, że program próbuje zlokalizować i rozpoznać drukarkę. Oprócz tego użytkownik będzie poproszony o określenie typu interfejsu sieci.

12. Jako typ urządzenia wybierz **Hewlett Packard JetDirect**.
- 13- Kliknij kolejno przyciski **Next** (Dalej) i **Finish** (Zakończ). Zostaje zamknięte okno programu *AM Standard TCP/IP Printer Port Wizard* (Kreator dodawania standardowego portu TCP/IP) i ponownie wyświetlone okno programu *Add Printer Wizard*.

Program kreatora poprosi o wskazanie producenta i modelu drukarki. Należy dodać drukarkę HP LaserJet 8100 Series PCL.



Wskazówka Lista drukarek uporządkowana jest w kolejności alfabetycznej. Jeśli nie można znaleźć nazwy drukarki, warto upewnić się, czy wyszukiwana jest ona w odpowiedniej lokalizacji.

14. Na liście producentów kliknij **HP**. Przewijaj listę drukarek i znajdź model urządzenia: **HP LaserJet 8100 Series PCL**, a następnie kliknij przycisk **Next** (Dalej).

Wyświetlona zostanie strona *Name Your Printer* (Nazwa drukarki). Domyślna nazwa drukarki jest nazwą modelu urządzenia — HP LaserJet 8100 Series PCL. Wprowadzana nazwa powinna być zgodna z konwencją nazewnictwa stosowaną w przedsiębiorstwie. W tym ćwiczeniu należy wpisać nazwę HPLJ8100.

15. Wpisz **HPLJ8100** i kliknij przycisk **Next** (Dalej).

Wyświetlona zostanie strona *Printer Sharing* (Udostępnianie drukarki), na której wprowadzane są informacje związane z udostępnianiem drukarki. Nazwa udostępniania powinna również być zgodna z konwencją nazewnictwa stosowaną w przedsiębiorstwie. Jak już wcześniej nadmieniono, nazwa UNC drukarki (w postaci \\Nazwa_serwera\Nazwa_udziału_drukarki) nie powinna być dłuższa niż 32 znaki.

16. Sprawdź, czy zaznaczona jest opcja **Share Name** (Nazwa udziału).

17. W polu tekstowym *Share Name* (Nazwa udziału) wpisz **HPLJ8100**, a następnie kliknij przycisk **Next** (Dalej).

Wyświetlona zostanie strona *Location And Comment* (Lokalizacja i komentarz).



Informacja Opisy Wprowadzone w polach tekstowych okna *Location and Comment* (Lokalizacja i komentarz) wyświetli program *Add Printer Wizard* (Kreator dodawania drukarki) podczas wyszukiwania drukarki w usłudze *Active Directory*. Wprowadzanie tych informacji nie jest obowiązkowe, ale pomaga użytkownikom zlokalizować drukarkę.

18. W polu tekstowym *Location* (Lokalizacja) wpisz **USA/NYC/1802Americas/42/B**.

- 19- W polu tekstowym *Comment* (Komentarz) wpisz **Black and White Output Laser Printer-High Volume**.

20. Kliknij przycisk **Next** (Dalej).

Wyświetlona zostanie strona *Print Test Page* (Drukowanie strony testowej). Wydrukowanie strony testowej potwierdza prawidłowe zainstalowanie drukarki.

21. Wybierz opcję **No** (Nie), ponieważ drukarka nie istnieje, a następnie kliknij przycisk **Next** (Dalej). Wyświetlona zostanie strona *Completing The Add Printer Wizard* (Kończenie pracy kreatora dodawania drukarki), która podsumowuje ustawienia zdefiniowane podczas instalowania drukarki.

22. Potwierdź informacje okna podsumowania i kliknij przycisk **Finish** (Zakończ).

W oknie foldera *Printers And Faxes* (Drukarki i faksy) pojawi się nowa ikona drukarki. Warto zauważyć, że system Windows Server 2003 poniżej ikony drukarki wyświetla symbol otwartej dłoni. Znak ten symbolizuje udostępnienie drukarki. Oprócz tego, obok ikony drukarki, wyświetlany jest znacznik wskazujący, że jest to drukarka domyślna serwera wydruku.

23. Pozostaw otwarte okno *Printers And Faxes* (Drukarki i faksy), ponieważ okno to będzie wykorzystywane podczas wykonywania następnego ćwiczenia.

Ćwiczenie 2: Podłączanie klienta do drukarki

Jeśli jest do dyspozycji drugi komputer, można zainstalować na obu stacjach roboczych drukarkę udostępnioną na serwerze Server01. W ćwiczeniu wymagane jest posiadanie tylko jednego komputera (Server01), ponieważ można zasymulować podłączenie klienta drukarki do drukarki logicznej serwera.

1. Otwórz folder *Printers And Faxes* (Drukarki i faksy).
2. Uruchom program **Add Printer Wizard** (Kreator dodawania drukarki), a następnie kliknij przycisk **Next** (Dalej).
3. W oknie dialogowym *Local Or Network Printer* (Drukarka lokalna lub sieciowa) wybierz opcję **A Network Printer Or A Printer Attached To Another Computer** (Drukarka sieciowa lub drukarka podłączona do innego komputera), a następnie kliknij przycisk **Next** (Dalej).
4. Sprawdź, czy zaznaczona jest opcja **Find A Printer In The Directory** (Znajdź drukarkę w katalogu), a następnie kliknij przycisk **Next** (Dalej). Wyświetlone zostanie okno *Find Printers* (Znajdowanie Drukarki).
5. W polu *Location* (Lokalizacja) wpisz ***NYC*** i kliknij przycisk **Find Now** (Znajdź teraz).
6. Z listy wyników wyszukiwania wybierz drukarkę **HPLJ8100** i kliknij przycisk OK.
7. W programie *Add Printer Wizard* na stronie *Default Printer* (Drukarka domyślna) zaznacz odpowiedź **Yes** (Tak) i kliknij przycisk **Next** (Dalej).
8. Kliknij przycisk **Finish** (Zakończ).

Ikona nowej drukarki *nie* pojawi się w folderze *Printers And Faxes* (Drukarki i faksy), ponieważ nie jest możliwe utworzenie klienta drukarki przyłączonego do drukarki logicznej na tym samym komputerze. Jeśli ćwiczenie byłoby przeprowadzane na innym komputerze, ikona nowej drukarki zostałaby wyświetlona.

Ćwiczenie 3: Odłączanie drukarki (tryb pracy offline) i próba wydruku dokumentu

W ćwiczeniu tym drukarka zostanie przełączona w tryb offline. Taki stan drukarki powoduje, że dokumenty do niej wysyłane będą przetrzymywane w kolejce tak długo, jak długo urządzenie będzie niedostępne. Postępowanie takie chroni przed wysyłaniem komunikatów o błędach informujących o niedostępności drukarki (zdarzenia omawiane w następnych ćwiczeniach). W przeciwnym razie, system Windows Server 2003 będzie wyświetlał komunikaty o błędach podczas próby wysyłania dokumentów do fikcyjnej drukarki, która rzeczywiście nie jest dostępna dla komputera.

1. W oknie *Printers And Faxes* (Drukarki i faksy) kliknij prawym przyciskiem myszy ikonę drukarki **HPLJ8100**.
2. Wybierz polecenie **Use Printer Offline** (Użyj drukarki w trybie offline). Warto zauważyć, że ikona drukarki stała się przyćmiona sygnalizując w ten sposób, że jest niedostępna (status offline).
3. Dwukrotnie kliknij ikonę drukarki **HPLJ8100**. Należy zauważyć, że lista dokumentów wysłanych do urządzenia drukującego jest pusta.
4. W menu **Start** kliknij kolejno polecenia **Programs** (Programy), **Accessories** (Akcesoria) i uruchom program **Notepad** (Notatnik).
5. Wpisz dowolny tekst.
6. Dostosuj okna programu *Notepad* (Notatnik) i drukarki HPLJ8100 tak, aby była widoczna zawartość każdego z nich.
7. W menu **File** (Plik) programu *Notepad* wybierz polecenie **Print** (Drukuj). Wyświetlone zostanie okno dialogowe *Print* (Drukowanie) umożliwiające wybór drukarki i opcji wydruku.

W oknie dialogowym wyświetlane są informacje o lokalizacji i komentarzach wprowadzonych podczas tworzenia drukarki, o tym, że HPLJ8100 jest drukarką domyślną oraz że znajduje się w trybie offline.

8. Kliknij przycisk **Print** (Drukuj). Program *Notepad* krótko wyświetla komunikat informujący, że następuje wydruk dokumentu. W przypadku szybkich komputerów, komunikatu tego można w ogóle nie zauważyć.

W oknie drukarki *HPLJ8100 - Use Printer Offline* (Użyj drukarki w trybie offline) wyświetlony zostaje dokument, który oczekuje na wydruk. Dokument umieszczony jest w kolejce, ponieważ drukarka jest w trybie offline. Po zmianie jej stanu (tryb pracy online), dokument zostanie przesłany do urządzenia drukującego.

9. Zamknij program *Notepad* (Notatnik) i nie zapisuj dokumentu.
10. Zaznacz dokument w oknie drukarki HPLJ8100 i w menu **Printer** (Drukarka) wybierz polecenie **Cancel AU Documents** (Anuluj wszystkie dokumenty). Wyświetlony zostanie komunikat, w którym użytkownik potwierdza czynność anulowania wydruku wszystkich dokumentów drukarki HPLJ8100.
11. Kliknij przycisk Yes (Tak). Dokument zostanie usunięty.
12. Zamknij okno drukarki *HPLJ8100- Use Printer Offline* (Użyj drukarki w trybie offline).
- 13- Zamknij okno *Printers AndFaxes* (Drukarki i faksy).

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Administrator konfiguruje drukarkę w systemie Windows Server 2003- W sieci, komputer ten będzie używany jako serwer wydruku. Urządzeniem drukującym ma być drukarka aktualnie przyłączona do sieci jako autonomiczne urządzenie drukujące. Który typ drukarki należy utworzyć na serwerze wydruku? Wybierz wszystkie właściwe odpowiedzi.
 - a. Network (Sieciowa)
 - b. Shared (Udostępniona)
 - c. Local (Lokalna)
 - d. Remote (Zdalna)
2. Administrator instaluje drukarkę na komputerze klienta. Drukarka będzie podłączona do drukarki logicznej serwera wydruku systemu Windows Server 2003. Jakiego rodzaju informacje należy wprowadzić, aby skonfigurować drukarkę? Wybierz wszystkie właściwe odpowiedzi.
 - a. Port TCP/IP drukarki
 - b. Model urządzenia drukującego
 - c. Adres URL drukarki na serwerze wydruku
 - d. Ścieżka UNC dla drukarki udostępnionej (udziału)
 - e. Sterownik drukarki

- 3- Jedna z drukarek funkcjonuje nieprawidłowo i należy zapobiec wysyłaniu przez użytkowników I zadań wydruku do drukarki logicznej obsługującej to urządzenie. Co należy zrobić?
- Zatrzymać udostępnianie drukarki
 - Usunąć drukarkę z usługi Active Directory
 - Zmienić port drukarki
 - Zmienić nazwę udziału
4. Administrator zarządza komputerem systemu Windows Server 2003 skonfigurowanym jako serwer wydruku. Administrator chce przeprowadzić konserwację drukarki podłączonej do serwera wydruku. W kolejce wydruku znajduje się kilka dokumentów. Administrator musi zapewnić, aby dokumenty przestały być drukowane i jednocześnie, żeby użytkownicy nie musieli ponownie wysłać dokumentów do wydruku. Jaki jest najlepszy sposób realizacji takiego zadania?
- W oknie dialogowym Properties (Właściwości) drukarki należy wybrać zakładkę Sharing (Udostępnianie), a następnie zaznaczyć opcję Do Not Share This Printer (Nie udostępniaj tej drukarki).
 - W oknie dialogowym Properties (Właściwości) drukarki należy wybrać port, który nie jest przypisany do urządzenia drukującego.
 - W oknie kolejki drukarki należy zaznaczyć pierwszy dokument, a następnie w oknie ■ dokumentu wybrać polecenie Pause (Wstrzymaj). Powtórzyć działanie dla każdego dokumentu.
 - W oknie kolejki drukarki, w menu Printer (Drukarka) należy wybrać polecenie Pause Printing (Wstrzymaj drukowanie).

Podsumowanie lekcji

- Klient drukarki wysyła zadanie wydruku do serwera wydruku, a ten z kolei zadanie wysyła do drukarki. Klient drukarki i serwer wydruku obsługują drukarkę logiczną reprezentującą drukarkę fizyczną.
- Drukarka lokalna obsługuje drukarkę podłączoną bezpośrednio do komputera lub przyłączoną do sieci.
- Drukarka sieciowa podłączana jest do drukarki logicznej obsługiwanej przez inny komputer - serwer wydruku.
- Klienci systemu Microsoft Windows automatycznie pobierają sterowniki drukarki z drukarki logicznej serwera wydruku. Drukarki są dodawane przy użyciu strony właściwości Sharing (Udostępnianie) drukarki.

Lekcja 2: Zaawansowana konfiguracja i zarządzanie drukarkami

W trakcie poprzedniej lekcji omawiany był najczęściej używany model drukarki systemu Windows. W modelu tym tworzona jest drukarka logiczna obsługująca urządzenie fizyczne podłączone bezpośrednio do komputera lub przyłączone do sieci, a następnie ta drukarka logiczna jest udostępniana klientom drukarki. Drukarka logiczna serwera wydruku staje się centralnym punktem konfiguracji i zarządzania. Zainstalowane sterowniki drukarki są automatycznie pobierane przez klientów systemu Windows, a ustawienia skonfigurowane dla drukarki są dystrybuowane jako ustawienia dla każdego z klientów drukarki.

Podczas niniejszej lekcji omawiany jest następny poziom wirtualizacji drukarek jako urządzeń logicznych. Po przeanalizowaniu właściwości drukarek, wliczając w to bezpieczeństwo drukowania, opisane zostanie, w jaki sposób utworzyć pulę drukarek umożliwiającą szybszą realizację zadań drukowania. Oprócz tego omówione zostaną sposoby lepszego wykorzystywania drukarek poprzez tworzenie kilku drukarek logicznych dla urządzeń, aby bardziej wydajne było konfigurowanie, zarządzanie i monitorowanie zadań wydruku i samych drukarek. Ostatnim omawianym zagadnieniem będą sposoby zarządzania obiektami drukarek usługi Active Directory oraz drukowanie w Internecie.

Materiały omówione podczas lekcji pozwalają na

- Zarządzanie i konfigurację właściwości drukarek
- Tworzenie puli drukarek
- Konfigurowanie kilku drukarek logicznych obsługujących pojedynczą drukarkę
- Zarządzanie i podłączanie do drukarek przy pomocy usługi Active Directory i protokołu IPP (Internet Printing Protocol)

Szacunkowy czas lekcji: 30 minut

Zarządzanie właściwościami drukarek

Drukarki i zadania wydruku są zarządzane za pomocą okien dialogowych ich właściwości. Te okna dialogowe są dostępne w folderze *Printers AndFaxes* (Drukarki i faksy). Aby skonfigurować drukarkę, należy kliknąć prawym przyciskiem myszy drukarkę i wybrać polecenie **Properties** (Właściwości). Podobnie dla zadania wydruku, aby je skonfigurować, należy dwukrotnie kliknąć ikonę drukarki w kolejce drukarki, kliknąć prawym przyciskiem myszy zadanie wydruku i wybrać polecenie **Properties** (Właściwości). Początkowe właściwości zadania wydruku są określone na podstawie właściwości samej drukarki, ale domyślne ustawienia zadania wydruku mogą być modyfikowane niezależnie od drukarki.

Kontrolowanie zabezpieczeń drukarki

System Windows Server 2003 umożliwia kontrolę wykorzystania drukarki i jej zarządzanie. Zadania te są realizowane poprzez przydział uprawnień na zakładce *Security* (Zabezpieczenia) okna dialogowego *Printer Properties* (Właściwości). Administrator może przydzielać uprawnienia kontrolując w ten sposób, kto używa drukarkę oraz kto może zarządzać drukarką lub przetwarzanymi przez nią

dokumentami. Typowa zakładka *Security* (Zabezpieczenia) okna dialogowego *Properties* (Właściwości) drukarki została przedstawiona na rysunku 8-5-



Rysunek 8-5 Zakładka *Security* (Zabezpieczenia) okna dialogowego *Properties* (Właściwości) drukarki

Lista kontroli dostępu ACL może być używana do ograniczenia wykorzystywania drukarki ora do przekazywania (delegowania) administracji drukarki użytkownikom, którzy nie należą do grupy administratorów. System Windows Server 2003 udostępnia trzy poziomy uprawnień dotyczących drukarek: *Print* (Drukowanie), *Manage Printers* (Zarządzanie drukarkami) oraz *Manage Documents* (Zarządzanie dokumentami).

Ustawienia domyślne określają, że uprawnienie *Print* (Drukowanie) jest przydzielone do grupy *Everyone* (Wszyscy). Dzięki temu każdy użytkownik może wysyłać dokumenty do drukarki. Aby ograniczyć wykorzystanie drukarki, należy usunąć to uprawnienie i zezwolić na drukowanie innym grupom bądź pojedynczym użytkownikom. Alternatywnym rozwiązaniem jest odmowa drukowania (*DenyPrint*) grup lub użytkowników. Podobnie jak dla list ACL systemu plików, odmowa uprawnień unieważnia zezwolenia, ale zalecaną praktyką jest przydzielanie zezwoleń drukowania do grup o mniejszym zakresie, zamiast przydzielania uprawnień do grup o szerokim zakresie, a następnie zarządzania dostępem poprzez dodatkowe przypisywanie odmowy uprawnień.

Uprawnienie *Manage Documents* (Zarządzanie dokumentami) umożliwia anulowanie, wstrzymywanie, wznowianie lub ponowne uruchamianie zadań wydruku. Członek grupy *Creator Owner* (Twórca właściciel) ma uprawnienia pozwalające zarządzać dokumentami. Ponieważ uprawnienia przydzielone dla grupy *Creator Owner* (Twórca właściciel) są dziedziczone przez użytkowników, którzy utworzyli obiekt, uprawnienia takie zezwalają na anulowanie, wstrzymywanie, wznowianie lub ponowne uruchamianie zadań drukowania, które zostały utworzone przez użytkownika. Grupy *Administrators*, *Print Operators* (Operatorzy drukowania) oraz *Server Operators* (Operatorzy serwerów) również posiadają uprawnienia zezwalające na zarządzanie dokumentami. Wynika z tego, że członkowie tych grup mogą anulować

wstrzymywać, wznawiać lub ponownie uruchamiać zadania druku *dowolnego* dokumentu kolejki wydruku. Te trzy grupy mają również przydzielone uprawnienia zezwalające na zarządzanie drukarkami, dzięki czemu mogą modyfikować ustawienia i konfiguracje drukarek, w tym samą listę ACL.

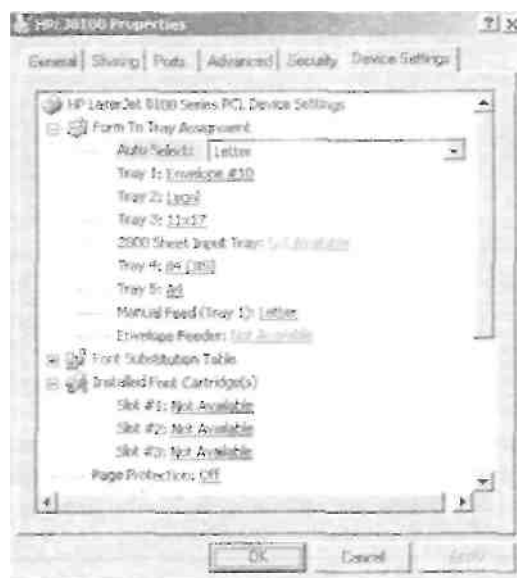


Wskazówka Jeśli zabezpieczenia drukarki nie stanowią problemu, można przekazać administrację drukarki do grup takich jak grupa Users (Użytkownicy), przydzielając im uprawnienia Manage Documents (Zarządzanie dokumentami) lub nawet Manage Printers (Zarządzanie drukarkami).

Przypisywanie rozmiaru papieru do zasobników drukarki

Jeśli urządzenie drukujące ma kilka zasobników, które rypowo przechowują papier różnego rozmiaru, można przypisać formularz druku do określonego zasobnika. Formularz definiuje rozmiar papieru. Jeśli użytkownik drukuje dokument określonych rozmiarów, system Windows Server 2003 automatycznie przekierowuje zadanie wydruku do zasobnika, który przechowuje odpowiedni formularz. Przykładami formularzy mogą być Legal, Letter, A4, Envelop oraz Executive.

Aby przypisać formularz do zasobnika papieru, należy wybrać zakładkę **Device Settings** (Ustawienia urządzenia) okna dialogowego *Properties* (Właściwości). Zakładka została pokazana na rysunku 8-6. Liczba zasobników pokazana w sekcji *Form To Tray Assignment* (Przypisanie formularzy do zasobników) oczywiście zależy od typu zainstalowanej drukarki i obsługiwanych przez nią zasobników. W niższych częściach drzewa *Device Settings* (Ustawienia urządzenia), umieszczone zostały ustawienia określające wartości opcji drukarki wybranych podczas instalacji, takie jak dodatkowe zasobniki papieru, ręczne podawanie papieru, zainstalowane czcionki i pamięć drukarki.



Rysunek 8-6 Zakładka *Device Settings* (Ustawienia urządzenia) okna dialogowego *Properties* (Właściwości) drukarki

Domyślne ustawienia zadania druku

Na zakładce *General* (Ogólne) okna dialogowego *Properties* (Właściwości) umieszczony został przycisk *Printing Preferences* (Preferencje drukowania), natomiast na zakładce *Advanced* (Zaawansowane) przycisk *Printing Defaults* (Domyślne ustawienia drukowania). Naciśnięcie obu przycisków powoduje wyświetlenie okien dialogowych umożliwiających kontrolę sposobu, w jaki zadania są drukowane przez drukarkę logiczną. Dotyczy to orientacji strony (pozioma, pionowa), drukowania dwustronnego (jeśli jest obsługiwane), źródła papieru, rozdzielczości i innych ustawień dokumentu. Oba okna dialogowe są identyczne, a także są takie same, jak okno dialogowe wyświetlane po kliknięciu przycisku *Properties* (Właściwości) w oknie dialogowym *Print* (Drukowanie).

Dlaczego występują te trzy okna dialogowe *Properties* (Właściwości) zadania druku? Okno dialogów *Printing Defaults* (Ustawienia domyślne drukowania) definiuje ustawienia domyślne dla wszystkich użytkowników drukarki logicznej. Jeśli drukarka zostaje udostępniona, jej ustawienia domyślne stają się właściwościami domyślnymi dla wszystkich drukarek podłączonych do drukarki udostępnionej. Okno dialogowe *Printing Preferences* (Preferencje drukowania) konfiguruje ustawienia dotyczące użytkownika, jego osobistych preferencji związanych z drukowaniem. Każde ustawienie okna dialogowego *Printing Preferences* (Preferencje drukowania) unieważnia domyślne ustawienia drukowania. Okno dialogowe *Properties* (Właściwości), które jest wywoływane po kliknięciu przycisku *Properties* (Właściwości) w oknie dialogowym *Print* (Drukowanie) określa właściwości konkretnego zadania, które zostanie wydrukowane. Właściwości te unieważniają zarówno domyślne ustawienia drukowania, jak i ustawienia zwane Preferencjami drukowania. Te trzy zestawy właściwości zadania druku pozwalają administratorowi centralnie określać konfigurację drukarki (poprzez ustawienia domyślne udostępnionej drukarki logicznej) oraz umożliwiają elastyczną i zdecentralizowaną konfigurację określaną przez użytkownika lub w oparciu o cechy kolejnych dokumentów.

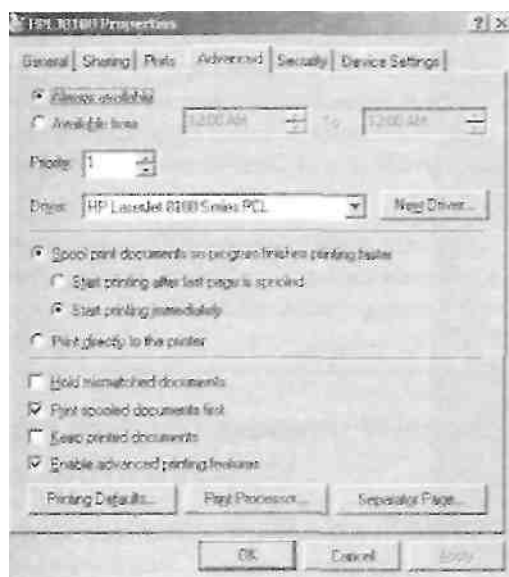
Harmonogram zadań drukarki

Pokazana na rysunku 8-7 zakładka *Advanced* (Zaawansowane) okna dialogowego *Properties* (Właściwości) umożliwia skonfigurowanie szeregu dodatkowych ustawień, które określają zachowanie drukarki logicznej, sposobu przetwarzania zadań druku i kolejki. Jednym z bardziej interesujących i przydatnych ustawień jest Harmonogram zadań drukarki.

Harmonogram drukarki logicznej określa, kiedy zadanie zostaje wysłane z bufora bądź z kolejki i przesłane do urządzenia drukującego. Użytkownik, który ma przydzielone uprawnienie *Print* (Drukowanie) może w dowolnym momencie wysłać zadanie do drukarki, ale zadanie jest wstrzymywane dopóki harmonogram drukarki nie zezwoli na przesłanie tego zadania do portu drukarki. Taka konfiguracja nie jest odpowiednia dla typowych, codziennych zadań druku. Funkcja harmonogramu jest natomiast przydatna w sytuacji, kiedy zadania wydruku użytkowników są duże i należałoby je wykonywać po godzinach pracy lub w okresach małego wykorzystywania drukarki. Dzięki skonfigurowaniu harmonogramu drukarki tak, aby zadania były drukowane w godzinach nocnych, użytkownicy mogą wysyłać zadania w ciągu pracy, drukarka wykona zadania nocą, a użytkownicy zabiorą wydruki rano następnego dnia.



Wskazówka Podczas konfigurowania puli drukarek, należy umieszczać urządzenia drukujące w tej samej fizycznej lokalizacji tak, aby użytkownicy mogli łatwo znaleźć swoje dokumenty. Jeśli użytkownicy wysyłają zadania druku do puli drukarek, nie można określić, która drukarka wydrukowała zadanie.



Rysunek 8-7 Zakładka *Advanced* okna dialogowego *Properties* dla drukarki

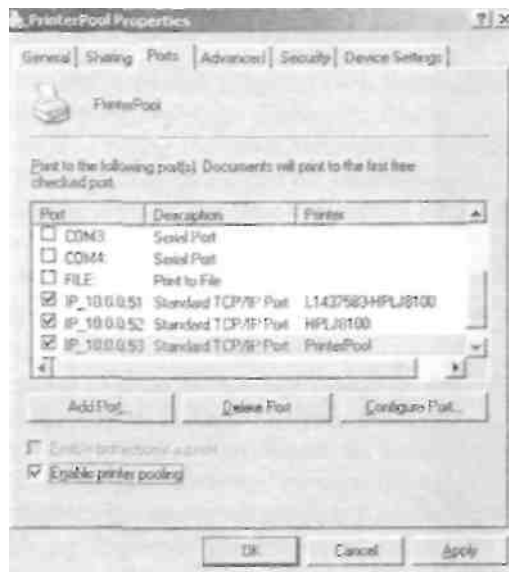
Konfigurowanie puli drukarek

Pula drukarek jest drukarką logiczną, która obsługuje kilka fizycznych drukarek podłączonych do serwera, do sieci lub stosowane są oba typy połączeń. Po utworzeniu puli drukarek dokumenty użytkownika wysyłane są do drukarki, która jest aktualnie wolna. Drukarka logiczna reprezentująca pulę automatycznie sprawdza dostępność portów drukarek.

Pula drukarek jest konfigurowana na zakładce *Ports* (Porty) okna dialogowego *Properties* (Właściwości) drukarki. Aby skonfigurować pulę drukarek, należy zaznaczyć pole wyboru **Enable Printer Pooling** (Włącz tworzenie puli drukarek), a następnie wybrać lub dodać porty zawierające urządzenia drukujące, które mają być elementami puli. Na rysunku 8-8 przedstawiona została pula drukarek podłączona do trzech drukarek sieciowych.



Wskazówka egzaminacyjna Sterownik używany przez pulę drukarek musi być kompatybilny z wszystkimi drukarkami, do których kierowane są zadania wysyłane przez pulę.



Rysunek 8-8 Zakładka *Ports (Porty)* okna dialogowego *Properties (Właściwości)* puli drukarek, przedstawiająca pulę trzech drukarek

Konfigurowanie kilku drukarek logicznych dla jednej drukarki fizycznej

Pula drukarek jest pojedynczą drukarką logiczną, która obsługuje kilka portów lub drukarek, jednak struktura odwrotna jest częściej wykorzystywana i jest bardziej wydajna. Struktura taka to kilka drukarek logicznych obsługujących pojedynczy port lub drukarkę. Utworzenie kilku drukarek logicznych powoduje, że różne zadania są kierowane do tej samej drukarki fizycznej, a administrator może dla każdej drukarki logicznej inaczej skonfigurować właściwości, ustawienia domyślne, ustawienia zabezpieczeń, inspekcji bądź monitorowania.

Na przykład można utworzyć taką konfigurację, która pozwala natychmiast drukować zadania członków grupy Zarząd firmy Contoso Ltd., wstrzymując zadania drukowane przez innych użytkowników. W tym celu należy utworzyć drugą drukarkę logiczną przekierowującą zadania do tego samego portu (do tej samej drukarki fizycznej) dla innych użytkowników, ale z wyższym priorytetem.

Dodatkowe drukarki logiczne tworzy się za pomocą programu *Add Printer Wizard* (Kreator dodawania drukarek). Aby zbudować strukturę kilku drukarek logicznych obsługujących pojedynczy port, dodatkowe drukarki muszą używać tego samego portu, co istniejąca drukarka logiczna. Nazwa drukarki i nazwa udziału nie mogą się powtarzać. Po utworzeniu nowej drukarki logicznej, należy otworzyć okno jej właściwości i skonfigurować sterownik, listę ACL, domyślne ustawienia drukowania oraz inne wymagane ustawienia.

Aby określić dla nowej drukarki logicznej wysoki priorytet, należy kliknąć zakładkę **Advanced** (Zaawansowane) i wybrać wartość z zakresu 1 (najniższy priorytet) do 99 (najwyższy priorytet). Zakładając, że dla drukarki logicznej dyrekcji przydzielony został priorytet 99, a dla drukarki używanej przez pozostałych użytkowników przydzielony będzie priorytet 1, dokumenty wysłane do drukarki dyrekcji będą

drukowane przed dokumentami kolejki drukarki pozostałych użytkowników. Dokumenty dyrekcji nie będą przerywały zadań druku użytkowników. Jeśli drukarka jest wolna, w pierwszej kolejności będzie realizować zadania nadsyłane z drukarki o wyższym priorytecie. Aby użytkownicy nie mogli drukować na drukarce dyrekcji, należy skonfigurować jej listę ACL usuwając uprawnienia drukowania przydzielone grupie *Everyone* (Wszyscy) i zezwolić na drukowanie jedynie członkom grupy „dyrekcja”.



Wskazówka egzaminacyjna Warto zapamiętać, że pula drukarek jest pojedynczą drukarką logiczną obsługującą kilka portów, a pozostałe kombinacje standardowej struktury: klient drukowania - serwer wydruku - drukarka są uzyskiwane poprzez utworzenie kilku drukarek logicznych obsługujących pojedynczy port.

Integracja drukarki systemu Windows Server 2003 z usługą Active Directory

Podsystem drukowania Windows Server 2003 jest ściśle związany z usługą Active Directory, dzięki czemu dla użytkowników i administratorów łatwiejsze staje się wyszukiwanie i podłączanie drukarek przedsiębiorstwa. Jedynym wymaganiem współdziałania pomiędzy drukarkami a usługą Active Directory jest domyślna konfiguracja określająca tryb pracy bez interwencji administratora. Potrzeba wprowadzania zmian zachodzi tylko wtedy, gdy domyślne zachowania nie spełniają wymagań.

Po dodaniu drukarki logicznej do serwera wydruku systemu Windows Server 2003, drukarka jest automatycznie ogłaszana w usłudze Active Directory. Serwer wydruku tworzy obiekt printQueue i publikuje jego właściwości w oparciu o sterownik i ustawienia drukarki logicznej.



Nieoficjalnie W przystawce Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) dość trudno wyszukać obiekty drukarek. Należy użyć przycisku Find Objects In Active Directory (Znajdź obiekty w usłudze Active Directory) umieszczonego na pasku narzędzi konsoli MMC lub w menu View (Widok) wybrać widok Users, Groups, And Computers As Containers (Użytkownicy, grupy i komputery jako kontenery), dzięki czemu obiekty drukarek zostają uwidocznione wewnątrz serwera wydruku. Drukarka zostaje umieszczona w obiekcie komputera serwera wydruku usługi Active Directory. Obiekt może być przenoszony do dowolnej jednostki organizacyjnej.

Dowolne zmiany konfiguracji drukarki wywołują aktualizację obiektu drukarki w usłudze Active Directory. Wszystkie informacje o konfiguracji zostają ponownie wysłane do bazy danych usługi Active Directory, nawet jeśli niektóre z nich pozostają niezmienione.



Planowanie Tworzenie i aktualizacja obiektów drukarki zdarzają się względnie często, ale obiekty i ich atrybuty muszą zostać replikowane, zanim zmienią się rezultaty operacji wyszukiwania Find Printers (Znajdowanie: Drukarki). Opóźnienie replikacji zależy od jej topologii i wielkości przedsiębiorstwa.

Jeśli serwer wydruku zostaje usunięty z sieci, jego obiekty drukarek zostają usunięte z usługi Active Directory. Usługa drukarki Pruner sprawdza udostępnione drukarki usługi Active Directory kontaktując się z nimi co 8 godzin. Jeśli dwa razy pod rząd usługa nie była w stanie skontaktować się z obiektem drukarki, obiekt taki zostaje usunięty. Sytuacja taka zdarza się, jeśli wyłączony jest serwer wydruku.

Często ma to miejsce, jeśli drukarki są udostępnione na stacjach roboczych systemów Windows 2000 lub Windows XP, które zostają wyłączane na noc lub na weekend. Jednakże po uruchomieniu komputera lub usługi bufora wydruku serwer wydruku ponownie utworzy obiekty drukarek. Tak więc i w tym przypadku nie jest potrzebna interwencja administratora.

Publikowanie drukarek systemu Windows

Ustawienia domyślne określają, że drukarki utworzone za pomocą programu *Add Printer Wizard* (Kreator dodawania drukarek) są publikowane. Podczas tworzenia lub instalowania drukarki, program *Add Printer Wizard* (Kreator dodawania drukarek) nie zezwala na blokowanie publikowania drukarki w usłudze Active Directory.

Jeśli zachodzi potrzeba ponownego publikowania drukarki (na przykład po aktualizacji jej nazwy lub innych właściwości) lub jeśli *nie* chcemy, aby udostępniona drukarka była publikowana w usłudze Active Directory, należy otworzyć okno *Properties* (Właściwości), kliknąć zakładkę **Sharing** (Udostępnianie), a następnie zaznaczyć lub usunąć zaznaczenie pola wyboru **List In The Directory** (Wyświetl w katalogu).



Informacja Drukarka podłączona do portu lokalnego będzie najprawdopodobniej automatycznie wykryta i zainstalowana przez usługę Plug And Play. W takim przypadku należy za pomocą zakładki Sharing (Udostępnianie) ręcznie udostępnić i publikować drukarkę.

Drukarki logiczne udostępnione na komputerach systemów Windows NT 4 lub Windows NT 3.51 nie są automatycznie publikowane. Można je publikować ręcznie przy użyciu przystawki *Active Directory Users And Computers* (Użytkownicy i komputery usługi Active Directory). Wystarczy po prostu kliknąć prawym przyciskiem myszy jednostkę organizacyjną lub kontener, w którym ma być utworzona drukarka i wybrać polecenie **New Printer** (Nowy Drukarka).



Planowanie Powinny być dodawane jedynie te obiekty drukarek, które przypisują drukarki systemów wcześniejszych niż Windows 2000. Nie należy dodawać obiektów drukarek dla drukarek komputerów działających pod kontrolą systemów Windows 2000 lub późniejszych. Należy zezwolić, aby drukarki te publikowane były automatycznie.

Ręczna konfiguracja publikowania drukarek

Wszystkie opisane powyżej domyślne zachowania systemu można modyfikować za pomocą zasady lokalnej lub zasady grupy. Zasady drukarek umieszczone są w węźle *Computer Configuration* (Konfiguracja komputera), poniżej węzła *Administrative Templates* (Szablony administracyjne). Aby uzyskać opis każdej z tych zasad, należy otworzyć okno dialogowe *Properties* (Właściwości) danej zasady i kliknąć zakładkę **Explain** (Wyjaśnienie).

Śledzenie lokalizacji drukarki

Funkcja śledzenia lokalizacji drukarki (domyślnie jest wyłączona) w sposób istotny ułatwia wyszukiwanie drukarek w dużych przedsiębiorstwach. Polega ona na wstępnym określeniu pola Location (Lokalizacja) w oknie dialogowym *FindPrinters* (Znajdowanie: Drukarki), co powoduje, że wyniki wyszukiwania są automatycznie ograniczane do listy drukarek znajdujących się w pobliżu użytkownika.

Aby przygotować funkcję śledzenia lokalizacji drukarki, musi być dostępna jedna lub kilka lokacji *lub* też jedna lub kilka podsieci. Obiekty lokacji i podsieci są tworzone i zarządzane za pomocą przystawki *Active Directory Sites And Services* (Lokacje i usługi Active Directory) lub za pomocą konsoli. Należy również skonfigurować zakładkę *Location* (Lokalizacja) okna dialogowego *Properties* (Właściwości) lokacji lub podsieci używając konwencji nazewnictwa, która tworzy hierarchię lokalizacji (oddzielanych ukośnikami). Przykładowo, lokalizacja USA/NYC/1802Americas/42/B może dotyczyć budynku przy 1802 Avenue of the Americas na Manhattanie, na 42 piętrze w części B. Lokalizacja może obejmować kilka podsieci i lokacji.

Następnie należy włączyć funkcję śledzenia lokalizacji drukarki za pomocą zasady *Pre-Populate Printer Search Location Text* (Wypełnij wstępnie tekst lokalizacji wyszukiwania drukarek).

Usługa Active Directory potrafi zidentyfikować powiązania podsieci lub lokacji komputera w oparciu o adres IP komputera. Kiedy wywoływane jest okno dialogowe *Find Printers* (Znajdowanie: Drukarki), lokalizacja komputera, zdefiniowana w jego odpowiednich obiektach lokacji lub podsieci, będzie automatycznie umieszczana w polu *Location* (Lokalizacja). Przycisk *Browse* (Przeglądaj) zostaje uaktywniony, umożliwiając użytkownikom wyszukiwanie drukarek w innych lokalizacjach.

Opisywana funkcja istotnie ułatwia administrację i konfigurację drukarek. Jednakże z drugiej strony, stosowanie tej funkcji wymaga uważnego planowania zapewniającego, że wszystkie podsieci zostały zdefiniowane oraz że spójnie zastosowana została sensowna konwencja nazewnictwa hierarchii lokalizacji. Dodatkowe informacje o tej funkcji można znaleźć w programie *Help and Support Center* (Centrum pomocy i obsługi technicznej).

Drukowanie w sieci Internet

System Windows Server 2003, za pomocą protokołu IPP (Internet Printing Protocol), obsługuje dodatkowy zestaw funkcji, który umożliwia użytkownikom przyłączenie drukarek i wysyłanie zadań wydruku przy użyciu protokołu HTTP (Hypertext Transfer Protocol) poddanego enkapsulacji. Drukowanie w sieci Internet udostępnia ponadto opcje zarządzania i konfigurowania drukarek za pomocą szeregu internetowych przeglądarek i platform.

Konfigurowanie drukowania w sieci Internet

W systemie Windows Server 2003 funkcje drukowania w sieci Internet nie są instalowane i włączane w sposób domyślny. Należy zainstalować usługę IIS (Internet Information Services), zgodnie z procedurą opisaną w rozdziale 6. Funkcje drukowania w sieci Internet stają się dostępne po zainstalowaniu usługi IIS. Aby zainstalować funkcję drukowania w sieci Internet, należy zrealizować następującą procedurę:

1. W programie *Control Panel* (Panel sterowania) otwórz moduł **Add/Remove Programs** (Dodaj lub usuń programy) i kliknij przycisk **Add/Remove Windows Components** (Dodaj/Usuń składniki systemu Windows).
2. Wybierz opcję **Application Server** (Serwer aplikacji) i kliknij przycisk **Details** (Szczegóły).
- 3- Zaznacz opcję **Internet Information Services** (Internetowe usługi informacyjne) i kliknij przycisk **Details** (Szczegóły).
4. Zaznacz opcję **Internet Printing** (Drukowanie internetowe).

Po zainstalowaniu usług IIS i opcji *Internet Printing* (Drukowanie internetowe), funkcje drukowania w sieci Internet można włączać lub wyłączać przy użyciu przystawki IIS lub konsoli. Należy rozwinąć węzeł serwera i kliknąć węzeł *Web Service Extensions* (Rozszerzenia usług sieci Web). W oknie szczegółów zaznacz opcję **Internet Printing** (Drukowanie internetowe) i kliknij przycisk **Prohibit** (Zabroń) lub **Allow** (Zezwalaj).

Funkcja drukowania internetowego tworzy katalog wirtualny *Printers* poniżej węzła *Default Web Site* (Domyślna witryna sieci Web). Ten katalog wirtualny odnosi się do katalogu %Systemroot%\Web\Printers. Witryna drukarki dostępna jest przy użyciu przeglądarki Microsoft Internet Explorer 4.01 i późniejszych jej wersji poprzez wpisanie adresu serwera wydruku w polu adresu, po którym wpisana jest nazwa katalogu wirtualnego Printers. Na przykład, aby uzyskać dostęp do strony drukowania internetowego dla serwera Server01, należy wpisać <http://Server01/printers/>.



Informacja Dla drukowania internetowego można konfigurować uwierzytelnienie i zabezpieczenia dostępu za pomocą okna dialogowego Properties (Właściwości) katalogu wirtualnego.

Wykorzystanie i zarządzanie drukarkami internetowymi

Łącząc się do adresu <http://printserver/printers> można przeglądać wszystkie drukarki serwera wydruku. Po znalezieniu i kliknięciu drukarki, wyświetlona zostaje strona sieci Web wybranej drukarki.

Operacje można skrócić, jeśli znana jest dokładna nazwa drukarki, do której chcemy się podłączyć. W tym celu należy wpisać adres drukarki używając następującego formatu:

http://serwer_wydruku/nazwa_udzialu_drukarki/

Po wyświetleniu strony sieci Web danej drukarki można podłączyć się do drukarki lub nią zarządzać, przy założeniu posiadania odpowiednich uprawnień. Po kliknięciu polecenia Connect (Podłącz) na stronie sieci Web drukarki serwer wygeneruje plik .cab, który zawiera odpowiednie sterowniki drukarki, a następnie plik ten jest przesyłany do komputera klienta. Zainstalowana drukarka zostanie wyświetlona w folderze Printers komputera klienta. Drukarka ta może być następnie używana i zarządzana tak samo jak pozostałe drukarki, za pomocą foldera *Printers And Faxes* (Drukarki i faksy). Wykorzystywanie do zarządzania drukarkami przeglądarki sieci Web ma szereg zalet:

- Umożliwia zarządzanie drukarkami z dowolnego komputera, na którym zainstalowana jest przeglądarka, niezależnie od tego, czy jest to system Windows Server 2003 i czy ma zainstalowane właściwe sterowniki.
- Umożliwia dostosowywanie interfejsu. Przykładowo, można utworzyć swoją własną stronę sieci Web zawierającą plan pięter z naniesioną lokalizacją drukarek i odnośnikami do tych drukarek
- Udostępnia stronę podsumowania wyświetlającą statusy wszystkich drukarek serwera druku.
- Funkcja drukowania internetowego umożliwia w czasie rzeczywistym tworzenie raportu o urządzeniach drukujących, zawierającego informacje o stanie drukarki, przykładowo, czy drukarka znajduje się w trybie energooszczędnym (jeśli sterownik drukarki udostępnia informacje o tym trybie). Informacje takie nie są dostępne w oknie *Printers And Faxes* (Drukarki i faksy).

Zadanie kontrolne: Zaawansowana konfiguracja drukarek i zarządzanie drukarkami

W zadaniu tym skonfigurowana zostanie pula drukarek oraz druga drukarka logiczna podłączona do pojedynczej drukarki sieciowej.

Ćwiczenie 1: Konfigurowanie puli drukarek

1. Utwórz nową drukarkę w oknie *Printers And Faxes* (Drukarki i faksy). Informacje o sposobie tworzenia drukarek można znaleźć w ćwiczeniu 1 lekcji 1. Drukarka powinna kierować do adresu sieci **10.0.0.52** (nowy port). Skonfiguruj drukarkę jako HP LaserJet 8100 Series PCL, przy czym nazwa drukarki i nazwa udziału to **PrinterPool**. Wszystkie inne właściwości, wliczając w to lokalizację i komentarz, są takie same jak w ćwiczeniu 1 lekcji 1.
2. Otwórz okno właściwości drukarki **PrinterPool**.
3. Kliknij zakładkę **Ports** (Porty).
4. Zaznacz pole wyboru **Enable Printer Pooling** (Włącz tworzenie puli drukarek), a następnie kliknij pole wyboru umieszczone obok portu IP_10.0.0.51.
5. Kliknij przycisk **Apply** (Zastosuj). Zaznaczone zostały teraz oba porty sieci.

Czy taka konfiguracja puli drukarek przyniesie korzyści użytkownikom wysyłającym zadania do drukarki HPLJ8100?

Nic. Pula drukarek została skonfigurowana dla drukarki udostępnionej nazwanej PrinterPool. Zadania wydruku wysyłane do drukarki PrinterPool mogą być realizowane na drukarkach a adresie 10.0.0.51 oraz 10.0.0.52. Zadania wysyłane do drukarki HPLJ8100 mogą być drukowane jedynie na drukarce o adresie 10.0.0.51.

Ćwiczenie 2: Konfigurowanie wielu drukarek logicznych dla pojedynczej drukarki

1. W oknie *Printers And Faxes* (Drukarki i faksy) utwórz nową drukarkę. Informacje o sposobie tworzenia drukarek można znaleźć w ćwiczeniu 1 lekcji 1. Drukarka powinna kierować do adresu sieci 10.0.0.52 (należy zwrócić uwagę, że port ten już istnieje). Skonfiguruj drukarkę jako HP LaserJet 8100 Series PCL, przy czym nazwa drukarki i nazwa udziału to **PriorityPrinter**. Wszystkie inne właściwości, wliczając w to lokalizację i komentarz, są takie same jak w ćwiczeniu 1 lekcji 1.
2. Otwórz okno właściwości drukarki **PriorityPrinter**.
3. Kliknij zakładkę **Advanced** (Zaawansowane).
4. Określ wartość priorytetu na 99 (najwyższy).

Ćwiczenie 3: Sprawdzenie obiektów drukarki usługi Active Directory

1. Otwórz przystawkę *Active Directory Users And Computen* (Użytkownicy i komputery usługi Active Directory).
2. W menu **View** (Widok) wybierz polecenie **Users, Groups, And Computers As Containers** (Użytkownicy, grupy i komputery jako kontenery).
- 3- Rozwiń jednostkę organizacyjną **Domain ControUers**. Warto zwrócić uwagę, że serwer Servcr01 wyświetlany jest jako podkontener.
4. Zaznacz serwer **Servcr01**.

Obiekty drukarek zostają wyświetlone w oknie szczegółów. Jeśli obiekt utworzony w ćwiczeniu 1 lekcji 1 nie jest widoczny, należy poczekać kilka minut. Publikowanie drukarek w usłudze Active Directory zabiera serwerowi wydruku kilka minut. Być może trzeba nacisnąć przycisk F5 (odśwież), aby po opublikowaniu obiekty drukarek zostały wyświetlone.

5. Otwórz okno właściwości obiektu PriorityPrinter.

Należy zwrócić uwagę na różnice pomiędzy właściwościami drukarki publikowanymi w usłudze Active Directory a właściwościami wyświetlanymi w folderze Printers And Faxes (Drukarki i faksy). Usługa Active Directory udostępnia mniejszą liczbę właściwości. Są to właściwości, które najprawdopodobniej będą używane w procesie wyszukiwania drukarki. Warto również zwrócić uwagę, że zmiana właściwości w usłudze Active Directory nie zmienia właściwości drukarki. Natomiast zmiana właściwości drukarki zmieni odpowiadającą właściwość obiektu drukarki usługi Active Directory.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiały lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Administrator zarządza komputerem systemu Windows Server 2003 skonfigurowanym jako serwer wydruku. Użytkownicy grupy Marketing narzekają, że nie mogą drukować dokumentów przy użyciu drukarki tego serwera. Administrator przejrzał uprawnienia w oknie właściwości drukarki i okazało się, że grupa Marketing ma przydzielone uprawnienia Manage Documents (Zarządzanie dokumentami). Dlaczego użytkownicy nie mogą drukować na tej drukarce?
 - a. Do grupy Everyone (Wszyscy) muszą być przydzielone uprawnienia Manage Documents (Zarządzanie dokumentami).
 - b. Do grupy Administratorzy muszą być przydzielone uprawnienia Manage Printers (Zarządzanie drukarkami).
 - c. Do grupy Marketing muszą być przydzielone uprawnienia Print (Drukowanie).
 - d. Do grupy Marketing muszą być przydzielone uprawnienia Manage Printers (Zarządzanie drukarkami).
2. Administrator konfiguruje pulę drukarek komputera systemu Windows Server 2003. Pula zawiera trzy jednakowe urządzenia drukujące. Administrator otworzył okno właściwości drukarki i na zakładce Ports (Porty) zaznaczył opcję Enable Printer Pooling (Włącz tworzenie puli drukarek). Jaka będzie kolejna czynność?
 - a. Skonfigurowanie portu LPT1 tak, aby obsługiwane były trzy drukarki.
 - b. Wybór lub utworzenie ponów mapowanych do trzech drukarek.
 - c. Na zakładce Device Settings (Ustawienia urządzenia) należy skonfigurować opcje dla obsługi dwóch dodatkowych urządzeń drukujących.
 - d. Na zakładce Advanced (Zaawansowane) należy określić priorytet dla każdego urządzenia drukującego tak, aby ten sposób drukowania został zastosowany do tych trzech urządzeń drukujących.

3. Administrator zarządza komputerem systemu Windows Server 2003 skonfigurowanym jako serwer wydruku i chce zarządzać usługami drukowania za pomocą przeglądarki sieci Web na komputerze klienta. Serwer nazywa się Mktgl, ale administrator nie zna nazwy drukarki. Jaki adres URL powinien być użyty, aby połączyć się z drukarką?
 - a. <http://lmktgl/printers>
 - b. <http://printers/mktgl>
 - c. <http://windows/web/printers>
 - d. <http://windouis/mktgl>
4. Administrator chce skonfigurować drukarkę logiczną tak, aby przy jej użyciu drukowane były w godzinach nocnych duże dokumenty mające niski priorytet. Którą z wymienionych poniżej opcji należy skonfigurować w oknie dialogowym Properties (Właściwości) drukarki?
 - a. Priority (Priorytet)
 - b. Available From /To (Dostępna od/do)
 - c. Start Printing After Last Page Is Spooled (Rozpocznij drukowanie po umieszczeniu w buforze ostatniej strony)
 - d. Print Directly To The Printer (Drukuj bezpośrednio do drukarki)
 - e. Keep Printed Documents (Przechowaj dokumenty po wydrukowaniu)

Podsumowanie lekcji

- Model drukarki systemu Windows, dzięki drukarkom logicznym, umożliwia pomysłów i elastyczne wykorzystanie drukarek. Istnieje możliwość utworzenia jednej drukarki logicznej, która wysyła zadania do kilku urządzeń drukujących (pula drukarek) lub można utworzyć kilka drukarek logicznych, które wysyłają zadania do jednego urządzenia drukującego, a każda drukarka logiczna ma wstępnie inaczej określone ustawienia drukarki, ustawienia domyślne wydruku oraz uprawnienia dla obsługi poszczególnych typów zadań wydruku.
- Drukarki są publikowane w usłudze Active Directory, dzięki czemu użytkownicy mogą łatwo wyszukać i podłączyć drukarki. System Windows Server 2003 obsługuje funkcję śledzenia lokalizacji drukarki, która jest dalszym uproszczeniem wyszukiwania drukarek. Za pomocą protokołu IPP, w systemie istnieje także możliwość zarządzania drukarkami i realizacji wydruków poprzez sieć intranet bądź Internet.

Lekcja 3: Konserwacja, monitorowanie i rozwiązywanie problemów związanych z drukarkami

Po skonfigurowaniu drukarek logicznych, ich udostępnieniu na serwerach wydruku oraz po połączeniu klientów do tych drukarek, administrator musi rozpocząć konserwację i monitorowanie tych logicznych i fizycznych drukarek. Niniejsza lekcja stanowi przewodnik obsługi i rozwiązywania problemów dotyczących drukarek w środowisku systemu Windows Server 2003. Omawiane zagadnienia obsługi sterowników drukarek, przekierowywania drukarek, konfigurowania dziennych wydajności i ich wykorzystania oraz sposoby metodycznego rozwiązywania problemów.

Materiały omówione podczas lekcji pozwalają na

- Zarządzanie sterownikami drukarek
- Przekierowanie drukarki
- Monitorowanie wydajności drukarki
- Inspekcję dostępu do drukarki
- Rozwiązywanie problemów związanych awariami drukarek

Szacunkowy czas lekcji: 20 minut

Konserwacja drukarek

W systemie Windows Server 2003 dla usług drukowania nie zostało przewidziane regularne wykonywanie zadań konserwacji. Jeśli zachodzi taka potrzeba, wymienione poniżej zadania wykonywane są okresowo. Warto zapamiętać, że czynności wykonywane podczas konserwacji drukarek mogą mieć wpływ na działanie wszystkich funkcji drukarki lub wszystkich drukarek serwera wydruku, a nie tylko na konkretne zadania wydruku.

Zarządzanie sterownikami drukarek

Pierwsza grupa zadań konserwacji dotyczy sterowników serwera wydruku. Jak już wcześniej nadmieniono, zaleca się instalowanie sterowników dla wszystkich platform klienta wykorzystujących udostępnione drukarki. Klienci systemu Windows automatycznie pobierają te sterowniki podczas przyłączania drukarki. Sterowniki dla różnych platform instalowane są w oknie dialogowym *Properties* (Właściwości) na zakładce *Sharing* (Udostępnianie) poprzez naciśnięcie przycisku *Additional Drivers* (Dodatkowe sterowniki).

Aby aktualizować sterowniki pojedynczej drukarki logicznej, należy w oknie dialogowym *Properties* (Właściwości) wybrać zakładkę **Advanced** (Zaawansowane) i kliknąć przycisk **New Driver** (Nowy sterownik). Następnie użytkownik może wybrać z listy dodatkowy sterownik wskazując producenta i model urządzenia lub klikając przycisk **Have Disk** (Z dysku) może kopiować sterowniki dostarczane przez producenta.

Istnieje również możliwość zarządzania wszystkimi sterownikami serwera wydruku. W tym celu należy w folderze *Printers And Faxes* (Drukarki i faksy) wybrać z menu **File** (Plik) polecenie **Server Properties**

(Właściwości serwera) i kliknąć zakładkę **Drivers** (Sterowniki). Na zakładce można dodawać, usuwać, ponownie instalować lub uzyskiwać dostęp do właściwości każdego sterownika serwera. Modyfikacje wprowadzone tutaj będą miały wpływ na wszystkie drukarki serwera wydruku.

Jeśli zachodzi potrzeba wygenerowania listy wszystkich plików dotyczących konkretnego sterownika drukarki, należy otworzyć zakładkę **Drivers** (Sterowniki), wybrać sterownik i kliknąć polecenie **Properties** (Właściwości). Wyświetlone zostaną nazwy i opisy wszystkich plików, które są częścią danego sterownika. Na tej liście, istnieje możliwość przeglądania szczegółów dotyczących każdego pliku. W tym celu wystarczy zaznaczyć plik i kliknąć przycisk **Properties** (Właściwości).

Przekierowanie zadań druku

Jeśli drukarka uległa awarii, można przesłać dokumenty jej kolejki do innej drukarki podłączonej do portu lokalnego komputera lub do sieci. Działania takie nazywane są *przekierowaniem* zadania wydruku. Dzięki tej funkcji użytkownicy mogą kontynuować wysyłanie zadań do drukarki logicznej, a użytkownicy, którzy już mieli zadania w kolejce, nie muszą ich ponownie wysłać.

Aby przekierować drukarkę, należy otworzyć okno dialogowe *Properties* (Właściwości) drukarki i kliknąć zakładkę **Ports** (Porty). Następnie należy zaznaczyć istniejący port lub utworzyć nowy. Zaznaczenie pola wyboru portu uszkodzonej drukarki zostanie natychmiast usunięte, chyba że włączone było tworzenie pul drukarek. W takim przypadku należy ręcznie usunąć zaznaczenie pola wyboru.

Ponieważ zadania wydruku były przygotowane dla poprzedniej drukarki, drukarka na nowym porcie musi być kompatybilna ze sterownikiem używanym przez drukarkę logiczną. Wszystkie zadania wydruku zostaną teraz przekierowane do nowego portu. Nie można przekierować poszczególnych dokumentów, a także dokumentów, które są aktualnie drukowane.

Monitorowanie drukarek

System Windows Server 2003 udostępnia szereg metod monitorowania drukarek i zasobów dotyczących drukowania.

Korzystanie z programu System Monitor (Monitor systemu) oraz Performance Logs and Alerts (Dzienniki wydajności i alerty)

Przystawki *System Monitor* (Monitor systemu) oraz *Performance Logs and Alerts* (Dzienniki wydajności i alerty) zostały umieszczone w konsoli MMC *Performance* (Wydajność). Umożliwiają one w czasie rzeczywistym obserwację drukarek, protokolowanie parametrów dla późniejszych analiz lub określanie poziomów alarmów i czynności z nimi związanych. Przystawki te omawiane są szczegółowo w rozdziale 12. Aby dodać licznik w przystawce *System Monitor* (Monitor systemu), należy kliknąć prawym przyciskiem myszy część graficzną okna i wybrać polecenie **Add Counters** (Dodaj liczniki). Do monitorowania należy zaznaczyć obiekt wydajności, w tym przypadku **Print Queue** (Kolejka wydruku) oraz potrzebne liczniki i instancje reprezentujące drukarkę logiczną.

Po wybraniu obiektu wydajności (Kolejka wydruku) wyświetlona zostaje lista wszystkich dostępnych liczników wydajności. Zaznaczając dowolny licznik i klikając przycisk **Explain** (Wyjaśnij) można dowiedzieć się, jakie pomiary wykonywane są przy użyciu poszczególnych liczników.

Poniżej wymienione zostały najważniejsze liczniki wydajności monitorujące wydajność drukowania:

- **Bytes Printed/Sec (Szybkość drukowania bajty/s)** Jest to liczba bajtów wiersza danych wysyłanych w ciągu sekundy do drukarki. Niska wartość tego licznika wskazuje, że drukarka nie jest w pełni wykorzystywana. Przyczyny takiego stanu mogą być różne — brak zadań, kolejki nie są równomiernie obciążane lub serwer jest przeciążony. Wartość licznika zmienia się w zależności od typu drukarki. Należy sprawdzić w dokumentacji, jakie wartości są dopuszczalne dla danej drukarki.
- **Job Errors (Błędy zadań)** Liczba błędów zadania. Błędy zadania najczęściej spowodowane są przez nieprawidłową konfigurację portu, należy więc sprawdzić konfigurację ustawień portu. Instancja zadania wydruku może zwiększyć wartość licznika tylko raz, nawet jeśli błąd powtarzał się kilka razy. Niektóre monitory druku nie obsługują liczników błędów zadania i w takim przypadku licznik nie będzie inkrementowany.
- **Jobs (Zadania)** Liczba zadań bufora.
- To tal **Jobs Printed (Wszystkie wydrukowane zadania)** Liczba zadań wysłanych do drukarki od momentu uruchomienia usługi bufora wydruku.
- **Total Pages Printed (Całkowita liczba wydrukowanych stron)** Liczba stron wydrukowanych od momentu uruchomienia usługi bufora wydruku. Licznik ten jest dobrym przybliżeniem wolumenu drukarki, chociaż mogą wystąpić różnice w zależności od typu zadań i właściwości dokumentów.

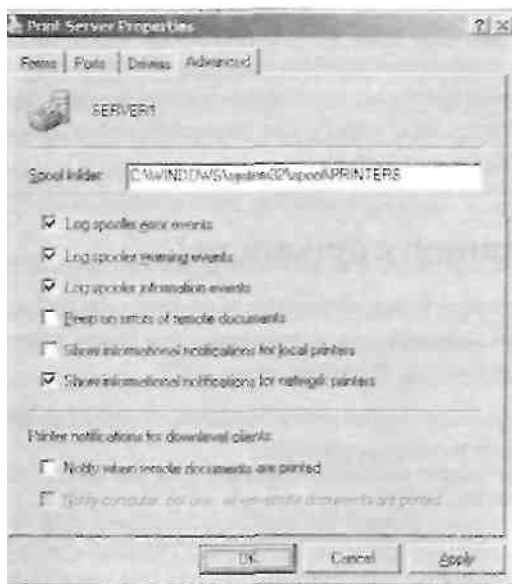


Wskazówka egzaminacyjna Liczniki Total Jobs Printed (Wszystkie wydrukowane zadania) i Total Pages Printed (Całkowita liczba wydrukowanych stron) kumulują mierzone wartości, które przedstawiają liczbę zadań lub stron wydrukowanych od momentu uruchomienia systemu lub usługi bufora wydruku.

Wykorzystanie dzienników systemu

Przy użyciu programu *Event Viewer* (Podgląd zdarzeń) można analizować dzienniki systemu będące źródłem informacji związanych z buforem wydruku i aktywnością drukarki. Ustawienia domyślne określają, że bufor wydruku rejestruje zdarzenia dotyczące utworzenia, usunięcia lub modyfikacji drukarki. Oprócz tego rejestrowane są zdarzenia zawierające informacje o natężeniu pracy drukarki, przestrzeni dysku twardego, błędów usługi bufora wydruku oraz innych zagadnień związanych z konserwacją drukarki.

Aby określić lub zmodyfikować ustawienia protokolowania zdarzeń usługi bufora wydruku, należy otworzyć folder *Printers And Faxes* (Drukarki i faksy) i z menu **File** (Plik) wybrać polecenie **Server Properties** (Właściwości serwera). Następnie należy kliknąć zakładkę **Advanced** (Zaawansowanie), aby uzyskać dostęp do odpowiednich właściwości. Widok zakładki został przedstawiony na rysunku 8-9). Na tej stronie można określać rodzaj wpisów rejestru zdarzeń drukarki oraz powiadomień zadań wydruku. Na tej zakładce można również przenosić folder bufora wydruku. Jest to istotne zadanie podczas konfigurowania aktywnych serwerów wydruku lub jeśli przepełni się wolumen istniejącego foldera bufora wydruku.



Rysunek 8-9 Zakładka *Advanced* (Zaawansowane) okna dialogowego *Print Server Properties* (Właściwości serwera wydruku)

Inspekcja dostępu do drukarki

Dostęp do drukarki, podobnie jak dostęp do plików bądź folderów, można poddawać inspekcji. Użytkownik może określić, że dla konkretnej drukarki inspekcji poddane zostaną określone grupy lub użytkownicy. Po włączeniu zasady inspekcji dostępu do obiektu, odpowiednie wpisy wyników przeprowadzenia inspekcji można przeglądać w programie *Event Viewer* (Podgląd zdarzeń).

Aby dla drukarki skonfigurować inspekcję, należy otworzyć jej okno dialogowe *Properties* (Właściwości), kliknąć zakładkę **Security** (Zabezpieczenia), a następnie kliknąć przycisk **Advanced** (Zaawansowane). Kolejno należy kliknąć zakładkę **Auditing** (Inspekcja) i dodać wpisy dla określonych grup lub użytkowników. Dla każdego konkretnego podmiotu zabezpieczeń dodanego do listy inspekcji użytkownik może skonfigurować inspekcję dla zdarzeń dostępu określanych jako powodzenie lub niepowodzenie, w oparciu standardowe uprawnienia drukarki, wliczając w to *Print* (Drukowanie), *Manage Documents* (Zarządzanie dokumentami) oraz *Manage Printers* (Zarządzanie drukarkami).

Następnie należy włączyć zasadę *Audit Object Access* (Inspekcja dostępu do obiektu), która umieszczona jest w zasadzie lokalnej lub zasadzie grupy poniżej węzłów *Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy* (Konfiguracja komputera\Ustawienia Windows\Ustawienia zabezpieczeń\Zasady lokalne\Zasada inspekcji). Po włączeniu zasady możliwa będzie analiza wpisów dziennika zdarzeń *Security* (Zabezpieczenia) zaprotokołowanych na podstawie ustawień inspekcji drukarki.



Wskazówka Inspekcja drukarki tworzy dziesiątki wpisów dla pojedynczego zadania wydruku. Dlatego jest ona użyteczna jedynie podczas rozwiązywania bardzo specyficznych problemów. Inspekcja drukarki nie powinna być używana do monitorowania lub oceny wykorzystania drukarki. Zamiast tego można analizować liczniki wydajności takie jak Total Jobs Printed (Wszystkie wydrukowane zadania) lub Total Pages Printed (Całkowita liczba wydrukowanych stron).

Rozwiązywanie problemów związanych z drukarkami

Rozwiązywanie problemów jest jednym z ważniejszych elementów zarządzania drukarkami. Poniższy fragment jest przewodnikiem ułatwiającym zrozumienie oraz rozpoznawanie typów zdarzeń i problemów występujących podczas drukowania w systemie Windows Server 2003.

Podczas rozwiązywania problemów warto pamiętać, że na proces drukowania składa się wiele elementów, z których najczęściej występujące zostały wymienione poniżej:

- Aplikacja dokonująca próby wydrukowania.
- Drukarka logiczna na komputerze, na którym uruchomiona jest aplikacja.
- Połączenie sieciowe pomiędzy klientem wydruku a udostępnioną drukarką logiczną serwera wydruku.
- Drukarka logiczna serwera wydruku, jej program buforujący, ustawienia zabezpieczeń itp.
- Połączenie sieciowe pomiędzy serwerem wydruku a drukarką.
- Sama drukarka, jej urządzenia sprzętowe, konfiguracja i status.

Najszybszym sposobem rozwiązania większości problemów związanych z drukowaniem jest logiczna i metodyczna analiza każdego elementu.

Rozpoznawanie zakresu uszkodzenia

Jeśli użytkownik może drukować przy użyciu innej aplikacji uruchamianej na jego komputerze, to najprawdopodobniej błąd związany jest z aplikacją, za pomocą której nie udało się wydrukować zadania, a nie z innymi elementami takimi jak komputer, sieć, serwer druku lub sprzęt drukarki. Jednakże w niektórych przypadkach użycie innych sterowników może rozwiązać problem drukowania w aplikacji.

Jeśli natomiast błędy drukowania występują podczas drukowania z dowolnej aplikacji użytkownika, należy sprawdzić, czy użytkownik może drukować na innych drukarkach tego samego serwera wydruku lub na innych serwerach wydruku. Jeśli wszystkie te próby kończą się niepowodzeniem, a inni użytkownicy mogą drukować na drukarkach sieciowych, to przyczyna błędu jest prawdopodobnie związana z komputerem użytkownika.

W tym systemie należy spróbować utworzyć drukarkę lokalną, która bezpośrednio kieruje zadania do portu drukarki. Inaczej mówiąc, należy pominąć serwer wydruku. Jeśli w tej konfiguracji drukowanie będzie możliwe, oznacza to, że problem dotyczy serwera wydruku w zakresie komunikacji pomiędzy systemem użytkownika a serwerem lub połączeniami drukarki na komputerze klienta.

Sprawdzanie, czy program klienta wydruku może łączyć się z serwerem wydruku

Połączenie między klientem druku a serwerem wydruku można sprawdzać otwierając folder *Printen And Faxes* (Drukarki i faksy) na komputerze klienta. Jeśli w otwartym oknie wyświetlane są dokumenty kolejki drukarki, oznacza to, że klient jest prawidłowo podłączony do udostępnionej drukarki.

Jeśli natomiast nie można otworzyć okna drukarki, może to wskazywać na problemy dotyczące sieci, uwierzytelnienia lub uprawnień. Należy, za pomocą programu Ping, sprawdzić dostęp do adresu IP serwera. W menu Start należy wybrać polecenie Run (Uruchom) i wpisać `\\serwer_wydfuku`. Jeśli okno zostanie otwarte, a w nim wyświetlony będzie folder *Printers And Faxes* (Drukarki i faksy) i inne foldery udostępnione, to oznacza, że klient jest przyłączony do serwera. Należy dokładnie sprawdzić uprawnienia zabezpieczeń drukarki logicznej.

Sprawdzenie, czy drukarka funkcjonuje prawidłowo

Należy sprawdzić samą drukarkę i upewnić się, że jest gotowa (stan gotowa do drukowania). Z konsoli drukarki można wydrukować stronę testową i sprawdzić kable połączeniowe drukarki do serwera wydruku lub do sieci. Jeśli drukarka jest podłączona do sieci, należy sprawdzić, czy dioda karty sieciowej sygnalizuje aktywne połączenie z siecią.

Sprawdzenie, czy serwer wydruku może uzyskać dostęp do drukarki

Większość drukarek wyświetla na konsoli swój adres IP lub informacje o tym adresie drukowane są na stronie konfiguracji drukarki. Należy sprawdzić, czy adres IP drukarki jest zgodny z adresem IP portu drukarki logicznej. Adres IP portu można odczytać na zakładce *Ports* (Porty) okna dialogowego *Properties* (Właściwości) drukarki. Należy także sprawdzić za pomocą programu Ping, czy poprzez sieć możliwa jest komunikacja z drukarką.

Sprawdzenie, czy uruchomione zostały usługi drukowania serwera wydruku

Przy użyciu konsoli MMC — *Services* (Usługi) można sprawdzić, czy usługi wymagane dla drukarki działają prawidłowo. Na przykład, należy sprawdzić, czy na serwerze wydruku została uruchomiona usługa zdalnego wywoływania procedur RPC. Usługa RPC jest wymagana dla standardowych połączeń sieci z drukarkami udostępnionymi. Należy również sprawdzić, czy na serwerze wydruku uruchomiona została usługa bufora wydruku.



Wskazówka Polecenia `Net Stop Spooler` i `Net Start Spooler` mogą być wprowadzane w wierszu poleceń w celu ponownego uruchomienia usługi bufora wydruku. Zatrzymanie i ponowne uruchomienie usługi bufora wydruku za pomocą komend wiersza poleceń lub metod interfejsu użytkownika powoduje, że wszystkie dokumenty kolejki drukarki serwera zostają usunięte.

Należy również sprawdzić, czy na wolumenie foldera usługi bufora wydruku jest wystarczająca ilość przestrzeni dyskowej. Lokalizacja foldera bufora wydruku jest określana i modyfikowana w oknie dialogowym *Server Properties* (Właściwości serwera), które jest dostępne po wybraniu polecenia *Server Properties* (Właściwości serwera) w menu *File* (Plik) foldera *Printers And Faxes* (Drukarki i faksy).



Informacja Ustawienia domyślne określają, że folder bufora wydruku wskazuje na lokalizację `%Systemroot%\System32\Spool\Printers`. Dla dużych wolumenów serwera wydruku należy rozważyć możliwość przeniesienia foldera bufora wydruku na partycję inną niż systemowa bądź rozruchowa. Jeśli partycja, na której przechowywany jest folder bufora wydruku, zostaje zapełniona zadaniami wydruku, to drukowanie zostaje wstrzymane, a co ważniejsze system operacyjny może pracować niestabilnie.

Należy także przejrzeć dzienniki systemu sprawdzając, czy bufor wydruku zarejestrował nieprawidłowe zdarzenia, a w folderze *Printers And Faxes* (Drukarki i faksy) należy sprawdzić, czy drukarka nie znajduje się w trybie offline.

Należy przeprowadzić próbny wydruk zadania z aplikacji i na serwerze wydruku. Jeśli zadanie wydrukuje się poprawnie, oznacza to, że problem nie dotyczy drukarki. Jeśli natomiast zadanie nie zostało wydrukowane, należy utworzyć nową drukarkę kierującą do tego samego portu i spróbować wydruku przy użyciu nowej drukarki. Jeśli wydruk jest poprawny, problem dotyczy konfiguracji pierwotnej drukarki i logicznej. Jeśli natomiast w dalszym ciągu nie można drukować, problem jest związany z komunikacją z drukarką lub samymi urządzeniami sprzętu.

Zadanie kontrolne: Rozwiązywanie problemów związanych z drukarkami

W zadaniu tym wykonane zostanie przekierowanie drukarki. Przekierowanie drukarki jest przydatną funkcją zarówno przy zapobieganiu problemom, jak i podczas ich rozwiązywania. Jeśli zachodzi potrzeba wprowadzenia drukarki w tryb offline, można przekierować jej drukarkę (lub drukarki) logiczną do innego urządzenia, które jest kompatybilne ze sterownikiem drukarki logicznej. Jeśli natomiast awaria drukarki wynika z zakleszczenia papieru lub innego błędu, już wysłane i buforowane zadania można przekierować do drukarki logicznej tak, aby użytkownicy nie musieli oczekiwać na zakończenie naprawy drukarki i nie musieli ponownie wysłać swoich zadań wydruku.

Dodatkowe ćwiczenia praktyczne związane z rozwiązywaniem problemów zostały zamieszczone w sekcji Zadanie praktyczne oraz Rozwiązywanie problemów.

Ćwiczenie 1: Przekierowanie drukarki

Jeśli drukarka ulega awarii, zadania wydruku można przekierować do innej drukarki. W ćwiczeniu zakłada się, że zadanie drukowane jest na drukarce HPLJ8100. Zadanie jest już w kolejce, a w drukarce nastąpiło zakleszczenie papieru.

1. Otwórz folder *Printers And Faxes* (Drukarki i faksy) i sprawdź, czy drukarka HPLJ8100 jest w trybie offline. Jeśli nie, kliknij drukarkę prawym przyciskiem myszy i wybierz polecenie **Use Printer Offline** (Użyj drukarki w trybie offline). Działanie takie zapobiega generowaniu błędów, ponieważ drukarka została skierowana do nieistniejącego portu sieci.
2. Otwórz program **Notepad** (Notatnik) i wprowadź tekst nowego dokumentu.
3. W menu **File** (Plik) wybierz polecenie **Print** (Drukuj) i do wykonania zadania wybierz drukarkę **HPLJ8100**.
4. W folderze *Printers And Faxes* (Drukarki i faksy) kliknij dwukrotnie drukarkę HPLJ8100, aby otworzyć jej okno. Sprawdź, czy zadanie jest w kolejce.
5. W menu **Printer** (Drukarka) wybierz polecenie **Properties** (Właściwości).
6. Kliknij zakładkę **Ports** (Porty).
7. Zgodnie z ustawieniami wprowadzonymi podczas lekcji 1, drukarka powinna używać w sieci portu IP_10.0.0.51-
8. Zaznacz pole wyboru obok portu IP_10.0.0.52.

9. Kliknij przycisk OK. Drukarka została przekierowana. Wszystkie zadania kolejki, za wyjątkiem rozpoczętego, zostaną przekierowane do nowego portu. Drukarka podłączona do nowego portu musi być kompatybilna ze sterownikiem używanym przez tę drukarkę logiczną, ponieważ zadania zostały już przetworzone i skierowane do bufora wydruku w oparciu o istniejący sterownik.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. System Windows 2003 Server został skonfigurowany jako serwer wydruku. W środku dnia pracy przepalił się bezpiecznik drukarki i musi zostać wymieniony. Użytkownicy mieli już powysyłane zadania do drukarki, która używa adresu IP 192.168.1.81. W sieci jest identyczna drukarka, do której przypisany został adres 192.168.1.217. Drukarka ta obsługiwana jest przez inną drukarkę logiczną na serwerze. Jaki czynności należy wykonać, aby zadania użytkowników zostały wydrukowane bez konieczności powtórzenia ich wysyłania do drukarki?
 - a. W oknie dialogowym Properties (Właściwości) uszkodzonej drukarki należy zaznaczyć opcję Enable Printer Pooling (Włącz tworzenie puli drukarek).
 - b. W wierszu poleceń należy wprowadzić komendę **Net Stop Spooler**.
 - c. W wierszu poleceń należy wprowadzić komendę **Net Start Spooler**.
 - d. W oknie dialogowym Properties (Właściwości) uszkodzonej drukarki należy wybrać port 192.168.1.217.
 - e. W oknie dialogowym Properties (Właściwości) uszkodzonej drukarki należy kliknąć przycisk Add Port (Dodaj port).
 - f. W folderze Printers And Faxes (Drukarki i faksy) należy kliknąć drukarkę prawym przyciskiem myszy i wybrać polecenie Use Offline (Użyj drukarkę w trybie offline).
2. Administrator konfiguruje usługi drukowania w systemie Windows Server 2003- Przyłączył drukarkę, skonfigurował drukarkę logiczną i wysłał dokumenty do druku, ale dokumenty nie drukują się w całości, a czasami są pozmieniane. Jaka jest najbardziej prawdopodobna przyczyna problemu?
 - a. Brak wystarczającej przestrzeni dyskowej dla bufora wydruku.
 - b. Użyty został niewłaściwy sterownik drukarki.
 - c. Wybrany port jest nieprawidłowy.
 - d. Ustawienia drukarki określają nieprawidłową czcionkę zastępczą.
3. Która z wymienionych poniżej opcji dobrze odzwierciedla wykorzystanie drukarki, umożliwiając użytkownikowi ocenę zużycia toneru i papieru?
 - a. Skonfigurować inspekcję drukarki logicznej i rejestrować zakończone powodzeniem użycie uprawnienia Print (Drukowanie) przez członków grupy Everyone (Wszyscy).
 - b. Wyeksportować dziennik System do pliku o wartościach rozdzielanych przecinkiem i użyć programu Excel do analizy zdarzeń bufora wydruku.
 - c. Skonfigurować dziennik wydajności i dla każdej drukarki logicznej monitorować licznik Total Pages Printed (Całkowita liczba wydrukowanych stron).

- d. Skonfigurować dziennik wydajności i dla każdej logicznej drukarki monitorować licznik Jobs (Zadania).

Podsumowanie lekcji

- Sterowniki drukarek logicznych mogą być aktualizowane lub dodawane przy użyciu właściwości danej drukarki. Dla wszystkich drukarek sterowniki mogą być dodawane, usuwane lub ponownie instalowane przy użyciu zakładki *Drivers* (Sterowniki) w oknie dialogowym *Server Properties* (Właściwości serwera).
- Jeśli drukarka jest w trybie offline lub uległa awarii, wszystkie jej zadania (za wyjątkiem rozpoczętych) można przekierować do innej drukarki. W tym celu, we właściwościach pierwotnej drukarki logicznej, należy dodać lub wybrać nowy port drukarki. Alternatywny port musi reprezentować drukarkę, która jest kompatybilna ze sterownikiem używanym przez pierwotną drukarkę.
- Liczniki wydajności *Total Jobs Printed* (Wszystkie wydrukowane zadania) oraz *Total Pages Printed* (Całkowita liczba wydrukowanych stron) pomagają monitorować wykorzystanie drukarki. Liczniki *Bytes Printed/Sec* (Szybkość drukowania bajty/s) oraz *Errors* (Błędy) ułatwiają monitorowanie potencjalnych problemów drukarki.
- Zdarzenia dziennika *System*, protokolowane przez usługę bufora wydruku oraz zdarzenia związane z bezpieczeństwem, rejestrowane poprzez włączenie inspekcji drukarki i zasady *Audit Object Access* (Inspekcja dostępu do obiektu), umożliwiają zebranie dodatkowych spostrzeżeń dotyczących działania drukarki.
- Ponieważ model drukarki systemu Windows Server 2003 jest modularny i składa się z samej drukarki, drukarki logicznej na serwerze wydruku oraz drukarki programu klienta podłączonej do drukarki udostępnionej na serwerze wydruku, to rozwiązywanie problemów drukarek może być przeprowadzane metodycznie poprzez sprawdzanie poszczególnych elementów i ich połączeń wzajemnych.

Zadanie praktyczne

Wykorzystanie drukarek w firmie Contoso Ltd. znacznie wzrosło i dyrektor poprosił administratora, aby rozpoczął wycenę wykorzystania drukarek w działach Marketing oraz Sales, gdyż dział te generują najwięcej wydruków.

Projektowanie rozwiązania

1. Który sposób monitorowania wykorzystania drukarki pod kątem wyceny wykonywanych przez nią zadań jest najbardziej efektywny?

System Windows Server 2003 wyposażony jest w obiekt wydajności *Printer Queue* (Kolejka wydruku), który umożliwia monitorowanie wykorzystania każdej zdefiniowanej na serwerze wydruku drukarki logicznej. Licznik *Total Pages Printed* (Całkowita liczba wydrukowanych stron) udostępnia ważne informacje o wykorzystaniu drukarki. Nie jest to narzędzie doskonałe, ponieważ pewne właściwości dokumentu i specjalne cechy wydruków (jak drukowanie broszur lub ustawienia umożliwiające drukowanie kilku pomniejszych stron na jednej stronie standardowych rozmiarów) wpływa bezpośrednio na urządzenia sprzętu drukarki bez możliwości śledzenia efektów przez usługę bufora wydruku. Jednakże omawiany licznik jest najlepszym dostępnym w systemie

przybliżeniem. Dzięki skonfigurowaniu dziennika wydajności i dodaniu licznika, można w późniejszym okresie analizować zawartość dziennika i wycenić wykorzystanie drukarki.

2. W jaki sposób za pomocą licznika *Total Pages Printed* (Całkowita liczba wydrukowanych stron) można oddzielnie monitorować grupy Sales oraz Marketing?

Licznik *Total Pages Printed* (Całkowita liczba wydrukowanych stron) przechwytywa dane dla pojedynczej drukarki logicznej. Aby oddzielnie monitorować dwie grupy, należy skonfigurować dwie drukarki logiczne. Każda drukarka będzie adresować ten sam port, czyli tę samą drukarkę fizyczną, ale umożliwiać będzie drukowanie tylko użytkownikom danej grupy.

Konfigurowanie drukarek

Informacje o sposobach instalowania drukarek logicznych zostały zamieszczone w ćwiczeniu 1 lekcji 1. Należy utworzyć dwie drukarki za pomocą programu *Add Printer Wizard* (Kreator dodawania drukarek). Poniższa tabela zawiera ustawienia, które należy zastosować podczas tworzenia drukarek za pomocą programów *Add Printer Wizard* oraz *Add Standard TCP/IP Port Wizard* (Kreator dodawania standardowych portów TCP/IP).

Tabela 8-1. Drukarka działu Sales

Opis	Ustawienie
Drukarka lokalna lub sieciowa	Drukarka lokalna podłączona do tego komputera Nie wykrywaj automatycznie drukarki przy pomocy usługi Plug and Play.
Wybór portu drukarki	Utwórz nowy port: „Standard TCP/IP Port”
Nazwa drukarki lub adres IP	10.0.0.53
Nazwa portu	IP_10.0.0.53
Typ urządzenia	Hewlett Packard Jet Direct
Producent	HP
Model drukarki	HP LaserJet 8100 Series PCL
Używany sterownik	Pozostaw istniejący sterownik
Nazwa drukarki	SalesPrinter
Domyślne opcje drukarki	No
Nazwa udziału	SalesPrinter
Lokalizacja	NYC/US/1802Americas/42/B
Komentarz	Drukarka laserowa, czarno-biała, wydajna
Wydruk strony testowej	Nie

2. Drukarka działu Marketing

Opis	Ustawienie
Drukarka lokalna lub sieciowa	Drukarka lokalna podłączona do tego komputera <i>Nie</i> wykrywaj automatycznie drukarki przy pomocy usługi Plug and Play.
Wybór portu drukarki	Użyj następującego portu: IP_10.0.0.53
Producent	HP
Model drukarki	HP LaserJet 8100 Series PCL
Używany sterownik	Pozostaw istniejący sterownik
Nazwa drukarki	MarketingPrinter
Domyślne opcje drukarki	No
Nazwa udziału	MarketingPrinter
Lokalizacja	NYC/US/1802Americas/42/B
Komentarz	Drukarka laserowa, czarno-biała, wydajna
Drukowanie strony testowej	Nie

Utworzenie grup użytkowników drukarki

Aby przydzielić uprawnienia do drukarek, konieczne jest utworzenie grup zabezpieczeń. W rozdziale omówione zostały sposoby tworzenia grup. Należy utworzyć dwie grupy zabezpieczeń zakresu lokalnej domeny (Domain Local): Marketing Printer Users oraz Sales Printer Users.

Przydział uprawnień do drukarek

1. W folder/.e *Printers And Faxes* (Drukarki i faksy) otwórz stronę *Properties* (Właściwości) drukarki SalesPrinter.
2. Kliknij zakładkę **Security** (Zabezpieczenia).
3. Wybierz grupę **Everyone** (Wszyscy) i kliknij przycisk **Remove** (Usuń).
4. Kliknij przycisk **Add** (Dodaj).
- 5- Wpisz nazwę grupy **Sales Printer Users** i kliknij przycisk OK.
6. Przypisz uprawnienie **Allow Print** (Zezwalaj na drukowanie) dla grupy Sales Printer Users.
7. Powtórz procedurę od punktu 1 do 6 tak, aby tylko członkowie grupy Marketing Printer Users mieli przydzielone uprawnienie Print (Drukuj) do drukarki MarketingPrinter.

Konfigurowanie dziennika wydajności

1. Otwórz konsolę MMC *Performance* (Wydajność) znajdującą się w grupie programów *Administrative Tools* (Narzędzia administracyjne).
2. Rozwiń węzeł **Performance Logs And Alerts** (Dzienniki wydajności i alerty) i wybierz dziennik **CounterLogs** (Dzienniki liczników).
3. Kliknij prawym przyciskiem myszy dziennik **Counter Logs** (Dzienniki liczników) i wybierz polecenie **New Log Settings** (Ustawienia nowego dziennika).
4. Wprowadź nazwę dziennika: **Printer Utilization**.
5. Kliknij przycisk OK. Wyświetlone zostanie okno dialogowe *Properties* (Właściwości) dziennika nazwanego Printer Utilization.
6. Kliknij przycisk **Add Counters** (Dodaj liczniki).
7. Z listy rozwijanej **Performance Object** (Obiekt wydajności) wybierz obiekt **Print Queue** (Kolejka wydruku).
8. Na liście **Counters** (Liczniki) wybierz licznik **Total Pages Printed** (Całkowita liczba wydrukowanych stron).
9. Na liście **Instances** (Wystąpienia) wybierz drukarkę **SalesPrinter**.
10. Kliknij przycisk **Add** (Dodaj).
11. Na liście **Instances** (Wystąpienia) wybierz drukarkę **MarketingPrinter**.
12. Kliknij przycisk **Add** (Dodaj).
13. Kliknij przycisk **Close** (Zamknij). W oknie dialogowym dziennika Printer Utilization zostaje wyświetlona informacja, że dla każdej kolejki wydruku dziennik będzie śledził licznik *Total Pages Printed* (Całkowita liczba wydrukowanych stron).
14. Wybierz wartość 30 minut jako interwał próbkowania. W tym celu wpisz 30 w polu *Interval* (Interwał) i z listy rozwijanej *Units* (Jednostki) wybierz jednostkę: **Minutes** (Minuty).



Informacja Ponieważ licznik Total Pages Printed (Całkowita liczba wydrukowanych stron) sumuje wyniki od momentu uruchomienia serwera wydruku lub od momentu uruchomienia usługi bufora wydruku, nie zachodzi potrzeba obsługiwanego krótszego okresu próbkowania. Interwał próbkowania może być bardzo długi, tak długo jak serwer lub usługa bufora wydruku nie zostanie ponownie uruchomiona pośrodku tego interwału.

15. Kliknij przycisk OK, aby zamknąć okno dialogowe dziennika Printer Utilization.
16. Jeśli na tym komputerze nie zostały skonfigurowane inne dzienniki wydajności, system poprosi o potwierdzenie operacji utworzenia foldera „C:\Perflogs”, w którym dzienniki są przechowywane zgodnie z ustawieniami domyślnymi systemu. Kliknij przycisk **Yes** (Tak), aby potwierdzić operację.
17. W oknie szczegółów węzła *Performance Logs* (Dzienniki wydajności) dziennik Printer Utilization jest koloru zielonego, co wskazuje, że został uruchomiony.
18. Zatrzymaj dziennik klikając go prawym przyciskiem myszy i wybierając polecenie **Stop**.

Po utworzeniu dziennika wydajności użytkownik może analizować dziennik w programie *System Monitor* (Monitor systemu). Na pasku narzędzi programu *System Monitor* należy kliknąć przycisk **View Log Data** (Wyświetl dane dziennika) i dodać wygenerowany dziennik wydajności. Ten szczególnie

dziennik wydajności nie jest prawidłowym dziennikiem z dwóch powodów. Po pierwsze musiałyby dokonać się co najmniej dwa wpisy, aby można było skorzystać z danych dziennika. Aby pobrać dziennik, trzeba więc odczekać 60 minut lub zmniejszyć interwał próbkowania. Po drugie, licznik *TotalPage Printed* (Całkowita liczba wydrukowanych stron) nie będzie inkrementowany, ponieważ drukarka nie istnieje i tym samym strony nie są drukowane.

Rozwiązywanie problemów

Pracownicy działu Marketing narzekają na jakość wydruków otrzymywanych z drukarki Marketing-Printer. Pracownicy używają systemów Windows XP i jeśli wydruki generowane są przy pomocy aplikacji Microsoft Office, dokumenty są drukowane prawidłowo. Natomiast, jeśli do wydruku używam aplikacji firmy Adobe, dokumenty nie zawsze spełniają wymagania jakości. Pracownicy działu Sales, którzy używają różnych aplikacji roboczych (komputery systemu Windows 2000 i Windows XP) oraz aplikacji Microsoft Office i Microsoft Customer Relationship Management (CRM), nie zgłaszają takich problemów odnośnie drukarki SalesPrinter.

Po analizie problemu można dojść do wniosku, że niektóre aplikacje uzyskują różne rezultaty w zależności od tego, czy drukarka wykorzystuje sterownik PostScript, czy też korzysta z innego sterownika.

Analiza rozwiązania

W którym miejscu można dodać sterowniki PostScript? Wybierz wszystkie właściwe odpowiedzi.

- a. Okno dialogowe *Properties* (Właściwości) serwera wydruku.
- b. Okno dialogowe *Properties* (Właściwości) drukarki MarketingPrinter.
- c. Okno dialogowe *Properties* (Właściwości) drukarki SalesPrinter.
- d. Drukarki zainstalowane na każdym komputerze użytkownika działu Marketing.

Prawidłowa odpowiedź to b. Dodanie sterownika PostScript dla drukarki MarketingPrinter spowoduje, że drukarka ta będzie go używać, natomiast nie zmieni się w konfiguracji drukarki SalesPrinter. Pomimo, że każdy klient drukarki będzie wymagał sterownika PostScript, nie trzeba go dodawać ręcznie. Klienci systemów Windows 2000 i Windows XP będą nowy sterownik pobierać automatycznie.

Zmiana sterownika drukarki

1. Otwórz folder Printers And Faxes (Drukarki i faksy).
2. Otwórz okno dialogowe Properties (Właściwości) drukarki MarketingPrinter. 3- Kliknij zakładkę Advanced (Zaawansowane).
4. Kliknij przycisk New Driver (Nowy sterownik). Zostanie wyświetlone okno programu Add Printer Driver Wizard (Kreator dodawania sterownika drukarki).
5. Kliknij przycisk Next (Dalej).
6. Wybierz producenta: HP.
7. Wybierz model drukarki: HP LaserJet 8100 Series PS.
8. Kliknij przycisk Next (Dalej), a następnie przycisk Finish (Zakończ).

9. Warto zwrócić uwagę, że sterownik PostScript stał się domyślnym sterownikiem.
10. Kliknij listę rozwijaną **Driver** (Sterownik). Na liście w dalszym ciągu widnieje poprzedni sterownik PCL. Jeśli zmiana sterownika nie rozwiąże problemu, można łatwo powrócić do używania poprzedniego sterownika.

Podsumowanie rozdziału

- Model drukarki systemu Windows Server 2003 jest modularny i składa się z urządzeń sprzętu drukarki, serwera wydruku razem z udostępnioną drukarką logiczną reprezentującą drukarkę fizyczną poprzez wskazanie portu sieci lub portu lokalnego tej drukarki oraz drukarki logicznej po stronie klienta, która jest podłączana do udostępnionej drukarki serwera wydruku. Zrozumienie struktury i terminologii ma podstawowe znaczenie, ponieważ dokumentacja i interfejs użytkownika nie są spójne, a czasami są nawet mylące.
- Drukarki udostępnione są publikowane w usłudze Active Directory, dzięki czemu ułatwione jest wyszukiwanie drukarek, które opiera się na lokalizacji oraz innych właściwościach drukarki.
- Jeśli użytkownik wyszukuje drukarkę w oknie dialogowym *Find Printers* (Znajdowanie: Drukarki), to dwukrotne kliknięcie drukarki spowoduje jej zainstalowanie na komputerze użytkownika. Komputery działające pod kontrolą systemu operacyjnego Windows automatycznie pobierają sterownik z serwera, jeśli administrator na udostępnionej drukarce zainstalował wszystkie wymagane sterowniki.
- Pojedyncza drukarka logiczna, skonfigurowana jako pula drukarek, może kierować zadania do kilku portów.
- Pojedyncza drukarka fizyczna (port) może być obsługiwana przez kilka drukarek logicznych. Każda z nich może mieć inaczej skonfigurowane właściwości, sterowniki, uprawnienia lub charakterystyki monitorowania. Taka struktura pozwala bardzo elastycznie instalować drukarki.
- Poprzez sieć Web można zarządzać, instalować drukarki oraz można na nich drukować, pod warunkiem, że na serwerze wydruku została zainstalowana i włączona usługa *Internet Printing* (Drukowanie internetowe).
- Dzienniki zdarzeń i liczniki wydajności umożliwiają monitorowanie drukarek w celu rozpoznania potencjalnych sygnałów o nieprawidłowym działaniu lub dla zapoznania się ze statystykami wykorzystania drukarek.

Informacje dla zdających egzamin

Przed przystąpieniem do egzaminu należy zapoznać się z przedstawionymi poniżej najważniejszymi faktami i pojęciami, aby określić które tematy wymagają pogłębienia. Należy powrócić do lekcji, aby osiągnąć większą wprawę oraz przejrzeć działy znajdujące się w części 2 — „Materiały dodatkowe”. Informacje tu zawarte kierują do materiałów uzupełniających tematy objęte zadaniami egzaminacyjnymi.

Najważniejsze fakty

- Podstawowe różnice pomiędzy drukarką sprzętową, nazywaną również urządzeniem drukującym lub drukarką fizyczną a drukarką logiczną, nazywaną również drukarką.
- Różnice pomiędzy drukarką w folderze *Printers And Faxes* (Drukarki i faksy) a obiektem drukarki w usłudze Active Directory.
- Sposoby zarządzania portami drukarek. Sposoby konfigurowania puli drukarek i przekierowania drukarek oraz różnice pomiędzy nimi.
- Sposoby konfigurowania kilku drukarek logicznych podłączonych do pojedynczej drukarki fizycznej. Zapoznanie się z szeregiem właściwości, które mogą być konfigurowane niezależnie dla każdej drukarki logicznej, wliczając w to uprawnienia zabezpieczeń.
- Sposoby monitorowania wykorzystania drukarek i rozwiązywania problemów związanych z ich działaniem.

Najważniejsze pojęcia

Logical printer (Drukarka logiczna) Reprezentuje drukarkę fizyczną poprzez obsługę portu drukarki. Drukarka logiczna ma kolejkę, sterowniki, ustawienia oraz domyślne ustawienia drukowania, które zarządzają tworzeniem zadania wydruku dla drukarki.

Network printer (Drukarka sieciowa) W kontekście interfejsu użytkownika systemu Microsoft Windows jest to drukarka logiczna, która jest klientem (jest podłączona do) udostępnionej drukarki logicznej innego komputera. Nie należy więc wpadać w zakłopotanie, jeśli mamy do czynienia z drukarką sieciową, która jest obsługiwana przez *drukarkę lokalną* na serwerze wydruku.

Pytania i odpowiedzi

289 Pytania do lekcji 1

1. Administrator konfiguruje drukarkę w systemie Windows Server 2003- W sieci, komputer ten będzie używany jako serwer wydruku. Urządzeniem drukującym ma być drukarka aktualnie przyłączona do sieci jako autonomiczne urządzenie drukujące. Który typ drukarki należy utworzyć na serwerze wydruku? Wybierz wszystkie właściwe odpowiedzi.
 - a. Network (Sieciowa)
 - b. Shared (Udostępniona)
 - c. Local (Lokalna)
 - d. Remote (Zdalna)

Prawidłowe odpowiedzi to b oraz c. Drukarka lokalna obsługuje drukarkę bezpośrednio przyłączoną do komputera lub autonomiczną drukarkę sieciową. Dla komputera, który działa jak serwer wydruku, drukarka musi być udostępniona.

2. Administrator instaluje drukarkę na komputerze klienta. Drukarka będzie podłączona do drukarki logicznej serwera wydruku systemu Windows Server 2003. Jakiego rodzaju informacje należy wprowadzić, aby skonfigurować drukarkę? Wybierz wszystkie właściwe odpowiedzi.
- a. Port TCP/IP drukarki
 - b. Model urządzenia drukującego
 - c. Adres URL drukarki na serwerze wydruku
 - d. Ścieżka UNC dla drukarki udostępnionej (udziału)
 - e. Sterownik drukarki

Prawidłowe odpowiedzi to c oraz d. Jeśli dodana zostanie drukarka sieciowa, drukarka ta może być wyszukiwana w usłudze Active Directory poprzez wprowadzenie nazwy UNC bądź adresu URL drukarki lub korzystając z funkcji przeglądania. Jeśli użytkownik podłącza się do drukarki, jej model jest określany przez udostępnioną drukarkę logiczną, a sterownik pobierany jest automatycznie.

3. Jedna z drukarek funkcjonuje nieprawidłowo i należy zapobiec wysyłaniu przez użytkowników zadań wydruku do drukarki logicznej obsługującej to urządzenie. Co należy zrobić?
- a. Zatrzymać udostępnianie drukarki
 - b. Usunąć drukarkę z usługi Active Directory
 - c. Zmienić port drukarki
 - d. Zmienić nazwę udziału

Prawidłowa odpowiedź to a. Jeśli zatrzymane zostanie udostępnianie drukarki, użytkownicy nie będą mogli korzystać z tego urządzenia drukującego. Aby zakończyć udostępnianie drukarki, należy posłużyć się zakładką Sharing (Udostępnianie) okna dialogowego właściwości drukarki.

4. Administrator zarządza komputerem systemu Windows Server 2003 skonfigurowanym jako serwer wydruku. Administrator chce przeprowadzić konserwację drukarki podłączonej do serwera wydruku. W kolejce wydruku znajduje się kilka dokumentów. Administrator musi zapewnić, aby dokumenty przestały być drukowane i jednocześnie, żeby użytkownicy nie musieli ponownie wysłać dokumentów do wydruku. Jaki jest najlepszy sposób realizacji takiego zadania?
- a. W oknie dialogowym Properties (Właściwości) drukarki należy wybrać zakładkę Sharing (Udostępnianie), a następnie zaznaczyć opcję Do Not Share This Printer (Nie udostępniaj tej drukarki).
 - b. W oknie dialogowym Properties (Właściwości) drukarki należy wybrać port, który nie jest przypisany do urządzenia drukującego.
 - c. W oknie kolejki drukarki należy zaznaczyć pierwszy dokument, a następnie w oknie dokumentu wybrać polecenie Pause (Wstrzymaj). Powtórzyć działanie dla każdego dokumentu.
 - d. W oknie kolejki drukarki, w menu Printer (Drukarka) wybrać polecenie Pause Printing (Wstrzymaj drukowanie)

Prawidłowa odpowiedź to d. Jeśli wybrana zostanie opcja Pause Printing (Wstrzymaj drukowanie), dokumenty pozostaną w kolejce drukarki, a drukowanie zostanie wznowione. Opcja ta dotyczy wszystkich dokumentów kolejki.

Pytania do lekcji 2

1. Administrator zarządza komputerem systemu Windows Server 2003 skonfigurowanym jako serwer wydruku. Użytkownicy grupy Marketing narzekają, że nie mogą drukować dokumentów przy użyciu drukarki tego serwera. Administrator przejrzał uprawnienia w oknie właściwości drukarki i okazało się, że grupa Marketing ma przydzielone uprawnienia Manage Documents (Zarządzanie dokumentami). Dlaczego użytkownicy nie mogą drukować na tej drukarce?
 - a. Do grupy Everyone (Wszyscy) muszą być przydzielone uprawnienia Manage Documents (Zarządzanie dokumentami).
 - b. Do grupy Administratorzy muszą być przydzielone uprawnienia Manage Printers (Zarządzanie drukarkami).
 - c. Do grupy Marketing muszą być przydzielone uprawnienia Print (Drukowanie).
 - d. Do grupy Marketing muszą być przydzielone uprawnienia Manage Printers (Zarządzanie drukarkami).

Prawidłowa odpowiedź to c. Uprawnienie Print (Drukowanie) umożliwia użytkownikom wysyłanie I dokumentów do drukarki.

2. Administrator konfiguruje pulę drukarek komputera systemu Windows Server 2003. Pula zawiera trzy jednakowe urządzenia drukujące. Administrator otworzył okno właściwości drukarki i na zakładce Ports (Porty) zaznaczył opcję Enable Printer Pooling (Włącz tworzenie puli drukarek). Jaka będzie kolejna czynność?
 - a. Skonfigurowanie portu LPT1 tak, aby obsługiwane były trzy drukarki.
 - b. Wybór lub utworzenie portów mapowanych do trzech drukarek.
 - c. Na zakładce Device Settings (Ustawienia urządzenia) należy skonfigurować opcje dla obsługi dwóch dodatkowych urządzeń drukujących.
 - d. Na zakładce Advanced (Zaawansowane) należy określić priorytet dla każdego urządzenia drukującego tak, aby ten sposób drukowania został zastosowany do tych trzech urządzeń drukujących.

Prawidłowa odpowiedź to b. Pula drukarek jest konfigurowana na zakładce Ports (Porty) okna dialogowego właściwości drukarki. Aby skonfigurować pulę drukarek, należy zaznaczyć pole wyboru Enable Printer Pooling (Włącz tworzenie puli drukarek), a następnie wybrać lub utworzyć porty odpowiadające drukarkom, które będą częścią puli.

3. Administrator zarządza komputerem systemu Windows Server 2003 skonfigurowanym jako serwer wydruku i chce zarządzać usługami drukowania za pomocą przeglądarki sieci Web na komputerze klienta. Serwer nazywa się Mktgl, ale administrator nie zna nazwy drukarki. Jaki adres URL powinien być użyty, aby połączyć się z drukarką?
 - a. <http://mktgl/printers>
 - b. <http://printers/mktgl>
 - c. <http://windows/web/printers>
 - d. <http://windows/mktgl>

Prawidłowa odpowiedź to a. Aby za pomocą przeglądarki sieci Web uzyskać dostęp do wszystkich drukarek na serwerze wydruku i przeglądać ich listę, należy otworzyć przeglądarkę i połączyć się z adresem <http://printserver/printers>. W oparciu o tę listę można uzyskać dostęp do konkretnej dru-

karki. Jeśli natomiast chcemy uzyskać dostęp do określonej drukarki nie przeglądając najpierw listy wszystkich drukarek, należy użyć adresu *http://płntserver/płntersharename*.

4. Administrator chce skonfigurować drukarkę logiczną tak, aby przy jej użyciu drukowane były w godzinach nocnych duże dokumenty mające niski priorytet. Którą z wymienionych poniżej opcji należy skonfigurować w oknie dialogowym Properties (Właściwości) drukarki?
 - a. Priority (Priorytet)
 - b. Available From /To (Dostępna od/do)
 - c. Start Printing After Last Page Is Spooled (Rozpocznij drukowanie po umieszczeniu w buforze ostatniej strony)
 - d. Print Directly To The Printer (Drukuj bezpośrednio do drukarki)
 - e. Keep Printed Documents (Przechowaj dokumenty po wydrukowaniu)

Prawidłowa odpowiedź to b. Harmonogram drukarki pozwala drukarce odbierać zadania i przechowywać je do momentu, «Ż drukarka jest dostępna. Domyślne ustawienia Always Available (Zawsze dostępna) umożliwiają wysyłanie zadania do drukarki wtedy, kiedy jest wolna. Jeśli skonfigurowana zostanie opcja Available From /To (Dostępna od/do), określone zostaną godziny, w których zadania wydruku będą mogły być wysłane do drukarki.

311 Pytania do lekcji 3

1. System Windows 2003 Server został skonfigurowany jako serwer wydruku. W środku dnia pracy przepalił się bezpiecznik drukarki i musi zostać wymieniony. Użytkownicy mieli już powysyłane zadania do drukarki, która używa adresu IP 192.168.1.81. W sieci jest identyczna drukarka, do której przypisany został adres 192.168.1.217. Drukarka ta obsługiwana jest przez inną drukarkę logiczną na serwerze. Jaki czynności należy wykonać, aby zadania użytkowników zostały wydrukowane bez konieczności powtórzenia ich wysyłania do drukarki?
 - a. W oknie dialogowym Properties (Właściwości) uszkodzonej drukarki należy zaznaczyć opcję Enable Printer Pooling (Włącz tworzenie puli drukarek).
 - b. W wierszu poleceń należy wprowadzić komendę **Net Stop Spooler**.
 - c. W wierszu poleceń należy wprowadzić komendę **Net Start Spooler**.
 - d. W oknie dialogowym Properties (Właściwości) uszkodzonej drukarki należy wybrać port 192.168.1.217.
 - e. W oknie dialogowym Properties (Właściwości) uszkodzonej drukarki należy kliknąć przycisk Add Port (Dodaj port).
 - f. W folderze Printers And Faxes (Drukarki i faksy) należy kliknąć drukarkę prawym przyciskiem myszy i wybrać polecenie Use Offline (Użyj drukarkę w trybie offline).

Prawidłowa odpowiedź to d. Ponieważ pozostałe drukarki są obsługiwane przez drukarki logiczne serwera wydruku, nie zachodzi potrzeba dodawania nowego portu. Po prostu wystarczy wybrać istniejący port.

2. Administrator konfiguruje usługi drukowania w systemie Windows Server 2003. Przyłączył drukarkę, skonfigurował drukarkę logiczną i wysłał dokumenty do druku, ale dokumenty nie drukują się w całości, a czasami są pozmieniane. Jaka jest najbardziej prawdopodobna przyczyna problemu?
 - a. Brak wystarczającej przestrzeni dyskowej dla bufora wydruku.

- b. Użyty został niewłaściwy sterownik drukarki.
- c. Wybrany port jest nieprawidłowy.
- d. Ustawienia drukarki określają nieprawidłową czcionkę zastępczą.

Prawidłowa odpowiedź to b. Niewłaściwy sterownik drukarki może powodować, że dokumenty zostaną pozmieniane lub nie są drukowane w całości. Należy zainstalować właściwy sterownik.

3. Która z wymienionych poniżej opcji dobrze odzwierciedla wykorzystanie drukarki, umożliwiając użytkownikowi ocenę zużycia toneru i papieru?
- a. Skonfigurować inspekcje drukarki logicznej i rejestrować zakończone powodzeniem użycie uprawnień Print (Drukowanie) przez członków grupy Everyone (Wszyscy).
 - b. Wyeksportować dziennik System do pliku o wartościach rozdzielanych przecinkiem i użyć programu Excel do analizy zdarzeń bufora wydruku.
 - c. Skonfigurować dziennik wydajności i dla każdej drukarki logicznej monitorować licznik Total Pages Printed (Całkowita liczba wydrukowanych stron).
 - d. Skonfigurować dziennik wydajności i dla każdej logicznej drukarki monitorować licznik Jobs (Zadania).

Prawidłowa odpowiedź to c. Licznik Total Pages Printed (Całkowita liczba wydrukowanych stron) jest najlepszym przybliżeniem oceny zużycia toneru i papieru, jako że zużycie to jest bardziej związane z ilością wydrukowanych stron, niż z liczbą wydrukowanych zadań. W tym zadaniu, protokolowanie w dziennikach System i Security (Zabezpieczenia) zdarzeń związanych z usługą bufora wydruku i zdarzeń związanych z dostępem do obiektu będzie w najlepszym razie nieefektywne, a prawdopodobnie w ogóle nieprzydatne.

9 Obsługa systemu t operacyjnego



Zadania egzaminacyjne omawiane w tym rozdziale:

- Zarządzanie infrastrukturą aktualizacji oprogramowania
- Zarządzanie licencjonowaniem oprogramowania lokacji

Cele rozdziału

W 2002 roku wirus Code Red i jego odmiany Code Red v2 oraz Code Red II, wykorzystując lukę w programie *Microsoft Index Server* wdarły się do sieci Internet. Pomimo, że wirusy te nie robiły wielkich szkód, zdumiewająca szybkość ich rozprzestrzeniania stała się sygnałem alarmowym dla tysięcy pracowników działów IT, którzy spędzili wiele godzin zabezpieczając i aktualizując swoje systemy. Sygnał alarmowy był szczególnie bolesny, ponieważ firma Microsoft opublikowała poprawkę usuwającą lukę programu Index Server na miesiąc wcześniej, zanim wirus zaczął się spustoszenie. Stało się jeszcze bardziej oczywiste, że serwery i stacje robocze muszą być stale aktualizowane. Okazało się, że postępowanie wielu administratorów w przedsiębiorstwach, polegające na oczekiwaniu na pojawienie się pakietu serwisowego numer 3 i nie instalowania w międzyczasie dostępnego już pakietu numer 2 było niezbyt rozsądne. Aktualizacja oprogramowania stała się częścią strategii zabezpieczeń organizacji.

W niniejszym rozdziale omówione zostały sposoby stosowania usług SUS (Microsoft Software Update Services) umożliwiających stałą aktualizację serwerów i stacji roboczych. Usługa SUS pozwala scentralizować pobieranie, testowanie, zatwierdzanie i dystrybucję najważniejszych aktualizacji systemu Windows. Usługa ta pełni istotną rolę w zachowaniu integralności sieci przedsiębiorstwa. W rozdziale tym omówione zostały również sposoby instalowania pakietów serwisowych na jednym lub na kilku komputerach oraz przeanalizowane zostały elementy systemu licencjonowania oprogramowania lokacji.

Lekcje rozdziału:

- Lekcja 1: Usługi aktualizacji oprogramowania 325
- Lekcja 2: Pakiety serwisowe 344
- Lekcja 3: Zarządzanie licencjami oprogramowania 347

Wymagania

Niniejszy rozdział omawia pojęcia i umiejętności związane z zarządzaniem usługami SUS (Windows Software Update Services), instalowaniem pakietów serwisowych oraz licencjonowaniem. Z pewnością podczas przeprowadzania ćwiczeń pomocne byłoby posiadanie dwóch komputerów (system Windows Server 2003 oraz system klienta Windows XP lub Windows 2000 Professional), ale zadania są tak pomyślane, że można je zakończyć mając tylko jeden komputer. W tym celu należy przygotować

- System Windows Server 2003 (Standard lub Enterprise). Serwer powinien nazywać się SerwOl i być kontrolerem domeny w domenie contoso.com
- Jednostkę organizacyjną pierwszego poziomu nazwaną Desktops
- Konfigurację sieci umożliwiającą dostęp do Internetu

Lekcja 1: Usługi aktualizacji oprogramowania

Dla utrzymania prawidłowej ochrony środowiska sieci komputerowej konieczne jest instalowanie najnowszych poprawek zabezpieczeń. Od roku 1998 firma Microsoft udostępnia usługę Windows Update, która jest źródłem informacji i umożliwia pobieranie plików uaktualnień z sieci Web. Firma Microsoft wprowadziła usługę *Automatic Updates* (Aktualizacje automatyczne) w systemach Windows XP oraz w systemach Windows 2000, które mają zainstalowany dodatek Service Pack 3. Dzięki temu system automatycznie łączy się z usługą Windows Update i pobiera wszystkie dostępne poprawki i uzupełnienia. Pomimo, że usługi Windows Update i Automatic Updates pozwalają osiągnąć dla serwerów i klientów zamierzony cel, czyli utrzymanie aktualnej wersji systemu, wielu administratorów nie jest zadowolonych z faktu, że komputery lub programy klienckie decydują, które poprawki powinny być zainstalowane, ponieważ poprawki te mogą mieć wpływ na działanie istotnych aplikacji przedsiębiorstwa.

Najnowszym usprawnieniem tej technologii jest usługa SUS (Software Update Services). Usługa SUS jest aplikacją typu klient-serwer, która umożliwia serwerowi Internetu działanie jako punkt centralny zarządzania aktualizacjami. Administrator może zatwierdzić aktualizacje wykonywane dla klientów usługi SUS, które następnie mogą być pobierane i instalowane już bez interwencji administratora.

Niniejsza lekcja omawia instalowanie i zarządzanie usługą SUS w systemie Windows Server 2003. Kolejne lekcje opisują zagadnienia dotyczące konfiguracji klienta.

Materiały omówione podczas lekcji pozwalają na

- Instalowanie usługi SUS na komputerze systemu Windows Server 2003
- Konfigurowanie usługi SUS
- Instalowanie i dystrybucję usługi Automatic Updates dla klientów SUS
- Zarządzanie usługami SUS i Automatic Updates
- Monitorowanie, rozwiązywanie problemów, wykonywanie kopii zapasowej oraz przywracanie usługi SUS

Szacunkowy czas lekcji: 30 minut

Omówienie usługi SUS

Od 1998 roku systemy operacyjne Microsoft Windows obsługują usługę Windows Update, która jest globalnym źródłem dystrybucji aktualizacji. Serwery usługi Windows Update współdziałają z oprogramowaniem po stronie klienta w celu rozpoznania aktualizacji o podstawowym znaczeniu, luk w zabezpieczeniach i usprawnień odpowiednich dla platformy klienta, a dopiero następnie pobierają zatwierdzone poprawki. Administratorzy postulowali zaprojektowanie bardziej scentralizowanego rozwiązania, które zapewniłoby bezpośrednią kontrolę nad przeprowadzanymi aktualizacjami. Usługa SUS jest właśnie odpowiedzią na te postulaty.

Usługa SUS składa się z kilku podstawowych elementów:

- **Usługa SUS (Software Update Services) uruchomiona na serwerze IIS (Internet Information Services)** Jest to element działający na serwerze odpowiedzialny za synchronizację informacji o dostępnych aktualizacjach i najczęściej pobierający aktualizacje z internetowych serwerów usług Windows Update firmy Microsoft lub innych serwerów, na których działa usługa SUS.
- **Administracja usługi SUS poprzez sieć Web** Cała administracja usługi SUS została oparta o funkcjonalność sieci Web. Po zainstalowaniu i skonfigurowaniu usługi SUS, zarządzanie najczęściej sprowadza się do sprawdzenia, czy dany serwer SUS został poprawnie synchronizowany, i a aktualizacje zostały zatwierdzone i mogą być rozprowadzane wśród klientów sieci.
- **Aktualizacje automatyczne** Klient usługi *Automatic Updates* (Aktualizacje automatyczne) jest odpowiedzialny za pobieranie aktualizacji z serwera usługi Windows Update lub SUS oraz za instalowanie tych aktualizacji w oparciu o harmonogram lub działania administratora.
- **Ustawienia zasady grupy** Klient usługi *Automatic Updates* może być tak skonfigurowany, aby synchronizował się z serwerem SUS, a nie z serwerami Windows Update. W tym celu modyfikowane są rejestry klienta lub, co jest bardziej wydajne, konfigurowane są zasady usługi Windows Update w obiekcie GPO (Group Policy Object).

Instalowanie usługi SUS w systemie Windows Server 2003

Usługa SUS składa się z komponentów: klient i serwer. Element serwera działa na komputerze systemu Windows 2000 Server (dodatek Service Pack 2 lub późniejsze) lub systemu Windows Server 2003. Usługi IIS (Internet Information Services) muszą zostać zainstalowane przed skonfigurowaniem usługi SUS. Należy pamiętać, że tak jak nadmieniono w rozdziale 6 „Pliki i foldery”, usługi IIS nie są domyślnie instalowane w systemie Windows Server 2003. Informacje dotyczące sposobu instalowania usługi IIS można znaleźć w rozdziale 6.

Usługa SUS nie jest dołączana do nośnika systemu Windows Server 2003, ale można ją pobrać bez opłat z witryny firmy Microsoft SUS Web o adresie: <http://go.microsoft.com/fwlink/?LinkID=6930>.



Informacja Usługa SUS nie jest dostępna dla wszystkich wersji językowych. Jednakże produkt ten określa tylko interfejs instalacji i pobierania dla elementu serwera. Za pomocą usługi SUS można instalować poprawki dla *wszystkich* regionalnych i językowych wersji.

Po pobraniu najnowszej wersji usługi SUS, aby uruchomić procedurę instalacyjną, należy dwukrotnie kliknąć pobrany plik. Następnym krokiem jest zaakceptowanie warunków licencji, po czym należy wybrać opcję instalacji *Custom* (niestandardowa), a program Setup Wizard poprosi o podanie następujących informacji:

- **Choose File Locations (Wybór lokalizacji pliku)** Każda poprawka usługi Windows Update składa się z dwóch elementów — z samego pliku poprawki i z metadanych określających platformy i języki, których poprawki te dotyczą. Usługa SUS zawsze pobiera te metadane, które będą używane do zatwierdzania aktualizacji i które są pobierane z usługi SUS przez klientów intranetu. Użytkownik może wybrać, czy pobrać same pliki, a jeśli tak, gdzie ma być przechowywana aktualizacja.



Wskazówka Jeśli na serwerach Microsoft Windows Update zostały wybrane pliki, które mają być aktualizowane, klient usługi Automatic Updates połączy się z serwerem SUS, aby pobrać listę zatwierdzonych aktualizacji, a następnie połączy się z serwerami Microsoft Windows Update, aby pobrać te pliki. Dzięki temu administrator zachowuje kontrolę nad aktualizacjami klienta i jednocześnie korzysta ze źródeł danych udostępnianych na całym świecie przez firmę Microsoft.

Jeśli została wybrana opcja *Save The Updates To This LocalFolder* (zapis/ aktualizacje w tym folderze), ustawienia domyślne programu Setup Wizard określają, że folder nazwany SUS zostanie utworzony na dysku, który ma najwięcej wolnej przestrzeni. Pliki mogą być przechowywane na dowolnej partycji systemu plików NTFS. Zalecana przez firmę Microsoft minimalna wielkość wolnej przestrzeni dyskowej to 6 GB.



Informacja Do formatowania partycji SUS i partycji systemowej musi być używany system NTFS.

- **Languages Settings (Ustawienia językowe)** Pomimo, że interfejs administracji usługi SUS jest dostarczany w wersji angielskiej oraz kilku dodatkowych językach, poprawki są wydawane dla wszystkich obsługiwanych ustawień regionalnych. Opcja ta określa regionalną wersję serwerów lub klientów systemu Windows, które są obsługiwane w danym środowisku.
- **Handling New Versions Of Previously Approved Updates (Obsługa nowych wersji poprzednio zatwierdzonych aktualizacji)** Czasami zdarza się, że sama aktualizacja też zostaje uaktualniona. Istnieje możliwość, aby usługa SUS automatycznie zatwierdzała nowe wersje poprzednio zatwierdzonych aktualizacji lub zatwierdzanie aktualizacji może być kontynuowane ręcznie.
- **ReadyTo Install (Gotowość do instalacji)** Przed rozpoczęciem instalacji program Setup Wizard będzie przypominał, że adres URL klienta powinien wskazywać na: *http://SUS__servername*. Warto zanotować tę ścieżkę, ponieważ będzie używana do konfigurowania sieci klientów.
- **Installing Microsoft Software Update Services (Instalowanie usługi SUS)** Program Setup Wizard instaluje usługi SUS.
- **Completing the Microsoft Software Update Services Setup Wizard (Kończenie instalacji i usługi SUS)** Ostatnia strona programu instalacyjnego Setup Wizard wyświetla adres URL witryny administracyjnej usługi SUS — *http://SUS_servername/SUSAdmin*. Warto zanotować tę ścieżkę, ponieważ usługa SUS będzie zarządzana z tej lokalizacji sieci Web. Po kliknięciu przycisku Finish (Zakończ), zostanie uruchomiona przeglądarka sieci Web i automatyczne połączenie ze stroną administracji usługi SUS.

Usługa SUS (Software Update Services) instaluje na serwerze następujące trzy elementy:

- Usługa *Software Update Synchronization Service*, która pobiera dane do serwera SUS
- Witryna sieci Web usługi IIS, która obsługuje żądania aktualizacji przychodzące od klientów usługi *Automatic Updates* (Aktualizacje automatyczne)
- Strona administracji usługi SUS, za pomocą której przeprowadzana jest synchronizacja serwera SUS i zatwierdzanie aktualizacji.

IIS Lockdown

Program instalacyjny usługi SUS uruchomiony na serwerze Windows 2000 wywołuje program IIS Lockdown Wizard, aby zabezpieczyć usługę IIS 5.0. Ustawienia domyślne określają, że system Windows Server 2003 jest zamknięty, tak więc blokowanie usługi IIS jest niepotrzebne.

Jeśli na serwerze były uruchamiane aplikacje sieci Web, po zainstalowaniu usługi SUS aplikacje te mogą przestać prawidłowo funkcjonować. Należy ponownie włączyć filtry ISAPI (Internet Server Application Programming Interface) i otworzyć inne komponenty, które zostały zabezpieczone przez program IIS Lockdown. Jednakże, ze względu na wrażliwość aktualizacji systemu operacyjnego, należy rozważyć uruchamianie usług SUS na dedykowanym serwerze, na którym nie działają inne aplikacje IIS.

Konfigurowanie i zarządzanie usługami SUS

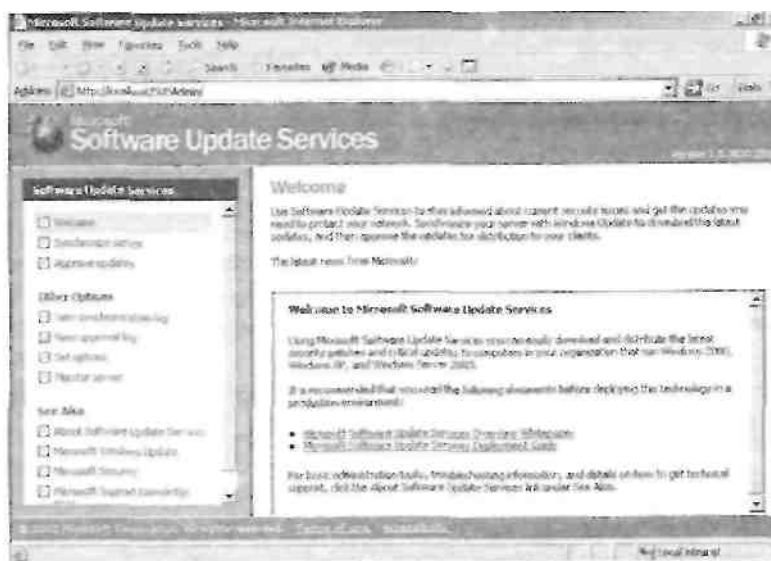
Administrator musi wykonać trzy zadania dotyczące usług SUS: konfiguracja ustawień usług SUS, synchronizacja danych oraz ich zatwierdzanie. Zadania te są przeprowadzane przy użyciu witryny *SUS Administration Web* pokazanej na rysunku 9-1. Dostęp do witryny można uzyskać wpisując w przeglądarce Internet Explorer 5.5 (lub jej wersji późniejszej) adres: `http://IISUS_servername/SUSAdmin` lub otwierając program **Microsoft Software Update Services** w grupie programów **Administrative Tools** (Narzędzia administracyjne). Administracja usług SUS w całości opiera się na funkcjonalności sieci Web.



Informacja Być może, aby uzyskać dostęp do tej witryny, zajdzie konieczność dodania serwera Server01 do listy zaufanych witryn *Local Intranet* (Lokalny intranet). W tym celu należy otworzyć przeglądarkę Internet Explorer i wybrać w menu **Tools** (Narzędzia) polecenie **Internet Options** (Opcje internetowe). Następnie należy kliknąć zakładkę **Security** (Zabezpieczenia) i wybrać ikonę **Trusted Sites** (Zaufane witryny). Wpisy Server01 i Server01.contoso.com należy dodać do listy zaufanych witryn.



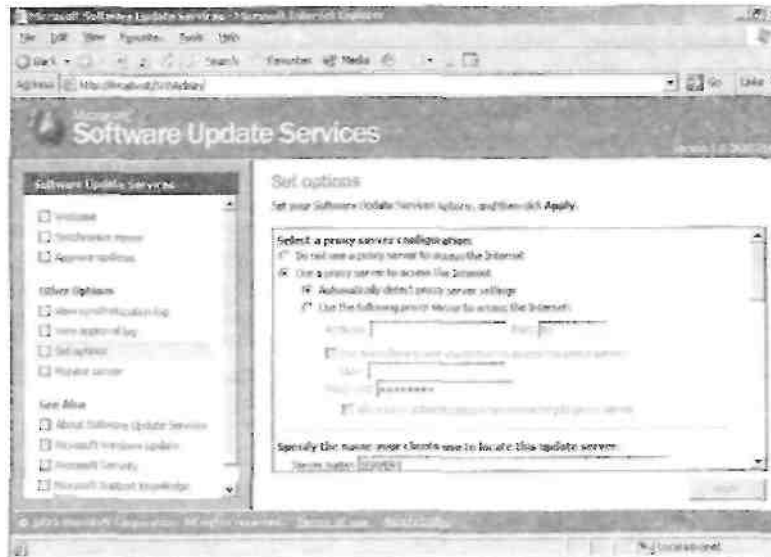
Informacja Aby konfigurować i zarządzać usługami SUS, użytkownik musi być administratorem lokalnym serwera SUS. Jest to również jedna z przyczyn, które warto rozważyć decydując się na tworzenie dedykowanego serwera SUS. W przypadku dedykowanego serwera SUS przekazywanie administracji usługi SUS jest bezpieczne i nie zdarzy się przypadkowe delegowanie uprawnień do innych ról bądź aplikacji serwera.



Rysunek 9-1 Witryna SUSAdministration Web

Konfigurowanie usługi SUS (Software Update Semces)

Niektóre ustawienia konfiguracji usługi SUS mogą być określone podczas instalacji niestandardowej, jednak wszystkie ustawienia są dostępne za pomocą witryny SUS Administration Web. Na stronie administracji usługi SUS (Software Update Services), w oknie nawigacyjnym umieszczonym po lewej stronie, należy kliknąć polecenie **Set Options** (określanie opcji). Strona *Set Options* została pokazana na rysunku 9-2.



Rysunek 9-2 5fr(?Wi7 usługi SUS: Set Options

Na stronie znajdują się następujące ustawienia konfiguracji:

- **Proxy server configuration (konfiguracja serwera proxy)** Jeśli serwer SUS łączy się do usługi Windows Update przy pomocy serwera proxy, należy skonfigurować ustawienia serwera proxy.



Wskazówka Pomimo, że serwer SUS może być tak skonfigurowany, aby uzyskiwał dostęp do usługi Windows Update poprzez serwer proxy, który wymaga uwierzytelnienia, to klient usługi *Automatic Updates* (Aktualizacje automatyczne) nie uzyska dostępu do usługi Windows Update (jeśli serwer proxy wymaga uwierzytelnienia). W takim przypadku należy skonfigurować usługę SUS, aby przeprowadzała uwierzytelnienie, a wszystkie dane aktualizacji (pliki i metadane) będą musiały być przechowywane lokalnie.

- **DNS name of the SUS server (nazwa DNS serwera SUS)** W polu *Server Name* (nazwa serwera) należy wpisać kwalifikowaną nazwę domeny (FQDN) serwera SUS, na przykład susl.contoso.com.
- **Content source (źródło danych)** Pierwszy instalowany serwer SUS przeprowadza synchronizację swoich danych z usługą Microsoft Windows Update. Dodatkowe serwery SUS mogą synchronizować swoje dane z usługą Windows Update, z nadrzędnym serwerem SUS lub z ręcznie utworzonym punktem dystrybucji. Dodatkowe informacje można znaleźć w temacie pomocy „SUS Topolog”.
- **New versions of approved updates (Nowe wersje zatwierdzonych aktualizacji)** Strona *Set Options* umożliwia modyfikację sposobu obsługi nowych wersji poprzednio zatwierdzonych aktualizacji. Poprzednie fragmenty lekcji opisywały już tę opcję.
- **File storage (magazyn pliku)** Użytkownik może modyfikować parametry magazynu przechowywania metadanych i plików aktualizacji. Również i ta opcja była już omówiona.



Wskazówka Jeśli zmieniona zostanie lokalizacja magazynu z serwera usługi Windows Update na folder lokalny, należy natychmiast wykonać synchronizację, dzięki której do wybranej lokalizacji pobrane zostaną niezbędne pakiety.

- * **Languages (języki)** Ustawienie to określa opcje regionalne aktualizacji, które będą synchronizowane. Należy wybrać tylko języki dla ustawień regionalnych, które są obsługiwane w środowisku danej sieci.



Wskazówka Jeśli ustawienia regionalne zostaną usunięte, nie spowoduje to usunięcia pobranych pakietów. Jednak klienci nie będą już odbierać tych pakietów. Jeśli natomiast ustawienia lokalne zostaną *dodane*, należy wykonać ręczną synchronizację celem pobrania odpowiednich pakietów dotyczących nowych ustawień regionalnych.

Topologia usługi SUS

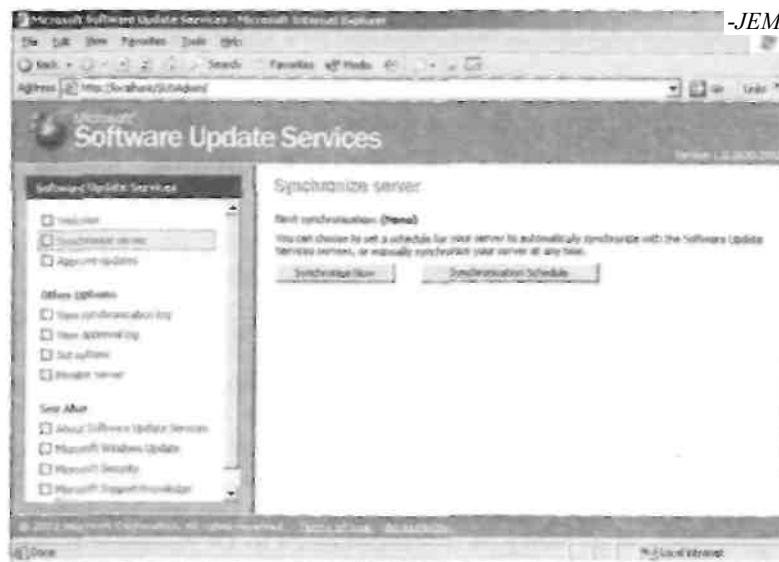
Usługa SUS (*Software Update Services*) umożliwia kontrolę zatwierdzania i dystrybucji aktualizacji pobieranych z usługi Microsoft Windows Update. W niedużych organizacjach usługa SUS może być po prostu pojedynczym serwerem, który synchronizuje dane z usługą Windows Update i udostępnia klientom listę zatwierdzonych aktualizacji.

W dużych organizacjach można stosować różne topologie usługi SUS, dzięki czemu jest ona bardziej wydajna i lepiej dostosowana do potrzeb. Chociaż podczas egzaminu 70-290 wymagana jest wiedza związana z administracją istniejących topologii, to warto zapoznać się z niektórymi możliwościami projektowymi usługi:

- **Topologia wieloserwerowa** Każdy serwer SUS synchronizuje dane z usługą Windows Update i zarządza swoją listą zatwierdzonych aktualizacji. Omawiana topologia mogłaby być odmianą modelu pojedynczego serwera, w którym każdy administrator usługi SUS kontroluje listę zatwierdzonych aktualizacji. Konfiguracja taka mogłaby także umożliwiać obsługę różnych zestawów poprawek i aktualizacji (odrębne zestawy na każdym serwerze). W celu pobrania aktualizacji, klienci mogą być kierowani do serwera SUS zawierającego odpowiednią listę zatwierdzonych aktualizacji.
- **Topologia o ścisłej zależności — nadrzędny/podrzędny** Nadrzędny serwer SUS synchronizuje dane z usługą Windows Update i przechowuje aktualizacje w folderze lokalnym. Następnie administrator zatwierdza aktualizacje. Inne serwery SUS przedsiębiorstwa synchronizują dane z serwerem nadrzędnym. Ustawienia takie można określić na stronie *Set Options* zaznaczając opcję **Synchronize List Of Approved Updates From "Hus Location (Replace Mode)**. Opcja ta powoduje, że podrzędne serwery SUS synchronizują dane z serwera nadrzędnego (zarówno pliki, jak i listę zatwierdzonych aktualizacji). Następnie można skonfigurować komputery klienta w sieci, aby aktualizacje pobierane były z najbliższego serwera. W tej konfiguracji (**Synchronize List Of Approved Items**) administratorzy podrzędnych serwerów SUS *nie mogą* zatwierdzać aktualizacji. Zadania te wykonywane są jedynie na nadrzędnym serwerze SUS.
- **Topologia o słabej zależności — nadrzędny/podrzędny** Nadrzędny serwer SUS synchronizuje dane z usługą Windows Update i przechowuje aktualizacje w folderze lokalnym. Inne serwery SUS przedsiębiorstwa synchronizują dane z serwerem nadrzędnym. Inaczej niż dla ścisłej zależności, dodatkowe serwery SUS nie synchronizują listy zatwierdzonych aktualizacji, dzięki czemu administratorzy tych serwerów mogą niezależnie zatwierdzać lub odrzucać poszczególne aktualizacje. Chociaż topologia ta zwiększa zakres pracy administracji, jest przydatna, gdyż minimalizuje obciążenie połączenia do sieci Internet (tylko serwer nadrzędny łączy się z Internetem), a także zapewnia (tak jak dla modelu wieloserwerowego) elastyczność przy dystrybucji aktualizacji oraz umożliwia stosowanie różnorodnych konfiguracji pakietów aktualizacji.
- **Topologia typu test/produkcja** Model ten umożliwia organizacji testowanie i weryfikację działania aktualizacji. Nadrzędny serwer SUS pobiera aktualizacje z usługi Windows Update, a administrator zatwierdza je do testów. Jeden lub kilku klientów pobiera te aktualizacje z serwera nadrzędnego SUS i przeprowadza ich testy. Po zatwierdzeniu, przetestowaniu i sprawdzeniu dane serwera nadrzędnego zostają skopiowane do ręcznie utworzonego punktu dystrybucji danych na drugim serwerze IIS. Produkcyjne serwery SUS synchronizują aktualizacje i listę zatwierdzonych aktualizacji z danymi w punkcie dystrybucji. Etapy ręcznej konfiguracji punktu dystrybucji są szczegółowo opisane w raporcie *Software Update Service Deployment White Paper*, dostępnym w witrynie Microsoft SUS Web.

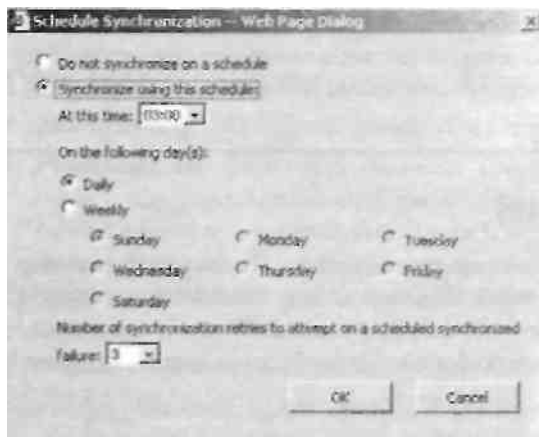
Synchronizacja usługi SUS

Na stronie *SUS Administration Web* należy kliknąć polecenie **Synchronize Server** (synchronizacji serwera). Wyświetlana strona pokazana została na rysunku 9-3. Użytkownik może uruchomić synchronizację ręcznie lub skonfigurować harmonogram synchronizacji automatycznej. Kliknięcie przycisku **Synchronize Now** uruchamia synchronizację, a po jej zakończeniu użytkownik zostanie poinformowany o jej przebiegu (o powodzeniu lub o niepowodzeniu operacji) i jeśli synchronizacja przebiegła prawidłowo, uruchomiona zostanie strona **Approve Updates** (aktualizacje zatwierdzone).



Rysunek 9-3 Strona *Synchronize Server*

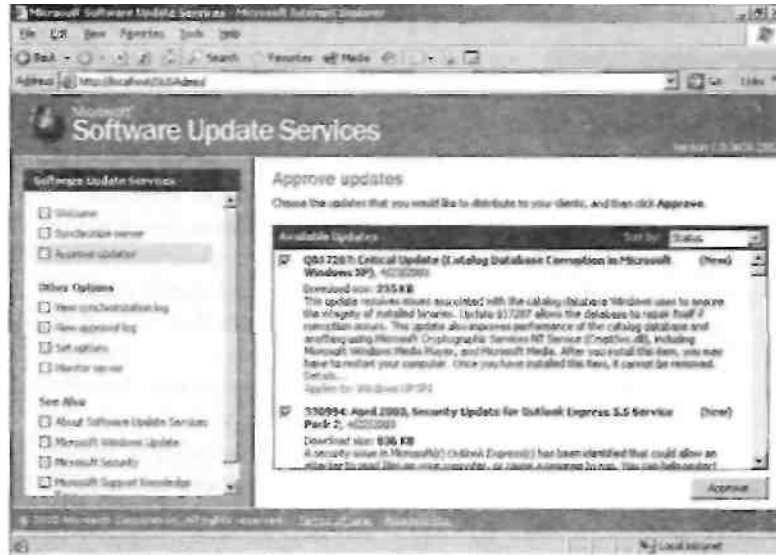
Aby zdefiniować harmonogram synchronizacji, należy kliknąć przycisk **Synchronization Schedule**. Można określić dzień i godzinę synchronizacji oraz czy operacje wykonywane będą codziennie, co tydzień lub w określony dzień. Okno harmonogramu synchronizacji zostało pokazane na rysunku 9-4. Jeśli określona harmonogramem operacja synchronizacji się nie powiedzie, usługa SUS ponawia próby zgodnie z ustawieniem opcji **Number Of Synchronization Retries To Attempt**. Próby przeprowadzania synchronizacji ponawiane są co 30 minut.



Rysunek 9-4 Strona *Schedule Synchronization Web Page Dialog* (Harmonogram synchronizacji — okno dialogowe sieci Web)

Zatwierdzanie aktualizacji

Aby zatwierdzić aktualizacje rozprowadzane wśród klientów, należy kliknąć polecenie **Approve Updates** znajdujące się w pasku nawigacyjnym po lewej stronie ekranu. Wyświetlona zostanie strona *Approve Updates*, tak jak przedstawia to rysunek 9-5. Należy zaznaczyć aktualizacje, która ma być zatwierdzona i kliknąć przycisk **Approve** (zatwierdź). Jeśli użytkownik nie jest pewny, jakie zastosowanie ma wybrana aktualizacja, może kliknąć odsyłacz **Details** (szczegóły) znajdujący się w ramce podsumowania aktualizacji. Kliknięcie odsyłacza otwiera stronę *Details* zawierającą odnośniki do rzeczywistych plików *.cab używanych podczas instalowania pakietu oraz odnośniki do strony *ReadMore* (informacje dodatkowe) dotyczącej wybranej aktualizacji, które otwierają odpowiedni artykuł w dziale Microsoft Knowledge Base.



Rysunek 9-5 Strona *Approve Updates*



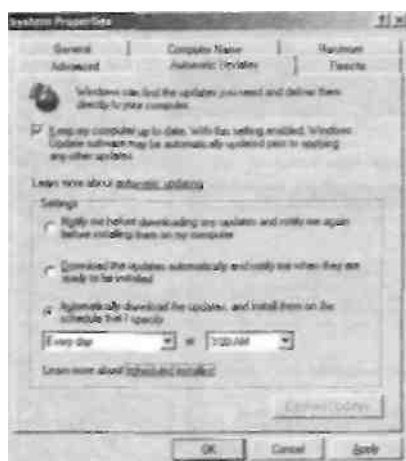
Wskazówka Pierwsza aktualizacja pobiera dziesiątki plików. Przewijanie i klikanie każdego pola wyboru może być nużące. Zamiast tego można, po kliknięciu pierwszego pola wyboru, nacisnąć dwukrotnie przycisk TAB, aby przejść do następnego pola wyboru i nacisnąć przycisk spacji, aby zaznaczyć (lub usunąć zaznaczenie) danej pozycji.

Klient aktualizacji automatycznej

Usługa *Windows Automatic Updates* (Aktualizacje automatyczne) to komponent klienta usługi SUS, który jest obsługiwany w systemach Windows 2000, Windows XP oraz Windows Server 2003. Klient usługi *Automatic Updates* (Aktualizacje automatyczne) dołączony został do Windows Server 2003, do dodatku Service Pack 3 systemu Windows 2000 oraz do dodatku Service Pack 1 w systemie Windows XP.

Dla klientów wcześniejszych wersji obsługiwanych platform, usługę *Automatic Updates* można pobrać w postaci autonomicznego klienta z witryny Microsoft SUS Web o adresie <http://go.microsoft.com/fwlink?LinkID=6930>. Klient udostępniany jest jako plik .msi i może być instalowany na komputerze autonomicznym, poprzez zasadę grupy przypisując pakiet zasadzie znajdującej się w węźle *Computer Configuration\Software Settings* (Konfiguracja komputera\Ustawienia oprogramowania), poprzez usługę SMS, lub nawet poprzez skrypty logowania. Jeśli wersja regionalna klienta nie jest dostępna, na dowolnej wersji regionalnej należy zainstalować wersję angielską.

Klient usługi *Automatic Updates* systemu Windows Server 2003 został tak skonfigurowany, aby automatycznie łączyć się z serwerem usługi Microsoft Windows Update i pobierać aktualizacje, a następnie proponować użytkownikowi zainstalowanie pobranych aktualizacji. Działanie to może być modyfikowane, a odpowiednie opcje wybierane są na zakładce *Automatic Updates* (Aktualizacje automatyczne) w oknie dialogowym *System Properties* (Właściwości systemu) dostępnym w programie Control Panel (Panelu sterowania) systemów Windows XP oraz Windows Server 2003. W systemie Windows 2000 należy kliknąć ikonę Automatic Updates (Aktualizacje automatyczne) w programie *Control Panel*. Zakładka *Automatic Updates* pokazana została na rysunku 9-6. Usługa *Automatic Updates* może być również konfigurowana przy użyciu obiektów GPO lub wartości rejestru.



Rysunek 9-6 Zakładka *Automatic Updates* (Aktualizacje automatyczne) okna dialogowego *System Properties* (Właściwości systemu)

Tryby pobierania aktualizacji

Usługa *Automatic Updates* obsługuje dwa tryby pobierania aktualizacji:

- **Automatyczny** Aktualizacje pobierane są bez powiadamiania użytkownika.
- **Powiadamiania** Jeśli usługa *Automatic Updates* (Aktualizacje automatyczne) została skonfigurowana, aby powiadamiać użytkownika przed rozpoczęciem pobierania aktualizacji, rejestruje powiadomienia o dostępnych aktualizacjach w dzienniku zdarzeń systemu i powiadamia administratora wyświetlając informację w obszarze powiadomień paska narzędzi systemu. Jeśli użytkownik o uprawnieniach administratora nie jest zalogowany na komputerze, usługa wstrzymuje powiadamianie.

Po rozpoczęciu pobierania aktualizacji funkcja *Automatic Updates* korzysta z usługi BITS (Background Intelligent Transfer Service), aby przeprowadzić transfer plików wykorzystując okresy bezruchu w sieci. Usługa BITS zapewnia, że wydajność sieci nie zostanie zmniejszona podczas transferu plików aktualizacji. Wszystkie poprawki są sprawdzane przez serwer SUS, czy zostały prawidłowo podpisane przez firmę Microsoft. Podobnie klient usługi *Automatic Updates* przed instalacją sprawdza podpis firmy Microsoft i weryfikuje sumę kontrolną CRC każdego pakietu.

Opcje instalacji

Funkcja *Automatic Updates* udostępnia dwie opcje instalacji:

- **Powiadomienie** Funkcja *Automatic Updates* rejestruje zdarzenie w dzienniku systemu informujące o tym, że aktualizacje są gotowe do zainstalowania. Powiadomienie jest wstrzymywane do momentu zalogowania się administratora lokalnego. Jeśli administrator zaloguje się w systemie, usługa wyświetli informację w obszarze powiadomień paska narzędzi systemu. Administrator następnie klika ikonę powiadomienia (lub „chmurkę”) i może zdecydować, które aktualizacje powinny być zainstalowane. Jeśli aktualizacja wymaga ponownego uruchomienia komputera, funkcja *Automatic Updates* (Aktualizacje automatyczne) do momentu ponownego uruchomienia nie potrafi wykryć dodatkowych aktualizacji, które mogłyby być zainstalowane.
- **Automatyczna (Zaplanowana)** Po poprawnym pobraniu aktualizacji w dzienniku systemu dokonywany jest odpowiedni wpis. Jeśli administrator jest zalogowany na komputerze, pojawia się ikona powiadomienia i administrator może w dowolnym momencie, do momentu określonego harmonogramem instalacji, ręcznie rozpocząć instalację.

W momencie określonym harmonogramem instalacji, administrator, który jest zalogowany, przed rozpoczęciem instalacji zostanie powiadomiony poprzez wyświetlenie komunikatu. W oknie komunikatu odliczany jest czas do rozpoczęcia instalacji, a administrator może jeszcze anulować instalację. W takim przypadku instalacja zostanie opóźniona do następnego momentu określonego harmonogramem. Jeśli zalogowany jest użytkownik, który nie posiada uprawnień administracyjnych, wyświetlone zostanie ostrzegawcze okno dialogowe, ale użytkownik nie może opóźnić instalacji. Jeśli w danym momencie w systemie nikt nie jest zalogowany, instalacja przebiega automatycznie. Jeśli aktualizacja wymaga ponownego uruchomienia komputera, wyświetlany jest komunikat informujący, że po upływie 5 minut rozpocznie się ponowne uruchamianie komputera. Proces ten może zatrzymać jedynie użytkownik mający uprawnienia administratora.

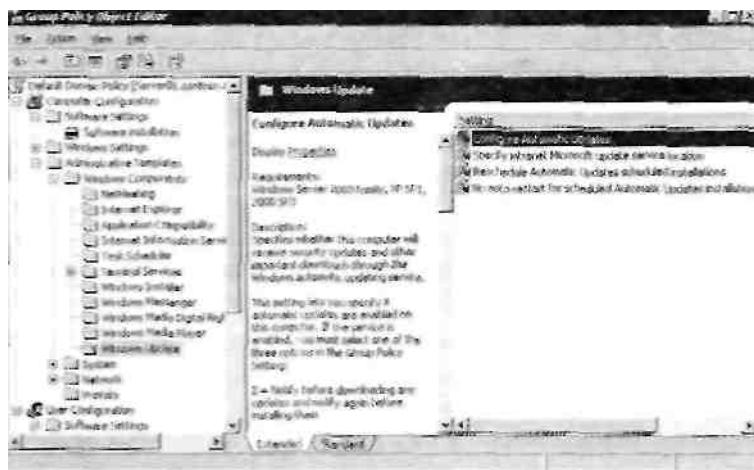


Wskazówka Jeśli w momencie instalacji określonym harmonogramem usługi *Automatic Update** (Aktualizacje automatyczne) komputer był wyłączony, instalacja będzie wykonana zgodnie z harmonogramem. Przy określaniu harmonogramu instalacji należy wybierać okresy, w których komputer będzie prawdopodobnie włączony.

Konfigurowanie funkcji *Automatic Updates* za pomocą Zasad grupy

Ustawienia domyślne określają, że klient usługi *Automatic Updates* (Aktualizacje automatyczne) łączy się z serwerem usługi Microsoft Windows Update. Po zainstalowaniu w przedsiębiorstwie usług SUS, poprzez ręczne skonfigurowanie rejestru klienta lub poprzez wykorzystanie zasad grupy usługi Windows Update, można spowodować, by funkcja *Automatic Updates* łączyła się z określonymi serwerami intranetu.

Aby przy użyciu obiektów GPO skonfigurować usługę *Automatic Updates*, należy otworzyć obiekt GPO i przejść do węzła **Computer Configuration\Administrative Templates\Windows Components\Windows Update** (Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows¹, Aktualizacje systemu Windows). Omawiane zasady usługi Windows Update pokazane zostały na rysunku 9-7.



Rysunek 9-7 Zasady usługi Windows Update



Informacja Jeśli zasada edytowana jest na serwerze usługi Active Directory systemu Windows 2000 Active Directory, zasady mogą nie być wyświetlane. Zasady funkcji *Automatic Updates* są opisane przez szablon administracyjny %Windir%\Inf\Wuau.inf, który jest instalowany w sposób domyślny podczas instalowania usługi *Automatic Updates*. Jeśli usługa nie została zainstalowana na kontrolerze domeny, do którego system został podłączony (najczęściej jest to emulator PDC), należy kliknąć prawym przyciskiem myszy węzeł **Administrative Templates** (Szablony administracyjne) i wybrać polecenie **Add/Remove Templates** (Dodaj lub usuń szablon), a następnie znaleźć szablon **Wuau.inf** (być może poprzez skopiowanie go z systemu, na którym zainstalowane zostały usługi *Automatic Updates*).

Poniżej wymienione zostały dostępne zasady odgrywające ważną rolę przy konfigurowaniu sprawnej dystrybucji aktualizacji w przedsiębiorstwie:

- **Configure Automatic Updates (Konfigurowanie aktualizacji automatycznych)** Ustawienie to określa działanie klienta usługi *Automatic Updates*. Możliwe są trzy opcje: **Notify For Download And Notify For Install** (Powiadom przed pobraniem aktualizacji i powiadom przed ich zainstalowaniem), **Auto Download And Notify For Install** (Pobierz aktualizacje automatycznie i powiadom, gdy są gotowe do zainstalowania) oraz **Auto Download And Schedule The Install** (Automatycznie pobierz aktualizacje i zainstaluj je według harmonogramu). Opcje te są połączeniem działania instalacji i pobierania opisywanego w poprzednich fragmentach lekcji.
- **Reschedule Automatic Updates Scheduled Installations (Zaplanuj ponownie zaplanowane instalacje aktualizacji automatycznej)** Jeśli instalacja została zaplanowana, a komputer w tym momencie był wyłączony, to usługa będzie czekać do następnego momentu określonego harmonogramem. Zasada ta określona wartościami z przedziału 1 do 60 powoduje, że usługa *Automatic Updates* powtarza instalację po określonej liczbie minut od momentu uruchomienia komputera.
- **No Auto-Restart For Scheduled Automatic Updates Installations (Bez automatycznego uruchamiania ponownego dla zaplanowanych instalacji aktualizacji automatycznych)** Zasada ta powoduje, że usługa *Automatic Updates* rezygnuje z wymaganego przez zainstalowaną aktualizację ponownego uruchomienia komputera, jeśli użytkownik jest zalogowany w systemie. Zamiast tego, użytkownik jest powiadamiany, że do zakończenia instalacji wymagane jest ponowne uruchomienie komputera, a decyzję o ponownym uruchamianiu systemu podejmie użytkownik. Warto zapamiętać, że usługa *Automatic Updates* nie potrafi wykrywać następnych aktualizacji, dopóki nie nastąpi ponowne uruchomienie komputera.
- **Specify Intranet Microsoft Update Service Location (Określ lokalizację intranetową firmy Microsoft)** Zasada ta umożliwia przekierowanie funkcji *Automatic Updates* do serwera, na którym uruchomiona jest usługa SUS. Ustawienia domyślnie określają, że klient będzie rejestrował swoje interakcje na serwerze SUS, do którego jest podłączony. Zasada ta pozwala jednak kierować klientów do innego serwera IIS w celu przechowywania statystyk. W ten sposób klienci mogą pobierać aktualizacje z lokalnego serwera SUS, natomiast wszyscy klienci mogą przechowywać statystyki usługi SUS w pojedynczej lokalizacji dla łatwiejszego uzyskiwania i analizy danych dziennika, które są przechowywane jako część dziennika usługi IIS. Dzienniki IIS najczęściej przechowywane są w folderze %Windir%\o\System32\Logfiles\W3svc1.

Funkcja *Automatic Updates* (Aktualizacje automatyczne) sprawdza serwery SUS co 22 godziny (minus przypadkowe przesunięcie).

Żadne opóźnienie instalowania poprawek nie powinno być dopuszczone, jeśli luka w zabezpieczeniach zaczęła być wykorzystywana. W takiej sytuacji należy zainstalować poprawki ręcznie, nie czekając na proces automatycznego sprawdzania, pobierania i instalowania poprawek.

Po pobraniu z serwera SUS zatwierdzonych aktualizacji, zostaną one zainstalowane tak, jak były skonfigurowane - ręcznie lub automatycznie w zaplanowanym terminie. Jeśli zatwierdzona aktualizacja stała się z czasem aktualizacją niezatwierdzoną, nie będzie instalowana. Nie będzie również instalowana przez dodatkowe programy klienckie. Zainstalowana aktualizacja *może być* odinstalowana ręcznie za pomocą modułu **Add Or Remove Programs** (Dodaj lub usuń programy) w programie **Control Panel** (Panel sterowania).

Rozwiązywanie problemów usługi SUS

Pomimo, że usługa SUS funkcjonuje prawidłowo, zdarzają się sytuacje, kiedy zachodzi konieczność monitorowania i rozwiązywania problemów dotyczących SUS.

Monitorowanie usługi SUS

Na stronie *Monitor Server witryny SUS Administration Web* wyświetlane są statystyki informujące o liczbie aktualizacji dostępnych dla każdej platformy oraz data i godzina powstania ostatniej aktualizacji. Jest to podsumowanie metadanych usługi Windows Update, które zostało pobrane w czasie trwania każdej synchronizacji. Metadane są zapisywane na dysku i przechowywane w pamięci dla zwiększenia wydajności obsługi żądań aktualizacji odpowiednich dla różnych platform.

Usługi SUS i *Automatic Updates* (Aktualizacje automatyczne) mogą być również monitorowane przy użyciu następujących dzienników:

- **Dziennik synchronizacji** Na podstawie tego dziennika można uzyskać informacje o bieżącej lub o poprzednich synchronizacjach oraz o konkretnych pakietach, które zostały pobrane. Informacje są wyświetlane poprzez kliknięcie polecenia **View Synchronization Log** (przeglądanie dziennika synchronizacji) znajdującego się w pasku nawigacyjnym z lewej strony ekranu. Użytkownik może również za pomocą dowolnego edytora tekstowego bezpośrednio w witrynie SUS Web otworzyć bazę danych opartą na XML (Extensible Markup Language). Jest to plik *History-Sync.xml* znajdujący się w katalogu *\AutoUpdate\Administration* programu IIS.
- **Dzienniki zatwierdzania** Aby uzyskać informacje o pakietach, które zostały zatwierdzone, należy kliknąć dziennik **View Approval Log** (przeglądanie dziennika zatwierdzania) znajdującego się w pasku nawigacyjnym z lewej strony ekranu. Innym sposobem jest otwarcie w witrynie SUS Web pliku *History-Sync.xml* przechowywanego w katalogu *\AutoUpdate\Administration* programu IIS.
- **Dziennik usługi Windows Update** Klient usługi *Automatic Updates* rejestruje czynności w pliku *%Windir%\Windows Update.log* przechowywanym na lokalnym dysku systemu klienta,
- **Wutrack.bin** Współdziałanie programu klienta z usługą SUS jest protokolowane w określonych statystykach dzienników programu usługi IIS. Najczęściej przechowywane są one w folderze: *%Windir%\System32\Logfiles\W3svc*. Te obszerne i mało czytelne dzienniki zaprojektowane zostały dla analizy programowej, a nie bezpośrednio przez użytkownika.



Wskazówka egzaminacyjna Chociaż osoba przystępująca do egzaminu powinna wiedzieć, które dzienniki są dostępne oraz gdzie są przechowywane, to na egzaminie 70-290 nie trzeba interpretować zagadkowych komunikatów i wpisów dziennika. Raport *SUS Deployment White Paper* zawiera dodatki szczegółowo informujące o opisach zdarzeń i składni dzienników.

Zdarzenia dziennika System usługi SUS

Usługa synchronizacji generuje komunikaty dziennika zdarzeń dla każdej synchronizacji wykonywanej przez serwer oraz podczas zatwierdzania aktualizacji. Komunikaty te mogą być przeglądane w dzienniku *System* przy użyciu programu **Event Viewer** (Podgląd zdarzeń). Zdarzenia odnoszą się do następujących sytuacji:

- **Połączenie nie zostało uzyskane** Funkcja Automatic Updates nie mogła połączyć się z usługą aktualizacji (rozszerzenie Windows Update lub serwer SUS przydzielony do tego komputera).
- **Gotowość instalacji - brak harmonogramu** Aktualizacje zarejestrowane w dzienniku zostały pobrane i oczekują na zainstalowanie. Administrator musi kliknąć ikonę powiadomienia, a następnie uruchomić instalację.
- **Gotowość instalacji — zgodnie z harmonogramem** Aktualizacje wymienione w zdarzeniu zostały pobrane i zostaną zainstalowane w dniu i o godzinie określonej w zdarzeniu.
- **Prawidłowa instalacja** Aktualizacje wymienione w zdarzeniu zostały prawidłowo zainstalowane.
- **Nieprawidłowa instalacja** Nic powiodła się instalacja aktualizacji wymienionych w zdarzeniu.
- **Wymagane ponowne uruchomienie - brak harmonogramu** Aktualizacja wymaga ponownego uruchomienia. Jeśli konfiguracja działania instalacji zakłada powiadomienie, ponowne uruchomienie instalacji musi być wykonane ręcznie. System Windows nie może wyszukiwać nowych aktualizacji dopóki nie zostanie ponownie uruchomiony.
- **Wymagane ponowne uruchomienie - zgodnie z harmonogramem** Jeśli usługa Automatic Updates (Aktualizacje automatyczne) została tak skonfigurowana, aby automatycznie instalowała aktualizacje, to zdarzenie zostanie zaprotokołowane w sytuacji, kiedy aktualizacja wymaga ponownego uruchomienia. Ponowne uruchomienie komputera nastąpi po upływie 5 minut. System Windows nie może wyszukiwać nowych aktualizacji dopóki nie zostanie ponownie uruchomiony.

Rozwiązywanie problemów związanych z usługą SUS

Rozwiązywanie problemów związanych z usługą SUS (Software Update Services) uruchomioną na komputerze systemu Windows Server 2003 może wymagać przeprowadzenia następujących działań:

- **Ponowne pobranie zawartości bufora** Jeśli nowe aktualizacje nie pojawiły się od momentu ostatniej synchronizacji serwera, może to być spowodowane po prostu brakiem nowych aktualizacji. Jest jednak również możliwe, że nowe aktualizacje nie zostały poprawnie pobrane do bufora. Na witrynie administracji usługi SUS należy kliknąć polecenie Monitor Server, a następnie przycisk Refresh.
- **Ponowne uruchomienie usługi synchronizacji** Jeśli pojawiają się komunikaty informujące, że usługa synchronizacji nie działa prawidłowo lub jeśli nie jest możliwa modyfikacja ustawień na stronie Set Options witryny administracji, należy otworzyć przystawkę konsoli MMC — Services (Usługi) i kliknąć prawym przyciskiem myszy węzeł Software Update Services Synchronization Service (Usługa synchronizacji aktualizacji oprogramowania), a następnie kliknąć polecenie Restart (Uruchom ponownie).
- **Ponowne uruchomienie usługi IIS** Jeśli nie można połączyć się z witryną administracji lub jeśli klienci nie mogą połączyć się do serwera SUS, należy w ten sam sposób ponownie uruchomić usługę World Wide Web Publishing Service (Usługa publikowania w sieci Web).

Jeśli wygląda na to, że klienci usługi *Automatic Updates* nie odbierają poprawnie aktualizacji, należy otworzyć rejestr systemu klienta i upewnić się, że następujące wartości zostały określone w kluczu HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate:

- **WUServer** Powinien być wpisany adres URL serwera SUS, na przykład http://SUS_Servername
- **WUStatusServer** Powinien być wpisany adres URL tego samego serwera SUS lub innego serwera IIS, na którym protokołowane są statystyki synchronizacji oraz w podkluczu AU:
- **UseWUServer** Powinna być określona wartość dword:00000001

Kopia zapasowa i przywracanie usługi SUS

Tak samo, jak dla innych ról i aplikacji serwera należy przewidzieć sposób przywrócenia systemu po ewentualnej jego awarii.

Wykonywanie kopii zapasowej usługi SUS

Aby wykonać kopię zapasową usługi SUS, należy skopiować folder, który zawiera dane usługi SUS, witrynę SUS Administration Web oraz metabazę usługi IIS.



Wskazówka egzaminacyjna Procedura opisująca wykonywanie kopii zapasowej metabazy IIS jest przydatna nie tylko podczas kopiowania usługi SUS, ale również podczas wykonywania kopii zapasowych innych witryn sieci Web lub aplikacji uruchomionych w systemie Windows Server 2003 i IIS 6.0.

W pierwszym kroku należy skopiować metabazę, czyli bazę danych XML zawierającą konfigurację usługi IIS. Przy użyciu przystawki *IIS* konsoli MMC należy zaznaczyć serwer, którego kopia zapasowa ma zostać wykonana i w menu **Action** (Akcja) wybrać kolejno polecenia **All Tasks** (Wszystkie zadania) i **Backup/Restore Configuration** (Wykonaj kopię zapasową/Odtwórz konfigurację). Następnie należy kliknąć przycisk **Create Backup** (Utwórz kopię zapasową) oraz wprowadzić nazwę dla tworzonej kopii. Po kliknięciu przycisku OK zostanie wykonana kopia zapasowa metabazy.

Następnie, za pomocą programu **Ntbackup** lub innego programu wykonywania kopii zapasowych, należy utworzyć kopie zapasowe następujących elementów:

- Domyślna witryna sieci Web, która przechowywana jest w katalogu <C:\inetpub\Wwwroot> (chyba, że zostało to inaczej skonfigurowane).
- Witryna SUS Administration Web. Domyślne ustawienia określają, że moduł SUSAdmin jest podfolderem <C:\inetpub\Wwwroot>. W takim przypadku, zostanie on skopiowany podczas wykonywania kopii zapasowej domyślnej witryny sieci Web.
- Katalog wirtualny AutoUpdate. Również i on jest domyślnie podfolderem <C:\inetpub\Wwwroot>.
- Lokalizacja danych usługi SUS określona podczas instalacji lub konfiguracji usługi. Lokalizację danych usługi SUS można sprawdzić w menedżerze IIS. W tym celu należy kliknąć węzeł Default Web Site (Domyślna witryna sieci Web) i w oknie szczegółów sprawdzić ścieżkę wirtualnego katalogu głównego Content (Dane).

Katalog kopii zapasowej metabazy %Windir%\System32\Inetsrv\Metaback, który zawiera kopię metabazy wykonanej wcześniej.



Zobacz także Informacje dodatkowe dotyczące programu Ntbackup można znaleźć w rozdziale 7.

Procedura wykonywania kopii zapasowych metabazy, a następnie komponentów usługi SUS powinna być przeprowadzana regularnie, ponieważ aktualizacje są dodawane i zatwierdzane z określoną częstotliwością.

Odtwarzanie serwera SUS

Aby odtworzyć uszkodzony serwer SUS, należy wykonać opisaną poniżej procedurę. Jeśli niektóre kroki procedury nie są konieczne, można je pominąć, ale należy pamiętać o zachowaniu podanej kolejności.

1. Odłącz serwer od sieci, aby zapobiec atakowi wirusów.
2. Zainstaluj system Windows Server 2003 i sprawdź, czy została określona taka sama, jak poprzednio nazwa serwera.
3. Zainstaluj usługę IIS wraz z takimi samymi komponentami, jak poprzednio.
4. Zainstaluj najnowsze dodatki SerWce Pack oraz poprawki zabezpieczeń. Jeśli wykonanie tego etapu wymaga podłączenia serwera do sieci, należy przedsięwziąć wszystkie możliwe środki ostrożności, aby zapobiec niepotrzebnemu „zdemaskowaniu” serwera.
- 5- Zainstaluj usługę SUS w tym samym, co poprzednio folderze.
6. Uruchom program **Ntbackup**, aby odtworzyć najnowsze kopie zapasowe usługi SUS. Operacje przywracania powinny dotyczyć foldera danych usługi SUS, domyślnej witryny sieci Web, katalogów wirtualnych SUSAdmin i AutoUpdate oraz kopii zapasowej metabazy.
- 7- Otwórz przystawkę *IIS* konsoli MMC i zaznacz serwer, który ma zostać odtworzony. W menu **Action** (Akcja) wybierz polecenie **All Tasks** (Wszystkie zadania). Następnie wybierz polecenie **Backup/Restore Configuration** (Wykonaj kopię zapasową/Odtwórz konfigurację) i zaznacz kopię zapasową, która została właśnie odtworzona. Kliknij przycisk **Restore** (Przywróć).
8. Sprawdź poprawność odtwarzania otwierając witrynę *SUS Administration Web* i klikając polecenie **Set Options**. Sprawdź, czy poprzednie ustawienia zostały odtworzone oraz czy poprzednio zatwierdzone aktualizacje w dalszym ciągu mają taki sam status.



Informacja Powyższa procedura dotyczy wyłącznie systemu Windows Server 2003. Jeśli zachodzi potrzeba odtworzenia serwera SUS uruchomionego w oparciu o system Windows 2000, odpowiednią procedurę należy odszukać w dokumentacji usługi SUS.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Administrator konfiguruje infrastrukturę usługi SUS (Software Update Services). Jeden serwer synchronizuje metabazę oraz dane z usługą Windows Update. Inne serwery (jeden w każdej lokacji) synchronizują dane z nadrzędnym serwerem SUS. Które z wymienionych poniżej czynności są wymagane, aby zakończyć konfigurację infrastruktury usługi SUS?
 - a. Skonfigurowanie w każdym systemie klientów usługi Automatic Updates (Aktualizacje automatyczne) przy użyciu programu Control Panel (Panel sterowania)
 - b. Skonfigurowanie obiektów GPO tak, aby kierowały programy klienckie do serwera SUS znajdującego się w danej lokacji
 - c. Skonfigurowanie ręcznego punktu dystrybucji danych
 - d. Zatwierdzenie aktualizacji przy użyciu strony administracyjnej usługi SUS
2. Administrator konfiguruje usługę SUS dla grupy serwerów sieci Web tak, aby serwery sieci Web same aktualizowały się w godzinach nocnych w oparciu o listę zatwierdzonych aktualizacji serwera SUS. Jednakże należy tak skonfigurować usługę, aby nie miała wpływu na, wykonywane również w nocy, prace administratora serwera sieci Web (w kontekście możliwości ponownego uruchamiania serwera po zainstalowanych aktualizacjach). Którą konfigurację zasady usługi Windows Update należy użyć w tej sytuacji?
 - a. Notify For Download And Notify For Install (Powiadom przed pobraniem aktualizacji i powiadom przed ich zainstalowaniem)
 - b. Auto Download And Notify For Install (Pobierz aktualizacje automatycznie i powiadom, gdy są gotowe do zainstalowania)
 - c. Auto Download And Schedule The Install (Automatycznie pobierz aktualizacje i zainstaluj je według harmonogramu)
3. Administrator konfiguruje systemy klientów sieci oraz harmonogram instalacji usługi Automatic Updates (Aktualizacje automatyczne) tak, aby automatycznie pobierały i instalowały aktualizacje w godzinach nocnych- Jednakże niektórzy użytkownicy wyłączają komputery na noc i na tych komputerach aktualizacje nie mogą zostać przeprowadzone. Która zasada pozwala naprawić zaistniałą sytuację bez konieczności zmiany harmonogramu instalacji?
 - a. Specify Intranet Microsoft Update Service Location (Określ lokalizację intranetową firmy Microsoft)
 - b. No Auto-Restart For Scheduled Automatic Updates Installations (Bez automatycznego uruchamiania ponownego dla zaplanowanych instalacji aktualizacji automatycznych)
 - c. Reschedule Automatic Updates Scheduled Installations (Zaplanuj ponownie zaplanowane instalacje aktualizacji automatycznej)
 - d. Configure Automatic Update (Konfigurowanie aktualizacji automatycznych)

Podsumowanie lekcji

- Usługa SUS jest aplikacją sieci intranet uruchamianą na serwerze IIS 6.0 (lub IIS 5.0 w systemie Windows 2000 Server) i jest zarządzana w oparciu o witrynę administracyjną sieci Web: http://SUS_Servername/SUSAdmin.
- Serwer SUS synchronizuje informacje dotyczące krytycznych aktualizacji i poprawek zabezpieczeń oraz umożliwia konfigurowanie i centralne zatwierdzanie każdej aktualizacji. Serwery SUS w przedsiębiorstwie są najczęściej konfigurowane tak, aby również pobierały pliki aktualizacji.
- Funkcja Automatic Updates (Aktualizacje automatyczne) uruchamiana w systemach Windows 2000, Windows XP oraz Windows Server 2003 jest odpowiedzialna za pobieranie i instalowanie aktualizacji na systemach klienta.
- Zasada grupy może być używana do konfigurowania funkcji Automatic Updates (Aktualizacje automatyczne) tak, aby usługa ta pobierała poprawki z serwera SUS, a nie z serwerów rozszerzenia Windows Update. Również obiekty GPO mogą określać działanie komputerów klienta związane z pobieraniem i instalowaniem aktualizacji oraz ponownym uruchamianiem systemów po zainstalowaniu poprawek.

Lekcja 2: Pakiety serwisowe

Firma Microsoft opracowuje dodatki Service Packs w celu skonsolidowania podstawowych aktualizacji, poprawek zabezpieczeń, uzupełnień, aktualizacji sterowników oraz usprawnień funkcjonalności. Zgodnie z sugestią wspomnianą na początku rozdziału, nie jest zalecane pomijanie instalacji dodatku Service Pack 2 w oczekiwaniu na pojawienie się dodatku Service Pack 3. Należy stale używać najnowszych pakietów serwisowych, aby zachować bezpieczeństwo i integralność sieci przedsiębiorstwa. Usługa SUS (Software Update Services), omawiana na poprzedniej lekcji, nie obsługuje dystrybucji pakietów serwisowych. Aby w sieci były używane najnowsze wersje i poprawki, należy zapoznać się z metodami instalowania pakietów serwisowych przy użyciu Zasady grupy.

Materiały omówione podczas lekcji pozwalają na

- Pobieranie i rozpakowywanie pakietów serwisowych
- Instalowanie pakietu serwisowego w oparciu o dystrybucję oprogramowania bazującą na zasadzie grupy

Szacunkowy czas lekcji: 5 minut

Pobieranie i rozpakowywanie pakietów serwisowych

Firma Microsoft po opracowaniu pakietu serwisowego udostępnia go na swojej witrynie sieci Web, skąd można go pobrać, a następnie zainstalować. Pakiet serwisowy może być instalowany bezpośrednio z serwera firmy Microsoft. W takim przypadku, program klienta uruchamia instalację pakietu serwisowego na witrynie firmy Microsoft, co powoduje pobranie niedużego programu instalacyjnego do komputera klienta. Program ten ponownie łączy się z serwerem firmy Microsoft i kontroluje pobieranie i instalowanie całego pakietu serwisowego. Pakiety serwisowe są pokaźnych rozmiarów i dlatego, za wyjątkiem niedużych środowisk, dystrybucja pakietów w sposób opisany powyżej nie jest wydajna.

Pakiety serwisowe można też otrzymać z firmy Microsoft na CD lub poprzez różne zasoby tej firmy, takie jak TechNet bądź MSDN. CD-ROM dodatków Service Pack często zawierają jeszcze inne programy, takie jak uaktualnione narzędzia administracyjne, nowe szablony zasad oraz inne dodatkowe oprogramowanie. Z tego powodu też zaleca się, aby w przedsiębiorstwie administratorzy zaopatrzyli się w nośniki pakietów serwisowych.

Jeśli nie dysponujemy CD zawierającym pakiet serwisowy i zachodzi potrzeba zainstalowania pakietu na kilku systemach, to z witryny sieci Web firmy Microsoft można pobrać cały pakiet w postaci pojedynczego pliku. Uruchomienie pobranego pliku wykonywalnego (na przykład poprzez dwukrotne kliknięcie) rozpoczyna instalację pakietu serwisowego. Ta pojedyncza wersja pliku wykonywalnego może być też *rozpakowana* do postaci struktury folderów i plików pakietu serwisowego, takiej jaka jest utworzona na CD- Nie jest dołączane dodatkowe oprogramowanie.

Aby rozpakować pakiet serwisowy, należy uruchomić plik w oknie wiersza poleceń wraz z przełącznikiem -x. Przykładowo, aby rozpakować dodatek Windows XP Service Pack 1, należy wpisać **xpspl.exe -x**. Następnie użytkownik zostanie poproszony o podanie foldera, w którym pakiet ma zostać rozpakowany. Po zakończeniu operacji, w docelowym folderze utworzona zostanie pełna struktura folderów

pakietu serwisowego. W tym momencie można uruchomić instalację w ten sam sposób, jak na CD, poprzez dwukrotne kliknięcie pliku I386\Update\Update.exe.

Instalowanie pakietów serwisowych za pomocą zasady grupy

Instalacja dodatku Service Pack wymaga uprawnień administratora komputera lokalnego, chyba że pakiet jest instalowany za pomocą zasady grupy lub serwera SMS (Systems Management Server). Ponieważ pakiet serwisowy dotyczy systemu, należy przydzielać go poprzez zasadę grupy dotyczącą komputera, a nie użytkownika.

Aby dystrybuować pakiet serwisowy, należy utworzyć folder udostępniony i rozpakować w nim pakiet lub skopiować zawartość CD pakietu serwisowego. Następnie, za pomocą przystawki *Active Directory Users And Computers* (Użytkownicy i komputery usługi Active Directory), należy utworzyć lub wybrać istniejący obiekt GPO. Kliknięcie polecenia **Edit** (Edytuj) otworzy konsolę edytora **Group Policy Object Editor** (Edytor obiektu zasady grupy), w którym będzie można modyfikować wybrany obiekt GPO.

Należy rozwinąć węzeł **Computer Configuration\Software Settings** (Konfiguracja komputera\Ustawienia oprogramowania) i prawym przyciskiem myszy kliknąć **Software Installation** (Instalacja oprogramowania), z menu wybrać polecenie **New** (Nowy), a następnie **Package** (Pakiet). W kolejnym kroku należy wprowadzić ścieżkę do pliku pakietu serwisowego **Update.msi**. Należy upewnić się, że używany jest format nazwy UNC (na przykład \\Server\Share), a nie ścieżka lokalnego woluminu typu Napęd\Ścieżka. W oknie dialogowym *Deploy Software* (Rozmieszczanie oprogramowania) należy wybrać polecenie **Assigned** (Przypisany) i zamknąć konsolę edytora *Group Policy Object Editor*. Komputery należące do zakresu obiektu GPO (lokacji, domeny lub jednostki organizacyjnej, z którą zasada jest powiązana) automatycznie zainstalują pakiet serwisowy podczas następnego uruchamiania.



Wskazówka Systemy Windows XP mające skonfigurowaną funkcję *Logon Optimization* (Optymalizacja logowania) mogą wymagać dwukrotnego uruchamiania. Funkcja *Logon Optimization* może być wyłączana poprzez włączenie zasady *Always Wait For The Network At Computer Startup And Logon* (Zawsze czekaj na sieć podczas uruchamiania komputera i logowania). Zasada ta umieszczona jest w ścieżce *ComputerConfiguration\Administrative Templates\System\Logon* (Konfiguracja komputera \Szablony administracyjne\System\Logowanie).

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Którego polecenia należy użyć, aby rozpakować pojedynczy plik pobranego pakietu serwisowego?
 - a. Setup.exe -u
 - b. Update.exe -x
 - c. Update.msi
 - d. <Nazwa_pakietu_serwisowego>.exe -x

2. Który typ rozmieszczania oprogramowania zasady grupy powinien zostać zastosowany do dystrybucji pakietu serwisowego?
 - a. Publikowany w węźle Computer Configuration Software Settings (Konfiguracja komputera, Ustawienia oprogramowania)
 - b. Przypisany w węźle Computer Configuration Software Settings (Konfiguracja komputera, Ustawienia oprogramowania)
 - c. Publikowany w węźle User Configuration Software Settings (Konfiguracja użytkownika, Ustawienia oprogramowania)
 - d. Przypisany w węźle User Configuration Software Settings (Konfiguracja użytkownika, Ustawienia oprogramowania)

Podsumowanie lekcji

- Pakiety serwisowe mogą być rozpakowywane przy użyciu przełącznika -x.
- Zasada grupy może instalować pakiety serwisowe poprzez przypisanie pliku Update.msi w zasadzie dotyczącej ustawień oprogramowania konfiguracji komputera.

Lekcja 3: Zarządzanie licencjami oprogramowania

Akceptacja warunków licencji EULA (*The End User License Agreement*) nie jest jedynie jedną z opcji, którą trzeba zaznaczyć podczas instalowania systemu operacyjnego, aktualizacji bądź programu. Porozumienie EULA jest wiążącą umową, która daje prawo do użytkowania danego oprogramowania. W środowisku przedsiębiorstwa zarządzanie licencjami oprogramowania ma podstawowe znaczenie. Niniejsza lekcja omawia wykorzystanie udostępnionych w systemie Windows Server 2003 narzędzi, które umożliwiają rejestrację oraz monitorowanie licencji i ich zgodności z używanym oprogramowaniem.

Materiały omówione podczas lekcji pozwalają na

- Omówienie trybów licencjonowania Per Server (na serwer) lub Per Device lub Per User (Na urządzenie lub na użytkownika)
- Konfigurowanie licencji przy użyciu właściwości modułu Licensing (licencjonowanie) umieszczonego w programie Control Panel (Panel sterowania) i programu narzędziowego Licensing (Licencjonowanie)
- Tworzenie grup licencji

Szacunkowy czas lekcji: 20 minut



Informacja Wersja testowa systemu Windows Server 2003 Enterprise Edition, dołączana do książki razem z dyskiem CD-ROM, nie obsługuje licencjonowania. Przeprowadzenie ćwiczeń opisywanych w niniejszej lekcji wymaga posiadania pełnej wersji produktu.

Otrzymywanie licencji dostępu klienta CAL

Licencja systemu Windows Server 2003 umożliwia instalowanie systemu operacyjnego na komputerze, ale legalny dostęp do serwera wymaga dla każdego użytkownika lub urządzenia licencji dostępu klienta CAL (*Client Access License*). Licencje CAL otrzymywane są w zestawie i najczęściej, ale nie zawsze, dołączane są podczas zakupu systemu operacyjnego. Należy przechowywać kopie certyfikatów licencji CAL oraz EULA na wypadek inspekcji oprogramowania, jakiej poddane może być przedsiębiorstwo.



Wskazówka Warto zapamiętać, że aktualizacja wersji serwera Windows NT 4 lub Windows 2000 do wersji Windows Server 2003 wymaga również zakupienia aktualizacji licencji CAL.

Licencja CAL jest wymagana dla wszystkich połączeń do systemu Windows Server 2003, które wykorzystują komponenty serwera, wliczając w to usługi plików i drukowania oraz uwierzytelnienie. Bardzo niewiele aplikacji serwera uruchamianych jest tak niezależnie, że licencja CAL nie jest wymagana. Najistotniejszym wyjątkiem odstępstwa wymogu licencji CAL jest niewierzytelniony dostęp do serwera realizowany poprzez sieć Internet. Jeśli podczas dostępu z sieci Internet nie było wymagane przedstawianie poświadczeń tożsamości, jak na przykład podczas przeglądania publikowanej witryny sieci Web, to licencja CAL nie jest wymagana. Z tego powodu licencje CAL nie są wymagane dla wersji systemu Windows Server 2003 Web Edition.

Rozróżniane są dwa rodzaje licencji CAL: licencje *Windows Device CAL*, które umożliwiają połączenie do serwera dla urządzenia, bez względu na to, ile użytkowników wykorzystuje to urządzenie, oraz licencje *Windows User CAL*, które umożliwiają użytkownikowi uzyskanie połączenia do serwera z kilku urządzeń. Licencja *Windows Device CAL* jest przydatna w przedsiębiorstwach, w których kilku użytkowników obsługuje jedno urządzenie, jak na przykład przy pracy zmianowej. Z kolei korzystanie z licencji *Windows User CAL* jest bardziej uzasadnione w organizacjach, której pracownicy uzyskują dostęp do sieci z kilku, niejednokrotnie „nieznanych” urządzeń.



Informacja Narzędzia licencjonowania oraz interfejs użytkownika nie zmienia się w zależności od trybu licencji CAL. Licencja CAL urządzenia jest rejestrowana pośrednio przy użyciu licencjonowania grup.

Wymagana liczba licencji CAL oraz sposób ich śledzenia zależy od zastosowanego trybu licencji dostępu klienta.

Tryb licencjonowania *PerServer* (Na serwer)

Licencjonowanie trybu „Na serwer” wymaga licencji dla każdego połączenia jednoczesnego. Jeśli serwer został skonfigurowany dla 1000 licencji CAL, dostęp dla 1001 połączenia (jednocześnie) zostanie zabroniony. Licencje CAL zostały zaprojektowane do wykorzystywania na konkretnym serwerze, tak więc, jeśli tych samych 1000 użytkowników chce nawiązać jednoczesne połączenie z innym serwerem, należy zakupić kolejne 1000 licencji CAL.

Licencjonowanie trybu „Na serwer” jest przydatne tylko w ograniczonym zakresie, kiedy część wszystkich użytkowników danej sieci uzyskuje dostęp do produktów serwera tylko na niewielu serwerach. Licencjonowanie trybu „Na serwer” jest mniej opłacalne w sytuacji, kiedy wielu użytkowników uzyskuje dostęp do wielu zasobów na kilku serwerach. Jeśli trudno określić, który tryb licencjonowania będzie odpowiedni, lepiej jest wybrać tryb „Na serwer”. Umowa licencyjna dopuszcza jednorazową zmianę trybu licencjonowania z trybu „Na serwer” do trybu „Na urządzenie lub na użytkownika”. Zmiana taka jest bezpłatna i jeśli okaże się, że inne tryby są odpowiedniejsze, można dokonać takiej zmiany.

Tryb licencjonowania *Per-Device or Per-User* (Na urządzenie lub na użytkownika)

Tryb licencjonowania „Na urządzenie lub na użytkownika” różni się od schematu licencjonowania *Per Seat* używanego w poprzednich wersjach systemu Windows. W tym nowym trybie, każde urządzenie lub użytkownik łączący się z serwerem wymaga licencji CAL, ale w oparciu o tę licencję, urządzenie lub użytkownik może łączyć się do kilku serwerów przedsiębiorstwa. Tryb „Na użytkownika lub na urządzenie” został zaprojektowany przede wszystkim dla rozproszonych środowisk, w których wielu użytkowników uzyskuje dostęp do wielu serwerów.

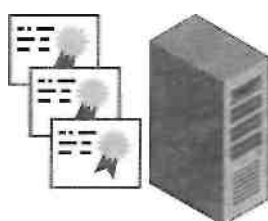
Na przykład, programista używający komputera przenośnego i dwóch komputerów stacjonarnych potrzebuje tylko jednej licencji użytkownika — *Windows User CAL*. Zespół 10 komputerów PC wykorzystywanych przez 30 pracowników zmianowych będzie potrzebował jedynie 10 licencji urządzenia — *Windows Device CAL*.

Całkowita liczba licencji CAL jest równa liczbie urządzeń lub użytkowników (lub też ich kombinacji), którzy uzyskują dostęp do serwerów. Pod pewnymi, jasno określonymi warunkami, licencje CAL mogą być ponownie przydzielane. Na przykład licencja użytkownika, Windows User CAL, może być zabrana pracownikowi zatrudnionemu na stałe i przydzielona pracownikowi pracującemu na czas określony, w okresie nieobecności pracownika zatrudnionego na stałe. Licencja urządzenia, Windows Device CAL, może być przydzielona do wypożyczonego urządzenia, w okresie naprawy urządzenia podstawowego.

Tryby licencjonowania *Per Server* (na serwer) i *Per Device or Per User* (Na urządzenie lub na użytkownika) zostały przedstawione w tabeli 9-1.

Tabela 9-1 Tryby licencjonowania CAL

Per Server (Na serwer)



Tradycyjny tryb licencjonowania „Na serwer”, gdzie występuje niewiele serwerów wymagających ograniczonego dostępu.

Liczba potrzebnych licencji CAL jest określona przez liczbę wymaganych połączeń jednoczesnych.

**Per Device or Per User
(Na urządzenie lub na użytkownika)**



Tradycyjny tryb licencjonowania „Na użytkownika lub na urządzenie”, gdzie występuje wiele serwerów, do których wymagany jest częsty dostęp w szerokim zakresie.

Tryb ten najczęściej jest bardziej opłacalny, kiedy liczba potrzebnych licencji CAL jest określana liczbą użytkowników lub urządzeń (lub ich połączeniem tych liczb), które wymagają dostępu do serwerów.

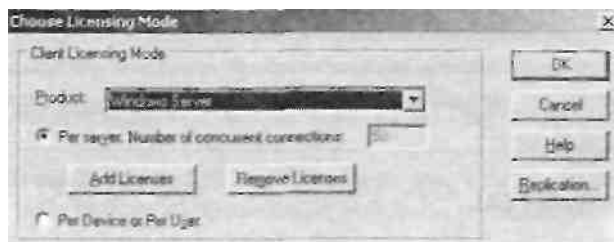


Wskazówka System Windows Server 2003 został wyposażony w usługi terminalowe, nazywane również *Remote Desktop* (Pulpit zdalny). Program *Remote Desktop* obsługuje dwa licencjonowane jednoczesne połączenia dla administratorów, którzy łączą się do serwerów zdalnych. Aby program *Terminal Services* (Usługi terminalowe) działał jako serwer aplikacji, umożliwiając uzyskanie dostępu do obsługiwanych aplikacji zwykłym użytkownikom, należy nabyć licencje *Terminal Services CAL*. Licencje takie są dołączane do systemu Windows XP Professional.

Użytkownik ma do dyspozycji dwa programy narzędziowe, które pomagają śledzić i zarządzać licencjonowaniem oprogramowania:

- **Narzędzie Licensing (Licencjonowanie) w programie Control Panel (Panel sterowania)** Narzędzie **Choose Licensing Mode** (Wybieranie trybu licencjonowania) umieszczone w programie *Control Panel* (Panel sterowania) zarządza wymaganiami licencjonowania dla pojedynczego komputera systemu Windows Server 2003. Okno tego programu zostało pokazane na rysunku 9-8.

Program Licensing (Licencjonowanie) jest używany do dodawania lub usuwania licencji CAL dla serwera działającego w trybie „Na serwer”, do zmiany trybu licencjonowania do trybu „Na urządzenie lub na użytkownika” lub do konfigurowania replikacji licencjonowania.



Rysunek 9-8 *Narzędzie Choose Licensing Mode (Wybieranie trybu licencjonowania) znajdujące się w programie Control Panel (Panel sterowania)*

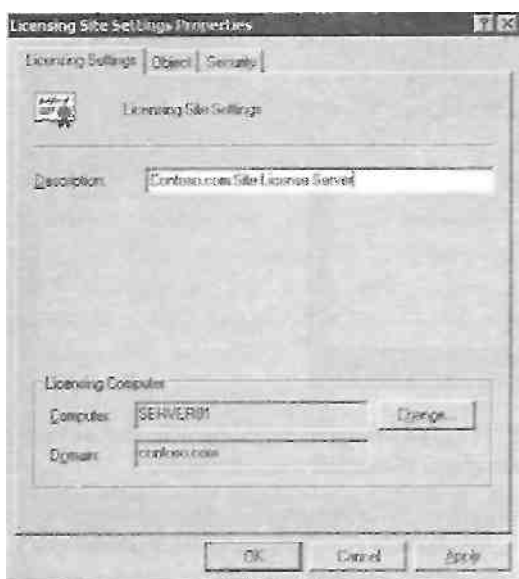
- **Narzędzie Licensing (Licencjonowanie) w grupie programów Administrative Tools (Narzędzia administracyjne)** Narzędzie administracyjne **Licensing (Licencjonowanie)** zostanie omówione w następnej sekcji. Umożliwia ono zarządzanie licencjonowaniem w przedsiębiorstwie poprzez scentralizowanie kontroli oraz poprzez replikację licencji w modelu opartym na lokalacji.

Administracja licencjonowania lokalacji

Usługa *License Logging* (Rejestrowanie licencji), uruchamiana na każdym serwerze systemu Windows Server 2003, przydziela i śledzi licencje podczas uzyskiwania dostępu do zasobów serwera. Dla zapewnienia zgodności, informacje o licencjach są replikowane do centralnej bazy danych licencji znajdującej się na serwerze lokalacji. Serwer ten nazywany jest serwerem licencji. Administrator serwera licencji może wykorzystywać narzędzie **Microsoft Licensing (Licencjonowanie)** znajdujące się w grupie programów **Administrative Tools (Narzędzia administracyjne)**, aby przeglądać i zarządzać licencjami całej lokalacji. Ta nowa funkcja śledzenia i zarządzania licencjami zawiera nie tylko licencje dla usług plików lub drukowania, ale również dla usług *IIS*, *Terminal Services* (usługi terminalowe) czy dla produktów BackOffice takich jak programy Exchange lub SQL Server.

Serwer licencji lokalacji

Serwer licencji lokalacji jest najczęściej pierwszym kontrolerem domeny utworzonym w lokalacji. Aby dowiedzieć się, który serwer jest serwerem licencji dla danej lokalacji, należy otworzyć przystawkę Aft w *Directory Sites And Services* (Lokacje i usługi Active Directory), rozwinąć węzeł, zaznaczyć węzeł lokalacji, a następnie kliknąć prawym przyciskiem myszy węzeł **Licensing Site Settings** (Ustawienia licencjonowania lokalacji) i wybrać polecenie **Properties** (Właściwości). Wyświetlony zostanie aktualny serwer licencji lokalacji, co ilustruje rysunek 9-9-



Rysunek 9-9 Identyfikacja i zmiana serwera licencji lokacji

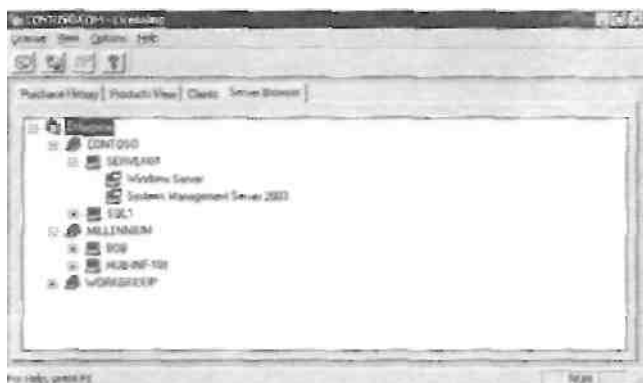
Aby przypisać rolę serwera licencji lokacji innemu serwerowi lub kontrolerowi domeny, należy kliknąć przycisk **Change** (Zmień) i wybrać inny komputer. W celu zachowania historii licencjonowania przedsiębiorstwa, po przydzieleniu innemu serwerowi tej roli, należy bezzwłocznie na nowym serwerze licencjonowania zatrzymać usługę *License Logging* (Rejestrowanie licencjonowania) i skopiować ze starego serwera do nowego następujące pliki:

- %Systemroot%\System32\Cpl.cfg — plik zawiera historię zakupów przedsiębiorstwa.
- %Systemroot%\Lls\Llsuser.lls - plik zawiera informacje o użytkownikach dotyczące liczby połączeń.
- %Systemroot%\Lls\Llsmapi.lls - plik zawiera informacje o licencjach grup-

Po skopiowaniu plików należy ponownie uruchomić usługę *License Logging* (Rejestrowanie licencji).

Administrowanie licencjami lokacji

Po zlokalizowaniu serwera licencji lokacji można przeglądać informacje dotyczące licencjonowania tego serwera za pomocą narzędzia **Licensing** (Licencjonowanie) w grupie programów **Administrative Tools** (Narzędzia administracyjne). Zakładka *Server Browser* (Przegląd serwerów), pokazana na rysunku 9-10, umożliwia zarządzanie licencjami całej lokacji lub przedsiębiorstwa.



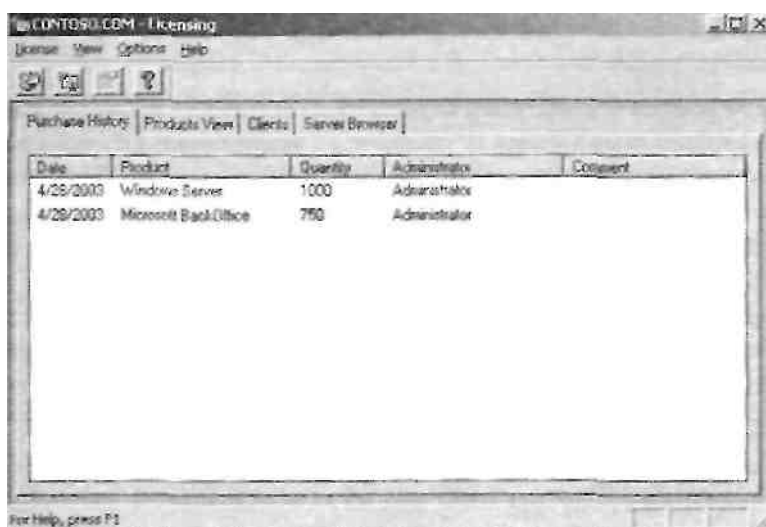
Rysunek 9-10 Zakładka *Server Browser* (Przegląd serwerów) programu *Microsoft Licensing* (Licencjonowanie) umieszczony w grupie *Narzędzia administracyjne*

Strona *Server Browser* (Przegląd serwerów) programu *Licensing* umożliwia zarządzanie dowolnym serwerem dowolnej lokacji lub domeny, do której użytkownik posiada uprawnienia administracyjne. Należy zlokalizować serwer i kliknąć go prawym przyciskiem myszy, a następnie wybrać polecenie **Properties** (Właściwości), gdzie realizowane jest zarządzanie licencjami. Dla każdego zainstalowanego na serwerze produktu można dodać lub usunąć licencje trybu „Na serwer”. Można również, jeśli zachodzi taka potrzeba, zmienić tryb licencjonowania. Warto zapamiętać, że tryb „Na serwer” wystawia licencję, jeśli użytkownik łączy się z dowolnym produktem serwera. Jeśli natomiast użytkownik rozłącza się, usługa *License Logging* (Rejestrowanie licencji) udostępnia tę licencję innym użytkownikom.

Właściwości serwera umożliwiają także skonfigurowanie replikacji licencji. Ustawienia te określone są w właściwościach licencjonowania serwera (narzędzie *Licensing*) w programie *Control Panel*. Ustawienia domyślne określają, że informacje o licencjach są replikowane z usługi serwera *License Logging Service* (Rejestrowanie licencji) do serwera licencji lokacji co 24 godziny, a system automatycznie ustawia replikację tak, aby unikać obciążania serwera licencji lokacji. Jeśli administrator chce kontrolować harmonogram replikacji lub jej częstotliwość, musi ręcznie określić różne wartości parametrów **Start At** (Uruchom w) oraz **Start Every** (Uruchom co) dla każdego serwera, który przeprowadza replikację do tego samego serwera licencji lokacji.

Aby zarządzać trybem licencjonowania „Na urządzenie lub na użytkownika”, należy uruchomić narzędzie **Licensing** znajdujące się w grupie programów **AdministrativeTools** (Narzędzia administracyjne), a następnie w menu **License** (Licencja) wybrać polecenie **New License** (Nowa licencja). W oknie dialogowym **New Client Access License** (Nowa licencja dostępu klienta) należy wybrać produkt serwera oraz liczbę zakupionych licencji. Licencje zostaną dodane do puli licencji. Jeśli gdziekolwiek w lokacji urządzenie lub użytkownik połączy się z produktem serwera, z puli zostanie mu przydzielona licencja, jedna licencja dla każdego użytkownika lub urządzenia. Jeśli dodatkowe urządzenie lub dodatkowy użytkownik próbuje uzyskać dostęp do produktu po wyczerpaniu licencji, zanotowane zostanie natęśnienie licencji.

Zakładka **Purchase History** (Historia zakupów) programu **Licensing** (Licencjonowanie), pokazana na rysunku 9-11, umożliwia przeglądanie zakupów licencji lokacji dokonywanych w przeszłości, jak również informacji o ilości, dacie i administracji zajmującym się dodawaniem bądź usuwaniem licencji.



Rysunek 9-11 Zakładka *Purchase History* (Historia zakupów) programu narzędziowego Microsoft Licensing (Licencjonowanie)

Aby przeglądać sumaryczne informacje dotyczące licencji i ich zgodności, należy kliknąć zakładkę **Products View** (Widok produktów). Na zakładce tej wyświetlone są informacje ile licencji zostało zakupionych i przydzielonych do użytkowników lub urządzeń (dla trybu „Na urządzenie lub na użytkownika”) lub ile licencji zostało zakupionych dla wszystkich serwerów lokacji oraz informacje o osiągniętej maksymalnej liczbie połączeń w danym dniu (dla trybu „Na serwer”). Użytkownik może również określić zgodność za pomocą symboli statusu licencjonowania pokazanych w tabeli 9-2.

Tabela 9-2. Symbole statusu licencjonowania

Symbol	Status licencjonowania
	Produkt jest zgodny z wymogami legalności licencjonowania. Liczba połączeń jest mniejsza niż liczba zakupionych licencji.
	Produkt nie jest zgodny z wymogami legalności licencjonowania. Liczba połączeń przekroczyła liczbę zakupionych licencji
	Dla danego produktu limit legalności został osiągnięty. Liczba połączeń jest równa liczbie zakupionych licencji. Jeśli dodatkowe urządzenia lub dodatkowi użytkownicy będą łączyć się z produktem serwera, należy zakupić i zarejestrować nowe licencje

Grupy licencji

Tryby licencjonowania „Na urządzenie lub na użytkownika” wymagają jednej licencji CAL dla każdego urządzenia. Jednakże usługa *License Logging* (Rejestrowanie licencji) przydziela i śledzi licencje według nazwy użytkownika. Jeśli wielu użytkowników współużytkuje jedno lub kilka urządzeń, należy utworzyć grupę licencji, w przeciwnym razie licencje będą zbyt szybko wykorzystywane.

Grupa licencji jest zbiorem użytkowników, którzy współdzielą jedną lub kilka licencji CAL. Kiedy użytkownik łączy się z produktem serwera, usługa *License Logging* śledzi użytkownika w oparciu o jego

nazwę, ale przypisuje licencje CAL Z przydziału przeznaczonego dla grupy licencji. Idea staje się bardziej prosta na podstawie przykładów:

- **10 użytkowników podczas inwentaryzacji współużytkuje pojedyncze urządzenie kieszonkowe.** Zostaje utworzona grupa licencji licząca 10 członków. Tej grupie licencji przypisana zostaje jedna licencja CAL, reprezentująca pojedyncze urządzenia współużytkowane przez 10 użytkowników.
- **100 studentów okazjonalnie korzysta z laboratorium komputerowego, w którym zainstalowanych jest 10 komputerów.** Utworzona zostaje grupa licencji, której członkami jest 100 studentów, a do tej grupy przydzielonych zostaje 10 licencji CAL.

Aby utworzyć grupę licencji, należy kliknąć menu **Option** (Opcje) i w menu **Advanced** (Zaawansowane) wybrać polecenie **New License Group** (Nowa grupa licencji). Należy wprowadzić nazwę grupy i przydzielić jedną licencję dla każdego klienta urządzenia używanego do uzyskiwania dostępu do serwera. Liczba licencji przydzielonych do grupy powinna odpowiadać liczbie urządzeń używanych przez członków grupy.

nia

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Które tryby licencjonowania są prawidłowymi trybami licencjonowania w systemie Windows Server 2003? Wybierz wszystkie właściwe odpowiedzi.
 - a. Per User (Na użytkownika)
 - b. Per Server (Na serwer)
 - c. Per Seat (Na stanowisko)
 - d. Per Device or Per User (Na urządzenie lub na użytkownika)
2. Do wykonania projektu został wynajęty zespół programistów. Utworzone zostały trzy zmiany programistów, a każda z nich liczy 6 osób. Każdy programista, do opracowywania i testowania programów¹, używa czterech urządzeń, dla których w systemie Windows Server 2003 sprawdzana jest tożsamość. Jaka jest minimalna liczba wymaganych licencji CAL, jeśli dla serwerów skonfigurowana został tryb licencjonowania Per Device or Per User (Na urządzenie lub na użytkownika)?
 - a. 6
 - b. 4
 - c. 18
 - d. 24
3. Za pomocą którego narzędzia można zidentyfikować serwer licencji lokacji?
 - a. Active Directory Domains And Trusts (Domeny i relacje zaufania usługi Active Directory)
 - b. Narzędzie Licensing (Licencjonowanie) programu Control Panel (Panel sterowania)
 - c. Active Directory Sites And Services (Lokacje i usługi Active Directory)
 - d. DNS

4. Administrator zarządza siecią zespołu 500 telefonicznych przedstawicieli handlowych. W sieci jest skonfigurowanych 550 licencji w trybie Per Device or Per User (Na urządzenie lub na użytkownika). Nowa kampania wymaga zatrudnienia dodatkowej zmiany 500 reprezentantów. Co należy zrobić, aby w sposób najbardziej efektywny zarządzać śledzeniem licencji i sprawdzaniem ich zgodności?
- Unieważnić licencje istniejących klientów
 - Usunąć istniejące licencje, a następnie dodać 500 licencji
 - Utworzyć grupę licencji
 - Tryb licencjonowania zmienić na tryb Per Server (Na serwer)

Podsumowanie lekcji

- W systemie Windows Server 2003 wprowadzony został nowy tryb licencjonowania, umożliwiający uzyskiwanie dostępu do serwera przez jednego użytkownika korzystającego z różnych urządzeń lub dostęp do serwera przez grupę użytkowników wykorzystujących jedno urządzenie. Tryb ten nazwany został Per Device or Per User (Na urządzenie lub Na użytkownika).
- Jeśli kilku użytkowników uzyskuje dostęp do produktu serwera za pomocą współużytkowanych urządzeń, należy dodać tych użytkowników do grupy licencji i przydzielić tej grupie liczbę licencji równą liczbie urządzeń wykorzystywanych przez użytkowników.
- Ustawienia domyślne określają, że informacje dotyczące licencji są replikowane do serwera licencji lokalnie co 24 godziny.
- Licencjonowanie może być zarządzane przy użyciu narzędzia Licensing (Licencjonowanie) umieszczonego w programie Control Panel (Panel sterowania) lub przy bardziej scentralizowanych zadaniach przy użyciu narzędzia Licensing (Licencjonowanie) umieszczonego w grupie programów Administrative Tools (Narzędzia administracyjne).

Zadanie praktyczne

Administrator opracowuje metodę aktualizacji sieci składającej się z 1000 klientów wykorzystujących systemy Windows XP i Windows 2000. Celem projektu jest uniemożliwienie pobierania aktualizacji bezpośrednio z usługi Windows Update i utworzenie struktury, w której administrator będzie mógł zatwierdzać do dystrybucji najważniejsze uzupełnienia i poprawki zabezpieczeń.

W firmie zostały niedawno zakupione komputery stacjonarne i przenośne, ale niestety do tych systemów zostały zastosowane standardowe obrazy utworzone w firmie pewien czas temu. Obraz systemu Windows XP używa kodu RTM (release-to-manufacture), a obraz systemu Windows 2000 ma zainstalowany dodatek SerWcc Pack 2. Tak więc pierwszym zadaniem administratora będzie aktualizacja systemów do poziomu najnowszych pakietów serwisowych tak, aby na komputerach zainstalowane zostały programy klienckie usługi Automatic Updates (Aktualizacje automatyczne), jak również wszystkie poprawki i uzupełnienia.



Informacja W tym ćwiczeniu praktycznym wyniki testów należy sprawdzać za pomocą drugiego komputera. W tym celu komputer należy połączyć z domeną i konto tego komputera umieścić w jednostce organizacyjnej Desktops. Jeśli komputer działa pod kontrolą systemu Windows 2000, należy w ćwiczeniu odpowiednio zmodyfikować rozmieszczanie pakietów serwisowych.

Ćwiczenie 1; Pobieranie i rozpakowywanie pakietu serwisowego

1. Na dysku C utwórz folder o nazwie ServicePack.
2. Z witryny firmy Microsoft <http://uiwww.microsoft.com/downloads> lub Z witryny systemu Windows XP <http://www.microsoft.com/windowsxp> pobierz najnowszy pakiet serwisowy. Zapisz go w folderze C:\ServicePack.
3. Otwórz okno wiersza poleceń i wpisz komendę cd C:\ServicePack, aby przejść do foldera, gdzie został skopiowany pakiet serwisowy.
4. Wpisz polecenie xpspl.exe -x. Zastąp nazwę xpspl nazwą najnowszego pakietu serwisowego, który właśnie został pobrany
5. Program poprosi o wskazanie miejsca, w którym pakiet ma zostać rozpakowany Wpisz C:\Service-Pack.
6. Pakiet serwisowy został rozpakowany. Przy użyciu programu Windows Explorer (Eksplorator Windows) przejdź do utworzonej struktury foldera i zanotuj położenie pliku update.exe (w folderze Update), który jest używany do uruchomienia instalacji pakietu serwisowego na pojedynczym komputerze oraz pliku update.msi (w tym samym folderze), który jest używany do instalowania pakietu serwisowego za pomocą zasady grupy dotyczącej dystrybucji oprogramowania.

Ćwiczenie 2: Instalowanie pakietu serwisowego za pomocą zasady grupy

1. Udostępnij folder C:\ServicePack. Nazwa udostępniania foldera to: ServicePack.
2. Otwórz/ przystawkę Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory).
3. Rozwiń węzeł domeny i znajdź (lub utwórz) jednostkę organizacyjną Desktops.
4. Utwórz obiekt komputera w jednostce organizacyjnej Desktops o nazwie Desktop0569, który będzie reprezentował jeden z nowych systemów.



Informacja Jeśli mamy do dyspozycji inny system używany do przeprowadzenia tego ćwiczenia, konto tego komputera należy umieścić w jednostce organizacyjnej Desktop.

5. Kliknij prawym przyciskiem myszy jednostkę organizacyjną Desktops i wybierz polecenie Properties (Właściwości).
6. Kliknij zakładkę Group Policy (Zasady grupy).
7. Kliknij polecenie New (Nowa), aby utworzyć nowy obiekt GPO. Nazwij ten obiekt SP-Deploy.
8. Zaznacz odnośnik do zasady grupy SP-Deploy i kliknij przycisk Edit (Edytuj). Wyświetlone zostanie okno edytora obiektów zasad grupy (Group Policy Object Editor).
9. Przejdź do węzła Computer Configuration\Software Settings (Konfiguracja komputera\Ustawienia oprogramowania).

10. Kliknij prawym przyciskiem myszy węzeł Software Installation (Instalacja oprogramowania) i polecenie New (Nowy), a następnie Package (Pakiet).
11. Wpisz ścieżkę Wserver01.contoso.com\Servicepack i naciśnij ENTER. W oknie dialogowym przeglądania należy wskazać katalog główny rozpakowanego pakietu serwisowego.
12. Przejdź do pliku Update.msi znalezionej w poprzednim ćwiczeniu. Plik ten należy zaznaczyć, a następnie kliknąć polecenie Open (Otwórz/).
- 13- Należy zaznaczyć opcje Assigned (Przypisany) i nacisnąć przycisk OK. Pakiet został utworzony.
14. Zamknij program Group Policy Object Editor (Edytor obiektów zasady grupy) i okno dialogowe Properties (Właściwości) jednostki organizacyjnej Desktop.
- 15- (Opcjonalne) Jeśli dysponujesz innym systemem, możliwe będzie przetestowanie zdalnej instalacji pakietu serwisowego. Warto zapamiętać, że komputery Windows XP domyślnie są tak skonfigurowane, aby optymalizować logowanie w systemie i dlatego zanim pakiet serwisowy zostanie zastosowany, trzeba będzie dwukrotnie uruchamiać komputer. Poziom pakietu serwisowego komputera można sprawdzić w menu Start, klikając polecenie Run (Uruchom), a następnie wpisując winver.

Ćwiczenie 3: Instalowanie usługi SUS

1. Przejdź do adresu <http://go.microsoft.com/fwlink/?LinkId=6930>. Program poprosi o dodanie witryny do listy witryn zaufanych. Należy to zrobić.
2. Pobierz pakiet instalacyjny usługi SUS.
3. Uruchom instalację usługi SUS dwukrotnie klikając pobrany plik.
4. Na ekranie powitalnym kliknij przycisk Next (Dalej).
- 5- Przeczytaj i zaakceptuj warunki umowy licencyjnej EULA (End User License Agreement), a następnie kliknij przycisk Next (Dalej).
- 6- Zaznacz instalację niestandardową (Custom), a następnie kliknij przycisk Next (Dalej).
7. Na stronie Choose File Locations (wybieranie lokalizacji pliku) wybierz opcję Save The Updates To This Local Folder (zapisz plik w tym folderze lokalnym). Nie trzeba zmieniać domyślnych ustawień - C:\SUS\Content. Kliknij przycisk Next (Dalej).



Informacja Wielkość plików aktualizacji może sięgać kilku setek megabajtów. Jeśli łącze do sieci Internet jest wolne lub jeśli chcemy zaoszczędzić czas, można zaznaczyć drugą opcję Keep The Updates On A Microsoft Windows Update Server (zachowaj aktualizacje znajdujące się na systemie Microsoft Windows Update Server).

- 8- Dla opcji Language Settings (ustawienia językowe) wybierz English Only (tylko angielski), a następnie kliknij przycisk Next (Dalej).
- 9- Na następnej stronie wybierz opcję I Will Manually Approve New Versions Of Approved Updates (ręczne zatwierdzanie nowych wersji zatwierdzonych aktualizacji), a następnie kliknij przycisk Next (Dalej).
10. Na następnej stronie powinna zostać wyświetlona informacja, że pobierane pliki zostaną zapisane w lokalizacji <http://SERVER01>. Kliknij przycisk Install.
11. Po zakończeniu instalacji kliknij przycisk Finish (Zakończ). Przeglądarka Internet Explorer zostanie otwarta na stronie administracji usługi SUS. Dalsza procedura opisana została w ćwiczeniu 4-

Ćwiczenie 4: Synchronizacja usługi SUS

1. Jeśli strona administracji usługi SUS nie została wyświetlona, należy otworzyć przeglądarkę Internet Explorer i wpisać adres <http://SERVER01SUSAd.min>.



Informacja Być może, aby przeglądać witrynę administracyjną usługi SUS, trzeba będzie dodać Server01 do listy zaufanych witryn grupy Local Intranet (Lokalny intranet). W tym celu należy otworzyć przeglądarkę Internet Explorer i wybrać w menu Tools (Narzędzia) polecenie Internet Options (opcje internetowe). Następnie należy kliknąć zakładkę Security (Zabezpieczenia), zaznaczyć ikonę Trusted Sites (Zaufane witryny) i kliknąć przycisk Sites (Witryny). Do listy zaufanych witryn należy dodać dwa wpisy **Server01** oraz **Server01.contoso.com**.

2. W pasku nawigacyjnym z lewej strony okna kliknij polecenie Synchronize Server (synchronizacja serwera).
3. Kliknij polecenie Synchronization Schedule (harmonogram synchronizacji).
W tym ćwiczeniu stosowana będzie synchronizacja ręczna. Opcje synchronizacji można jednak przeanalizować klikając polecenie Synchronize Using Truś Schedule (synchronizacja przy użyciu tego harmonogramu). Po zakończeniu przeglądania ustawień kliknij przycisk Cancel (Anuluj).
4. Na stronie Synchronize Server (Synchronizacja serwera) kliknij przycisk Synchronize Now (synchronizuj teraz). Jeśli wybrane zostało pobieranie aktualizacji do serwera, proces synchronizacji może zająć dłuższy czas.
5. Po zakończeniu synchronizacji program automatycznie przełączy wyświetlanie do strony Approve Updates (zatwierdzanie aktualizacji). Stronę tę można również otworzyć klikając polecenie Approve Updates (zatwierdzanie aktualizacji) znajdujące się w pasku nawigacyjnym po lewej stronie okna.
6. Zatwierdź niewielką liczbę aktualizacji tak, aby później powrócić do kontynuacji ćwiczeń związanych z zatwierdzaniem i automatyzacją aktualizacji.
7. Przeanalizuj inne strony witryny administracyjnej usługi SUS. Po zapoznaniu się z witryną zamknij przeglądarkę Internet Explorer.

Ćwiczenie 5: Konfigurowanie aktualizacji automatycznych

1. Otwórz przystawkę Active Directory Sites and Seraces (Lokacje i usługi Active Directory).



Informacja Większość przedsiębiorstw wybiera powiązanie obiektów GPO do lokacji, a nie do jednostek organizacyjnych lub domen. Jednakże zasady dotyczące usługi SUS nadają się dobrze do zastosowania w lokacji, jeśli programy klienckie zostaną skierowane do najbardziej odpowiedniego serwera lokacji.

2. Kliknij prawym przyciskiem myszy witrynę Default-First-Site-Name i wybierz polecenie Properties (Właściwości).
3. Kliknij zakładkę Group Policy (Zasady grupy).
4. Kliknij polecenie New (Nowa) i nazwij nowy obiekt GPO **SUS-Sitel**.
5. Kliknij przycisk Edit (Edytuj). Wyświetlone zostanie okno programu Group Policy Object Editor (Edytor obiektów zasady grupy).

6. Przejdź do węzła **Computer** Configuration\Administrative Templates\Windows Components\ Windows Update (Konfiguracja komputera\Szablony administracyjne\Składniki systemu Windows\Windows Update).
7. Dwukrotnie kliknij zasadę: Specify Intranet Microsoft Update Service Location (Określ lokalizację intranetową usługi aktualizacji firmy Microsoft).
8. Kliknij opcję Enabled (Włączone).
- 9- W *obu* polach tekstowych wpisz [http://server01 .contoso.com](http://server01.contoso.com).
10. Kliknij przycisk OK.
11. Dwukrotnie kliknij zasadę: Configure Automatic Updates (Konfigurowanie aktualizacji automatycznych).
12. Kliknij opcję Enabled (Włączone).
- 13- Na liście rozwijanej Configure Automatic Updating (Konfigurowanie aktualizacji automatycznych) wybierz opcję 4 — Auto Download And Schedule The Install (4 — Pobierz automatycznie i zaplanuj instalację).
14. Potwierdź harmonogram instalacji: codziennie o godzinie 3:00.
15. Kliknij przycisk OK.
16. Dwukrotnie kliknij zasadę: Reschedule Automatic Updates Scheduled Installations (Zaplanuj ponownie zaplanowane instalacje aktualizacji automatycznych).
17. Kliknij opcję Enabled (Włączone).
18. W polu tekstowym Wait After System Startup (Minutes) [Czekaj po uruchomieniu systemu (minuty)] wpisz 1.



Wskazówka egzaminacyjna Zasada Wait After System Startup (Czekaj po uruchomieniu systemu) jest używana do ponownego zaplanowania harmonogramu instalacji, który był nieprawidłowo określony, najczęściej z powodu wyłączania komputera w zaplanowanych okresach instalacji.

19. Kliknij przycisk OK.
20. Zamknij program Group Policy Object Editor (Edytor obiektów zasady grupy) i okno dialogowe Properties (Właściwości) dla węzła Default-First-Site-Name.
21. W celu sprawdzenia konfiguracji uruchom ponownie serwer, który jest objęty zakresem działania nowej zasady. Otwórz moduł System w programie Control Panel (Panel sterowania) i kliknij zakładkę Automatic Updates (Aktualizacje automatyczne). W oknie można zobaczyć, że opcje konfiguracyjne zostały wyłączone i są obecnie określone przez zasadę.

Podsumowanie rozdziału

- Usługa SUS (Software Update Services) firmy Microsoft umożliwia centralne zarządzanie zatwierdzaniem i dystrybucją istotnych aktualizacji i poprawek zabezpieczeń systemu Windows. Jeden lub kilka serwerów SUS przechowuje listy zatwierdzonych aktualizacji i opcjonalnie, chociaż tak jest najczęściej, serwery same pobierają pliki aktualizacji. Konfiguracja klientów usługi Automatic Updates (Aktualizacje automatyczne), najczęściej przeprowadzana za pomocą obiektów GPO, zezwala na pobieranie plików z serwerów SUS intranetu, a nie bezpośrednio z usługi Microsoft Windows Update.
- Usługa SUS (Software Update Services) nie rozprowadza pakietów serwisowych.
- Pakiety serwisowe są udostępniane bezpłatnie przez firmę Microsoft. Jeśli pakiet serwisowy jest w postaci pojedynczego pliku, może być rozpakowany w oknie wiersza poleceń poprzez wprowadzenie nazwy pakietu serwisowego, po której umieszczony zostaje przełącznik -x.
- Instalacja pakietów serwisowych jest prosta. W tym celu należy w obiekcie GPO przydzielić pakiet instalacji oprogramowania do zasad ustawień oprogramowania konfiguracji komputera.
- Siedzenie oraz zarządzanie licencjami i ich zgodnością jest ważnym zadaniem administracji sieci. System Windows Server 2003 umożliwia przydzielanie licencji w oparciu o liczbę jednoczesnych połączeń do serwera lub w oparciu o licencje każdego urządzenia lub użytkownika, którzy przyłączyli się do dowolnej liczby serwerów przedsiębiorstwa.
- Licencje są replikowane pomiędzy usługami License Logging (Rejestrowanie licencji) a serwerami licencji lokalnej. Serwer licencji lokalnej można zidentyfikować za pomocą przystawki Active Directory Sites And Services (Lokacje i usługi Active Directory), natomiast licencjonowanie w lokalnej sieci zarządzane jest przy użyciu narzędzia Licensing (Licencjonowanie) znajdującego się w grupie programów Administrative Tools (Narzędzia administracyjne).
- Grupa licencji umożliwia użytkownikom współdzielenie jednego lub kilku urządzeń. Liczba licencji Windows Device CAL zostaje przypisana do grupy licencji.

Informacje dla zdających egzamin

Przed przystąpieniem do egzaminu, należy zapoznać się z przedstawionymi poniżej najważniejszymi faktami i pojęciami, aby określić które tematy wymagają pogłębienia. Należy powrócić do lekcji, aby osiągnąć większą wprawę oraz przejrzeć działy znajdujące się w części 2 - „Materiały dodatkowe”. Informacje tu zawarte, kierują do materiałów uzupełniających tematy objęte zadaniami egzaminacyjnymi.

Najważniejsze fakty

- Umiejętność instalacji i konfiguracji usługi SUS. Pomimo, że zadania egzaminacyjne nie obejmują w sposób bezpośredni konfiguracji usługi SUS, metody konfigurowania usługi SUS wpływają na obsługę infrastruktury SUS i dlatego istotnym zagadnieniem jest poznanie ogólnego obrazu usługi SUS.
- Zwrócenie uwagi na zadania administracyjne związane z usługą SUS, takie jak synchronizacja, zatwierdzanie aktualizacji, przegląd dzienników i zdarzeń oraz konfigurowanie usługi Automatic Updates (Aktualizacje automatyczne) za pomocą modułu System w programie Control Panel (Panel

sterowania) dla komputerów autonomicznych lub za pomocą zasady grupy w dużych środowiskach. Warto zapamiętać, że za pomocą właściwości klienta usługi Automatic Updates (Aktualizacje automatyczne) nie można skierować komputera do serwera SUS. Aby przekierować klienta do serwera intranetu, a nie do serwera usługi Microsoft Windows Update, należy posłużyć się zasadą grupy lub wpisami rejestru.

- Umiejętność obliczania wymagań licencji dla różnych sytuacji i różnych trybów licencjonowania - Per Server (Na serwer) lub Per Device or Per User (Na urządzenie lub na użytkownika). Warto zapamiętać, że grupy licencji umożliwiają wielu użytkownikom współdzielenie jednego lub kilku urządzeń.

Najważniejsze pojęcia

Licencja CAL (Client Access License) Licencja pozwala użytkownikowi lub urządzeniu przyłączyć się do produktu serwera celem wykorzystania dowolnej jego funkcjonalności, wliczając w to usługi plików i drukowania lub uwierzytelnienia.

Tryb licencjonowania Per Server (Na serwer) Licencje zostają przydzielone, kiedy użytkownik lub urządzenie łączy się z serwerem lub produktem serwera. Jeśli użytkownik odłącza się od serwera, licencja zostaje zwrócona do puli dostępnych licencji. Tryb ten wymaga zapewnienia wystarczającej liczby licencji, aby obsłużyć maksymalną liczbę jednoczesnych połączeń na każdym serwerze.

Tryb licencjonowania Per Device or Per User (Na urządzenie lub na użytkownika) W tym trybie pojedyncza licencja CAL umożliwia autoryzację użytkownika (który może wykorzystywać kilka urządzeń) lub urządzenia (które może być używane przez kilku użytkowników) podczas łączenia się z dowolną liczbą serwerów.

Grupa licencji Ponieważ usługa License Logging (Rejestrowanie licencji) przydziela licencje w oparciu o nazwę użytkownika, a nie w oparciu o nazwę urządzenia, licencje urządzeń Windows Device CAL zostają przypisane do grupy licencji. Grupa licencji ma jednego lub kilku użytkowników i zostaje jej przydzielony ekwiwalent liczby urządzeń, za pomocą których grupa łączy się do produktów serwera.

Pytania i odpowiedzi

342 Pytania do lekcji 1

1. Administrator konfiguruje infrastrukturę usługi SUS (Software Update Services). Jeden serwer synchronizuje metabazę oraz dane z usługą Windows Update. Inne serwery (jeden w każdej lokacji) synchronizują dane z nadrzędnym serwerem SUS. Które z wymienionych poniżej czynności są wymagane, aby zakończyć konfigurację infrastruktury usługi SUS?
 - a. Skonfigurowanie w każdym systemie klientów usługi Automatic Updates (Aktualizacje automatyczne) przy użyciu programu Control Panel (Panel sterowania)
 - b. Skonfigurowanie obiektów GPO tak, aby kierowały programy klienckie do serwera SUS znajdującego się w danej lokacji
 - c. Skonfigurowanie ręcznego punktu dystrybucji danych
 - d. Zatwierdzenie aktualizacji przy użyciu strony administracyjnej usługi SUS

Prawidłowe odpowiedzi to b oraz d.
2. Administrator konfiguruje usługę SUS dla grupy serwerów sieci Web tak, aby serwery sieci Web same aktualizowały się w godzinach nocnych w oparciu o listę zatwierdzonych aktualizacji serwera SUS. Jednakże należy tak skonfigurować usługę, aby nie miała wpływu na wykonywane również w nocy, prace administratora serwera sieci Web (w kontekście możliwości ponownego uruchamiania serwera po zainstalowanych aktualizacjach). Którą konfigurację zasady usługi Windows Update należy użyć w tej sytuacji?
 - a. Notify For Download And Notify For Install (Powiadom przed pobraniem aktualizacji i powiadom przed ich zainstalowaniem)
 - b. Auto Download And Notify For Install (Pobierz aktualizacje automatycznie i powiadom, gdy są gotowe do zainstalowania)
 - c. Auto Download And Schedule The Install (Automatycznie pobierz aktualizacje i zainstaluj je według harmonogramu)

Prawidłowa odpowiedź to c. Serwery sieci Web mogą same przeprowadzać aktualizacje, należy jedynie określić harmonogram instalowania aktualizacji. Administrator może anulować instalację.
3. Administrator konfiguruje systemy klientów sieci oraz harmonogram instalacji usługi Automatic Updates (Aktualizacje automatyczne) tak, aby automatycznie pobierały i instalowały aktualizacje w godzinach nocnych. Jednakże niektórzy użytkownicy wyłączają komputery na noc i na tych komputerach aktualizacje nie mogą zostać przeprowadzone. Która zasada pozwala naprawić zaistniałą sytuację bez konieczności zmiany harmonogramu instalacji?
 - a. Specify Intranet Microsoft Update Service Location (Określ lokalizację intranetową firmy Microsoft)
 - b. No Auto-Restart For Scheduled Automatic Updates Installations (Bez automatycznego uruchamiania ponownego dla zaplanowanych instalacji aktualizacji automatycznych)
 - c. Reschedule Automatic Updates Scheduled Installations (Zaplanuj ponownie zaplanowane instalacje aktualizacji automatycznej)
 - d. Configure Automatic Update (Konfigurowanie aktualizacji automatycznych)

Prawidłowa odpowiedź to c. Aktualizacje są automatycznie pobierane przy zastosowaniu procesów realizowanych w tle i w sytuacji bezczynności w sieci, ale aktualizacje te są uruchamiane według określonego harmonogramu. Jeśli komputer zostanie wyłączony w zaplanowanym okresie instalacji, instalacja zostaje przesunięta do następnego terminu zaplanowanych instalacji. Jeśli zasada Reschedule Wait Time (Zaplanuj ponownie czas oczekiwania) została określona przez liczbę z przedziału 1 do 60, liczba ta określi w minutach opóźnienie uruchomienia aktualizacji w odniesieniu do uruchomienia systemu.

Pytania do lekcji 2

1. Którego polecenia należy użyć, aby rozpakować pojedynczy plik pobranego pakietu serwisowego?
 - a. Setup.exe -u
 - b. Update.exe -x
 - c. Update.msi
 - d. <Servicepackname>.exe -x

Prawidłowa odpowiedź to d.

2. Który typ rozmieszczania oprogramowania zasady grupy powinien zostać zastosowany do dystrybucji pakietu serwisowego?
 - a. Publikowany w węźle Computer Configuration Software Settings (Konfiguracja komputera, Ustawienia oprogramowania)
 - b. Przypisany w węźle Computer Configuration Software Settings (Konfiguracja komputera, Ustawienia oprogramowania)
 - c. Publikowany w węźle User Configuration Software Settings (Konfiguracja użytkownika, Ustawienia oprogramowania)
 - d. Przypisany w węźle User Configuration Software Settings (Konfiguracja użytkownika, Ustawienia oprogramowania)

Prawidłowa odpowiedź to b.

Pytania do lekcji 3

1. Które tryby licencjonowania są prawidłowymi trybami licencjonowania w systemie Windows Server 2003? Wybierz wszystkie właściwe odpowiedzi.
 - a. Per User (Na użytkownika)
 - b. Per Server (Na serwer)
 - c. Per Seat (Na stanowisko)
 - d. Per Device or Per User (Na urządzenie lub na użytkownika)

Prawidłowe odpowiedzi to b oraz d.

2. Do wykonania projektu został wynajęty zespół programistów. Utworzone zostały trzy zmiany programistów, a każda z nich liczy 6 osób. Każdy programista, do opracowywania i testowania programów, używa czterech urządzeń, dla których w systemie Windows Server 2003 sprawdzana jest tożsamość. Jaka jest minimalna liczba wymaganych licencji CAL, jeśli dla serwerów skonfigurowany został tryb licencjonowania Per Device or Per User (Na urządzenie lub na użytkownika)?

- a. 6
- b. 4**
- c. 18
- d. 24

Prawidłowa odpowiedź to c. Jeśli licencjonowanie zostanie oparte na urządzeniach, to można wyliczyć, że liczba urządzeń to sześć razy cztery, czyli 24. Bardziej opłacalne jest licencjonowanie oparte na liczbie użytkowników, czyli w tym przypadku wymaganych będzie 18 licencji.

3. Za pomocą którego narzędzia można zidentyfikować serwer licencji lokacji?
- a. Active Directory Domains And Trusts (Domeny i relacje zaufania usługi Active Directory)
 - b. Narzędzie Licensing (Licencjonowanie) programu Control Panel (Panel sterowania)
 - c. Active Directory Sites And Services (Lokacje i usługi Active Directory)
 - d. DNS

Prawidłowa odpowiedź to c.

4. Administrator zarządza siecią zespołu 500 telefonicznych przedstawicieli handlowych. W sieci jest skonfigurowanych 550 licencji w trybie Per Device or Per User (Na urządzenie lub na użytkownika). Nowa kampania wymaga zatrudnienia dodatkowej zmiany 500 reprezentantów. Co należy zrobić, aby w sposób najbardziej efektywny zarządzać śledzeniem licencji i sprawdzaniem ich zgodności?
- a. Unieważnić licencje istniejących klientów
 - b. Usunąć istniejące licencje, a następnie dodać 500 licencji
 - c. Utworzyć grupę licencji
 - d. Tryb licencjonowania zmienić na tryb Per Server (Na serwer)

Prawidłowa odpowiedź to c.

10 Zarządzanie sprzętem i sterownikami



Zadania egzaminacyjne omawiane w tym rozdziale

- Instalowanie i konfigurowanie urządzeń sprzętu serwera
 - » Konfigurowanie opcji podpisu sterownika
 - » Konfigurowanie ustawień zasobów urządzenia »Konfigurowanie właściwości i ustawień urządzenia
- Monitorowanie urządzeń sprzętu serwera. Omawiane narzędzia to Device Manager (Menedżer urządzeń), program Hardware Troubleshooting Wizard (Kreator rozwiązywania problemów sprzętu) oraz odpowiednie moduły programu Control Panel (Panel sterowania).

Cele rozdziału

Urządzenia sprzętu umożliwiają dostęp do informacji przetwarzanych na komputerze. Komputer bez urządzeń takich jak monitor, klawiatura, mysz, urządzenia multimedialne jest nieprzydatny. Urządzenia systemu Microsoft Windows Server 2003 zostały podzielone na kategorie, a ich lista dostępna jest w programie Device Manager (Menedżer urządzeń), który umożliwia sprawdzanie i konfigurowanie urządzeń.

Urządzenia i oprogramowanie (sterowniki) używane przez system operacyjny do komunikacji z tymi urządzeniami są połączeniem ściśle związanym z konkretnym urządzeniem i wersją systemu operacyjnego. Większości sterowników nie można wymieniać pomiędzy różnymi systemami operacyjnymi, co oznacza, że nie można używać sterownika opracowanego dla systemu Windows 98 w systemach Windows XP bądź Windows Server 2003.

Oprócz tego, po prawidłowej instalacji początkowej, stale będzie potrzebna obsługa konfiguracji urządzeń i sterowników. Aktualizacje sterowników są częste, powodowane przez zmiany funkcjonalności systemu operacyjnego. Również nowe technologie stosowane w urządzeniach wymuszają odpowiednie zmiany sterowników. Zmiany instalowane są w postaci nowych sterowników, które są najczęściej dostarczane przez producentów urządzeń. Również pakiety serwisowe mogą zawierać aktualizacje sterowników.

Między urządzeniami, sterownikami i systemem operacyjnym musi być zachowana pełna zgodność, w przeciwnym razie urządzenie nie pracuje poprawnie. Prawidłowy sterownik dla urządzenia i systemu operacyjnego powinien działać właściwie, a administrator łatwo może przeprowadzić aktualizację takiego sterownika przy użyciu programu Device Manager (Menedżer urządzeń).

Dla większości środowisk nie jest wskazane, aby użytkownik końcowy mógł instalować nowe sterowniki. Z kolei administratorzy nie chcą (lub nie mają czasu) pracować osobno na każdym komputerze i poprawnie konfigurować urządzenia oraz sterowniki. Większą elastyczność konfigurowania urządzeń i instalacji sterowników stwarzają opcje podpisu sterowników oraz przydzielanie wybranych uprawnień odpowiednim użytkownikom.

Lekcje rozdziału:

- Lekcja 1: Instalowanie urządzeń sprzętu i sterowników 367
- Lekcja 2: Konfigurowanie urządzeń sprzętu i sterowników.....374
- Lekcja 3: Rozwiązywanie problemów związanych z urządzeniami sprzętu i sterownikami.....380

Wymagania

Opracowując niniejszy rozdział przyjęto założenie, że student posiada solidną wiedzę dotyczącą najczęściej używanych urządzeń komputera, takich jak drukarki, myszy, klawiatury, karty sieciowe itp. Zagadnienia optymalizacji, testowania oraz rozwiązywania problemów urządzeń fizycznych są poza zaplanowanym zakresem tego rozdziału.

Przykłady i ćwiczenia praktyczne dotyczące instalacji, konfiguracji oraz rozwiązywania problemów urządzeń sprzętu i sterowników będą wykonywane przy użyciu standardowych urządzeń środowiska systemu Windows Server 2003. Podczas ćwiczeń potrzebny będzie system Windows Server 2003. Serwer ten powinien zostać nazwany Server01 i powinien być kontrolerem domeny contoso.com.

Lekcja 1: Instalowanie urządzeń sprzętu i sterowników

Urządzenia sprzętu komunikują się z systemem operacyjnym Windows Server 2003 poprzez oprogramowanie sterownika. Urządzenia i ich sterowniki, jeśli nie zostały zainstalowane automatycznie za pomocą technologii Plug and Play, mogą być konfigurowane w programie Device Manager (Menedżer urządzeń).

Materiały omówione podczas lekcji pozwalają na

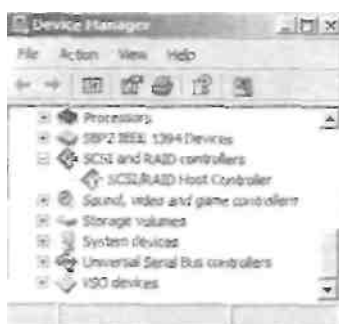
- Zrozumienie zależności pomiędzy urządzeniami a sterownikami
- Wykorzystywanie programu Device Manager (Menedżer urządzeń) do analizy wykrytych urządzeń
- Wykorzystywanie programu Device Manager (Menedżer urządzeń) do instalowania urządzeń

Szacunkowy czas lekcji: 20 minut

Urządzenia i sterowniki

Urządzenia i związane z nimi sterowniki najprościej można podzielić na dwie kategorie logiczne: urządzenia Plug-and-Play (PnP) oraz urządzenia niezgodne z technologią Plug-and-Play (niższego poziomu). Większość urządzeń wyprodukowanych po 1997 to urządzenia typu PnP, a większość sterowników tych urządzeń została dołączona do instalacyjnego dysku CD systemu Windows Server 2003. Jeśli urządzenie zostaje wykryte przez system Windows Server 2003 oraz jeśli dla tego urządzenia zostaje znaleziony odpowiedni sterownik, urządzenie zostaje zainstalowane, a zasoby, takie jak przerwania (IRQ) czy bezpośredni dostęp do pamięci (DMA), zostają przydzielone temu urządzeniu. Po zainstalowaniu, urządzenie zostaje wyświetlone w odpowiedniej kategorii listy urządzeń programu *Device Manager* (Menedżer urządzeń).

Jeśli sterownik typu PnP nie został dołączony do instalacyjnego dysku CD systemu Windows Server 2003, należy znaleźć i zainstalować sterowniki dostarczone przez producenta urządzenia. System Windows Server 2003 po wykryciu urządzeń prosi o dostarczenie sterownika. Jeśli podczas instalacji użytkownik pominie etap związany z dostarczeniem sterownika, system Windows Server 2003 w programie *Device Manager* (Menedżer urządzeń) zaznaczy wykryte i nieskonfigurowane urządzenie za pomocą żółtej ikony ostrzeżenia. Ikona ta została pokazana na rysunku 10-1 i jest również wykorzystywana do oznaczania w systemie sytuacji powielenia urządzeń, konfliktów pomiędzy żądaniami zasobów sterowników, co dla nowszych systemów i urządzeń zdarza się niezwykle rzadko.



Rysunek 10-1 Ikona ostrzeżenia programu Device Manager (Menedżer urządzeń)

Jeśli urządzenie nie może zostać rozpoznane przez system Windows Server 2003, to nie pojawi się żadne żądanie związane z instalacją, a nieznanne urządzenie w programie *Device Manager* zostaje oznaczone żółtym znakiem zapytania. Aby nierozpoznane lub nieskonfigurowane urządzenia funkcjonowały prawidłowo, odpowiednie ich sterowniki muszą być instalowane ręcznie.

Korzystanie z programu Device Manager (Menedżer urządzeń)

Wygląd programu *Device Manager* jest podobny do programu *Windows Explorer* (Eksplorator Windows), z tym że przedstawiane są urządzenia sprzętu zainstalowanego na komputerze. Za pomocą programu Device Manager (Menedżer urządzeń) można aktualizować sterowniki urządzeń sprzętu oraz modyfikować ustawienia dotyczące tych urządzeń. Program **Device Manager** uruchamiany jest jako część konsoli **Computer Management** (Zarządzanie komputerem) umieszczonej w grupie programów **Administrative Tools** (Narzędzia administracyjne) lub może też być uruchomiony w programie **Control Panel** (Panel sterowania) poprzez wybranie modułu **System**, następnie zakładki **Hardware** (Sprzęt) w oknie dialogowym **System Properties** (Właściwości systemu) i naciśnięcie przycisku **Device Manager** (Menedżer urządzeń). W tabeli 10-1 zostały wymienione zadania realizowane za pomocą programu *Device Manager*.

Tabela 10-1. Zadania programu Device Manager (Menedżer urządzeń)

Zadanie	Wykorzystanie
Określenie, czy sprzęt komputera funkcjonuje prawidłowo	Prawidłowo skonfigurowane urządzenia są wyświetlane według kategorii, Wykryte urządzenia, ale nieskonfigurowane ze względu na brak odpowiedniego sterownika lub występującego konfliktu zasobów, są oznaczone żółtą ikoną wykrzyknika. Urządzenia, które nie zostały rozpoznane oznaczane są ikoną żółtego znaku zapytania.
Drukowanie listy zawierającej podsumowanie zainstalowanych urządzeń komputera	W menu Action (Akcja) programu Device Manager (Menedżer urządzeń) należy wybrać polecenie Print (Drukuj). Opcje drukowania są następujące: System Summary (Podsumowanie systemu), Selected Class or Device (Wybrana klasa lub urządzenie) oraz All Devices And System Summary (Wszystkie urządzenia i podsumowanie systemu).

ciąg dalszy na następnej stronie

ciąg dalszy ze strony poprzedniej

Zadanie	Wykorzystanie
Zmiana ustawień konfiguracji sprzętu	W tym celu należy kliknąć prawym przyciskiem myszy dowolne urządzenie i wybrać polecenie Properties (Właściwości) lub dwukrotnie kliknąć wybrane urządzenie.

Strony właściwości urządzeń

Zakładka General (Ogólne)	Na zakładce wyświetlony jest typ, producent, lokalizacja oraz status urządzenia. Na liście rozwijanej Device Usage (Użycie urządzenia) można wybrać opcje włączające lub wyłączające urządzenie.
Zakładka Driver (Sterownik)	Na zakładce wyświetlone są informacje szczegółowe o sterowniku urządzenia, takie jak wersja, producent oraz to, czy sterownik ma cyfrowy podpis. Oprócz tego zakładka umożliwia instalowanie uaktualnionych sterowników oraz powrót do poprzednio zainstalowanej wersji sterownika. Na zakładce wyświetlone są zasoby używane przez urządzenie, wliczając w to zakresy adresów We/Wy, adresy pamięci oraz używane przerwania. W zależności od typu urządzenia, użytkownik może wyłączyć konfigurację automatyczną i włączyć konfigurację ręczną. Niektóre urządzenia nie zezwalają na ręczną konfigurację urządzenia.
Zakładka Resources (Zasoby)	



Wskazówka egzaminacyjna Program *Device Manager* może być używany jedynie do zarządzania urządzeniami komputera lokalnego. W przypadku komputera zdalnego, *Device Manager* działa tylko w trybie odczytu.

Lista urządzeń, sterowników i konfiguracji systemu może zostać wydrukowana za pomocą polecenia **Print** (Drukuj) umieszczonego w menu **Action** (Action) programu *Device Manager* lub może być zapisana w pliku o wartościach rozdzielanych przecinkami (CSV) za pomocą komendy **Driverquery** w wierszu poleceń. Parametry tego polecenia zostały wymienione w tabeli 10-2.

Tabela 10-2. Parametry polecenia Driverquery

Parametr	Dane wyjściowe
/S system	Określa nazwę lub adres IP (Internet Protocol) komputera zdalnego, z którym program będzie się łączył. Domyślne ustawienia dotyczą komputera lokalnego.
/U domena\użytkownik	Polecenie zostaje uruchomione w kontekście użytkownika określonego przez wartość parametru Użytkownik lub Domena\Użytkownik. Domyślne ustawienia dotyczą uprawnień użytkownika, który zalogował się na komputerze, gdzie uruchomione zostało polecenie.
/P hasło	Określa hasło konta użytkownika wyspecyfikowanego w parametrze /U.
/FO format (TABLE LIST CSV)	Określa format wyświetlania informacji o sterowniku. Parametr może przyjmować wartości TABLE, LIST oraz CSV. Formatem domyślnym danych wyjściowych jest TABLE.

ciąg dalszy na następnej stronie

ciąg dalszy ze i trony poprzedniej

Parametr	Dane wyjściowe
/NH	Pomija wiersz nagłówka informacji o sterowniku. Parametr jest ważny, jeśli parametr /FO został określony wartościami TABLE lub CSV.
/V	Określa, że wyświetlone zostaną szczegółowe informacje o sterowniku. Opcja nie jest ważna dla podpisanych sterowników.
/SI	Powoduje wyświetlenie właściwości podpisanych sterowników.
/?	W oknie wiersza poleceń wyświetlone zostają informacje pomocy.

Użytkownicy i administratorzy a instalacja urządzeń

Tak jak dla większości zadań dotyczących instalacji, administratorzy mogą instalować dowolne urządzenia i ich sterowniki. Z kolei możliwości użytkowników w tym względzie są bardzo ograniczone. Ustawienia domyślne określają, że użytkownicy mogą instalować jedynie urządzenia typu PnP przy spełnieniu następujących warunków:

- Sterownik urządzenia ma podpis cyfrowy.
- W związku z instalacją sterownika nie są wymagane żadne inne działania, a system Windows wyświetla interfejs użytkownika.
- Sterownik urządzenia znajduje się na komputerze.

Jeśli którykolwiek z tych warunków nie jest spełniony, użytkownik nie może instalować urządzenia dopóki nie zostaną mu przydzielone dodatkowe uprawnienia administracyjne.



Wskazówka egzaminacyjna Jeśli urządzenie typu PnP podczas instalacji nie wymaga żadnej interakcji ze strony użytkownika, a sterownik znajduje się na komputerze, użytkownik domyślny może przyłączyć i używać urządzenie. Dotyczy to głównie urządzeń stosujących interfejs USB, interfejs równoległy, urządzeń zgodnych z normą IEEE 1394, w szczególności dotyczy to drukarek. Uprawnienia użytkownika Load And Unload Device Drivers (Ładowanie i zwalnianie sterowników urządzeń), konfigurowane za pomocą zasady grupy, nie stosują się do sterowników typu PnP i nie muszą być przydzielane użytkownikom instalującym urządzenia PnP.

Opcje podpisywania sterownika

Sterowniki urządzeń i pliki systemu operacyjnego dołączane do wersji Windows 2000 lub późniejszych mają cyfrowy podpis firmy Microsoft. *Podpis cyfrowy* wskazuje, że dany sterownik lub plik nie został zmieniony lub zastąpiony przez inny proces instalacji programów. Sterowniki urządzeń dostarczanych przez innych producentów mogą nie mieć podpisu cyfrowego.

Użytkownik może kontrolować, w jaki sposób komputer będzie instalował niepodpisane sterowniki. Ustawienia te określone są w programie *Control Panel* (Panel sterowania), w module *System*. Należy otworzyć okno dialogowe **Systems Properties** (Właściwości systemu) i na zakładce **Hardware** (Sprzęt) kliknąć przycisk **Driver Signing** (Podpisywanie sterowników). Uruchomiona zostanie strona *Driver Signing Options Properties* (Opcje podpisywania sterowników) dotycząca danego komputera. Opcje dotyczące reakcji komputera na niepodpisane sterowniki są następujące:

- **Ignore (Ignoruj)** Opcja umożliwia instalowanie na komputerze wszystkich sterowników, bez względu na to, czy mają podpis cyfrowy. Opcja ta jest dostępna jedynie, jeśli użytkownik zalogował się jako administrator lub członek grupy Administratorzy.
- **Warn (Ostrzegaj)** Wyświetlony zostaje komunikat ostrzegający, dzięki czemu użytkownik może zezwolić lub zabronić przeprowadzenia instalacji sterownika urządzenia bez podpisu cyfrowego. Jest to domyślna opcja.
- **Block (Blokuj)** Opcja uniemożliwia programom lub systemowi Windows instalację sterowników urządzeń, które nie mają podpisu cyfrowego.

Zasada grupy jest efektywnym narzędziem do przeprowadzania jednoczesnych zmian ustawień opcji podpisu sterownika na wielu komputerach. Aby zabronić użytkownikom przeprowadzania zmian na ich komputerze, należy zabronić dostępu do stron *Hardware Properties* (Właściwości sprzętu) w programie *Control Panel* oraz wyłączyć przystawkę *Device Manager* (Menedżer urządzeń) w konsoli *Computer Management* (Zarządzanie komputerem). Ustawienia te nie ograniczają użytkownikowi możliwości instalowania urządzeń typu PnP.

Zadanie kontrolne: Instalowanie sterowników urządzenia

W zadaniu tym będzie instalowana karta sieciowa, zostaną zmienione opcje podpisywania cyfrowego, a następnie z powrotem zostanie wprowadzona konfiguracja domyślna.

Ćwiczenie 1: Instalacja karty sieciowej

1. W programie **Control Panel** (Panel sterowania) otwórz stronę **System Properties** (Właściwości systemu), następnie zakładkę **Hardware** (Sprzęt) i kliknij przycisk **Add Hardware Wizard** (Kreator dodawania sprzętu).
2. Kliknij przycisk **Next** (Dalej) i poczekaj aż program wyszuka nowe urządzenie. Jeśli nowe urządzenie nie zostało dodane, program zapyta, czy nowe urządzenie zostało podłączone.
3. Zaznacz opcję **Yes, I Have Already Connected The Hardware** (Tak, sprzęt został już podłączony), a następnie kliknij przycisk **Next** (Dalej).
4. Z listy zainstalowanego sprzętu wybierz opcję **Add A New Hardware Device** (Dodaj nowe urządzenie sprzętowe), a następnie kliknij przycisk **Next** (Dalej).
5. Zaznacz opcję **Install The Hardware That I Manually Select From A List (Advanced)** [Zainstaluj sprzęt, który wybiorę ręcznie z listy (zaawansowane)], a następnie kliknij przycisk **Next** (Dalej).
6. Z listy **Common Hardware Types** (Popularne typy sprzętu) wybierz opcję **Network Adapters** (Karty sieciowe), a następnie kliknij przycisk **Next** (Dalej).
7. Zaznacz firmę **Microsoft** jako producenta i **Microsoft Loopback Adapter** (Karta Microsoft Loopback) jako kartę sieciową, a następnie kliknij przycisk **Next** (Dalej).
8. Aby zamknąć program kreatora, kliknij kolejno przyciski **Next** (Dalej) i **Finish** (Zakończ).

System Windows Server 2003 zainstaluje sterownik i urządzenie. Karta sieciowa o nazwie *Microsoft Loopback Adapter* (Karta Microsoft Loopback) wyświetlona zostanie na liście programu *Device Manager* w kategorii *Network Adapters* (Karty sieciowe).

Ćwiczenie 2: Określanie opcji podpisu sterownika

1. W programie **Control Panel** (Panel sterowania) otwórz **stronę System Properties** (Właściwości systemu), a następnie kolejno kliknij zakładkę **Hardware** (Sprzęt) i przycisk **Add Driver Signing** (Podpisywanie sterowników).
2. Zaznacz opcję **Block** (Blokuj).
3. Kliknij przycisk OK.

Możliwość instalowania niepodpisanych sterowników została wyłączona.

Ćwiczenie 3: Przywrócenie ustawień domyślnych komputera

1. Otwórz program **Device Manager** (Menedżer urządzeń). Kliknij prawym przyciskiem myszy kartę **Microsoft Loopback Adapter** (Karta Microsoft Loopback) i wybierz polecenie **Uninstall** (Odinstaluj).
2. Aby potwierdzić operację, kliknij przycisk OK.
3. Zamknij program **Device Manager**.
4. Otwórz ponownie stronę **Driver Signing Properties** (Podpisywanie sterowników) i zaznacz opcję **Warn** (Ostrzegaj).
5. Zaznacz opcję **Make This Action The System Default** (Uczyń tę akcję domyślną dla systemu).
6. Dwukrotnie kliknij przycisk OK.

Ustawienia domyślne konfiguracji komputera zostały przywrócone.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec rozdziału.

1. Administrator chce zapewnić, aby w sieci na komputerach nie były używane niepodpisane sterowniki. Które ustawienia i opcje konfiguracji strony Driver Signing (Podpisywanie sterowników) Zapewnią takie wymagania?
2. Użytkownik chce zainstalować drukarkę USB podłączoną do komputera. Sterowniki tej drukarki zostały dołączone do systemu Windows Server 2003- Czy użytkownik może zainstalować drukarkę?
3. Użytkownik chce zainstalować drukarkę USB podłączoną do komputera lokalnego. Sterownik dostarczony jest przez producenta i nie został dołączony do systemu Windows Server 2003. Sterownik został podpisany cyfrowo. Czy użytkownik może zainstalować drukarkę?

Podsumowanie lekcji

- W programie Device Manager (Menedżer urządzeń) wyswiedone są wszystkie wykryte urządzenia. Urządzenia nierozpoznane lub te, dla których wystąpiły problemy z konfiguracją sterownika, są specjalnie oznaczane.
- Konfiguracja sterowników może być wydrukowana za pomocą programu Device Manager (Menedżer urządzeń) lub zapisana w pliku CSV przy użyciu polecenia Driverquery.
- Użytkownicy mogą instalować i przyłączać dowolne urządzenia zgodne z technologią PnP. Jeśli podczas instalacji wymagana jest jakakolwiek interwencja ze strony użytkownika, nie będzie on mógł przeprowadzić tej instalacji.
- Punkty dostępu interfejsu do konfiguracji urządzeń i sterowników mogą być blokowane w oparciu o lokalne zasady grupy bądź w oparciu o zasady grupy domeny.
- Reakcja na instalowanie niepodpisanych sterowników określana jest za pomocą trzech ustawień: Ignore (Ignoruj), Warn (Ostrzegaj) oraz Block (Blokuj).

Lekcja 2: Konfigurowanie urządzeń sprzętu i sterowników

Urządzenia mogą wymagać aktualizacji sterowników wymuszonej zmianami w systemie operacyjnym Windows Server 2003 lub zmianami funkcjonalnymi urządzeń, wprowadzanymi przez producentów. Sterowniki aktualizowane są za pomocą programu *Device Manager* (Menedżer urządzeń).

Ewentualne problemy powstałe po zainstalowaniu nowego sterownika mogą być łatwo rozwiązane dzięki funkcji programu *Device Manager* umożliwiającej powrót do poprzednio zainstalowanego sterownika. Funkcja przywracania poprzedniej wersji sterownika dostępna jest na stronie *Properties* (Właściwości) danego urządzenia.

Czasami automatyczna konfiguracja zasobów w systemie Windows Server 2003 jest niewystarczająca, aby dostosować unikalny sposób wykorzystania urządzenia w danym komputerze. Jeśli urządzenie musi mieć statycznie określone zasoby (IRQ, porty I/O, DMA lub zakres pamięci), można zastosować program *Device Manager* do wyłączenia automatycznej konfiguracji, dzięki czemu administrator lub użytkownik będzie mógł skonfigurować urządzenie ręcznie.

Materiały omówione podczas lekcji pozwalają na

- Używanie programu Device Manager (Menedżer urządzeń) do aktualizacji, przywracania oraz odinstalowywania sterowników
- Używanie programu Device Manager (Menedżer urządzeń) do analizy i konfigurowania zasobów wykorzystywanych przez urządzenia

Szacunkowy czas lekcji: 15 minut

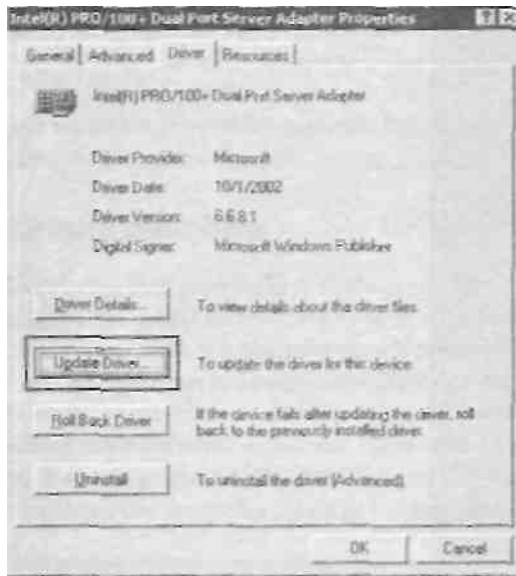
Aktualizacja sterowników

Większość urządzeń w programie *Device Manager* ma zaktualizowane sterowniki. Proces aktualizacji jest automatyczny lub ręczny w zależności od tego, czy urządzenie jest lub nie jest zgodne z technologią PnP. Aktualizacja może być przeprowadzana przez administratorów przy konsoli komputera lokalnego (zakładając, że pozostali użytkownicy nie mają przydzielonych wystarczających uprawnień).



Informacja Jeśli sterownik jest dostarczany poprzez usługę Windows Update, dla instalacji lokalnej nie są wymagane uprawnienia administratora. Więcej informacji o usłudze SUS (Software Update Services) i Windows Updates można znaleźć w rozdziale 9 „Obsługa systemu operacyjnego”.

Proces aktualizacji sterownika jest bardzo zbliżony do procesu instalowania sterownika poprawnie wykrytego urządzenia, z tą różnicą, że podczas instalacji sterownik nie był dostępny. Po rozpoczęciu aktualizacji sterownika urządzenia w programie *Device Manager*, program *Add Hardware Wizard* (Kreator dodawania sprzętu) poprosi o podanie lokalizacji nowego sterownika, a następnie zainstaluje sterownik. Niektóre główne sterowniki systemu wymagają ponownego uruchomienia komputera, ale dla większości urządzeń peryferyjnych nie jest to konieczne. Strona **Properties** (Właściwości), na której uruchamiany jest proces aktualizacji sterownika, została pokazana na rysunku 10-2.



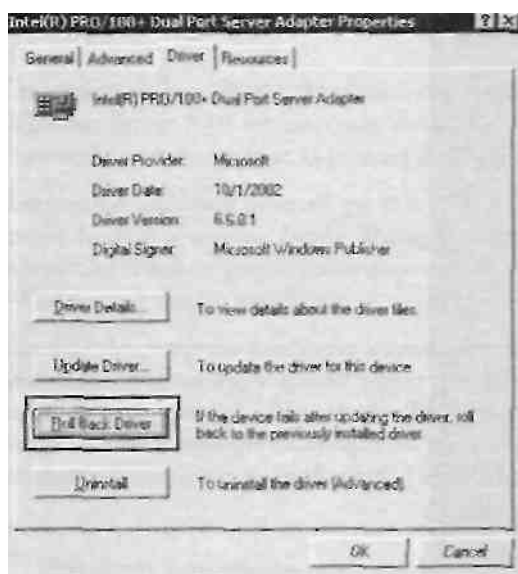
Rysunek 10-2 Aktualizacja sterownika



Informacja Jeśli odinstalowywane urządzenie było skonfigurowane z wykorzystaniem technologii PnP, w programie Device Manager (Menedżer urządzeń) należy uruchomić wyszukiwanie zmian urządzeń sprzętu, aby urządzenia zostały ponownie zainstalowane. Jest to spowodowane tym, że system Windows Server 2003 usuwa urządzenie z konfiguracji, nawet jeśli urządzenie to pozostaje podłączone do komputera.

Przywracanie sterowników

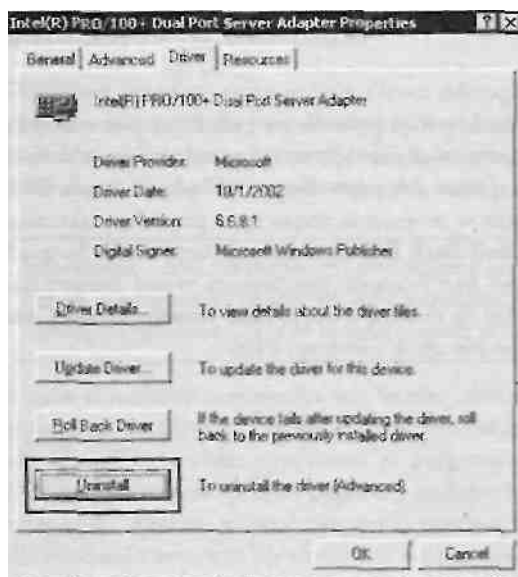
Czasami zdarza się, że nowy sterownik nie funkcjonuje prawidłowo i nie może pozostać w konfiguracji urządzenia. Jeśli zastąpiony sterownik funkcjonował prawidłowo, poprzednia wersja sterownika może zostać przywrócona za pomocą programu *Device Manager*. System Windows Server 2003 automatycznie wykonuje kopię zapasową sterownika w momencie rozpoczęcia procedury aktualizacji, dzięki czemu jest on dostępny przy użyciu opcji **Roll Back Driver** (Przywróć sterownik). Strona **Properties** (Właściwości), na której można rozpocząć przywracanie poprzedniej wersji sterownika pokazana została na rysunku 10-3. Różnice pomiędzy tą funkcją a opcją **Last Known Good Configuration** (Ostatnia znana dobra konfiguracja) opisane zostały w następnej lekcji.



Rysunek 10-3 Opcja Roli Back Driver (Przwróć sterownik)

Odinstalowywanie sterowników

Za pomocą programu *Device Manager* (Menedżer urządzeń) sterowniki mogą być odinstalowywane. Proces **Uninstall Driver** (Odinstaluj sterownik) rozpoczynany jest na stronie **Properties** (Właściwości) pokazanej na rysunku 10-4.

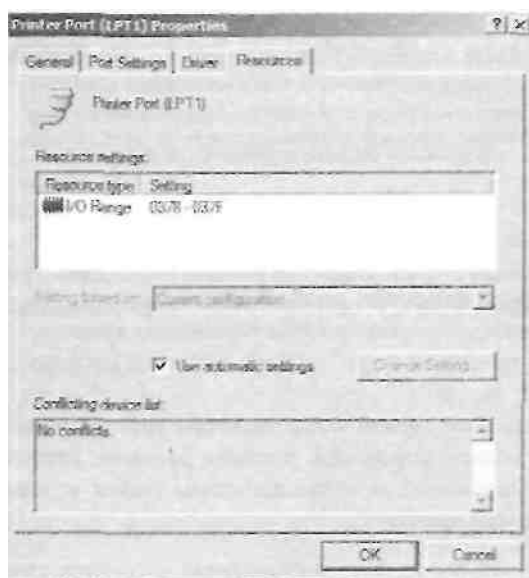


Rysunek 10-4 Uninstall Driver (Odinstaluj sterownik)

W wyniku odinstalowania sterownika uzyskuje się różne efekty w zależności od tego, czy urządzenie było wykryte i skonfigurowane w trybie PnP. Jeśli urządzenie zostało skonfigurowane w trybie PnP, to usunięcie sterownika spowoduje również usunięcie urządzenia z listy programu *Device Manager*. Jeśli natomiast sterownik urządzenia był dodawany ręcznie, urządzenie pozostanie w programie *Device Manager* jako urządzenie, dla którego nie został skonfigurowany sterownik.

Konfiguracja zasobów

Urządzenia i ich sterowniki potrzebują zasobów systemu podczas przetwarzania danych i komunikacji z systemem operacyjnym. Zasoby te są automatycznie konfigurowane przez system Windows Server 2003, czasami dla współużytkowanych funkcji przy udziale innych urządzeń systemu. W przypadku, kiedy zasoby muszą być konfigurowane statycznie, program *Device Manager* umożliwia pewną kontrolę zasobów przydzielanych do wykorzystywania przez urządzenie. Jeśli konfiguracja nie jest dostępna, zasoby używane przez urządzenie i jego sterownik nie mogą być konfigurowane ręcznie. Na rysunku 10-5 została pokazana zakładka *Resources* (Zasoby) znajdująca się na stronie *Properties* (Właściwości) urządzenia dla przypadku ręcznego konfigurowania zasobów.



Rysunek 10-5 Zakładka *Resources* (Zasoby) strony *Properties* (Właściwości) urządzenia, którego konfigurację można modyfikować

Aby ręcznie konfigurować przydział zasobów, należy w pierwszej kolejności usunąć zaznaczenie pola wyboru **Use Automatic Settings** (Użyj ustawień automatycznych), a dopiero następnie zasoby te mogą być określone.



Ostrzeżenie Ustawianie ręczne zasobu powoduje, że zasób nie może być konfigurowany automatycznie, co ogranicza możliwości dostosowawcze systemu Windows Server 2003. Może to stać się przyczyną problemów dla innych urządzeń.

Program Control Panel i konfiguracja urządzeń

W programie *Control Panel* (Panel sterowania) dla kilku urządzeń opracowano aplikacje umożliwiające konfigurację sprzętu. W programie *Control Panel* istnieją takie same ograniczenia, jak w programie *Device Manager*, dotyczące uprawnień użytkownika.

Strony *Properties* (Właściwości) są administrowane oddzielnie poprzez zasady grupy, a dostęp do nich oraz możliwości przeglądania mogą być dla użytkownika zabronione. Ustawienie to znajduje się w sekcji *User Configuration* (Konfiguracja użytkownika) zasad grupy.

Zadanie kontrolne: Konfigurowanie urządzeń

W zadaniu tym przeprowadzona zostanie chwilowa zmiana konfiguracji karty sieciowej polegająca na usunięciu jej z usługi bez odinstalowywania samego urządzenia.

Ćwiczenie 1: Wyłączenie urządzenia

1. Otwórz program *Device Manager*, a następnie zaznacz kartę sieciową skonfigurowaną w komputerze.
2. Kliknij dwukrotnie kartę sieciową.
3. Na liście rozwijanej **Device Usage** (Użycie urządzenia) zaznacz opcję **Do Not Use This Device (Disable)** [Nie używaj tego urządzenia (wyłącz)].

Urządzenie zostanie wyłączone w zakresie operacji wykonywanych w tym profilu *Hardware* (Sprzęt).

4. Otwórz stronę *Properties* (Właściwości) karty sieciowej i wybierz opcję **Use This Device (Enable)** [Użyj tego urządzenia (włącz.)], aby ponownie włączyć kartę sieciową w tym profilu sprzętowym. Innym sposobem włączania lub wyłączania karty jest klikanie jej prawym przyciskiem myszy i wybranie poleceń **Enable** (Włącz) lub **Disable** (Wyłącz) w zależności od bieżącego stanu urządzenia.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Jakie warunki muszą być spełnione, aby można było dostosowywać ustawienia zasobów urządzenia?
2. Administrator potrzebuje na krótko usunąć z konfiguracji urządzenie PnP, ale nie chce usuwać fizycznego połączenia urządzenia z komputerem, dzięki czemu późniejsze wykorzystanie urządzenia będzie wiązało się z minimalnym nakładem pracy. Która z poniżej wymienionych opcji najlepiej nadaje się do zrealizowania tego zadania?
 - a. Na stronie *Properties* (Właściwości) urządzenia należy wybrać opcję **Do Not Use this Device (Disable)** [Nie używaj tego urządzenia (wyłącz)].
 - b. Na stronie *Properties* (Właściwości) urządzenia należy wybrać opcję **Uninstall** (Odinstaluj).

- c. Wykorzystując program narzędziowy Safely Remove Hardware (Bezpieczne usuwanie urządzeń) usuń urządzenie.
- 3- Komputer użytkownika Greg jest wyposażony w zewnętrzny dysk twardy USB przyłączony do koncentratora USB tego komputera. Użytkownik powiadomił, że dysk jest podłączony prawidłowo, ale napęd (G), zazwyczaj skojarzony z tym dyskiem, nie jest dostępny. Po sprawdzeniu okazało się, że lampka kontrolna koncentratora nie świeci się, a urządzenie nie jest wymienione na liście urządzeń programu Device Manager (Właściwości). Odłączenie i ponowne przyłączenie urządzenia nie zmieniło sytuacji. Jaka jest prawdopodobnie najszybsza droga przywrócenia prawidłowego działania urządzenia?

Podsumowanie lekcji

- Program Device Manager (Właściwości) może być używany do włączania lub wyłączania poszczególnych urządzeń.
- Ręczna konfiguracja zasobów jest możliwa dla niektórych urządzeń, ale powinna być przeprowadzana jedynie, jeśli występuje konflikt z innymi zasobami tego komputera. Ręczna konfiguracja powinna być stosowana w minimalnym zakresie, aby nie ograniczać elastyczności konfiguracji automatycznej pozostałych urządzeń przeprowadzanej przez system Windows Server 2003.
- Aktualizacja sterowników przeprowadzana jest za pomocą programu Device Manager (Menedżer urządzeń).
- Funkcja Roll Back (Przywróć sterownik) w programie Device Manager (Menedżer urządzeń) umożliwia używanie poprzednio zainstalowanej wersji sterownika urządzenia.
- Aby urządzenie typu PnP, po jego odinstalowaniu, zostało ponownie włączone, wymagane jest ponowne przeszukanie zasobów komputera. Natomiast ponowne włączenie urządzenia, które nie jest zgodne z technologią PnP (po jego odinstalowaniu), wymaga ponownej instalacji urządzenia.

Lekcja 3: Rozwiązywanie problemów związanych z urządzeniami sprzętu i sterownikami

Problemy związane ze sterownikami narastają, w szczególności jeśli konfiguracja sterownika nie jest możliwa poprzez technologię PnP lub jeśli aktualizowane zostają sterowniki podstawowych komponentów systemu. Jeśli konfiguracja urządzenia nie jest możliwa poprzez PnP, wzrastają szanse na powstanie niezgodności pomiędzy urządzeniami i ich sterownikami. Podczas aktualizacji sterowników głównych elementów systemu, które wymagają ponownego uruchomienia komputera, problemy sterownika nie będą znane dopóki komputer nie zostanie ponownie uruchomiony.

Materiały omówione podczas lekcji pozwalają na

- Opanowanie sposobów wykorzystywania metod odzyskiwania urządzeń po awarii
- Zrozumienie i analizę problemów dotyczących sterowników

Szacunkowy czas lekcji: 15 minut

Przywracanie po awarii urządzenia

Czasami po instalacji lub aktualizacji sterownika występują problemy związane z funkcjonowaniem urządzenia w systemie. W zależności od roli urządzenia skutki problemu mogą być jedynie irytujące lub wręcz „katastroficzne”. W szczególności dla sterowników głównych elementów systemu, takich jak karty grafiki, awaria może spowodować, że komputer staje się bezużyteczny. W takiej sytuacji, kiedy na ekranie nic nie jest wyświetlane, trudne jest nawet przywrócenie poprzedniej wersji sterownika.

Na szczęście istnieje kilka metod odzyskiwania systemu po awarii wywołanej nieprawidłową konfiguracją sterownika. Dostępne narzędzia zostały opracowane dla różnych zastosowań i ich stosowanie wiąże się z różną szansą powodzenia operacji. W tabeli 10-3 zostały wymienione narzędzia, które mogą być używane w przypadku nieprawidłowej konfiguracji sterownika.

Tabela 10-3. Narzędzia odzyskiwania prawidłowej konfiguracji sterownika

Narzędzie	Skutki uszkodzenia	Wykorzystanie
Driver Rollback (Device Manager) fPrzywróć sterownik (Menedżer urządzeń)	Nieduże. Bez wpływu na większość funkcji systemu.	Należy użyć strony Property (Właściwości) urządzenia, aby powrócić do poprzedniej wersji sterownika, która funkcjonowała prawidłowo, a następnie skontaktować się z dostawcą, aby rozwiązać problem związany z nowym sterownikiem.

ciąg dalszy >ia następnej stronie

ciąg dalszy ze strony poprzedniej

Narzędzie	Skutki uszkodzenia	Wykorzystanie
Last Known Good Configuration (Ostatnia znana dobra konfiguracja)	Średnie/Poważne. Aktualizacja sterownika wymaga ponownego uruchamiania, a zmiany od ostatniego pomyślnego załogowania się zostaną utracone	W przypadku, kiedy zmiany sterowników wymagają ponownego uruchomienia komputera, można przywrócić informacje dotyczące starego sterownika modyfikując klucz rejestru HKLM\ System\CurrentControlSct. W tym celu, podczas uruchamiania systemu, należy nacisnąć przycisk F8 i wybrać opcję Last Known Good Configuration (Ostatnia znana dobra konfiguracja), za pomocą której odtworzone zostaną klucze rejestru. Jeśli problem nie zostanie rozwiązany do momentu załogowania się (co często zdarza się w przypadku aktualizacji sterowników karty grafiki), opcja Last Known Good (Ostatnia znana dobra konfiguracja) będzie mało użyteczna, ponieważ ustawienia zostaną zastąpione po pomyślnym załogowaniu się w systemie.
Safe mode (Tryb awaryjny)	Średnie/Poważne. System jest bezużyteczny.	Należy nacisnąć przycisk F8 i wybrać opcję Safe modę (Tryb awaryjny) jako opcję rozruchową. Tryb ten używa minimalnego zestawu sterowników systemu i urządzeń, który umożliwia uruchomienie komputera i załogowanie się w systemie, dzięki czemu możliwy będzie dostęp do programu Device Manager (Menedżer urządzeń) i wyłączenie źle działających urządzeń.
Recovery Console (Konsola odzyskiwania)	Poważne. Opcje Last Known Good (Ostatnia znana dobra konfiguracja) i Safe modę (Tryb awaryjny) nie działają.	Program Recovery Console (Konsola odzyskiwania) umożliwia załogowanie się i uzyskanie z okna wiersza poleceń dostępu do ograniczonej części systemu plików. Za pomocą konsoli Recovery Console można wyłączyć sterownik urządzenia powodującego problem, ale trzeba znać dokładną nazwę sterownika lub urządzenia (lub jednego i drugiego), a nazwy te mogą być dość trudne do zapamiętania.

Kody statusu w programie Device Manager

Jeśli urządzenie funkcjonuje nieprawidłowo, w programie *Device Manager* (Menedżer urządzeń) wyświetlany jest najczęściej komunikat o błędzie, a urządzenie oznaczane jest ikoną żółtego wykrzyknika umieszczaną obok urządzenia. Po dwukrotnym kliknięciu urządzenia (lub po kliknięciu prawym przyciskiem myszy i wybraniu właściwości), wyświetlone zostanie okno dialogowe, które zawiera listę wszystkich komunikatów o błędach wykrytych przez program *Deuice Manager*. W ramce *Deuice Status* (Stan urządzenia) umieszczany jest tekst opisujący stan urządzenia, ale podczas rozwiązywania problemów informacje tam zamieszczone mogą być niewystarczające. Często oprócz tekstu opisowego

umieszczany jest kod, na podstawie którego łatwiej będzie znaleźć rozwiązanie problemu. W tabeli 10-4 zostały wymienione te kody i związany z nimi sugerowany sposób postępowania.

Tabela 10-4. Rozwiązywanie problemów uszkodzonych urządzeń

Kod	Opis	Sposób rozwiązania problemu
1	Urządzenie nie jest prawidłowo skonfigurowane. Aby aktualizować sterownik tego urządzenia, należy kliknąć przycisk Update Driver (Aktualizuj sterownik). Jeśli to nie pomaga, w dokumentacji urządzenia sprzętu należy poszukać dodatkowych wskazówek.	Aby zaktualizować sterownik, należy użyć przycisku Update Driver (Aktualizuj sterownik).
3	Sterownik tego urządzenia może być uszkodzony lub w systemie brakuje pamięci bądź innych zasobów.	Sterownik tego urządzenia może być uszkodzony. Jeśli dokonywana jest próba uruchomienia uszkodzonego pliku, system może taką sytuację rozpoznawać jako brak pamięci.
10	Urządzenia nie można uruchomić. Należy spróbować aktualizować sterownik tego urządzenia.	Należy uruchomić program Hardware Update Wizard (Kreator aktualizacji sprzętu) przy użyciu przycisku Update Driver (Aktualizuj sterownik), ale nie należy zezwolić na to, aby system Windows Server 2003 automatycznie wykrywał urządzenia. Zamiast tej opcji, należy wybrać opcję Install From A List Or Specific Location (Advanced) [Zainstaluj z listy lub określonej lokalizacji (zaawansowane)] i ręcznie określić lokalizację sterownika. Należy kliknąć zakładkę Resources (Zasoby) strony Properties (Właściwości) zawierającej błąd. System Windows Server 2003 prawdopodobnie wymieni urządzenie, które jest w konflikcie z danym urządzeniem. Należy albo wyłączyć, albo usunąć urządzenie wywołujące konflikt. Następnie można ponownie dodać usunięte urządzenie i zobaczyć, czy urządzenie otrzymało dla siebie nowe zasoby lub czy zasoby te należy przydzielić ręcznie. Dla większości tych kodów, wywołanych przez nieprawidłowy sterownik, należy ponownie zainstalować sterownik.
12	Urządzenie nie potrafi wyszukać odpowiednich wolnych zasobów, które musi używać. Jeśli urządzenie to ma być wykorzystywane, należy wyłączyć inne urządzenie systemu.	
Większość pozostałych kodów	Różny	



Wskazówka Warto zapamiętać, że jeśli sterownik jest podpisany, został sprawdzony i powinien prawidłowo funkcjonować w systemie Windows Server 2003. Listę podpisanych sterowników można uzyskać przy użyciu programu Software Environment of the System Information (Informacje o systemie). Program ten jest dostępny w grupie programów System Tools (Narzędzia systemowe) lub poprzez wpisanie polecenia winmsd w wierszu programu Run (Uruchom).

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Administrator zakończył konfigurowanie nowego sterownika karty grafiki, który wymaga ponownego uruchomienia komputera. Krótco po zalogowaniu ekran komputera zrobił się „pusty” uniemożliwiając pracę na komputerze. Które techniki rozwiązywania problemów lub narzędzia pozwolą najłatwiej przywrócić funkcjonalność systemu po awarii sterownika karty grafiki?
 - a. Last Known Good Configuration (Ostatnia znana dobra konfiguracja)
 - b. Driver Rollback (Przywróć sterownik)
 - c. Safe mode (Tryb awaryjny)
 - d. Recovery Console (Konsola odzyskiwania)
2. W programie Device Manager (Menedżer urządzeń) wyświetlane jest urządzenie oznaczone przez ikonę błędu. Na stronie Properties (Właściwości) tego urządzenia, w ramce Device Status (Status urządzenia) umieszczona została informacja: „urządzenie nie może być uruchomione”. Jakie działania należy przedsięwziąć, aby rozwiązać problem?
3. Producent karty sieciowej bezprzewodowej, która jest zainstalowana w komputerze, opublikował nowy sterownik. Administrator chce sprawdzić funkcjonowanie sterownika. Którą opcję programu Device Manager (Menedżer urządzeń) wybierze administrator, aby przetestować nowy sterownik?

Podsumowanie lekcji

- Opcja Last Known Good Configuration (Ostatnia znana dobra konfiguracja) jest przydatna podczas przywracania poprzednio używanych sterowników, które nie spełniają normy PnP, ale tylko wtedy, jeśli użytkownik po ponownym uruchomieniu nie zalogował się w systemie.
- Uruchomienie komputera w trybie Safe (Tryb awaryjny) powoduje uruchomienie minimalnego zestawu sterowników umożliwiając dostęp do programu Device Manager (Menedżer urządzeń), dzięki czemu można wyłączyć, odinstalować lub przywrócić poprzednią wersję sterownika, który spowodował awarię.

- Większość problemów związanych ze sterownikami powstaje podczas ręcznej konfiguracji nieodpowiedniego sterownika.
- Ustawienia zasobów powinny być dostosowywane jedynie wtedy, gdy konflikt ustawień nie może być rozwiązany przez system operacyjny.
- Wszystkie ręcznie skonfigurowane przydziały zasobów nie mogą się powtarzać.

Zadanie praktyczne

Jeśli w komputerze występują konflikty przydziału zasobów urządzeń sprzętu, profile sprzętowe umożliwiają wybór urządzeń, które mają być włączane w zależności od spełnienia różnych warunków. Jest to alternatywne rozwiązanie w stosunku do prób konfiguracji ręcznej określającej, jakie zasoby należy przydzielić poszczególnym urządzeniom. Próby te zresztą nie muszą się zakończyć sukcesem, czyli utworzeniem działającej konfiguracji. Zdefiniowanie profilu sprzętowego, w którym dane urządzenie nie jest włączone, pozwala innym urządzeniom wykorzystywać zwolnione zasoby.

Profile sprzętowe umożliwiają również optymalizację wydajności oraz pewną kontrolę poboru mocy poprzez wyłączanie urządzeń lub usług nieużywanych w określonych sytuacjach. Przykładowo dla komputera przenośnego można wydłużyć czas życia baterii poprzez utworzenie profilu „mobilnego”, który wyłącza urządzenia niewykorzystywane w komputerze przy braku połączeń sieciowych.

W niniejszym ćwiczeniu wyłączana będzie karta sieciowa dla profilu sprzętowego komputera przenośnego.

1. W oknie **System Properties** (Właściwości systemu), na zakładce **Hardware** (Sprzęt) kliknij przycisk **Hardware Profiles** (Profile sprzętu).
2. Skopiuj bieżący profil do nowego profilu. Nazwij profil „mobile” i pozostaw ustawienia sekcji **Hardware Profiles Selection** (Wybór profilu sprzętu) zgodne z ustawieniami domyślnymi (wybierz pierwszy profil na liście, jeśli użytkownik nie wybierze profilu w ciągu 30 sekund).
3. Uruchom ponownie komputer. W oknie wyboru profilu wybierz profil **Mobile**, jako profil sprzętu używanego w systemie.
4. Zaloguj się i otwórz program **Device Manager** (Menedżer urządzeń) znajdujący się na zakładce **Hardware** (Sprzęt) w oknie **System Properties** (Właściwości systemu).
5. Kliknij prawym przyciskiem myszy kartę sieciową i wybierz polecenie **Properties** (Właściwości).
6. Na stronic **Properties** (Właściwości) karty sieciowej, na liście rozwijanej **Device Usage** (Użycie urządzenia) wybierz opcję **Do Not Use This Device In The Current Hardware Profile (disable)** [Nie używaj tego urządzenia w bieżącym profilu sprzętu (wyłącz)].

Dla jednego z profili sprzętu została wyłączona karta sieciowa. Opisywana metoda może być wykorzystywana w różnych sytuacjach, wliczając w to rozwiązywanie problemów urządzeń. Poprzez utworzenie profili sprzętu, które wyłączają lub włączają różne urządzenia, można przetestować interakcje poszczególnych urządzeń i wzajemne wykorzystanie zasobów.

Rozwiązywanie problemów

Pliki dystrybucji systemu Windows Server 2003 zawierają większość sterowników potrzebnych do skonfigurowania nowych urządzeń sprzętu, dzięki czemu błędne konfiguracje zdarzają się bardzo rzadko. Jednakże w przypadku ręcznego rozwiązywania konfliktów konfiguracji, błędne konfiguracje są najczęściej występującą sytuacją.

Jeśli konfiguracja urządzenia powoduje awarię komputera podczas jego uruchamiania, opcja Last Known Good Configuration (Ostatnia znana dobra konfiguracja) pozwala przywrócić używanie poprzednio zastosowanego sterownika. Zakładając, że nie dokonano logowania w systemie od momentu zainstalowania problematycznego sterownika, opcja Last Known Good Configuration (Ostatnia znana dobra konfiguracja) jest użytecznym narzędziem.

Jeśli użytkownik zalogował się w systemie, ustawienia opcji Last Known Good Configuration (Ostatnia znana dobra konfiguracja) zostaną zastąpione bieżącą konfiguracją. Jeśli więc uszkodzenie sterownika uniemożliwia działanie komputera po zalogowaniu się w systemie, należy zastosować tryb Safe (Tryb awaryjny), który jest opcją rozruchową komputera. Dzięki niej ładowany jest tylko minimalny zestaw sterowników, aby możliwe było skonfigurowanie źle funkcjonującego sterownika.

W niniejszym ćwiczeniu, podczas uruchamiania komputera aktywowane będą opcje Last Known Good Configuration (Ostatnia znana dobra konfiguracja) oraz Safe (Tryb awaryjny).

1. Uruchom ponownie komputer.
2. Podczas uruchamiania naciśnij przycisk F8.
3. Wybierz opcję **Last Known Good Configuration** (Ostatnia znana dobra konfiguracja).

W tym momencie wszystkie sterowniki nie spełniające normy PnP zainstalowane od momentu ostatniego uruchomienia zostaną zastąpione ich poprzednimi wersjami.

4. Uruchom ponownie komputer.
5. Podczas uruchamiania naciśnij przycisk F8.
6. Uruchom komputer w trybie Safe (Tryb awaryjny).
7. Zaloguj się na komputerze, a następnie uruchom program **Device Manager**.

Takie uruchomienie komputera umożliwia konfigurowanie urządzeń i ich sterowników, które będą używane podczas normalnego rozruchu.

Podsumowanie rozdziału

- Użytkownik musi posiadać uprawnienia administratora, aby mógł instalować urządzenia i sterowniki, które nie są zgodne z technologią PnP.
- Użytkownicy mogą instalować urządzenia zgodne z technologią PnP. Jeśli jednak podczas instalacji wymagane jest, aby sterownik był dodawany do komputera lub zachodzi konieczność konfigurowania sterownika, użytkownik nie będzie mógł przeprowadzać instalacji urządzenia.
- Program Device Manager (Menedżer urządzeń) za pomocą kilku rodzajów ikon zaznacza urządzenia, które nie mogły być skonfigurowane ze względu na konflikty zasobów lub nierozpoznanie sterownika.
- Dostęp do programu Device Manager (Menedżer urządzeń) oraz aplikacji w grupie programów Control Panel (Panel sterowania) służących do konfigurowania sprzętu może być blokowany dla użytkowników poprzez działanie zasady grupy.
- Po aktualizacji sterownika można powrócić do używania jego poprzedniej wersji za pomocą funkcji Driver Rollback (Przywróć sterownik) uruchamianej w programie Device Manager (Menedżer urządzeń).
- Urządzenia mogą być włączane lub wyłączane za pomocą programu Device Manager (Menedżer urządzeń).
- Urządzenia zgodne z technologią PnP posiadające podpisane sterowniki umieszczone na instalacyjnym dysku CD systemu Windows Server 2003 są konfigurowane automatycznie, a instalacja nie wymaga interwencji użytkownika.

Informacje dla zdających egzamin

Przed przystąpieniem do egzaminu należy zapoznać się z przedstawionymi poniżej najważniejszymi faktami i pojęciami, aby określić które tematy wymagają pogłębienia. Należy powrócić do lekcji, aby osiągnąć większą wprawę oraz przejrzeć działy znajdujące się w części 2 - „Materiały dodatkowe”. Informacje tu zawarte kierują do materiałów uzupełniających tematy objęte zadaniami egzaminacyjnymi.

Najważniejsze fakty

- Omówienie programu Device Manager (Menedżer urządzeń) w kontekście instalowania, aktualizacji, przywracania poprzedniej wersji sterowników urządzeń oraz włączania i wyłączania sterowników w profilach sprzętu. Warto zapamiętać, że za pomocą programu Device Manager (Menedżer urządzeń) można zmieniać ustawienia jedynie systemu lokalnego. W przypadku systemów zdalnych, program Device Manager (Menedżer urządzeń) może tylko odczytywać konfigurację.
- Użytkownicy mogą instalować wyłącznie urządzenia zgodne z technologią PnP.
- Uprawnienia administratora są wymagane podczas instalowania sterowników dostarczanych przez producentów oraz sterowników urządzeń nie spełniających normy PnP.
- Ponowna instalacja sterowników jest konieczna, chyba że konflikt zasobów został rozwiązany.
- Konflikty zasobów są rozwiązywane poprzez usunięcie zaznaczenia pola wyboru Use Automatic Settings (Użyj ustawień automatycznych), a następnie poprzez konfigurowanie ustawień zasobów.

- Opcja Last Known Good Configuration (Ostatnia znana dobra konfiguracja) jest przydatna jedynie, jeśli naprawa nastąpiła przed zakończeniem procedury związanej z ponownym uruchomieniem i logowaniem w systemie.
- Tryb awaryjny uruchamia minimalny zestaw sterowników tak, aby możliwe było przeprowadzenie odpowiednich zmian konfiguracji.

Najważniejsze pojęcia

Porównanie funkcji Roli Back Driver (Przywróć sterownik) z funkcją Last Known Good Configuration (Ostatnia znana dobra konfiguracja) Przywracanie sterownika wymaga logowania, podczas gdy logowanie unieważnia ustawienia opcji Last Known Good Configuration (Ostatnia znana dobra konfiguracja). Funkcje Roli Back Driver (Przywróć sterownik) i Last Known Good Configuration (Ostatnia znana dobra konfiguracja) odtwarzają poprzednią konfigurację sterownika urządzenia.

Porównanie funkcji odinstalowania i wyłączenia urządzenia Odinstalowanie urządzenia usuwa urządzenie ze wszystkich konfiguracji. W zależności od typu urządzenia, funkcja wykrywania urządzeń PnP lub wyszukiwania zmian konfiguracji sprzętu może zostać włączona podczas następnego uruchomienia komputera. W takiej sytuacji odinstalowane urządzenie będzie traktowane jak nowe urządzenie.

Wyłączenie urządzenia uniemożliwia jego używanie, ale po ponownym włączeniu urządzenia sterownik będzie obsługiwany i skonfigurowany.

Porównanie trybu Safe Modę (Tryb awaryjny) i funkcji Last Known Good Configuration (Ostatnia znana dobra konfiguracja) Uruchomienie w trybie awaryjnym powoduje załadowanie minimalnego zestawu sterowników, natomiast funkcja Last Known Good Configuration (Ostatnia znana dobra konfiguracja) przywraca poprzednią konfigurację sterowników.

Pytania i odpowiedzi

373 Pytania do lekcji 1

1. Administrator chce zapewnić, aby w sieci na komputerach nie były używane niepodpisane sterowniki. Które ustawienia i opcje konfiguracji strony Driver Signing (Podpisywanie sterowników) zapewnią takie wymagania?

W zasadzie grupy dla pulpitu komputerów należy ustawić opcje zabezpieczeń (Security Option) dla urządzeń (Devices): Unsigned Driver Installation Behavior (Zachowanie przy instalacji niepodpisanego sterownika) tak, aby obowiązywała opcja Do Not Allow Installation (Nie zezwalaj na instalację). Istnieje również możliwość wykorzystywania zasad grupy domeny do blokowania dla użytkowników komputerów dostępu do stron właściwości urządzeń i do przystawki Device Manager (Menedżer urządzeń).

2. Użytkownik chce zainstalować drukarkę USB podłączoną do komputera. Sterowniki tej drukarki zostały dołączone do systemu Windows Server 2003- Czy użytkownik może zainstalować drukarkę?

Tak. Drukarka USB, której sterownik został dołączony do systemu Windows Server 2003 jest drukarką typu PnP, a jej sterownik jest podpisany, czyli jej instalacja nie powinna wymagać interwencji ze strony użytkownika. Należy założyć, że w komputerze nie występują konflikty zasobów.

3. Użytkownik chce zainstalować drukarkę USB podłączoną do komputera lokalnego. Sterownik dostarczony jest przez producenta i nie został dołączony do systemu Windows Server 2003. Sterownik został podpisany cyfrowo. Czy użytkownik może zainstalować drukarkę?

Nie. Sterownik musi być wybrany za pomocą programu Add Hardware Wizard (Kreator dodawania sprzętu) systemu Windows Server 2003, co oznacza, że wymagana jest interakcja ze strony użytkownika. Ustawienia domyślne określają, że działanie takie jest zabronione.

378 Pytania do lekcji 2

1. Jakie warunki muszą być spełnione, aby można było dostosowywać ustawienia zasobów urządzeń?

Dostosowywanie sterownika jest najczęściej potrzebne podczas rozwiązywania problemów konfliktów wywołanych przez urządzenia, których konfiguracja nie została zakończona automatycznie przez system operacyjny, takich jak starsze urządzenia standardu ISA (Industry Standard Architecture) lub urządzenia mostkowane do magistrali PCI (Peripheral Component Interconnect).

2. Administrator potrzebuje na krótko usunąć z konfiguracji urządzenie PnP, ale nie chce usuwać fizycznego połączenia urządzenia z komputerem, dzięki czemu późniejsze wykorzystanie urządzenia będzie wiązało się z minimalnym nakładem pracy. Która z poniżej wymienionych opcji najlepiej nadaje się do zrealizowania tego zadania?

- a. Na stronie Properties (Właściwości) urządzenia należy wybrać opcję Do Not Use this Device (Disable) [Nie używaj tego urządzenia (wyłącz)].
- b. Na stronie Properties (Właściwości) urządzenia należy wybrać opcję Uninstall (Odinstaluj).
- c. Wykorzystując program narzędziowy Safely Remove Hardware (Bezpieczne usuwanie urządzeń) usunąć urządzenie.

Prawidłowa odpowiedź to a. Metoda ta umożliwia chwilowe wyłączenie urządzenia. Umożliwienie ponownego wykorzystywania urządzenia wiąże się jedynie z zaznaczeniem opcji „włącz”. Pozostałe wymienione opcje wymagają dodatkowo ponownej instalacji lub ponownego skanowania komputera.

3. Komputer użytkownika Greg jest wyposażony w zewnętrzny dysk twardy USB przyłączony do koncentratora USB tego komputera. Użytkownik powiadomił, że dysk jest podłączony prawidłowo, ale napęd (G) zazwyczaj skojarzony z tym dyskiem nie jest dostępny. Po sprawdzeniu okazało się, że lampka kontrolna koncentratora nie świeci się, a urządzenie nie jest wymienione na liście urządzeń programu Device Manager (Właściwości). Odlączenie i ponowne przyłączenie urządzenia nie zmieniło sytuacji. Jaka jest prawdopodobnie najszybsza droga przywrócenia prawidłowego działania urządzenia?

W programie Device Manager (Menedżer urządzeń) należy kliknąć prawym przyciskiem myszy koncentrator USB i wybrać opcję Scan for Hardware Changes (Skanuj w poszukiwaniu sprzętu). Działanie takie wykryje dysk twardy podłączony do koncentratora tak, jakby było to nowe urządzenie.

383 Pytania do lekcji 3

1. Administrator zakończył konfigurowanie nowego sterownika karty grafiki, który wymaga ponownego uruchomienia komputera. Krótco po zalogowaniu ekran komputera zrobił się „pusty” uniemożliwiając pracę na komputerze. Które techniki rozwiązywania problemów lub narzędzia pozwolą najszybciej przywrócić funkcjonalność systemu po awarii sterownika karty grafiki?
- a. Last Known Good Configuration (Ostatnia znana dobra konfiguracja)
 - b. Driver Rollback (Przywróć sterownik)
 - c. Safe mode (Tryb awaryjny)
 - d. Recovery Console (Konsola odzyskiwania)

Prawidłowe odpowiedzi to b oraz c. Opcja Last Known Good Configuration (Ostatnia znana dobra konfiguracja) jest nieprzydatna, ponieważ użytkownik zalogował się na komputerze, co spowodowało, że zmiany wprowadzone zostały na stałe. Tryb awaryjny pozwoli przywrócić sterownik przy użyciu programu Device Manager (Menedżer urządzeń).

2. W programie Device Manager (Menedżer urządzeń) wyświetlane jest urządzenie oznaczone przez ikonę błędu. Na stronie Properties (Właściwości) tego urządzenia, w ramce Device Status (Status urządzenia) umieszczona została informacja: „urządzenie nie może być uruchomione”. Jakiego działania należy przedsięwziąć, aby rozwiązać problem?

Należy zainstalować odpowiedni sterownik urządzenia za pomocą funkcji Update Driver (Aktualizuj sterownik) programu Device Manager (Menedżer urządzeń).

3. Producent karty sieciowej bezprzewodowej, która jest zainstalowana w komputerze, opublikował nowy sterownik. Administrator chce sprawdzić funkcjonowanie sterownika. Którą opcję programu Device Manager (Menedżer urządzeń) wybierze administrator, aby przetestować nowy sterownik?

Opcją programu Device Manager (Menedżer urządzeń), którą należy wybrać jest Update Driver (Aktualizuj sterownik). Opcja Reinstall Driver (Zainstaluj ponownie sterownik) może być pomocna dla nowych sterowników, to jednak wybranie opcji Update Driver (Aktualizuj sterownik) umożliwia

utworzenie pliku kopii zapasowej zawierającego bieżący sterownik, dzięki czemu w sytuacji, kiedy nowy sterownik nie funkcjonuje prawidłowo, można przywrócić poprzednią wersję sterownika.

11 Zarządzanie pamięcią dyskową w systemie Microsoft Windows Server 2003



Zadania egzaminacyjne omawiane w tym rozdziale:

- Zarządzanie dyskami podstawowymi i dynamicznymi
- Optymalizacja wydajności serwera
- Implementacja macierzy dyskowych RAID
- Defragmentacja woluminów i partycji
- Monitorowanie i optymalizacja środowiska serwera pod kątem wydajności aplikacji
- Monitorowanie przydziałów dysku
- Przywracanie po awarii sprzętu

Cele rozdziału

Jednym z truizmów związanych z branżą IT jest powiedzenie — nieważne jak dużą pamięć dysponujemy dzisiaj, jutro i tak będzie zapelniona. Całkiem niedawno pojemność napędów dyskowych mierzona była w megabajtach. Dzisiaj przedsiębiorstwa dyskutują o terabajtach. Wraz z tą mnogością danych i użytkowników, którzy je potrzebują, do niespotykanych rozmiarów wzrasta obciążenie podsystemów dyskowych serwerów.

Duże organizacje zaczynają stosować technologie SAN (Storage Area Network), które zbudowane są z połączonych światłowodami, niezawodnych macierzy dyskowych. Jednak pamięci dyskowe fizycznie podłączone do serwerów nie znikną tak szybko i dlatego warto sprawdzić, czy konfiguracja pamięci dyskowej serwera zapewnia optymalne zrównoważenie pomiędzy pojemnością, wydajnością i niezawodnością.

W niniejszym rozdziale zostały omówione sposoby organizowania jednego bądź kilku dysków, aby zostały spełnione wymagania postawione przed systemem pamięci dyskowych. Opisane zostały opcje dotyczące pamięci udostępniane w systemie Microsoft Windows Server 2003, wliczając w to elastyczne struktury umożliwiające zwiększanie pojemności, zapewnianie nadmiarowości oraz poprawę wydajności, najczęściej bez konieczności ponownego uruchamiania urządzeń! Informacje zamieszczone w rozdziale pozwalają zapoznać się ze sposobami konfigurowania i przywracania zestawów dyskowych utworzonych w oparciu o obsługę macierzy RAID (Redundant Array of Independent Disks) systemu Windows Server 2003- Oprócz tego, przeanalizowane zostanie działanie programów Check Disk (Sprawdź dysk), Disk Quotas (Przydział dysku) oraz Disk Defragmenter (Defragmentator dysków), które umożliwiają sprawne działanie dysku i być może wydłużą okres nieuchronnego zapelnienia pamięci dyskowej.

Lekcje rozdziału:

- Lekcja 1: Omówienie opcji dotyczących pamięci dyskowych 393
- Lekcja 2: Konfigurowanie dysków i woluminów 401
- Lekcja 3: Obsługa woluminów pamięci dyskowej 414
- Lekcja 4: Implementacja macierzy dyskowych RAID 423

Wymagania

W niniejszym rozdziale zostały przedstawione pojęcia i opisane umiejętności dotyczące pamięci dyskowych. Do przeprowadzenia ćwiczeń praktycznych związanych z omawianymi tematami wymagana jest następująca konfiguracja:

- Komputer z zainstalowanym systemem Windows Server 2003, Standard Edition lub Enterprise Edition.
- W serwerze powinien być zainstalowany co najmniej jeden dysk, który ma minimum 1 GB wolnej przestrzeni dyskowej.
- Komputer powinien nazywać się Server01 i powinien być kontrolerem domeny contoso.com.

Lekcja: Omówienie opcji dotyczących pamięci dyskowych

Przed przystąpieniem do instalacji napędu dyskowego warto zapoznać się z kilkoma ważnymi pojęciami dotyczącymi pamięci dyskowych. Niniejsza lekcja jest omówieniem pojęć, technologii, cech i terminologii związanej z pamięciami dyskowymi systemu Windows Server 2003. Opisane zostaną różnice pomiędzy podstawowymi a dynamicznymi dyskami oraz różne obsługiwane przez nie woluminy logiczne.

Materiały omówione podczas lekcji pozwalają na

- Zrozumienie pojęć i terminologii dotyczących pamięci dyskowych
- Rozróżnianie dynamicznych i podstawowych pamięci dyskowych
- Rozróżnianie zalet i ograniczeń podstawowych i dynamicznych dysków
- Rozróżnianie typów woluminów pamięci obsługiwanych w systemie Windows Server 2003

Szacunkowy czas lekcji: 15 minut

Dyski fizyczne

Dyski fizyczne są zestawem elementów wykonanych z plastiku, metalu oraz krzemu, które umożliwiają użytkownikom przechowywanie ogromnej liczby bezużytecznych danych i plików MP3, a czasami dokumentów biznesowych. W powyższym zdaniu jest dużo sarkazmu, ale z pewnością ważną sprawą jest zrozumienie różnic pomiędzy dyskiem fizycznym a jego woluminami logicznymi omawianymi w następnym paragrafie. Warto również zapamiętać, że zaawansowane podsystemy dyskowe, takie jak sprzętowe macierze RAID (*Redundant Array of Independent Disks*), mogą zawierać kilka dysków fizycznych, a dedykowane kontrolery ukrywają fizyczny układ dysków tak, że system Windows Server 2003 postrzega i przedstawia je jako pojedynczy dysk fizyczny.

Woluminy logiczne

Wolumin logiczny jest podstawową jednostką pamięci dyskowej, która jest konfigurowana i zarządzana przez administratora. Wolumin logiczny może rozciągać się na jednym lub kilku dyskach fizycznych. Woluminy logiczne (w kontekście monitorowania wydajności nazywane również dyskami logicznymi) są fizycznie rozróżnianymi jednostkami pamięci, umożliwiającymi rozdzielenie różnego typu informacji, takich jak system operacyjny, aplikacje czy dane użytkownika. Tradycyjnie, woluminy logiczne są przedstawiane za pomocą dysku oznaczonego pojedynczą literą.

Zapoznając się z terminologią dotyczącą dysków, na pewno natkniemy się na pojęcia takie jak partycje, dyski logiczne czy woluminy. Wiele opracowań używa tych pojęć zamiennie, ponieważ techniczne różnice pomiędzy nimi są niewielkie, a interfejs użytkownika i narzędzia wiersza poleceń jasno określają odpowiedni typ woluminu logicznego w oparciu o zadania wykonywane przez użytkownika. Nie warto zbyt długo zastanawiać się nad różnicami pomiędzy poszczególnymi pojęciami, gdyż jeśli nie są zrozumiałe na podstawie analizy, na pewno staną się jasne na podstawie doświadczeń.

Woluminy zainstalowane

Jak już wcześniej było powiedziane - woluminy logiczne są tradycyjnie reprezentowane przez dysk oznaczony pojedynczą literą. Struktura taka mocno ogranicza liczbę woluminów, które można utworzyć w systemie oraz elastyczność ich wykorzystywania. System plików NTFS Windows Server 2003 umożliwia przydzielenie jednej litery dysku do woluminu lub zezwala na nieprzydzielanie żadnej litery do woluminu. Oprócz tego, istnieje możliwość *zainstalowania woluminu* w jednym lub kilku pustych folderach istniejących woluminów NTFS. Na przykład, można utworzyć pusty folder Docs na istniejącym woluminie oznaczonym literą X: i zainstalować w nim nowy wolumin logiczny o pojemności 120 GB. Jeśli użytkownik przechodzi do foldera X:\Docs, podsystem dyskowy przekierowuje żądanie I/O (wejście/wyjście) do nowego woluminu. Wszystkie te operacje są niewidoczne dla użytkownika.

Możliwości tej ważnej cechy są, można powiedzieć, „nieograniczone”. Poprzez zainstalowanie woluminu w ścieżce foldera, rozszerzona zostaje dostępna przestrzeń dyskowa istniejącego woluminu. Jeśli istniejący wolumin nie jest odporny na uszkodzenia, a nowy wolumin ma taką właściwość, to folder, w którym zainstalowany został wolumin (X:\Docs) reprezentuje część przestrzeni nazw istniejącego woluminu, który jest odporny na uszkodzenia. Teoretycznie można by zainstalować wszystkie woluminy logiczne na serwerze w folderach na dyskach C lub D i tym samym utworzyć pamięć dyskową o ogromnej pojemności, przyporządkowaną napędowi oznaczonemu pojedynczą literą.

Odporność na uszkodzenia

Odporność na uszkodzenia odnosi się do właściwości systemu umożliwiającej kontynuowanie działania w sytuacji, kiedy jeden z komponentów, w tym przypadku dysk, ulega uszkodzeniu. System Windows Server 2003 umożliwia tworzenie dwóch typów woluminów logicznych, które są odporne na uszkodzenia: *dublowany* (RAID-1) i *rozłożony z parzystością* (RAID-5). Taki podsystem dyskowy nazywany jest często programową macierzą RAID. Szczegółowe informacje o tych konfiguracjach przedstawione zostały w dalszej części rozdziału, ale warto zapamiętać kilka faktów dotyczących odporności na uszkodzenia dysków w systemie Windows Server 2003:

- W konfiguracji dysków odpornej na uszkodzenia, używane są dwa lub kilka dysków, a pewna przestrzeń zostaje przydzielona do przechowywania danych, które umożliwią przywrócenie systemu w przypadku awarii pojedynczego dysku.
- Opcje związane z odpornością na uszkodzenia obsługiwane w systemie Windows Server 2003 nie umożliwiają pracy systemu, jeśli awarii ulegną jednocześnie co najmniej dwa dyski.
- System operacyjny umożliwia używanie dowolnych dwóch lub większej liczby dysków do utworzenia woluminów odpornych na uszkodzenia. Nie zachodzi konieczność zakupu dodatkowego sprzętu lub oprogramowania, aby od razu wykorzystywać odporne na uszkodzenia konfiguracje serwera. Jeśli w systemie Windows Server 2003 używane są woluminy dublowane lub RAID-5, to jednak na tej samej magistrali zaleca się stosowanie podobnych lub identycznych dysków. Łączenie różnych typów dysków lub używanie różnych magistral, jak SCSI (Small Computer Systems Interface) lub IDE (Integrated Device Electronics), może znacząco wpłynąć na wydajność systemu.
- Mówiąc o wydajności, aby zarządzać woluminami, funkcje zapewniające odporność na uszkodzenia systemu Windows Server 2003 wykorzystują cykle procesora oraz inne zasoby serwera. Macierz RAID-5 obniża wydajność serwera. Lepszym rozwiązaniem może okazać się zakup sprzętowego rozwiązania, zwanego *sprzętową macierzą RAID*. Sprzętowe macierze RAID wykorzystują dedykowane

kontrolery, a takie systemy, w porównaniu do macierzy RAID systemu Windows Server 2003, są na ogół szybsze i bardziej elastyczne podczas przywracania po awarii.

- Ponieważ sprzętowe kontrolery RAID przejmują zadania związane z zarządzaniem macierzy, macierz sprzętowa RAID pojawia się w systemie Windows Server 2003 jako pojedynczy dysk.

Separacja danych

Przed skonfigurowaniem podsystemu dyskowego serwera warto przeanalizować uważnie wymagania związane z pamięcią dyskową. Administratorzy najczęściej instalują system operacyjny na woluminie logicznym innym niż wolumin przeznaczony dla aplikacji i danych. Izolowanie systemu jest najprostszym sposobem zabezpieczenia woluminu systemu operacyjnego oraz zabezpieczeniem, że na woluminie tym nie zabraknie przestrzeni dyskowej. Oprócz tego, dla systemu operacyjnego zwykle instalowane są pewne mechanizmy odporności na uszkodzenia.

Aplikacje są przeważnie przechowywane na odrębnym woluminie, a dane i pliki użytkownika na jeszcze innym woluminie. W tym wypadku również izolowanie różnych rodzajów danych umożliwia zarządzanie zabezpieczeniami, wydajnością i odpornością na uszkodzenia oddzielnie dla każdego typu danych. Jeśli aplikacja używa dziennika transakcji do przygotowania wpisów do bazy danych tak, jak w przypadku usługi katalogowej Microsoft Active Directory czy programu Microsoft Exchange Server, to najczęściej dzienniki te przechowywane są na woluminach, które instalowane są na dyskach fizycznych innych niż dyski bazy danych. Dzięki temu, w przypadku awarii bazy danych, możliwe jest jej przebudowanie na podstawie dzienników.

Po przeanalizowaniu wymagań systemu pamięci dyskowej w kontekście typów danych, zabezpieczeń, wydajności i odporności na uszkodzenia, można przystąpić do określania z ilu dysków ma składać się system oraz w jaki sposób powinien być skonfigurowany.

Dyski podstawowe i dynamiczne

System operacyjny musi w sensowny sposób wykorzystywać fizyczną przestrzeń napędu dyskowego. System Windows Server 2003 został wyposażony w dwie struktury, które wspomagają przydział przestrzeni dyskowej: podstawowe i dynamiczne magazyny, nazywane również podstawowymi i dynamicznymi dyskami.

Dyski podstawowe, partycje i dyski logiczne

Dyski podstawowe obsługują dość dobrze znaną strukturę. Każdy dysk podstawowy jest podzielony na partycje, a każda partycja funkcjonuje jako fizycznie odrębna jednostka magazynu. Informacje o lokalizacji i rozmiarach każdej partycji przechowywane są w tablicy partycji głównego rekordu rozruchowego MBR (*Master Boot Record*) napędu dyskowego. Dysk podstawowy może zawierać najwyżej cztery partycje, składające się maksymalnie z czterech partycji podstawowych lub z trzech partycji podstawowych i jednej partycji rozszerzonej.

Woluminy logiczne dysku podstawowego są partycjami podstawowymi lub dyskami logicznymi. Jak już było nadmienione, wolumin logiczny może, ale nie musi być oznaczony przez litery dysku oraz może być instalowany w folderach na istniejącym woluminie NTFS.

- **Partycja podstawowa** Każda partycja podstawowa obsługuje jeden wolumin logiczny na dysku podstawowym. Jeśli dysk podstawowy używany jest do uruchomienia systemu operacyjnego, jedna i tylko jedna partycja podstawowa musi być oznaczona jako aktywna.



Wskazówka Program BIOS (input/output system) komputera wyszukuje aktywną partycję, aby zlokalizować pliki specyfikujące wymagania urządzeń sprzętu potrzebne do uruchomienia systemu operacyjnego. Partycja ta jest nazywana *partycją systemową* i zazwyczaj przydzielana jest jej litera „C”. Po rozpoczęciu procesu rozruchu następuje uruchamianie systemu operacyjnego. Również konfiguracja systemu operacyjnego większości serwerów używa litery C do oznaczenia dysku rozruchowego. Partycja, na której przechowywany jest system operacyjny, nazywana jest *partycją rozruchową*. Może to być trochę mylące, w szczególności, że ten sam wolumin oznaczony jest poprzez zmienną %Sysvol%. Na szczęście, prawdopodobnie nie trzeba będzie tego rozróżniać, ponieważ instalacja przeprowadzana jest w całości na dysku C, dzięki czemu dysk C staje się partycją systemową, partycją rozruchową i woluminem %Sysvol%.

- **Partycja rozszerzona** Dysk podstawowy może również zawierać partycję rozszerzoną. Inaczej niż w przypadku partycji podstawowych, partycje rozszerzone nie są formatowane i do oznaczenia dysku nie jest im przydzielana litera. Zamiast, partycje rozszerzone zostają podzielone na dyski logiczne. Dyski logiczne są woluminami logicznymi dysku podstawowego.

W przypadku poprzednich wersji systemu operacyjnego, takich jak Windows 95, Windows 98 bądź MS-DOS, system operacyjny mógł „widzieć” jedynie partycję podstawową, na której był zainstalowany oraz partycję rozszerzoną dysku, jeśli taka istniała. Jeśli na dysku zachodziła potrzeba zainstalowania dodatkowych segmentów pamięci, należało skonfigurować partycję rozszerzoną i przydzielić ją do jednego lub kilku dysków logicznych. Systemy Windows NT, Windows 2000, Windows XP oraz Windows Server 2003 mają dostęp do wszystkich partycji dysku, więc jeśli konfiguracja wymaga stosowania na pojedynczym dysku więcej niż czterech dysków logicznych, wystarczająca w tym celu będzie jedynie partycja rozszerzona.

Dynamiczne dyski i woluminy

Systemy Microsoft Windows, 2000, Windows XP oraz Windows Server 2003 obsługują dyskowe magazyny dynamiczne. Jednostki pamięci dysków dynamicznych nazywane są woluminami, a najważniejsza różnica pomiędzy magazynami dynamicznymi i podstawowymi polega na tym, że dynamiczne dyski obsługują nieograniczoną liczbę woluminów oraz że informacje o konfiguracji woluminów przechowywane są w bazie danych kontrolowanej przez usługę LDM (Logical Disk Manager).

Woluminem logicznym dysków dynamicznych jest wolumin. Dyski dynamiczne obsługują woluminy proste na pojedynczym dysku. Jeśli na komputerze są co najmniej dwa dyski dynamiczne, użytkownik ma do wyboru więcej opcji konfiguracyjnych. Woluminy łączone, dublowane (RAID-1), rozłożone (RAID-0) oraz rozłożone z parzystością (RAID-5) są woluminami logicznymi, które wykorzystują przestrzeń co najmniej dwóch dysków. Każdy typ woluminu inaczej wykorzystuje przestrzeń dyskową i opisany jest innym poziomem odporności na uszkodzenia. Poniższa lista jest podsumowaniem typów woluminu, chociaż pewne niuanse zostaną omówione w następnych fragmentach rozdziału.

- **Wolumin prosty** Ekwiwalentem partycji dysku podstawowego jest wolumin prosty dysku dynamicznego. Woluminy proste korzystają z przestrzeni pojedynczego dysku fizycznego, co odpowiada pojedynczemu woluminowi logicznemu. Woluminy proste mogą być rozszerzane poprzez dodawanie

nieprzydzielonej przestrzeni dyskowej tego samego dysku, dzięki czemu istnieje możliwość dostosowywania pojemności woluminu wraz ze wzrostem wielkości przechowywanych danych. Ponieważ woluminy proste istnieją tylko na dyskach fizycznych, nie są odporne na uszkodzenia.

- **Woluminy łączone** Wolumin łączony zawiera przestrzeń dyskową co najmniej dwóch dysków fizycznych. Wolumin łączony może składać się maksymalnie z 32 dysków fizycznych, a pojemność poszczególnych dysków może być różna. Zapis danych na woluminie rozpoczyna się od zapisu na pierwszym dysku zestawu. Po zapełnieniu pierwszego dysku, zaczyna się zapis na drugim dysku zestawu i tak dalej. Woluminy łączone są metodą zwiększania pojemności dysków. Jeśli wolumin prosty lub łączony zostanie zapełniony, można rozszerzyć wolumin dodając nową pamięć dyskową.

Woluminy łączone nie są odporne na uszkodzenia i nie mogą być używane w żadnej konfiguracji, która miałyby być odporna na uszkodzenia. Woluminy mają tendencję do zwiększania pojemności, co oznacza, że w zestawie stosowanych będzie coraz więcej dysków fizycznych, przez co ryzyko uszkodzenia woluminu wzrasta. Jeśli jeden dysk zestawu ulega awarii, uszkodzony zostaje również cały wolumin. Z tego powodu, Windows Server 2003 nie dopuszcza instalacji systemu na woluminie łączonym, jak również nie zezwala na rozszerzanie bądź łączenie woluminu systemowego. Stosowanie woluminów łączonych jest zalecane jako środek zaradczy w momencie zapełnienia istniejącego woluminu lub w sytuacji wysokiej odporności na uszkodzenia, przykładowo w dużej bibliotece niemodyfikowanych informacji, która w przypadku awarii może być łatwo odtworzona na podstawie kopii zapasowych.

- **Wolumin rozłożony** Wolumin rozłożony (RAID-0) łączy obszary wolnej przestrzeni dyskowej kilku dysków w jeden wolumin logiczny. Inaczej jednak jak w przypadku woluminów łączonych, dane są zapisywane na wszystkich dyskach fizycznych z taką samą prędkością. Ponieważ wykorzystywanych jest jednocześnie kilka napędów, wraz z dodaniem dysku fizycznego do zestawu wzrasta wydajność operacji odczytu i zapisu w tempie niemal geometrycznym. Jednak, podobnie jak w przypadku woluminów prostych i łączonych, jeśli dysk woluminu rozłożonego ulega awarii, cały wolumin zostaje uszkodzony.
- **Woluminy dublowane** Wolumin dublowany (nazywany również macierzą dyskową poziomu 1 lub RAID-1) składa się z dwóch identycznych kopii woluminu prostego, każda na innym dysku. Woluminy dublowane są odporne na uszkodzenia w sytuacji, kiedy jeden dysk zestawu ulega awarii.
- **Wolumin RAID-5** Wolumin RAID-5 jest odpornym na uszkodzenia woluminem rozłożonym. Przestrzeń co najmniej trzech dysków fizycznych jest traktowana jak pojedynczy wolumin. Dane są zapisywane na wszystkich dyskach fizycznych z taką samą prędkością, ale inaczej niż w przypadku woluminów rozłożonych, dane są przeplatane informacjami sumy kontrolnej, nazywanej parzystością. Pomimo awarii pojedynczego dysku woluminu, dane zapisane na tym dysku mogą być odtworzone na podstawie danych i sum kontrolnych zapisanych na pozostałych dyskach. Jest to ciekawa metoda, przy czym warto zapamiętać, że sumy kontrolne są zapisywane na wszystkich woluminach zestawu RAID-5.

Porównanie dysków podstawowych i dynamicznych

Po zapoznaniu się z dyskowymi pamięciami dynamicznymi i podstawowymi oraz z rodzajami obsługiwanych partycji, dysków logicznych i partycji nasuwa się pytanie: które rozwiązanie jest lepsze? W takim przypadku najczęściej pada odpowiedź: „To zależy...”.

Dyski dynamiczne zawierające dane można łatwo przenosić pomiędzy serwerami, dzięki czemu w przypadku awarii można je szybko zainstalować w sprawnym serwerze. Jednakże dyski dynamiczne mogą

stanowiąc problem, jeśli kilka takich dysków używanych jest w systemie. Każdy komputer systemu Windows 2000, Windows XP oraz Windows Server 2003 może obsługiwać grupę dysków, która sama może zawierać kilka dysków dynamicznych. Baza danych LDM jest replikowana na wszystkich dyskach grupy, co zwiększa elastyczność informacji związanych z konfiguracją dysku dla całej grupy dysków. Oprócz tego, dyski mogą być skonfigurowane łącznie, tworząc różne rodzaje woluminów, wliczając w to woluminy łączone, rozłożone (RAID-0), dublowane (RAID-1) oraz rozłożone z parzystością (RAID-5).

Istnieje kilka powodów, dla których w dalszym ciągu stosowane będą dyski podstawowe:

- Używanie dyskowej pamięci podstawowej jest opcją domyślną systemu Windows Server 2003, tak więc wszystkie nowe dyski, dopóki nie zostaną przekształcone na dyski dynamiczne, są dyskami podstawowymi (procedura została opisana w lekcji 2).
- Jeżeli w komputerze używany jest tylko jeden dysk, dyski dynamiczne nie są lepszym rozwiązaniem niż dyski podstawowe.
- W sytuacji, kiedy uszkodzeniu ulega dysk, działanie bazy danych LDM jest utrudnieniem podczas przeniesienia na inny komputer dysku dynamicznego używanego do uruchomienia systemu operacyjnego.
- Dyski dynamiczne nie są obsługiwane przez napędy nośników wymiennych oraz w komputerach przenośnych.
- Dyskowe magazyny podstawowe są standardem, dzięki któremu dyski podstawowe dostępne są dla wielu systemów operacyjnych, wliczając w to MS-DOS, wszystkie wersje systemów Microsoft Windows oraz większość systemów operacyjnych firm innych niż Microsoft (jest kilka takich systemów). Z tego powodu dyski dynamiczne nie mogą być używane, jeśli zachodzi potrzeba skonfigurowania komputera tak, aby możliwy był rozruch dwóch systemów operacyjnych (dual-boot), a jeden z nich jest starszą wersją systemu, która wymaga dostępu do dysku podstawowego. Warto zapamiętać, że omawiany jest wyłącznie dostęp *lokalny*. Jeśli dostęp do plików uzyskiwany jest poprzez sieć, dla dowolnej platformy niewidoczna jest warstwa związana z rodzajami pamięci dyskowych i woluminów.



Wskazówka egzaminacyjna Sytuacje, w których zachodzi potrzeba rozruchu kilku systemów operacyjnych komputera występują obecnie coraz rzadziej w oczekiwaniu na pojawienie się technologii maszyny wirtualnej (zobacz http://www.microsoft.com/windows/owsserver2003/techinfo/overview/_vrtual/zat/on.mspx). Jednakże, jeśli stosowany jest rozruch kilku systemów operacyjnych, a jednym z nich jest system Windows Server 2003, należy każdy system instalować na oddzielnej partycji podstawowej. Można powiedzieć, że inne konfiguracje są w najlepszym razie ryzykowne. Informacje o sposobach rozruchu kilku systemów operacyjnych można znaleźć w programie Help and Support Center (Centrum pomocy i obsługi technicznej).

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Administrator instaluje nowy dysk o pojemności 200 GB. Dysk ma być podzielony na pięć woluminów logicznych z przeznaczeniem dla systemu operacyjnego, aplikacji, katalogów macierzystych użytkowników, udostępnionych danych oraz punktu dystrybucji oprogramowania. Woluminy powinny mieć jednakową pojemność. 50 GB przestrzeni dyskowej powinno pozostać nieprzydzielone, aby można było w przyszłości rozszerzać wolumin logiczny. Biorąc pod uwagę dyski dynamiczne i podstawowe oraz obsługiwane przez nie rodzaje woluminów logicznych, jakie opcje konfiguracji należałoby zastosować?
2. Która z wymienionych poniżej konfiguracji umożliwia przywrócenie systemu po awarii pojedyn czego dysku twardego?
 - a. Primary partition (Partycja podstawowa)
 - b. Extended partition (Partycja rozszerzona)
 - c. Logical drive (Dysk logiczny)
 - d. Simple volume (Wolumin prosty)
 - e. Spanned volume (Wolumin łączony)
 - f. Mirrored volume (Wolumin dublowany)
 - g. Striped volume (Wolumin rozłożony)
 - h. RAID-5 volume (Wolumin RAID-5)
3. W systemie testowym używany jest rozruch dwóch systemów operacyjnych. Na pierwszej partycji podstawowej komputera zainstalowany został system Windows NT 4, a na drugiej partycji podstawowej system Windows Server 2003. Ponieważ w komputerze zaczyna brakować pamięci dyskowej, w systemie zainstalowany zostanie nowy napęd dyskowy. System został uruchomiony w oparciu o Windows Server 2003, a dysk skonfigurowany został jako dysk dynamiczny. Po rozruchu komputera w oparciu o system Windows NT 4 okazało się, że dysk nie jest widoczny. Dlaczego?
4. W celu zagwarantowania odporności na uszkodzenia, maksymalnej wydajności oraz możliwości wymiany uszkodzonych dysków bez wyłączania systemu (hot-swap) administrator zakupił macierz dyskową RAID składającą się z siedmiu dysków. Po zainstalowaniu macierzy, w systemie Windows Server 2003 widoczny był tylko jeden nowy dysk. Dlaczego?

Podsumowanie lekcji

- Terminologia dotycząca dysków może być myląca, ale ostatecznie wolumin logiczny jest praktycznie synonimem pojęć *partycja*, *dysk logiczny* lub *wolumin*.
- System Windows Server 2003 obsługuje dyski dynamiczne i podstawowe. Dyski podstawowe obsługują maksymalnie do czterech partycji: cztery partycje podstawowe lub trzy partycje podstawowe i jedna partycja rozszerzona, która obsługuje kilka dysków logicznych. Dyski dynamiczne obsługują woluminy proste lub jeśli w systemie zainstalowane zostały co najmniej dwa dyski, obsługują woluminy łączone, dublowane, rozłożone oraz RAID-5-
- Odporność na uszkodzenia zapewniają woluminy dublowane (RAID-1), które utrzymują pełną kopię danych woluminu na każdym z dwóch dysków zestawu oraz woluminy rozłożone z parzystością (RAID-5), które rozmieszczają dane na kilku dyskach i wykorzystują informacje sumy kontrolnej do obliczania brakujących danych uszkodzonego dysku.
- Woluminy proste, łączone, rozłożone (RAID-0) oraz wszystkie podstawowe napędy dysków logicznych nie zapewniają odporności na uszkodzenia. Wszystkie dane zostają utracone, jeśli jeden z dysków woluminu ulega awarii. Powiększanie tych woluminów lub dodawanie dysków fizycznych do zestawów zwiększa prawdopodobieństwo awarii.

Lekcja 2: Konfigurowanie dysków i woluminów

W trakcie niniejszej lekcji będą wykorzystywane pojęcia związane z pamięciami dyskowymi, opisane podczas poprzedniej lekcji. W oparciu o nie, przedstawione zostaną rzeczywiste umiejętności potrzebne do instalowania, konfigurowania i zarządzania pamięciami dyskowymi. Opisane zostaną sposoby używania programu narzędziowego *Disk Management* (Zarządzanie dyskami) w celu wykrywania i inicjowania nowo zainstalowanych dysków oraz w celu przydzielenia tych dysków do partycji, dysków logicznych i woluminów. Przedstawione zostaną również sposoby rozszerzania pojemności woluminu w sytuacji, kiedy wolumin zostaje zapelniony. Przeanalizowany zostanie proces przenoszenia dysków pomiędzy serwerami, a na koniec omówiony będzie program narzędziowy DISKPART, który umożliwia zarządzanie pamięciami dyskowymi za pomocą komend wiersza poleceń.

Materiały omówione podczas lekcji pozwalają na

- Instalowanie i inicjowanie dysków fizycznych
- Zarządzanie konfiguracją woluminów logicznych dysków dynamicznych i podstawowych
- Instalowanie woluminu w folderze woluminu NTFS
- Rozszerzanie pojemności woluminu
- Przenoszenie dysków pomiędzy serwerami
- Przekształcanie dysków dynamicznych i podstawowych
- Zarządzanie dyskami przy użyciu programu DISKPART

Szacunkowy czas lekcji: 25 minut

Zarządzanie dyskami

Zadania związane z zarządzaniem dyskami wykonywane są za pomocą przystawki *Disk Management* (Zarządzanie dyskami) konsoli MMC (Computer Management Console). W konsoli MMC należy otworzyć tę przystawkę lub dodać ją do niestandardowej konsoli.

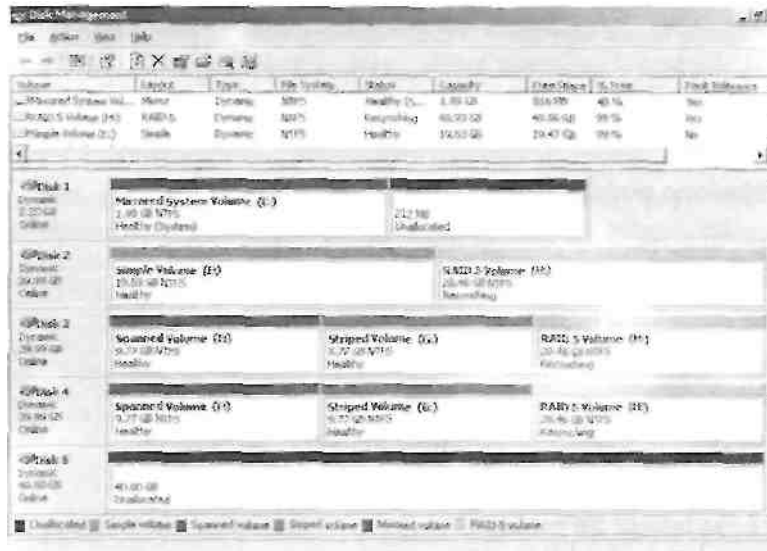


Wskazówka Istnieje możliwość uruchomienia pojedynczej konsoli *Disk Management*, ale nie jest to możliwe w folderze *Administrative Tools* (Narzędzia administracyjne). W tym celu należy kliknąć menu **Start**, następnie wybrać polecenie **Run** (Uruchom) i wpisać komendę **diskmgmt.msc**.

Za pomocą programu *Disk Management* można zarządzać pamięciami dyskowymi systemów lokalnych i zdalnych. Przystawka nie wykonuje swoich operacji bezpośrednio na dyskach, ale działa wspólnie z usługą *Dmadmin*. Usługa *Logical Disk Manager Administrative Service* (Menedżer dysków logicznych) jest uruchamiana na komputerze w momencie uruchomienia przystawki *Disk Management*.

Na rysunku 11-1 przedstawiony został interfejs programu *Disk Management*. W górnej ramce (lista woluminów) wyświetlone są informacje o każdej partycji, dysku logicznym lub woluminie. W dolnej ramce (widok graficzny) przedstawione są przydziały przestrzeni dyskowej poszczególnych dysków fizycznych tak, jak rejestruje to system Windows Server 2003. Kliknięcie prawym przyciskiem myszy

woluminów w którejkolwiek ramce powoduje wyświetlenie menu skrótów. W menu tym dostępne są polecenia formatowania, usuwania lub przydzielania do woluminu litery oznaczającej dysk. Natomiast kliknięcie prawym przyciskiem myszy obszaru nieprzydzielonej przestrzeni dyskowej umożliwia utworzenie partycji lub woluminu. Z kolei kliknięcie prawym przyciskiem myszy znajdującego się po lewej stronie widoku graficznego, okna statusu napędu dysku umożliwia zainicjowanie nowego dysku, konwersję pomiędzy dyskami dynamicznymi i podstawowymi oraz dostęp do okna dialogowego właściwości urządzenia dyskowego.



Rysunek 11-1 Konsola Disk Management (Zarządzanie dyskami)

Konfigurowanie dysków i woluminów

Procedura konfiguracji pamięci dyskowej składa się z następujących etapów:

1. Fizyczne zainstalowanie dysku (lub dysków).
2. Inicjowanie dysku.
3. Na dysku podstawowym — utworzenie partycji i dysków logicznych (jeśli istnieje partycja rozszerzona).
Na dysku dynamicznym - utworzenie woluminów.
4. Sformatowanie woluminów.
5. Przypisanie liter oznaczających dyski do woluminów lub zainstalowanie woluminów w pustym folderze istniejących woluminów NTFS.

Aby wykonać te zadania, użytkownik musi być członkiem grupy *Administrators* bądź *Backup Operator* (Operacorky kopii zapasowych), albo też musi posiadać odpowiednie uprawnienia. Formatować wolumin mogą jedynie administratorzy.

Instalowanie dysku

Aby dodać nowy dysk do komputera, należy zainstalować lub przyłączyć nowy dysk (lub dyski) fizycznie. Następnie należy otworzyć program *Disk Management* (Zarządzanie dyskami) i jeśli dysk nie został automatycznie wykryty, należy kliknąć prawym przyciskiem myszy węzeł przystawki **Disk Management** i wybrać polecenie **Rescan Disks** (Skanuj dyski ponownie). Jeśli system musi zostać wyłączony, aby możliwe było zainstalowanie nowego dysku, należy ponownie uruchomić komputer, a następnie otworzyć przystawkę *Disk Management*. Jeśli dysk nie został automatycznie wykryty, należy ponownie skanować dyski.

Inicjowanie dysku

Po dodaniu dysku do serwera, należy przeprowadzić inicjowanie dysku, zanim możliwe będzie przydzielanie jego przestrzeni dyskowej do partycji, dysków logicznych i woluminów. Inicjowanie dysku pozwala systemowi operacyjnemu zapisać sygnaturę dysku, znacznik końca sektora (nazywany również sygnaturą słowa) oraz rekord MBR lub identyfikator GUID (Globally Unique Identifier) tablicy partycji dysku.

Jeśli konsola *Disk Management* została uruchomiona po zainstalowaniu nowego dysku, automatycznie zostanie uruchomiony program *Initialize Disk Wizard* (Kreator inicjowania dysku). Aby za pomocą przystawki *Disk Management* zainicjować dysk ręcznie, należy kliknąć prawym przyciskiem myszy okno statusu dysku i wybrać polecenie **Initialize Disk**.



Informacja W komputerach opartych na procesorze Itanium można wybrać styl partycji. Komputery te wyposażone w kilka dysków obsługują dwa style partycji - partycja GUID z tabelą partycji (GPT) oraz partycja z rekordem MBR. Partycja systemowa komputerów wyposażonych w procesory Itanium używa interfejsu EFI (Extensible Firmware Interface) oraz stylu partycji GPT do obsługi 64-bitowej wersji systemu Windows Server 2003. Więcej informacji o partycjach GPT i EFI można znaleźć w programie Help And Support Center (Centrum pomocy i obsługi technicznej).

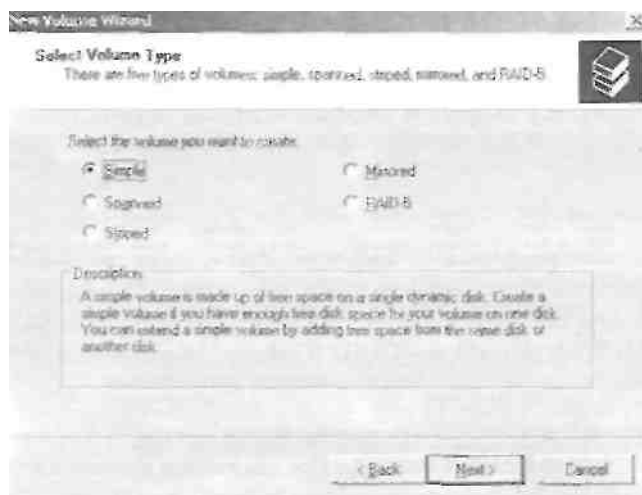
Tworzenie partycji i woluminów

Po zainicjowaniu dysku można rozpocząć wprowadzanie struktury partycji, dysków logicznych lub woluminów.

Ustawienia domyślne określają, że nowo zainicjowany dysk zostaje skonfigurowany jako dysk podstawowy. Jeśli w systemie ma być używany dysk podstawowy, to można podzielić dysk na partycje podstawowe i rozszerzone. W tym celu należy kliknąć prawym przyciskiem myszy nieprzydzieloną przestrzeń i wybrać polecenie **New Partition** (Nowa partycja). Utworzenie partycji podstawowej powoduje, że partycja ta staje się woluminem logicznym. Po utworzeniu partycji rozszerzonej, należy ponownie kliknąć prawym przyciskiem myszy partycje i wybrać polecenie **New Logical Drive** (Nowy dysk logiczny). Zgodnie z wcześniejszym opisem, dyski logiczne są woluminami logicznymi partycji rozszerzonej.

Jeśli chcemy, aby dysk był dyskiem dynamicznym, należy w przystawce *Disk Management* kliknąć prawym przyciskiem myszy okno statusu dysku i wybrać polecenie **Convert To Dynamic Disk** (Konwertuj na dysk dynamiczny). Następnie można kliknąć nieprzydzieloną przestrzeń dyskową i wybrać polecenie **New Volume** (Nowy wolumin). Uruchomiony zostanie program *New Volume Wizard*.

(Kreator nowego woluminu), za pomocą którego użytkownik dokonuje wyboru rodzaju obsługiwanych w systemie woluminów. Strona kreatora *Select Volume Type* (Wybieranie rodzaju woluminu) została pokazana na rysunku 11-2.



Rysunek 11-2 Strona *Select Volume Type* (Wybieranie rodzaju woluminu) programu *New Volume Wizard* (Kreator nowego woluminu)

Użytkownik może przekształcić istniejący dysk podstawowy na dysk dynamiczny. Rozwiązanie takie zostało omówione w dalszej części lekcji.

Formatowanie woluminów

System Windows Server 2003 obsługuje trzy systemy plików: FAT, FAT32 oraz NTFS. Tworząc niniejszy rozdział przyjęto następujące założenie: systemy plików FAT lub FAT32 są używane tylko, gdy występują ku temu szczególne powody. Jedynie system NTFS zapewnia poziom stabilności, skalo-walności, elastyczności i bezpieczeństwa wymagany przez większość organizacji. Wiele głównych komponentów systemu Windows Server 2003, takich jak zabezpieczenia plików czy usługi Active Directory i RIS (Remote Installation Services), wymagają stosowania NTFS. Podobnie, używanie systemu NTFS jest wymagane dla wszystkie zaawansowanych zadań związanych z zarządzaniem pamięcią dyskową, wliczając w to woluminy wielodyskowe i przydziały dysku. Podsumowując, podejmując decyzję o wykorzystywaniu systemu plików FAT32, trzeba bardzo uważnie przeanalizować wszystkie wady i zalety tego rozwiązania.

Przypisywanie litery oznaczającej dysk lub instalowanie woluminów

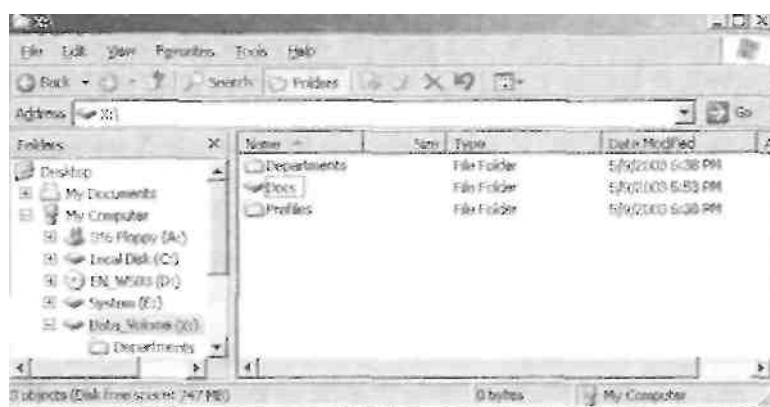
Podczas tworzenia woluminu jest on domyślnie przypisywany do następnej dostępnej litery oznaczającej dysk. Programy *New Volume Wizard* (Kreator nowego woluminu) oraz *New Partition Wizard* (Kreator nowej partycji) dają możliwość alternatywnego określenia nowego woluminu logicznego. Można również kliknąć prawym przyciskiem myszy istniejący wolumin i wybrać polecenie **Change Drive Letter and Paths** (Zmień literę dysku i ścieżki).

Wolumin może być reprezentowany tylko przez jedną literę, ale może też w ogóle nie być oznaczany literą. Istnieje możliwość zainstalowania woluminu w jednym lub kilku pustych folderach lokalnych woluminów NTFS. W oknie dialogowym *Change Drive Letter And Paths* (Zmień literę dysku i ścieżki) można kliknąć przyciski **Remove** (Usuń) lub **Change** (Zmień), aby odpowiednio usunąć lub zmodyfikować przypisanie do woluminu litery dysku bądź foldera.



Informacja Nie można zmieniać litery dysku woluminu, który jest partycją systemową lub rozruchową.

W celu dodania litery dysku lub punktu instalowania, należy kliknąć przycisk **Add** (Dodaj). Na rysunku 11-3 został pokazany serwer, którego folder Docs na dysku X jest punktem instalacji innego woluminu. Warto zauważyć, że w przestrzeni nazw programu Explorer (Eksplorator) folder pojawia się dokładnie tam, gdzie powinien, ale wyświetlana jest przy nim ikona woluminu. Przejście do tego foldera powoduje niewidoczne dla użytkownika przekierowanie do woluminu.



Rysunek 11-3 Wolumin zainstalowany na ścieżce foldera

Instalowanie woluminu na ścieżce istniejącego woluminu jest efektywnym sposobem zwiększania pojemności woluminu docelowego i wolnej przestrzeni dyskowej. Woluminy można instalować niezależnie od tego, czy są one podstawowe czy dynamiczne, a także niezależnie od ich rodzaju. Wymogiem jest, że pusty folder, czyli ścieżka, na podstawie której powstaje ścieżka instalacji woluminu, musi znajdować się na woluminie NTFS. Z technicznego punktu widzenia, zainstalowany wolumin może zostać sformatowany jako FAT lub FAT32, ale nie jest to oczywiście zalecana praktyka.

Woluminy rozszerzone

Innym sposobem zwiększenia pojemności woluminu jest jego rozszerzanie. Rozszerzane mogą być woluminy proste lub łączone dysków dynamicznych, o ile woluminy są sformatowane jako NTFS oraz o ile woluminy nie są woluminami systemowymi bądź rozruchowymi. Aby rozszerzyć wolumin, należy kliknąć go prawym przyciskiem myszy i wybrać polecenie **Extend Volume** (Rozszerz wolumin). Zgodnie z instrukcjami programu *Extend Volume Wizard* (Kreator rozszerzonego woluminu) należy wybrać nieprzydzieloną przestrzeń dysków dynamicznych, o którą rozszerzony zostanie istniejący wolumin.

Jeśli wolumin prosty zostanie rozszerzony o przestrzeń innego dysku fizycznego, utworzony zostanie wolumin łączony.

Partycję dysku podstawowego można rozszerzać za pomocą polecenia DISKPART. Partycja podstawowa musi być sformatowana jako NTFS, nie może być partycją systemową lub rozruchową oraz musi być rozszerzana w oparciu o bezpośrednio przylegającą ciągłą przestrzeń tego samego dysku fizycznego, która jest nieprzydzielona i niesformatowana lub jest sformatowana za pomocą systemu NTFS.

Przenoszenie dysków pomiędzy serwerami

Istnieje możliwość przenoszenia dysków pomiędzy komputerami. Jeśli na przykład administrator planuje wyłączyć komputer, może przyłączyć jego dyski fizyczne do innego serwera, dzięki czemu dane będą stale dostępne. Procedura jest następująca:

1. Sprawdź status dysku w pierwszym serwerze. W tym celu zaleca się otworzyć program *Disk Management* (Zarządzanie dyskami) i przed przeniesieniem dysku sprawdzić, czy wyświetlany status określany jest jako *Healthy* (Zdrowy). Jeśli dysk jest uszkodzony, należy go najpierw naprawić.
2. Odinstaluj dysk pierwszego komputera. Jeśli pierwszy serwer jest włączony (w trybie online), odinstaluj dysk klikając go prawym przyciskiem myszy w programie *Device Manager* i wybierając polecenie **Uninstall** (Odinstaluj).
3. Usuń dysk dynamiczny. Jeśli pierwszy serwer jest włączony (w trybie online), otwórz program *Disk Management*, kliknij prawym przyciskiem myszy dysk dynamiczny i wybierz polecenie **Remove** (Usuń). Dla dysków podstawowych ten krok nie jest ani potrzebny, ani możliwy.
4. Fizycznie odłącz dysk. Jeśli komputer obsługuje dyski, które umożliwiają odłączenie ich od systemu bez wyłączania zasilania (hot-swap), użytkownik może taki dysk odłączyć. W innym razie, aby fizycznie odłączyć dysk, należy wyłączyć komputer.
5. Podłącz dysk do komputera docelowego. Otwórz program *Disk Management* i jeśli dysk nie został automatycznie wykryty, kliknij prawym przyciskiem myszy węzeł programu **Disk Management** i wybierz polecenie **Rescan Disks** (Ponownie skanuj dyski). W innym przypadku, przed dodaniem dysku, należy wyłączyć serwer docelowy.
6. Postępuj zgodnie z instrukcjami programu *Found New Hardware Wizard* (Kreator wyszukiwania nowego sprzętu). Jeśli kreator nie został uruchomiony, otwórz program *Device Manager* sprawdzając, czy dysk został automatycznie wykryty i zainstalowany. Jeśli nie, należy otworzyć program **Add Hardware** (Dodaj sprzęt) w folderze *Control Panel*.
7. Kliknij prawym przyciskiem myszy dowolny dysk oznaczony jako *Foreign* (Obcy) i wybierz polecenie **Import Foreign Disks** (Importuj obce dyski). Importowanie dysku powoduje synchronizację baz danych LDM nowego dysku dynamicznego i istniejących dysków.

Kilka istotnych uwag dotyczących przenoszenia dysków fizycznych:

- Jeśli dysk importowany zawiera woluminy, które łączą inne dyski fizyczne, zanim będzie możliwe uzyskanie dostępu do woluminu, należy przyłączyć i zaimportować wszystkie dyski fizyczne.
- Jeśli dyski kilku komputerów przenoszone są do pojedynczego komputera, należy przenosić je kolejno, najpierw wszystkie dyski jednego komputera, a następnie dyski następnego komputera.
- Do woluminu podstawowego przeniesionego do nowego komputera przydzielona zostanie kolejna dostępna litera dysku. Woluminy dynamiczne zachowują oznaczenie literowe, jakie miały

w komputerze pierwotnym. Jeśli na poprzednim komputerze wolumin dynamiczny nie miał przydzielonej litery, po przeniesieniu do innego komputera nie otrzymuje litery dysku. Jeśli na komputerze docelowym, dana litera dysku jest już w użyciu, do woluminu przydzielona zostanie kolejna dostępna litera.

- Użycie poleceń **Mountvol /n** lub **DISKPART automount** zapobiega automatycznej instalacji i automatycznemu przydzielaniu litery dysku. Jeśli polecenia te zostały zastosowane podczas dodawania nowego dysku, użytkownik musi ręcznie zainstalować woluminy i przydzielić litery lub ścieżki dysku.

Konwersja pamięci dyskowych

Dysk podstawowy może zostać przekształcony na dysk dynamiczny. Jeśli dysk ma już partycje i dyski logiczne, jednostki te zostaną przekształcone na równoważne jednostki dysku dynamicznego, czyli woluminy proste. Struktura danych na dysku nie zostaje zmieniona, dzięki czemu istnieje możliwość konwersji dysku podstawowego, który zawiera dane, chociaż zalecaną praktyką jest utworzenie kopii zapasowych zawsze przed wykonywaniem zadań związanych z zarządzaniem dyskami.

Aby przekształcić dysk podstawowy na dysk dynamiczny, należy kliknąć prawym przyciskiem myszy okno statusu dysku i wybrać polecenie **ConvertTo Dynamic Disk** (Konwertuj na dysk dynamiczny). Jest więc to bardzo prosta operacja. Jeśli dysk zawiera partycję systemową lub rozruchową, należy ponownie uruchomić komputer.



Wskazówka Nie należy przekształcać dysków podstawowych na dynamiczne, jeśli dyski te zawierają kilka systemów operacyjnych (na przykład konfiguracja dysku umożliwia rozruch dwóch systemów operacyjnych). Po przekształceniu, będzie możliwe uruchomienie systemu operacyjnego, który był używany pod czas konwersji dysku, ale rozruch w oparciu o drugi system nie będzie możliwy.

Niestety proces odwrotny nie jest taki prosty. Przekształcenie odwrotne (na dysk podstawowy) usuwa dane zapisane na dysku. Dlatego najpierw należy wykonać kopię zapasową wszystkich danych dysku. Następnie należy usunąć wszystkie istniejące woluminy dysku dynamicznego, a dopiero następnie można kliknąć prawym przyciskiem myszy okno statusu dysku w programie *Disk Management* i wybrać polecenie **Convert To Basic Disk** (Konwertuj do dysku podstawowego). Po ponownym utworzeniu partycji i dysków logicznych należy odtworzyć dane dysku. Chociaż z technicznego punktu widzenia można przekształcić dysk dynamiczny na podstawowy, tak naprawdę dane są usuwane i konfigurowanie dysku rozpoczyna się od początku.

Wykonywanie zadań związanych z zarządzaniem dyskami w oknie wiersza poleceń

System Windows Server 2003 umożliwia zarządzanie dyskiem za pomocą komend wiersza poleceń. Używane są następujące polecenia:

- **Chkdsk** Skanuje dysk w poszukiwaniu błędów i ewentualnie próbuje je usunąć.
- **Convert** Przekształca wolumin sformatowany jako FAT lub FAT32 na NTFS.
- **Fsutil** Wykonuje różne zadania dotyczące zarządzania woluminami FAT, FAT32 lub NTFS.
- **Mountvol** Zarządza zainstalowanymi woluminami i punktami ponownej analizy.

Jednak najważniejszym narzędziem wiersza poleceń dotyczącym zarządzania dyskami jest **DISKPART**. Tabela 11-1 przedstawia podsumowanie poleceń programu DISKPART, za pomocą których można zrealizować najczęściej używane zadania. Program Diskpart może być używany w trybie interakcyjnym lub poprzez wywołanie skryptu. Aby uruchomić program w trybie interakcyjnym, należy w wierszu poleceń wpisać komendę **diskpart**. Po wyświetleniu znaku zachęty programu (DISKPART>), w dowolnym momencie można wpisać znak zapytania ?, aby wyświetlić informacje wbudowanej pomocy (Help). Dokumentacja modułu wyświetlana jest automatycznie, jeśli podczas wykonywania zadań użytkownik potrzebuje odpowiedzi. Aplikacja jest również dokładnie opisana w programie *Help And Support Center* (Centrum pomocy i obsługi technicznej).

Tabela 11-1. Sposoby realizacji najczęściej wykonywanych zadań dotyczących zarządzania dyskami przeprowadzane w oknie wiersza poleceń

Zadanie	Wpis po znaku zachęty DISKPART>	Opis
Utworzenie listy z informacjami o dysku, takimi jak partycje, woluminy	list di sk list partition list volume	Pierwsze polecenie wymienia informacje o dysku, drugie polecenie wymienia informacje o partycjach bieżącego dysku, a trzecie polecenie tworzy listę informacji o woluminach i partycjach wszystkich dysków.
Utworzenie woluminu prostego	create volume simple size=500 disk=2	Wpisane w jednym wierszu, polecenie to utworzy wolumin prosty o pojemności 500 MB na dysku 2.
Przypisanie litery dysku	select volume 4 assign letter j	Polecenie przypisze do woluminu 4 literę dysku J.
Rozszerzenie woluminu prostego	select volume 4 extend size=250 disk=2	Polecenie rozszerza wolumin 4 (wolumin prosty na dysku 2) o dodatkowe 250 MB tego samego dysku.
Utworzenie woluminu łączonego	select volume 4 extend size=250 disk=1	Polecenie łączy wolumin 4 (wolumin prosty na dysku 2) z dodatkowym obszarem o pojemności 250 MB na dysku 1.

ciąg dalszy na następnej stronie

ciąg dalszy ze strony poprzedniej

Zadanie	Wpis po znaku zachęty DISKPART>	Opis
Usunięcie woluminu łączonego	<code>select volume 4 delete volume</code>	Polecenie usuwa wolumin 4 (wolumin łączony). Jeśli wolumin rozciągał się na dwóch dyskach — na dysku 1 i dysku 2, przestrzeń zajmowana na tych dyskach pozostanie nieprzydzielona.
Utworzenie punktu instalacji woluminu	<code>select volume 4 assign mount=e:\Folder1</code>	Przypisuje punkt instalacji woluminu do woluminu 4, który będzie dostępny z ścieżki <u>E:\Folder1</u> .
Utworzenie woluminu rozłożonego	<code>create volume stripe size=500 disk=1,2</code>	Polecenie, wpisane w jednym wierszu, utworzy wolumin rozłożony wykorzystujący 500 MB pojemności na dysku 1 i na dysku 2 tworząc sumaryczną pojemność woluminu 1 GB
Utworzenie woluminu dublowanego	<code>create volume simple size= 00 di"sk=1 add disk 2</code>	Polecenie, wpisane w jednym wierszu, utworzy wolumin dublowany wykorzystujący 500 MB na dysku 1 i na dysku 2 tworząc całkowitą pojemność 500 MB woluminu odpornego na uszkodzenia.
Zakończenie dublowania	<code>select volume 5 break disk 2</code>	Wybiera do dublowania wolumin 5 i przerywa dublowanie na dysku 2.
Usuwanie dublowania	<code>break disk 2 nokeep</code>	Usuwa dublowanie i usuwa dane dysku 2, które było poprzednio dublowane.
Utworzenie woluminu RAID-5	<code>create volume raid size=500 disk=1,2,3</code>	Polecenie, wpisane w jednym wierszu, utworzy wolumin RAID-5, który wykorzystuje dyski 1, 2 oraz 3 dając w przybliżeniu pojemność 1 GB odpornej na uszkodzenia przestrzeni dyskowej.
Konwersja dysku podstawowego do dynamicznego	<code>select disk 2 corwert dynamic</code>	Polecenie przekształca dysk 2 z dysku podstawowego na dynamiczny.
Konwersja dysku zawierającego nieprzydzieloną przestrzeń z dysku dynamicznego na podstawowy	<code>select disk 2 convert basic</code>	Polecenie przekształca dysk 2 z dysku dynamicznego na podstawowy.

Zadanie kontrolne: Konfigurowanie dysków i woluminów

W zadaniu tym wykorzystywana będzie przystawka *Disk Management* oraz program *Diskpart* do przeprowadzenia szeregu zadań dotyczących zarządzania dyskami. Zadania wykonywane będą na dysku Disk 0. Aby wykonać ćwiczenia, Disk 0 musi być skonfigurowany jako dysk podstawowy i musi zawierać co najmniej 1 GB nieprzydzielonej przestrzeni dyskowej.

Ćwiczenie 1: Utworzenie partycji za pomocą przystawki Disk Management

1. Zaloguj się do serwera Server01 jako administrator i w konsoli Computer Management (Zarządzanie komputerem) otwórz przystawkę Disk Management (Zarządzanie dyskami).

W górnej części okna wyświetlana jest lista woluminów, natomiast w dolnej części przedstawiony jest widok graficzny.

2. W dolnej ramce kliknij prawym przyciskiem myszy nieprzydzieloną przestrzeń dyskową na dysku oznaczonym Disk 0 i wybierz polecenie New Partition (Nowa partycja). Wyświetlony zostanie program *New Partition Wizard* (Kreator nowej partycji).
3. Utwórz partycję podstawową o pojemności 250 MB. Zaakceptuj domyślne określenie litery dysku. Oznacz wolumin etykietą Data_Volume i wykonaj szybkie formatowanie stosując system NTFS.

Po chwili wyświetlony zostanie nowy dysk nazwany Data_V<>lunie (litera_dysku:), gdzie litera dysku jest literą przydzieloną do partycji przez program *New Partition Wizard*. Po zakończeniu formatowania status partycji zostaje określony jako *Healthy* (Zdrowy).

Ćwiczenie 2: Konwersja dysku podstawowego na dysk dynamiczny za pomocą przystawki Disk Management

1. W dolnej ramce (widok graficzny) programu *Disk Management* kliknij prawym przyciskiem myszy okno statusu dysku Disk 0 i wybierz polecenie Convert To Dynamic Disk (Konwertuj na dysk dynamiczny). Wyświetlone zostanie okno dialogowe *Convert To Dynamic Disk* (Konwertowanie na dysk dynamiczny), a pokazane w nim pole wyboru Disk 0 jest zaznaczone.
2. Postępuj zgodnie z instrukcjami, aby przekształcić Disk 0 na dysk dynamiczny. Ponieważ Disk 0 jest dyskiem systemowym, komputer trzeba będzie uruchomić ponownie.

Ćwiczenie 3: Korzystanie z polecenia DiskPart

1. Otwórz okno wiersza poleceń.
2. Wpisz polecenie diskpart i naciśnij ENTER. Wyświetlony zostanie znak zachęty DI SKPART>.
3. Wpisz ? i naciśnij ENTER. Wyświetlona zostanie lista poleceń programu *Diskpart*.
4. Wpisz list disk i naciśnij ENTER. Wyświetlona zostanie lista dysku (lub dysków) serwera Server01.
5. Wpisz create volume simple size = 250 disk = 0 i naciśnij ENTER.
6. Wpisz list volume i naciśnij ENTER.

Utworzony został nowy wolumin. Przed nazwą nowego woluminu wyświetlany jest znak gwiazdki, który oznacza, że dany wolumin został zaznaczony. Warto zauważyć, że do woluminu nie została przypisana żadna litera.

7. Wpisz assign letter z i naciśnij ENTER.
8. Wpisz list volume i naciśnij ENTER. Do wybranego woluminu została przypisana litera Z.
- 9- Wpisz extend size=250 disk=0 i naciśnij ENTER.
10. Wpisz list volume i naciśnij ENTER. Pojemność wybranego woluminu (dysk Z) wynosi obecnie 500 MB.
11. Wpisz exit i naciśnij ENTER. Ponownie wyświetlone zostanie okno wiersza poleceń.

12. Wpisz **format z:/fs:NTFS /v:Extended_Volume /q** i naciśnij ENTER. Wyświetlone zostanie ostrzeżenie informujące, że usunięte zostaną wszystkie dane dysku Z.
13. Naciśnij przycisk Y, a następnie i naciśnij ENTER. W tym momencie na dysku Z wykonywane jest szybkie formatowanie przy użyciu systemu NTFS.
14. Wpisz **exit**, aby zamknąć okno wiersza poleceń.

Ćwiczenie 4: Rozszerzanie woluminów za pomocą programu Disk Management

1. Otwórz program *Disk Management* (Zarządzanie dyskami).
2. Kliknij prawym przyciskiem myszy **Extended_Volume** i wybierz polecenie **Delete Volume** (Usuń wolumin).
3. Potwierdź operację usuwania woluminu klikając przycisk **Yes** (Tak).
4. Kliknij prawym przyciskiem myszy **Data_Volume** i wybierz polecenie **Extend Volume** (Rozszerz wolumin). Wyświetlony zostanie program *Extend Volume Wizard* (Kreator woluminu rozszerzonego).
5. Kliknij przycisk **Next** (Dalej).
6. Zmień wielkość używanej przestrzeni woluminu tak, aby jego pojemność wynosiła 500 MB.
7. Kliknij przycisk **Next** (Dalej).
8. Przeczytaj informacje podsumowania. Kliknij przycisk **Finish** (Zakończ).

Ćwiczenie 5: Litera dysków i woluminy instalowane

1. Kliknij prawym przyciskiem myszy **Data_Volume** i wybierz polecenie **Change Drive Letter And Paths** (Zmień literę dysku i ścieżki).
2. Zmień literę dysku na X.
3. Kliknij prawym przyciskiem myszy **Data_Volume (X:)** i wybierz polecenie **Open** (Otwórz). Uruchomiony zostanie program Windows Explorer (Eksplorator Windows).
4. Utwórz folder o nazwie Docs.
5. Zamknij program Windows Explorer.
6. Kliknij prawym przyciskiem myszy nieprzydzieloną przestrzeń dyskową na dysku Disk 0 i wybierz polecenie **New Volume** (Nowy wolumin).
7. Utwórz wolumin prosty wykorzystując całą pozostałą na dysku przestrzeń. Zamiast przypisywać literę dysku, zainstaluj wolumin w ścieżce **X:\Docs**. Sformatuj wolumin stosując system NTFS i dla woluminu utwórz etykietę **More_Space**.
8. Otwórz program Windows Explorer i sprawdź, czy w menu *View* (Widok) włączone jest wyświetlanie paska stanu (Status Bar). Sprawdź wolumin X:. Ile wolnej przestrzeni ma wolumin? Ile wolnej przestrzeni jest wykazywane, jeśli zostanie utworzony folder Docs?

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Niniejsze pytanie jest kontynuacją sytuacji opisanej w pytaniu pierwszym lekcji 1. W komputerze zainstalowany jest nowy dysk o pojemności 200 GB. Dysk został skonfigurowany jako podstawowy, a na dysku utworzone zostały trzy 30 GB partycje przeznaczone na system operacyjny, katalogi macierzyste użytkowników oraz dane udostępnione. Skonfigurowana została również partycja rozszerzona i dwa 30 GB dyski logiczne przeznaczone na instalowanie aplikacji oraz dla punktu dystrybucji oprogramowania. Na dysku pozostało 50 GB nieprzydzielonej przestrzeni. Kilka miesięcy później okazało się, że trzy woluminy są prawie całkowicie wypełnione. Administrator przygotowuje się do odpowiedniego zareagowania w sytuacji, kiedy jeden z woluminów trzeba będzie rozszerzyć. Jakie działania musi przedsięwziąć?
2. Który rodzaj obszarów dysku obsługuje dyski logiczne?
 - a. Partycja podstawowa
 - b. Woluminy proste
 - c. Woluminy łączone
 - d. Partycje rozszerzone
 - e. Nieprzydzielona przestrzeń
- 3- Niedawno do komputera dodany został dysk. Dysk był poprzednio używany w systemie Windows 2000 Server. Dysk jest wyświetlany w programie Device Manager (Menedżer dysku), ale nie jest prawidłowo pokazywany w programie Disk Management (Zarządzanie dyskami). Jakie zadanie należy wykonać?
 - a. Import Foreign Disk (Zaimportuj obce dyski)
 - b. Format volume (Formatuj wolumin)
 - c. Rescan (Ponownie skanuj)
 - d. Change Drive Letter or Path (Zmień literę dysku i ścieżki)
 - e. Convert to Dynamic Disk (Konwertuj na dysk dynamiczny)
4. Administrator próbuje przekształcić zewnętrzny dysk standardu FireWire z dysku podstawowego na dynamiczny, ale opcja umożliwiająca konwersję jest niedostępna. Jaka jest najbardziej prawdopodobna tego przyczyna?

Podsumowanie lekcji

- Zadania dotyczące zarządzania dyskami mogą być wykonywane przy użyciu przystawki Disk Management (Zarządzanie dyskami) lub w oknie wiersza poleceń za pomocą narzędzi takich jak Diskpart.
- Podczas zarządzania dyskami najczęściej wykonywanymi zadaniami są tworzenie i usuwanie partycji i woluminów oraz przypisywanie liter dysku i punktów instalacji.

- System Windows Server 2003 umożliwia przypisanie jednej litery dysku do woluminu, jak również do woluminu można w ogóle nie przypisywać litery. Opcjonalnie można zainstalować wolumin w jednym lub kilku pustych folderach na woluminach NTFS.
- Dyski podstawowe mogą być przekształcane na dyski dynamiczne; w tym celu trzeba usunąć wszystkie dane i woluminy.

Lekcja 3: Konserwacja woluminów pamięci dyskowej

Woluminy systemu Windows Server 2003 pracują sprawnie i stabilnie, jeśli zostały sformatowane jako NTFS, trochę gorzej sytuacja wygląda dla formatów FAT lub FAT32. System plików NTFS rejestruje wszystkie transakcje plików, automatycznie zastępuje uszkodzone klastry i przechowuje kopie najważniejszych informacji o wszystkich plikach woluminu NTFS. Dzięki tym mechanizmom, system plików NTFS aktywnie chroni integralność struktury woluminu i metadanych systemu plików (danych dotyczących samego systemu plików). Jednakże dane użytkownika mogą czasami zostać uszkodzone i mogą w pewnym stopniu ulegać fragmentacji. Oprócz tego użytkownicy mają irytujący zwyczaj przechowywania *ogromnej* ilości archaicznych i nie związanych z biznesem danych na woluminach, do których mają dostęp. W trakcie niniejszej lekcji opisane zostaną sposoby utrzymywania integralności woluminów dyskowych oraz optymalizacji ich wydajności poprzez przeprowadzanie defragmentacji i określanie limitów pamięci za pomocą mechanizmu przydziału dysku.

Materiały omówione podczas lekcji pozwalają na

- Monitorowanie i zachowanie integralności dysku przy użyciu programu CHKDSK
- Monitorowanie i poprawę wydajności dysku przy użyciu programu Disk Defragmenter (Defragmentator dysku)
- Konfigurowanie i monitorowanie pamięci dyskowych za pomocą programu Disk Quotas (Przydziały dysku)

Szacunkowy czas lekcji: 20 minut

Program CHKDSK

Program **CHKDSK** lub inaczej „**Check Disk**” jest narzędziem dostępnym w aplikacji Windows Explorer (Eksplorator Windows) lub w wierszu poleceń i umożliwia sprawdzanie woluminu dyskowego pod kątem wyszukiwania błędów systemu plików oraz opcjonalnie pod kątem wykonania prób dostępu do uszkodzonych sektorów dysku twardego.

Aby użyć polecenia **Check Disk** (Sprawdź dysk) w programie Windows Explorer, należy otworzyć okno dialogowe właściwości woluminu, który ma zostać sprawdzony. Na zakładce **Tools** (Narzędzia) należy kliknąć przycisk **Check Now** (Sprawdź). W oknie dialogowym *Check Disk* należy zaznaczyć zadanie, które będzie uruchomione. Okno to zostało przedstawione na rysunku 11-4.



Rysunek 11-4 Okno dialogowe programu *Check Disk*

Jeśli zostanie wybrana opcja **Automatically Fix File System Errors** (Automatycznie napraw błędy systemu plików), program *Check Disk* będzie próbował naprawić niespójności występujące w katalogu systemu plików, takie jak pliki, które pozostają w katalogu na woluminie, ale brak dla nich odpowiednich wpisów. Program *Check Disk* trzykrotnie analizuje dysk, sprawdzając metadane opisujące sposób organizacji plików na dysku. Próby te dotyczą sprawdzenia, czy wszystkie pliki woluminu są zgodne z opisem głównej tablicy plików MFT, czy prawidłowa jest struktura katalogu oraz czy spójne pozostają deskryptory zabezpieczeń.

Jeśli zostanie wybrana opcja **Scali For And Attempt Recovety Of Bad Sectors** (Skanuj dysk i próbuj odzyskać uszkodzone sektory), program *Check Disk* wykonuje czwarte sprawdzenie, które analizuje sektory woluminu zarezerwowane dla danych użytkownika (metadane systemu plików są zawsze sprawdzane). Jeśli zostaje znaleziony uszkodzony sektor, dane są odtwarzane i przenoszone do sprawnego sektora, o ile wolumin jest odporny na uszkodzenia. Jeśli natomiast wolumin nie jest odporny na uszkodzenia, za pomocą programu *Check Disk* dane nie mogą zostać przywrócone i trzeba posłużyć się kopią zapasową. Następnie uszkodzony sektor jest wyłączany z użycia, a kolejne dane nie będą w tym miejscu zapisywane.

Przed uruchomieniem programu *Check Disk*, wszystkie pi iki korzystające z otwartych dojsć muszą zostać zamknięte. Jeśli nie można zwolnić wszystkich dojsć (co może zdarzyć się, jeśli program *Check Disk* ma analizować wolumin systemowy), użytkownikowi zostanie przedstawiona sugestia, aby zaplanował uruchomienie programu *Check Disk* podczas uruchamiania systemu. Uruchomienie programu *Check Disk* blokuje dostęp do woluminu dla innych procesów. W zależności od rozmiaru woluminu, wybranych opcji sprawdzania oraz od uruchomienia innych procesów komputera, sprawdzanie dysku może trwać długo, a swoim działaniem program praktycznie całkowicie zajmuje procesor i dysk komputera.

Program *Check Disk* może być również uruchamiany w wierszu poleceń poprzez wpisanie komendy **Chkdsk**. Bez przełączników program zostanie uruchomiony w trybie umożliwiający wyłącznie odczyt dysku. Użytkownik będzie mógł przejrzeć raport dotyczący wykorzystania przestrzeni dyskowej. Program **Chkdsk** obsługuje kilka przełączników umożliwiających naprawę błędów systemu plików (/f) oraz uszkodzonych sektorów (/r), podobnie jak wersja uruchamiana w programie Explorer (Eksplorator).

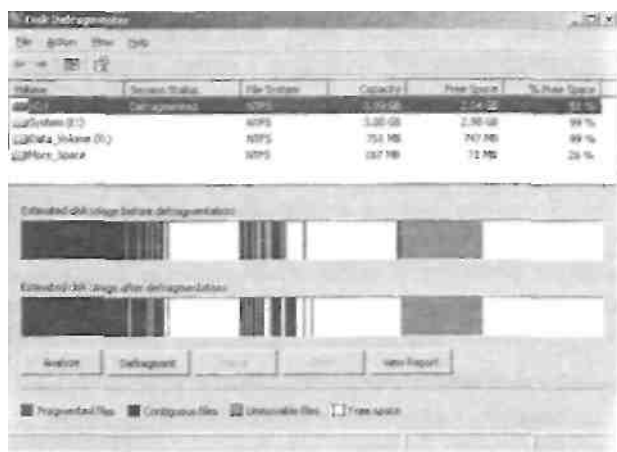
Defragmentator dysku

Pliki na woluminie są przechowywane w jednostkach zwanych *klastrami*. Rozmiar klastra zostaje określony podczas formatowania dysku. Większość woluminów NTFS używa domyślnej wielkości klastra, czyli 4 kB. Każdy klastr zawiera tylko jeden plik, jeśli plik jest mniejszy niż rozmiar klastra. Jeśli plik jest większy, jest zapisywany w wielu klastrach, a każdy klastr zawiera wskaźnik informujący o następnym segmencie pliku. Jeśli dysk jest nowy, wszystkie klastry są puste, tak więc pliki zapisywane na dysku zajmują klastry fizycznie ze sobą sąsiadujące. Jednak w miarę usuwania bądź powiększania plików, wolne klastry nie tworzą ciągłej przestrzeni, a pliki muszą być zapisywane w klastrach, które nie sąsiadują ze sobą. Fragmentacja ta powoduje spowolnienie operacji odczytu i zapisu, i z czasem zmniejszenie wydajności serwera może być znaczące.

System Windows Server 2003 został wyposażony w zestaw narzędzi przeprowadzających analizę i defragmentację woluminów. Narzędzia te dostępne są zarówno jako program graficzny, jak i uruchamiany w wierszu poleceń. Narzędzia te, w porównaniu do wersji systemu Windows 2000, zostały znacznie ulepszone. Obecnie mogą przeprowadzać defragmentację klastrów o rozmiarach większych niż 4kB, a także mogą defragmentować główną tablicę plików. Narzędzia służą do defragmentacji

dowolnego woluminu dysku lokalnego. Jeśli jednak zachodzi potrzeba przeprowadzenia defragmentacji woluminu zdalnego lub jej zaplanowania, trzeba poszukać programów innych producentów, takich jak na przykład program Diskeeper firmy Executive Software.

Na rysunku 11-5 przedstawiony został ekran programu *Disk Defragmenter* (Defragmentator dysku). Aby zastosować program, należy otworzyć właściwości woluminu dyskowego i na zakładce Tools (Narzędzia) kliknąć przycisk **Defragment Now** (Defragmentuj). To samo można uzyskać otwierając przystawkę **Disk Defragmenter** (Defragmentacja dysku) w niestandardowej konsoli MMC. Należy zaznaczyć wolumin i kliknąć przycisk **Analyze** (Analizuj). Program wyświetla w tym momencie wyniki analizy i sugestie dotyczące rodzaju wykonywanych operacji. Jeśli narzędzie podpowiada, że wolumin jest uszkodzony, to przed uruchomieniem defragmentacji dysk powinien być sprawdzony za pomocą programu CHKDSK.



Rysunek 11-5 Program *Disk Defragmenter* (Defragmentator dysku)

Jeśli program podpowiada, że wymagana jest defragmentacja, należy kliknąć przycisk Defragment (Defragmentuj). Można przeprowadzać defragmentację dowolnego typu woluminu: FAT lub NTFS, podstawowego bądź dynamicznego. Na woluminie mogą znajdować się otwarte pliki, ale defragmentacja tych plików nie będzie efektywna, co spowolni proces i dlatego zaleca się przed rozpoczęciem defragmentacji zamknąć wszystkie otwarte pliki. Próbuując zapisać wszystkie pliki w sąsiadujących ze sobą klastrach, program *Disk Defragmenter* potrafi przenosić pliki pomiędzy dyskami. W wyniku defragmentacji konsolidowana jest też przestrzeń wolna, co powoduje, że nowe pliki nie będą prawdopodobnie ulegały fragmentacji.



Informacja Aby przeprowadzić defragmentację woluminu, wolumin musi mieć co najmniej 15% wolnej przestrzeni. Przestrzeń ta jest używana do przechowywania plików podczas defragmentacji woluminu. Jeśli wolumin zawiera dużo pofragmentowanych plików o znacznych rozmiarach, to do przeprowadzenia sprawnej defragmentacji potrzeba będzie większej ilości wolnej przestrzeni. Na woluminie, który ma mniej niż 15% wolnej przestrzeni, defragmentacja może być przeprowadzona tylko częściowo.

Przydziały dysku

W systemie Windows 2000 została wprowadzona obsługa przydziałów dysku w postaci wbudowanej funkcji. Umożliwiała ona administratorom ograniczanie pamięci dyskowej bez konieczności inwestowania w programy narzędziowe innych producentów. Ta sama funkcjonalność obsługiwana jest w systemie Windows Server 2003. Po włączeniu przydziałów, program zaczyna śledzić pliki woluminu, których właścicielem jest dany użytkownik. Następnie obliczone całkowite wykorzystanie dysku przez tego użytkownika jest porównywane z limitem przyznanym przez administratora. Po przekroczeniu limitu użytkownik zostaje o tym powiadomiony, a w zależności od ustawień, funkcja przydziału dysku może zablokować zapis na dysku.

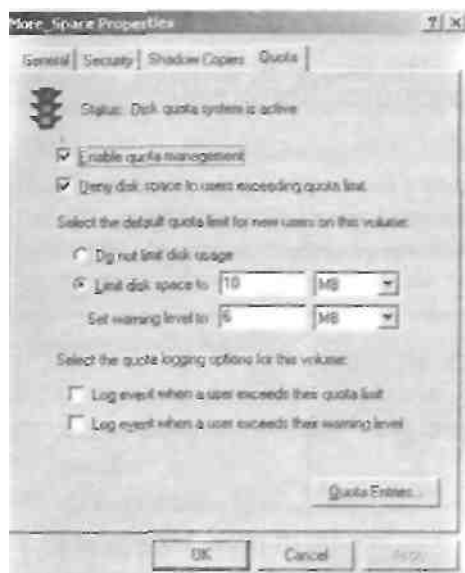
Menedżer przydziału informuje o wielkości wolnej przestrzeni woluminu w oparciu o przydział przyznany użytkownikowi. Tak więc, jeśli przydział użytkownika wynosi 50 MB na woluminie RAID o pojemności 500 GB, wolna przestrzeń widoczna dla użytkownika podczas pierwszego dostępu do woluminu to 50 MB. Kiedy użytkownik osiąga przyznany limit, wyświetlane zostają komunikaty podobne do pojawiających się, kiedy wolumin zostaje zapełniony. System ostrzega użytkownika, że zaczyna brakować wolnej przestrzeni i w związku z tym należy usunąć niepotrzebne pliki.

Wskazówka egzaminacyjna Przydziały dysku są obsługiwane jedynie na woluminach NTFS.



Konfigurowanie przydziałów

Konfigurowanie przydziałów wymaga przeprowadzenia następujących czynności: włączenie funkcji przydziału dysku na woluminie, skonfigurowanie ustawień domyślnych przydziału oraz skonfigurowanie wpisów odstępstw w stosunku do ustawień domyślnych. Ustawienia domyślne systemu Windows Seryer 2003 określają, że funkcja przydziału jest wyłączona i musi być włączana oddzielnie dla każdego woluminu. Aby włączyć funkcję przydziału dysku, należy otworzyć okno właściwości woluminu i kliknąć zakładkę **Quota** (Przydział). Zakładka ta została pokazana na rysunku 11-6.



Rysunek 11-6 Zakładka Quota (Przydział) w oknie dialogowym Properties (Właściwości) woluminu



Wskazówka Informacje zamieszczone w większości dokumentacji sugerują, żeby otwierać okno właściwości woluminu w programie Explorer (Eksplorator) poprzez kliknięcie prawym przyciskiem myszy dysku i wybranie polecenia Properties (Właściwości). Niestety ten sposób można wykorzystywać tylko dla woluminów oznaczonych literą, ponieważ program Explorer (Eksplorator) nie wyświetla zakładki Quota (Przydział) dla woluminów zainstalowanych w ścieżce foldera. Dlatego zalecane jest konfigurowanie przydziałów za pomocą programu Disk Management (Zarządzanie dyskami). Narzędzie to umożliwia otwieranie właściwości dowolnego woluminu wraz z możliwością uzyskania dostępu do zakładki Quota (Przydział).

Należy zaznaczyć pole wyboru **Enable Quota Management** (Włącz zarządzanie przydziałami). Jeśli dla użytkowników, którzy przekroczyli limię, administrator chce zablokować możliwość zapisu na woluminie, musi zaznaczyć opcję **Deny Disk Space To Users Exceeding Quota Limit** (Odmów miejsca na dysku użytkownikom przekraczającym limit). Jeśli to pole wyboru nie zostanie zaznaczone, użytkownik w dalszym ciągu będzie mógł zapisywać dane na woluminie.

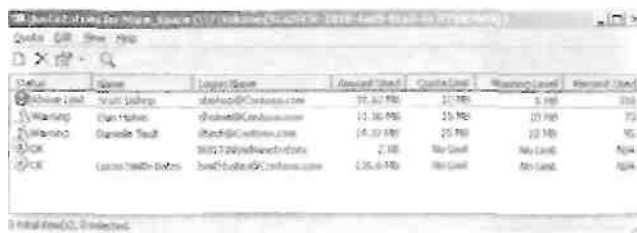
Przydziałami można zarządzać na dwa sposoby: pierwszy polega na określeniu wpisów przydziału dla określonych użytkowników i zdefiniowaniu limitu pamięci dyskowej dla każdego użytkownika (istnieje możliwość wybrania opcji „bez ograniczeń”) oraz drugi korzystający z ustawień domyślnych stosowanych dla wszystkich użytkowników, dla których nie zostały określone wpisy przydziału. Domyślne ustawienia przydziałów można konfigurować na zakładce Quota (Przydział). Domyślny limit lub „brak ograniczeń” należy skonfigurować dla jak największej liczby użytkowników, dzięki czemu minimalizowana jest liczba wpisów przydziału, które trzeba tworzyć dla użytkowników, dla których limity są inne niż określają to ustawienia domyślne. Warto zauważyć, że można również skonfigurować limit przestrzeni dyskowej dla ostrzeżenia (oczywiście ograniczenie to powinno zadziałać wcześniej niż sam limit przydziału).

Na końcu należy zdefiniować opcje protokołowania. Menedżer przydziałów rejestruje zdarzenia w dzienniku System, w którym użytkownik identyfikowany jest według nazwy oraz zapisywane są informacje o przekroczeniu limitów dla ostrzeżeń lub przydziału.

Po skonfigurowaniu na zakładce Quota ustawień domyślnych dla woluminu, należy kliknąć przycisk **Quota Entries** (Wpisy przydziałów), aby otworzyć okno dialogowe *Quota Entries*, pokazane na rysunku 11-7.



Wskazówka egzaminacyjna Przydział dysku dla administratorów określony jest opcją No Limit (Bez ograniczeń). Dzięki temu administrator może instalować system operacyjny, usługi oraz dane bez obawy o przekroczenie limitu.



Rysunek 11-7 Okno dialogowe *Quota Entries* (Wpisy przydziałów)

Na pasku narzędzi kliknij przycisk **New Quota Entry** (Nowy wpis przydziału) lub w menu **Quota** (Przydział) wybierz polecenie **New Quota Entry**. Istnieje możliwość wyboru kilku użytkowników, dla których określany będzie wpis przydziału. Niestety system Windows Server 2003 nie pozwala określać wpisów przydziałów dla grup (większość narzędzi zarządzania przydziałami ma takie funkcje). W oknie dialogowym *Select Users* (Wybór użytkowników) istnieje możliwość wyboru wielu użytkowników. Limity skonfigurowane w oknie dialogowym *AddNew Quota Entry* (Dodawanie nowych wpisów przydziału) stosowane są indywidualnie dla wszystkich zaznaczonych użytkowników.

Eksport wpisów przydziału

Jeśli zachodzi potrzeba zastosowania takich samych wpisów przydziału dla innego woluminu NTFS, można wyeksportować te wpisy, a następnie zaimportować je do innego woluminu. W tym celu, w menu **Quota** (Przydział) należy zaznaczyć jeden lub kilka wpisów przydziału i kliknąć przycisk **Export**. Z kolei dla innego woluminu należy kliknąć przycisk **Import**.

Monitorowanie przydziałów i pamięci dyskowej

W oknie dialogowym *Quota Entries* (Wpisy przydziału) wyświetlana jest pamięć dyskowa w odniesieniu do użytkownika oraz pokazywane jest, czy dla danej pamięci przekroczony został poziom ostrzeżenia lub limitu przydziału. Administrator może porządkować listę według kolumn w celu zidentyfikowania użytkowników, dla których przekroczone zostały poziomy przydziału lub ograniczenia. W systemie brak mechanizmów powiadamiania o przekroczeniu limitów przydziału i dlatego administrator musi przeglądać okno dialogowe *Quota Entries* lub w programie *Event Viewer* (Podgląd zdarzeń) monitorować dziennik System.



Wskazówka egzaminacyjna Przydziały dysku mogą być wprowadzane jedynie w odniesieniu do woluminu lub użytkownika, nie można natomiast wprowadzać przydziałów w odniesieniu do folderów bądź grup.

Zadanie kontrolne: Implementacja przydziałów dysku

W zadaniu tym konfigurowane będą domyślne ustawienia przydziału, aby ograniczyć dla użytkowników ilość danych przechowywanych na serwerze Server01. Następnie konfigurowane będą niestandardowe ustawienia przydziałów, które umożliwiają użytkownikom działu Marketing przechowywanie większej ilości danych, ponieważ pliki użytkowników tego działu są przeważnie większe niż inne dokumenty biznesowe. Dla grupy projektowej ograniczenie zostanie zniesione.

Ćwiczenie 1: Konfigurowanie ustawień domyślnych przydziału dysku

1. Otwórz program **Disk Management** (Zarządzanie dyskami).
2. Kliknij prawym przyciskiem myszy wolumin **More_Space** i wybierz polecenie **Properties** (Właściwości).
3. Kliknij zakładkę **Quota** (Przydział).
4. Kliknij pole wyboru **Enable Quota Management** (Włącz zarządzanie przydziałami).
5. Zaznacz pole wyboru **Deny Disk Space To Users Exceeding Quota Limit** (Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału).

6. Zaznacz opcję **Limit Disk Space To** (Ogranicz miejsce na dysku do).
Określ limit wartością 10 MB, a poziom ostrzeżenia jako 6 MB.
7. Zaznacz oba pola dotyczące opcji protokołowania.
8. Kliknij przycisk **Apply** (Zastosuj).

Wyświetlone zostanie okno dialogowe *Disk Quota* (Przydział dysku), informujące, że jeśli włączona zostanie funkcja przydziału, wolumin będzie ponownie skanowany w celu uaktualnienia statystyk wykorzystania dysku. Kliknij przycisk OK.

9. Nie zamykaj okna dialogowego *Volume Properties* (Właściwości woluminu), ponieważ będzie wykorzystywane w następnym ćwiczeniu.

Ćwiczenie 2: Utworzenie niestandardowych wpisów przydziału dysku dla użytkowników

1. W oknie dialogowym *Properties* (Właściwości) woluminu *More_Space*, na zakładce *Quota* (Przydział) kliknij przycisk **Quota Entries**, aby otworzyć odpowiednie okno dialogowe.



Nieoficjalnie Warto zwrócić uwagę, że na liście została wymieniona grupa *BuiltinAdministrators*. Jeśli użytkownik nie będący członkiem grupy administracyjnej utworzy pliki, również dla tego użytkownika będą istniały wpisy przydziału, ponieważ konto użytkownika jest właścicielem plików na tym woluminie.

Poniżej opisana została procedura tworzenia wpisów przydziału dla pracowników działu Marketing, Dan Holme oraz Danielle Tiedt, dla których zostanie przydzielone więcej pamięci dyskowej niż określają to ustawienia domyślne.

2. W menu **Quota** (Przydział) kliknij polecenie **New Quota Entry** (Nowy wpis przydziału).
3. Kliknij przycisk **Advanced** (Zaawansowane), a następnie **Find Now** (Znajdź teraz). Wyświetlona zostanie lista wszystkich użytkowników domeny.
4. Zaznacz użytkownika **Dar Holme** oraz **Danielle Tiedt** i dwukrotnie kliknij przycisk OK.
5. Określ wpis przydziału, aby ograniczał użycie dysku do 15 MB, a ostrzeżenie było wysyłane po przekroczeniu 10 MB. Kliknij przycisk OK.

Poniżej opisana została procedura, która znosi ograniczenie przydziału dysku dla dwóch projektantów Lorrin Smith-Bates oraz Scott Bishop.

6. Powtórz czynności opisane w punktach od 2 do 5, aby skonfigurować wpisy przydziału dla użytkowników Lorrin Smith-Bates i Scott Bishop, przy czym określ wpisy tak, aby nie ograniczały wykorzystywania dysku.

Ćwiczenie 3 (Opcjonalne): Sprawdzenie przydziałów dysku

1. Zaloguj się jako użytkownik **DanielleTiedt**.
2. Utwórz folder *Dtiedt* wewnątrz foldera X:\Docs.
3. Skopiuj folder *Support* z dysku CD-ROM systemu Windows Server 2003 CD-ROM do foldera X:\Docs\Dtiedt. Folder *Support* zajmuje 11 MB pamięci i jest to mniej niż przydział określony dla użytkownika Danielle Tiedt. Kopiowanie zakończy się poprawnie.

4. Zaloguj się jako użytkownik Dan Holme.
5. Utwórz folder Dholmc wewnątrz foldera X:\Docs.
6. Skopiuj folder Support z dysku CD-ROM systemu Windows Server 2003 CD-ROM do foldera X:\Docs\Dholmc. Folder Support jest mniejszy niż przydział określony dla użytkownika Dan Holme. Kopiowanie zakończy się poprawnie.
- 7- Skopiuj folder Valueadd z dysku CD-ROM systemu Windows Server 2003 CD-ROM do foldera X:\Docs\Dholmc. Folder zajmuje 6 MB i dlatego przekroczony zostanie limit przydziału określony dla użytkownika Dan Holme. Kopiowanie zostanie przerwane.
8. Zaloguj się jako administrator i otwórz okno dialogowe *Quota Entries* dla woluminu More_Space. Warto zauważyć, że prezentowane informacje o wykorzystaniu dysku pokazywane są w odniesieniu do każdego użytkownika.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdujące się pod koniec tego rozdziału.

1. Administrator systemu Windows Server 2003 chce naprawić błędy systemu plików i odtworzyć uszkodzone sektory dysku twardego komputera. Które narzędzie powinien zastosować administrator?
 - a. Check Disk (Sprawdź dysk)
 - b. Disk Defragmenter (Defragmentator dysku)
 - c. DISKPART
 - d. Disk quotas (Przydziały dysku)
2. Komputer działa pod kontrolą systemu Windows Server 2003. Dysk twardy komputera zawiera dwa woluminy danych: D oraz E. Administrator włączył przydziały dysku na woluminach D oraz E, które dla każdego użytkownika określają limit przestrzeni dyskowej równy 20 MB. Jednakże, administrator chce ograniczyć wielkość folderów macierzystych użytkowników przechowywanych w ścieżce D:\Users do wartości 10 MB dla każdego użytkownika. Czy jest to możliwe? Dlaczego tak lub dlaczego nie? Gdzie można wprowadzać przydziały?
 - a. Na dowolnym serwerze dla wszystkich dysków
 - b. Na dowolnym dysku fizycznym dla wszystkich woluminów
 - c. Na dowolnym woluminie dla wszystkich folderów
 - d. Na dowolnym folderze
3. Jaki jest wymóg minimalnej wielkości wolnej przestrzeni dyskowej, aby można było przeprowadzić defragmentację?
 - a. 5%
 - b. 10%
 - c. 15%
 - d. 25%
 - e. 50%

Podsumowanie lekcji

- Program narzędziowy Check Disk (Sprawdź dysk) umożliwia naprawę systemu plików oraz wyszukiwanie i przeprowadzanie prób odtworzenia uszkodzonych sektorów dysku twardego.
- Program Disk Defragmenter (Defragmentator dysku) zwiększa wydajność poprzez rozmieszczenie plików w ciągłym obszarze klastrow.
- Program Disk Quotas (Przydziały dysku) umożliwia określenie i monitorowanie limitów pamięci dyskowej oraz opcjonalnie umożliwia zablokowanie zapisu dla użytkowników, którzy przekroczyli swoje limity- Przydziały są konfigurowane w odniesieniu do użytkownika i w odniesieniu do woluminu.

Lekcja 4: Implementacja macierzy dyskowych RAID

Podsystem dyskowy zawierający macierz RAID umożliwia współdzielenie dysków dla zwiększenia wydajności i odporności na uszkodzenia. Niniejsza lekcja przedstawia trzy poziomy macierzy RAID, które mogą być tworzone i zarządzane w systemie Windows Server 2003. Opisany został również wpływ każdego z tych typów macierzy RAID na wydajność, pojemność i odporność na uszkodzenia oraz omówione zostały sposoby odtwarzania danych w przypadku odpornych na uszkodzenia konfiguracji RAID.

Materiały omówione podczas lekcji pozwalają na

- Dokonywanie wyboru implementacji macierzy RAID w kontekście konkretnych wymagań dotyczących wykorzystania pojemności, odporności na uszkodzenia oraz wydajności
- Konfigurowanie woluminów rozłożonych (RAID-0)
- Konfigurowanie woluminów dublowanych (RAID-1)
- Konfigurowanie woluminów RAID-5 (rozłożone z parzystością)
- Odtwarzanie danych woluminu odpornego na uszkodzenia po awarii pojedynczego dysku

Szacunkowy czas lekcji: 25 minut

Podczas lekcji 1 opisane zostały rodzaje jednostek pamięci dyskowych dostępnych w systemie Windows Server 2003. Typy woluminów: rozłożony, dublowany oraz RAID-5 odzwierciedlają konfiguracje stosowanych macierzy RAID.

Wprowadzanie odporności na uszkodzenia

Zgodnie z opisem zamieszczonym w lekcji 1, odporność na uszkodzenia jest cechą systemu operacyjnego lub komputerowego dotyczącą systemu reagowania na katastroficzne zdarzenia, takie jak brak zasilania czy uszkodzenie sprzętu, dzięki której nie następuje utrata danych, a rozpoczęte zadania nie ulegają uszkodzeniu. System w pełni odporny na uszkodzenia, aby zapobiec utracie danych, wykorzystuje odporne na uszkodzenia macierze dyskowe. Stosowane macierze RAID mogą być albo sprzętowe albo programowe.

Sprzętowa macierz RAID

W sprzętowym rozwiązaniu interfejs kontrolera dysku obsługuje tworzenie i regenerację informacji nadmiarowych. Niektórzy producenci macierzy RAID zastosowali ochronę danych bezpośrednio w urządzeniu sprzętu, czyli na karcie kontrolera macierzy dyskowej. Ponieważ są to rozwiązania dotyczące odporności na uszkodzenia opracowane przez producenta, z pominięciem sterowników systemu operacyjnego, w porównaniu do rozwiązań programowych stanowią zwiększenie wydajności.

Przy podejmowaniu *decyzji* o stosowaniu programowego lub sprzętowego rozwiązania należy rozważyć następujące zagadnienia związane z wykorzystywaniem macierzy RAID:

- Rozwiązanie sprzętowe odporności na uszkodzenia jest droższe niż programowe i może ograniczać możliwości wyboru wyposażenia do pojedynczego producenta.
- Ogólnie, rozwiązanie sprzętowe odporności na uszkodzenia w kontekście dyskowych operacji we/wy jest szybsze niż rozwiązanie programowe.
- Rozwiązanie sprzętowe odporności na uszkodzenia może wprowadzać cechy systemu pozwalające na wymianę urządzeń podczas pracy komputera, bez konieczności jego wyłączania (hot swap) oraz na instalowanie urządzeń (dysków) zapasowych, które automatycznie zastępują uszkodzone urządzenie (hot sparing).

Programowa macierz RAID

System Windows Server 2003 obsługuje jeden typ macierzy RAID (rozłożona, RAID-0), która nie jest odporna na uszkodzenia oraz dwa rodzaje macierzy, które są odporne na uszkodzenia: woluminy dublowane (RAID-1) oraz woluminy rozłożone z parzystością (RAID-5). Woluminy RAID odporne na uszkodzenia mogą być tworzone jedynie na dyskach dynamicznych sformatowanych za pomocą systemu plików NTFS.

Implementacja programowej macierzy RAID w systemie Windows Server 2003 nie przewiduje odporności na uszkodzenia w okresie po wystąpieniu awarii do momentu naprawy uszkodzenia. Jeśli w tym czasie nastąpi drugie uszkodzenie, dane mogą być odtworzone tylko na podstawie kopii zapasowych.

Woluminy rozłożone

Wolumin rozłożony o konfiguracji macierzy RAID poziomu 0 używa co najmniej dwóch dysków i zapisuje dane na wszystkich dyskach w takim samym tempie. W związku z tym, żądania systemu we/ wy są obsługiwane przez kilka napędów, co jest korzystne dla wydajności odczytu i zapisu. Woluminy rozłożone są często stosowane w konfiguracjach, gdzie najważniejsza jest wydajność i wielkość pamięci, jak na przykład dla aplikacji CAD (Computer-Aided Design).



Informacja Poprawy wydajności można nie zauważyć dla dysków IDE, chyba że wykorzystywane są oddzielne kontrolery. Używanie oddzielnego kontrolera dla każdego dysku poprawia wydajność poprzez rozłożenie żądań systemu we/wy zarówno na kontrolery, jak i na dyski.

Tworzenie woluminów rozłożonych

Aby możliwe było utworzenie woluminu rozłożonego, trzeba dysponować nieprzydzieloną przestrzenią na co najmniej dwóch dyskach dynamicznych. Należy kliknąć prawym przyciskiem myszy jedną z rycb przestrzeni i wybrać polecenie **Create Volutne** (Utwórz wolumin). Zgodnie z instrukcjami uruchomionego programu *New Volume Wizard* (Kreator nowego woluminu), jako typ woluminu należy wybrać wolumin rozłożony oraz należy wskazać przestrzeń innego dysku, który będzie objęty tym woluminem. Do woluminów rozłożonych można przypisywać litery dysku i ścieżki folderów. Woluminy te mogą być formatowane jedynie za pomocą systemu NTFS.

Wolumin rozłożony może zawierać do 32 dysków. Przestrzeń używana na każdym dysku woluminu będzie równa najmniejszej przestrzeni jednego z dysków zestawu. Na przykład, jeśli dysk 1 ma 200 MB nieprzydzielonej przestrzeni, a dysk 2 ma 120 MB przestrzeni, wolumin rozłożony może zawierać maksymalnie 120 MB przestrzeni, jako że wielkość obszaru przeznaczonego na wolumin rozłożony

na dysku 1 nie może być większa niż obszar przeznaczony na dysku 2. Cała przestrzeń woluminu używana jest do przechowywania danych, a żaden obszar nie jest zarezerwowany na informacje związane z odpornością na uszkodzenia.

Odtwarzanie woluminu rozłożonego

Ponieważ dane przechowywane są na co najmniej dwóch dyskach fizycznych, wydajność zostaje poprawiona, ale zmniejszeniu ulega odporność na uszkodzenia — istnieje większe ryzyko, gdyż jeśli jeden z dysków zestawu zostanie uszkodzony, utracone zostaną wszystkie dane woluminu. Dlatego ważną sprawą jest wykonywanie kopii zapasowych woluminów rozłożonych. Jeśli uszkodzeniu ulega jeden z dysków woluminu rozłożonego, w konsekwencji trzeba usunąć wolumin, wymienić uszkodzony dysk, ponownie utworzyć wolumin i na koniec przywrócić dane na podstawie kopii zapasowych.



Uwaga Woluminy rozłożone udostępniają maksymalny obszar pamięci dyskowej i najlepszą wydajność, ale nie są odporne na uszkodzenia. Jedynym „lekarstwem” jest regularne wykonywanie kopii zapasowych.

Woluminy dublowane

Woluminy dublowane charakteryzują się dobrą wydajnością i jednocześnie są odporne na uszkodzenia. Wolumin dublowany składa się z dwóch dysków, a wszystkie dane zapisywane są na obu woluminach. Konfiguracja, w której zastosowane są dwa kontrolery (konfiguracji tej przypisana jest także nazwa - duplexing) jest najbardziej wydajna. Woluminy dublowane odnoszą się do konfiguracji sprzętowej oznaczanej RAID-1.

Tworzenie woluminów dublowanych

Aby możliwe było utworzenie woluminu dublowanego, trzeba dysponować nieprzydzieloną przestrzenią na co najmniej dwóch dyskach dynamicznych. Należy kliknąć prawym przyciskiem myszy jedną z tych przestrzeni i wybrać polecenie **Create Volume** (Utwórz wolumin). Zgodnie z instrukcjami uruchomionego programu *New Volume Wizard* (Kreator nowego woluminu), jako typ woluminu należy wybrać wolumin dublowany oraz należy wskazać przestrzeń innego dysku, który będzie objęty tym woluminem. Do woluminów rozłożonych można przypisywać litery dysku i ścieżki folderów. Obie kopie zestawu dublowanego współdzielą takie samo oznaczenie.

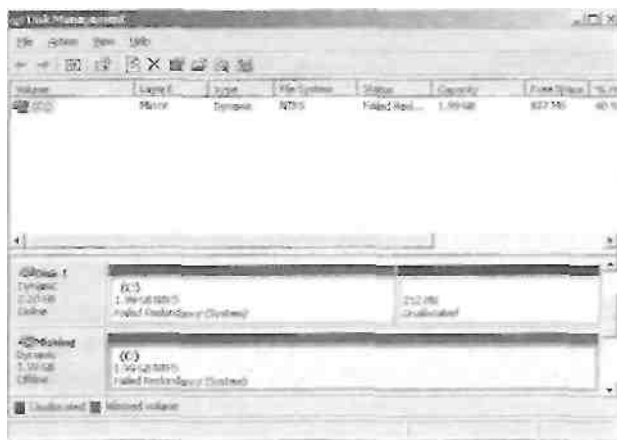
Istnieje również możliwość dublowania istniejącego woluminu prostego. W tym celu należy kliknąć prawym przyciskiem myszy wolumin i wybrać polecenie **Add Minor** (Dodaj dublowanie) oraz wskazać dysk, który posiada nieprzydzieloną przestrzeń wystarczającej wielkości.

Po utworzeniu woluminu dublowanego, system rozpoczyna kopiowanie danych (sektor za sektorem). W tym okresie status woluminu określany jest jako **Resynching** (Ponowne synchronizowanie).

Odtwarzanie danych po uszkodzeniu dysku zestawu dublowanego

Proces przywracania danych po awarii dysku woluminu dublowanego zależy od rodzaju uszkodzenia. Jeśli uszkodzenie dotyczyło przejściowych błędów systemu we/wy, status obu części zestawu dublowanego jest oznaczany jako *Failed Redundancy* (Niepowodzenie nadmiarowości). Status dysków, które

zostały uszkodzone trwale, jest oznaczany jako *Offline* lub *Missing* (Brak), tak jak przedstawione to zostało na rysunku 11-8.



Rysunek 11-8 Wolumin dublowany zawierający uszkodzony dysk

Po naprawie błędów systemu we/wy (na przykład nieprawidłowo podłączony kabel lub problemy z zasilaniem), należy kliknąć prawym przyciskiem myszy wolumin, dokładnie dysk, z którym był problem i wybrać polecenie **Reactivate Vblume** (Uaktywnij ponownie dysk). Po zakończeniu aktywowania dysk lub wolumin ponownie będzie w stanie „online”. Funkcja dublowania dysków automatycznie rozpocznie ponowną ich synchronizację.

Podczas zatrzymywania dublowania istnieją trzy możliwości zależne od zamierzonego efektu końcowego:

- **Usunięcie woluminu** Jeśli wolumin zostanie usunięty, on sam i wszystkie dane, które zawiera! zostają usunięte. W rezultacie utworzona zostaje nieprzydzielona przestrzeń dostępna dla nowych woluminów.
- **Usunięcie dublowania** Jeśli dublowanie zostanie usunięte, przerwane zostaje kopiowanie danych, a jeden dysk będzie nieprzydzielony. Drugi dysk zachowuje kopię danych, które były poprzednio dublowane, ale dane te, rzecz jasna, nie są już odporne na uszkodzenia.
- **Przerwanie dublowania** Jeśli dublowanie zostało przerwane, dane nie są już powielane, ale oba dyski zachowują kopie danych. Dysk, który został wskazany podczas wybierania polecenia Break **Mirror** (Przerwij dublowanie) zachowuje przypisaną woluminowi dublowanemu literę dysku, foldery udostępnione, pliki stronicowania oraz punkty ponownej analizy. Do drugiego dysku zostaje przypisana kolejna dostępna litera.

Pamiętając o tych informacjach, należy zastanowić się nad sposobem wymiany trwale uszkodzonego dysku, który jest częścią woluminu dublowanego. Po fizycznej wymianie dysku należy otworzyć program *Disk Management*, aby ponownie skanować urządzenia, następnie trzeba zainicjować dysk i przekształcić go na dysk dynamiczny. Po zakończeniu tych czynności okaże się, że nie można ponownie włączyć dublowania woluminu, pomimo że jego druga część nie istnieje. Z punktu „widzenia” dysku, wolumin dublowany wciąż istnieje, jedynie jego część nadmiarowa nie została uruchomiona. Należy więc przerwać dublowanie poprzez kliknięcie prawym przyciskiem myszy woluminu i wybranie polecenia **Remove Mirror** (Usuń dublowanie). Warto przypomnieć, że w oknie dialogowym *Remwe*

Minor trzeba zaznaczyć tę część woluminu, której brakuje — zaznaczony wolumin zostanie usunięty w momencie kliknięcia przycisku **Remove Mirror**. Drugi (nie zaznaczony) wolumin stanie się woluminem prostym. Po zakończeniu operacji, należy kliknąć prawym przyciskiem myszy zdrowy wolumin prosty i wybrać polecenie **Add Mirror** (Dodaj dublowanie). Następnie trzeba wybrać nowy dysk, po czym dublowanie zostanie ponownie utworzone.



Wskazówka egzaminacyjna Woluminy dublowane zapewniają odporność na uszkodzenia oraz lepszą niż woluminy RAID-5 wydajność podczas operacji zapisu. Jednak z tego względu, że każdy dysk zestawu dublowanego zawiera pełną kopię danych, wolumin dublowany jest mniej efektywnym rodzajem woluminów ocenianym pod kątem wykorzystania dysków.

Woluminy RAID-5

Wolumin RAID-5 wykorzystuje co najmniej trzy dyski fizyczne zapewniając odporność na uszkodzenia oraz bardzo dobrą wydajność operacji odczytu.

Koszt odporności na uszkodzenia zmniejszona zostaje pojemność dysków. Dane są zapisywane na wszystkich dyskach woluminu RAID-5 z wyjątkiem jednego. Zapisywane są ponadto dodatkowe dane, nazywane parzystościami, które działają podobnie jak suma kontrolna zapewniająca odporność woluminu na uszkodzenia. Podczas operacji zapisu dokonywane są obliczenia sum kontrolnych, co oznacza, że wolumin RAID-5 znacznie intensywniej wykorzystuje procesor podczas operacji zapisu niż odczytu. Wolumin RAID-5 zapewnia lepszą wydajność dla operacji odczytu, ponieważ dane są jednocześnie pobierane z kilku dysków.

Zapis danych pliku na woluminie powoduje, że informacje sum kontrolnych (parzystość) są zapisywane na każdym dysku zestawu. Z punktu widzenia pojemności, wielkość przestrzeni używanej w celu zapewnienia odporności na uszkodzenia jest równa przestrzeni używanej przez jeden z dysków woluminu.

Oceniając pojemność woluminu RAID-5, jest on bardziej ekonomicznym rozwiązaniem w porównaniu do woluminu dublowanego. Stosując minimalną konfigurację trzech dysków woluminu RAID-5, jedna trzecia pojemności zostaje zajęta przez sumy kontrolne, kiedy w przypadku woluminu dublowanego połowa pojemności jest zajęta dla zapewnienia odporności na uszkodzenia. Ponieważ do utworzenia woluminu RAID-5 można użyć maksymalnie 32 dysków, teoretycznie można zbudować wolumin, który dla zapewnienia odporności na uszkodzenia całego woluminu rezerwuje jedynie 1/32 swojej pojemności.

Konfigurowanie woluminów RAID-5

Aby utworzenie woluminu RAID-5 było możliwe, trzeba dysponować co najmniej trzema dyskami dynamicznymi. Należy kliknąć prawym przyciskiem myszy jeden z tych dysków i wybrać polecenie **New Volume** (Nowy wolumin). Zgodnie z instrukcjami uruchomionego programu **New Volume Wizard** (Kreator nowego woluminu), jako typ woluminu należy wybrać wolumin **Raid-5** oraz należy wskazać inne dyski, które będą objęte tym woluminem.

Pojemność woluminu jest ograniczona przez najmniejszą część nieprzydzielonej przestrzeni jednego z dysków zestawu. Jeśli dysk 2 ma 50 GB nieprzydzielonej przestrzeni, a dysk 3 i dysk 4 mają po 100 GB nieprzydzielonej przestrzeni dyskowej, wolumin może wykorzystać tylko 50 GB przestrzeni dysku 3 i 4, ponieważ każdy przestrzeń używana na każdym dysku woluminu musi być jednakowa.

Pojemność lub parametr *Volume Size* (Wielkość woluminu) wyświetlana w programie *New Volume Wizard* (Kreator nowego woluminu) przedstawia wielkość dostępnej przestrzeni po uwzględnieniu parzystości. Opierając się na powyższym przykładzie, wielkość woluminu RAID-5 wyniesie 100 GB, całkowita pojemność minus pojemność jednego dysku przeznaczona na sumy kontrolne.

Do woluminów RAID-5 można przypisywać litery dysku lub ścieżki foldera, a formatowane mogą być jedynie za pomocą systemu NTFS.

Ponieważ woluminy RAID-5 są tworzone w oparciu o nieprzydzieloną przestrzeń jako macierzyste woluminy dynamiczne, nie można dołączyć innego typu woluminu do zestawu RAID-5 bez wykonania kopii zapasowej danych i ich odtworzenia w nowym woluminie RAID-5-

Przywracanie uszkodzonego woluminu RAID-5

Jeśli uszkodzony zostanie pojedynczy dysk woluminu RAID-5, dane wciąż są dostępne. Podczas operacji odczytu, brakujące dane są odtwarzane „w locie” na podstawie pozostałych danych i sum kontrolnych. Zmniejszona zostaje wydajność i oczywiście, jeśli w tym czasie awarii ulegnie kolejny dysk, pozostaje tylko odtworzenie danych na podstawie kopii zapasowych. Woluminy RAID-5 i dublowane są odporne jedynie na uszkodzenia pojedynczego dysku.

Jeśli dysk odzyskał sprawność, trzeba będzie ponownie uruchomić skanowanie urządzeń, a następnie kliknąć prawym przyciskiem myszy wolumin i wybrać polecenie **Reactivate Volume** (Uaktywnij ponownie dysk). Po odtworzeniu przez system brakujących danych wolumin będzie w pełni funkcjonalny.

Jeśli dysk nie udostępnia opcji **Reactivate** (Uaktywnij ponownie) lub jeśli trzeba było wymienić dysk, należy uruchomić skanowanie, a następnie zainicjować dysk. W kolejnym kroku trzeba przeprowadzić konwersję dysku na dynamiczny, kliknąć prawym przyciskiem myszy wolumin i wybrać polecenie **Repair Volume** (Napraw wolumin). Użytkownik musi zaznaczyć dysk, na którym odtworzone zostaną brakujące dane woluminu. Należy zaznaczyć nowo zainstalowany dysk, a system ponownie wygeneruje brakujące dane.

Porównanie woluminów dublowanych i RAID-5

Woluminy dublowane (RAID-1) i woluminy RAID-5 udostępniają różny poziom odporności na uszkodzenia. Decyzja dotycząca wykorzystywania konkretnego rozwiązania zależy od wymaganego poziomu ochrony oraz kosztu sprzętu. Główne różnice pomiędzy woluminami dublowanymi a RAID-5 to wydajność i koszt. Tabela 11-2 opisuje niektóre różnice pomiędzy programowanymi rozwiązaniami macierzy poziomów RAID-1 oraz RAID-5-

Tabela 11-2. Koszt i wydajność macierzy RAID

Woluminy dublowane (RAID-1)	Woluminy rozłożone z parzystością (RAID-5)
Mogą chronić partycje rozruchowe lub systemowe	Nic mogą chronić partycji systemowych lub rozruchowych
Wymagają dwóch dysków	Wymagają używania co najmniej trzech dysków twardych i pozwalają rozbudowywać zestaw do 32 dysków
Wyższy koszt w przeliczeniu na 1 MB	Niższy koszt w przeliczeniu na 1 MB
50% nadmiarowości	Maksymalna nadmiarowość wynosi 33%
Dobra wydajność operacji odczytu i zapisu	Bardzo dobra wydajność dla operacji odczytu i średnia dla operacji zapisu
Wykorzystują mniej pamięci systemu	Wymagają więcej pamięci systemu

Tworzenie woluminu odpornego na uszkodzenia dla woluminu systemowego

Ponieważ woluminy RAID-5 są tworzone jako macierzyste woluminy dynamiczne, nie istnieje możliwość zainstalowania lub uruchomienia systemu operacyjnego Windows Server 2003 w oparciu o woluminy RAID-5 utworzone z zastosowaniem technologii odporności na uszkodzenia dysków systemu Windows Server 2003-



Wskazówka Sprzętowa macierz RAID jest jednak niewidoczna dla systemu Windows Server 2003, więc system operacyjny może (a nawet powinien) być instalowany na sprzętowej macierzy dyskowej RAID.

Jedyną opcją utworzenia odpornego na uszkodzenia woluminu dla systemu (nie zaopatrując się w sprzętowe rozwiązanie RAID) jest utworzenie woluminu dublowanego. Wolumin systemowy może zostać zdublowany za pomocą procedury opisanej dla woluminów dublowanych: kliknięcie prawym przyciskiem myszy woluminu systemowego i wybranie polecenia **Add Mirror** (Dodaj dublowanie). Inaczej niż dla systemu Windows 2000, nie jest wymagane ponowne uruchomienie systemu, a plik BOOT.INI jest automatycznie aktualizowany tak, aby w przypadku uszkodzenia pierwszego dysku możliwe było uruchomienie systemu z dysku drugiego.

Jeśli dyski są podłączone do kontrolera IDE, a uszkodzeniu ulega dysk główny, trzeba usunąć ten dysk i skonfigurować drugi dysk tak, aby był widziany przez system jako dysk główny. W przeciwnym razie systemu nie będzie można uruchomić.



Wskazówka Jeśli decydujemy się na dublowanie woluminu systemowego, konfiguracja sprzętu powinna zakładać wykorzystanie jednego lub dwóch kontrolerów SCSI. Kontrolery powinny być tego samego typu. Obsługa i przywracanie takiej konfiguracji jest najprostsze.

Aktualizacja dysków

Warto pamiętać o dwóch potencjalnych „trikach” podczas aktualizacji dysków poprzedniej wersji systemu Windows lub podczas próby przeniesienia dysków do systemu Windows Server 2003 z komputera działającego pod kontrolą poprzedniej wersji systemu Windows.

Pierwszy to sytuacja, kiedy dysk był skonfigurowany w systemie Windows 2000 jako dysk podstawowy, następnie został przekształcony na dysk dynamiczny. Wolumin prosty takiego dysku nie może być rozszerzany na inne dyski wykorzystywane w systemie Windows Server 2003. Inaczej mówiąc, jeśli taki dysk zostanie przeniesiony do systemu Windows Server 2003 lub system operacyjny zostanie zaktualizowany do wersji Windows Server 2003, to nie będzie możliwe utworzenie woluminów łączonych poza woluminami prostymi dysku.

Drugi dotyczy faktu, że system Windows Server 2003 nie obsługuje już wielodyskowych macierzy utworzonych w systemie Windows NT 4. System ten obsługiwał zestawy dublowane, rozłożone oraz rozłożone z parzystością (RAID-5) w oparciu o dyski podstawowe. W systemie Windows 2000 obsługa tych zestawów była możliwa, chociaż trzeba było szybko dokonać konwersji zestawów na dynamiczne, aby ułatwić rozwiązywanie problemów i przywracanie danych. System Windows Server 2003 nie rozpoznaje tych woluminów. Po zaktualizowaniu systemu Windows NT 4 do Windows Server 2003, żaden zestaw RAID nie będzie widoczny. Przed aktualizacją trzeba wykonać kopię zapasową lub przenieść dyski, a dopiero następnie ponownie utworzyć zestawy dyskowe odporne na uszkodzenia w systemie Windows Server 2003 i przywrócić dane.

Zadanie kontrolne: Planowanie konfiguracji macierzy RAID

W zadaniu tym sprawdzany będzie serwer i jego pojemność pamięci dyskowej w kontekście wymaga domeny contoso.com oraz określania odpowiedniej konfiguracji.

Serwer firmy Contoso, Ltd. jest wyposażony w cztery dyski podsystemu SCSI:

- Dysk 0: 80 GB
- Dysk 1: 80 GB
- Dysk 2: 40 GB
- Dysk 3: 40 GB

Niedawno została wykonana nowa instalacja systemu Windows Server 2003 przeprowadzona poprzez | zarchiwizowanie danych wszystkich dysków, usunięcie wszystkich partycji tych dysków i zainstalowanie systemu operacyjnego na partycji dysku 0 o pojemności 20 GB.

Po instalacji systemu należy skonfigurować pozostałą przestrzeń dyskową. Dane użytkowników nie będą przechowywane na woluminie systemu operacyjnego. Należy maksymalizować pojemność pamięci i zapewnić ciągłą pracę systemu w przypadku awarii pojedynczego dysku. Jaka konfiguracja powinna być zastosowana oraz jaka będzie całkowita pojemność pamięci dyskowej przeznaczonej dla danych użytkowników?

Odpowiedź na te pytania to: połączenie woluminów dublowanego i RAID-5, przy czym pojemność całkowita woluminu danych użytkowników wyniesie 140 GB.

Aby zapewnić ciągłą pracę w przypadku uszkodzenia pojedynczego dysku, należy również zapewnić odporność na uszkodzenia dla systemu operacyjnego. W tym celu można zastosować jedynie wolumin dublowany, gdyż system operacyjny nie może być instalowany lub utrzymywany na woluminach RAID-5. Minimalna przestrzeń dyskowa dla systemu operacyjnego wynosi 20 GB i tym samym taka musi być pojemność woluminu dublowanego.

Przy założeniu maksymalnej wielkości przestrzeni dyskowej i odporności na uszkodzenia pojedynczego dysku, należy zastosować konfigurację macierzy RAID-5. Macierz RAID-5 może być zbudowana w oparciu o co najmniej trzy dyski. W przykładzie skonfigurowanie woluminu RAID-5 w oparciu o cztery dyski pozwoli uzyskać maksymalną pojemność zestawu. Wielkość woluminu RAID-5 determinowana jest najmniejszym fragmentem nieprzydzielonej przestrzeni dyskowej i chociaż dysk 0 oraz dysk 1 mają odpowiednio 60 i 80 GB wolnej przestrzeni, to mniejsze są dyski 40 GB i one określają pojemność zestawu. Przy 40 GB przestrzeni na czterech dyskach potencjalna pojemność woluminu wynosi 160 GB, ale wolumin RAID-5 dla zapewnienia odporności na uszkodzenia rezerwuje pojemność równoważną jednemu dyskowi zestawu. W rezultacie pojemność tego woluminu wyniesie 120 GB.

Pozostaje 20 GB nieprzydzielonej przestrzeni na dysku 0 oraz 40 GB na dysku 1. Można skonfigurować dublowanie systemu operacyjnego na dysku 1, pozostawiając na tym dysku 20 GB przestrzeni. Pozostała przestrzeń (20 GB na dyskach 0 oraz 1) może zostać skonfigurowana jako wolumin dublowany o pojemności 20 GB przeznaczony na dane użytkowników. Woluminy proste, łączone lub rozłożone nie są odporne na uszkodzenia, natomiast zastosowanie woluminu RAID-5 wymaga co najmniej trzech dysków fizycznych, tak więc dublowanie jest najlepszym sposobem wykorzystania pozostałej przestrzeni przy założeniu, że wolumin musi być odporny na uszkodzenia.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nic potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Administrator instaluje programową macierz RAID w systemie Windows Server 2003 i zakłada, że partycje rozruchowa i systemowa mają być odporne na uszkodzenia. Która wersja macierzy RAID powinna zostać wykorzystana?
 - a. RAID-0
 - b. RAID-1
 - c. RAID-5
 - d. Nic można użyć programowej macierzy RAID do ochrony partycji rozruchowej.
2. Administrator konfiguruje system Windows Server 2003 i chce chronić dane dysku twardego. Administrator zakłada także, że wprowadzone zostanie rozwiązanie o najszybszym z możliwych systemie we/wy oraz takie, które umożliwia wymianę dysków bez konieczności wyłączania komputera (hot swap). Która konfiguracja macierzy RAID powinna zostać zainstalowana?
 - a. RAID-0

- b. RAID-1
 - c. RAID-5
 - d. Sprzętowa macierz RAID
- 3- Administrator konfiguruje macierz RAID-5 w systemie Windows Server 2003 i ma zamiar do jej zbudowania użyć pięciu dysków twardych o pojemności 20 GB każdy. Jaki procent nadmiarowości należy przewidzieć dla takiej konfiguracji?
- a. 20
 - b. 25
 - c. 33
 - d. 50
4. Administrator konfiguruje programową macierz RAID w systemie Windows Server 2003, aby zapewnić odporność na uszkodzenia danych przechowywanych w tym systemie. Komputer jest wykorzystywany jako serwer bazy danych. Na serwerze wykonywanych jest wiele operacji odczytu i stosunkowo mało operacji zapisu. Po analizie administrator zdecydował, że zastosuje rozwiązanie, które jest odporne na uszkodzenia i zapewnia doskonałą wydajność dla operacji odczytu. Która konfiguracja macierzy RAID powinna zostać zainstalowana?
- a. RAID-0
 - b. RAID-1
 - c. RAID-5
5. Komputer, na którym ma zostać zainstalowana macierz RAID, jest wyposażony w trzy dyski, a każdy z nich ma 2 GB nieprzydzielonej przestrzeni. Administrator za pomocą przystawki Disk Management (Zarządzanie dyskami) uruchomił program New Volume Wizard (Kreator nowego woluminu), klikając prawym przyciskiem myszy obszar nieprzydzielonej przestrzeni dyskowej. Po wyświetleniu ekranu Select Volume Type (Wybieranie typu woluminu) okazało się, że opcja RAID-5 nie jest dostępna. Jaka jest najbardziej prawdopodobna tego przyczyna?
- a. Została już zainstalowana sprzętowa macierz RAID-5-
 - b. Jeden lub dwa dyski są skonfigurowane jako dyski podstawowe.
 - c. Wszystkie trzy dyski są skonfigurowane jako dyski dynamiczne.
 - d. Wszystkie trzy dyski są skonfigurowane jako dyski podstawowe.
 - e. Została już zainstalowana programowa macierz RAID-5.
6. Awarii uległ dysk woluminu dublowanego. Administrator zdecydował się zastąpić uszkodzony dysk. Jak należy przygotować zestaw dublowany do wymiany dysku?

Podsumowanie lekcji

- Niektóre poziomy macierzy RAID zapewniają odporność na uszkodzenia wprowadzając nadmiarowość danych. Istnieje możliwość instalowania macierzy RAID zapewniającej odporność na uszkodzenia w postaci rozwiązania sprzętowego lub programowego.
- Rozwiązania sprzętowe, w porównaniu do programowych, charakteryzują się lepszą wydajnością, ale są droższe.
- System Windows Server 2003 obsługuje trzy rodzaje programowych macierzy RAID: woluminy rozłożone (RAID-0), woluminy dublowane (RAID-1) oraz woluminy rozłożone z parzystością (RAID-5).
- W przypadku woluminu rozłożonego (RAID-0) dane zapisywane są na każdym dysku woluminu, dzięki czemu zwiększona zostaje wydajność operacji zapisu i odczytu, ale konfiguracja ta nie zapewnia odporności na uszkodzenia.
- Odporność na uszkodzenia woluminu RAID-5 uzyskiwana jest poprzez dodanie sumy kontrolnej (parzystości) zapisywanej na każdym dysku zestawu.
- W przypadku woluminu dublowanego odporność na uszkodzenia jest uzyskiwana poprzez jednoczesny zapis danych na dwóch dyskach fizycznych.
- Główne różnice pomiędzy woluminami dublowanym a woluminami RAID-5 to wydajność i koszt. Woluminy zapewniają dobrą wydajność podczas operacji zapisu i odczytu. Woluminy RAID-5 charakteryzują się lepszą wydajnością operacji odczytu, ale tylko średnią podczas operacji zapisu.
- Jedynie wolumin dublowany może być używany przez wolumin systemowy.

Zadanie praktyczne



Informacja Niniejsze zadanie praktyczne wymaga dostępu do sieci Internet.

Na serwerze plików firmy Contoso, Ltd. wyczerpana została pamięć dyskowa i w związku z tym należy dokonać aktualizacji serwera. Poprzednio ochrona danych w firmie sprowadzała się do wykonywania kopii zapasowych na nośnikach taśmowych. Jednak wraz z rozwojem firmy zmieniły się wymagania i obecnie, w przypadku awarii dysku, maksymalny czas przestoju serwera nie może być dłuższy niż kilka minut. Z tego względu zadaniem administratora jest przedstawienie rozwiązania dla pamięci dyskowych zapewniające odporność na uszkodzenia.

Ćwiczenie 1: Analiza woluminów systemu Windows Server 2003, które zapewniają odporność na uszkodzenia

Należy przejrzeć informacje zamieszczone w lekcji 4, aby zastanowić się, w jaki sposób używając woluminów dynamicznych można najlepiej skonfigurować serwery systemu Windows Server 2003 tak, aby zapewniona została odporność na uszkodzenia. Warto również posłużyć się zadaniem kontrolnym lekcji 4, aby przypomnieć sobie, w jaki sposób różne typy woluminów obsługują odporność na uszkodzenia.

Analizując rozwiązanie oparte na dyskach IDE i zakładając, że system operacyjny zainstalowany jest na dublowanym dysku głównym IDE, który uległ awarii wiemy, że konieczna będzie zmiana konfiguracji dysku pomocniczego IDE (zmiana konfiguracji zworek lub położenia kabli) oraz przełożenie kabla interfejsowego do głównego kanału kontrolera IDE. Mając to na uwadze, lepszym rozwiązaniem będzie konfiguracja, która wykorzystuje dwa kontrolery SCSI, a dublowane kopie systemu będą przechowywane na pierwszych dyskach obu kanałów SCSI. Konfiguracja taka zapewnia szybkie odtworzenie systemu, nie tylko w przypadku awarii pojedynczego dysku, ale również w przypadku awarii jednego z kontrolerów.

Na tym etapie należy jeszcze rozważyć zagadnienia związane z wydajnością i pojemnością woluminu RAID w systemie Windows Server 2003- Należy uwzględnić czas potrzebny do odtworzenia po awarii dysku, czyli czas operacji związanych z wyłączeniem serwera, wymianą dysku, ponownym uruchomienie serwera oraz czas potrzebny do regeneracji brakującego woluminu.

Ćwiczenie 2: Analiza sprzętowej macierzy RAID

Mając na uwadze powyższe rozważania, należy zastanowić się nad możliwością zastosowania sprzętowej macierzy RAID. Inaczej mówiąc, trzeba zadać sobie pytanie: jakie są zalety rozwiązania sprzętowego? Niektóre odpowiedzi na tak postawione pytanie można znaleźć w lekcji 4.

Należy otworzyć przeglądarkę Internet Explorer i przejrzeć witryny sieci Web dostawców i producentów urządzeń komputerowych wyszukując oferty macierzy dyskowych RAID. Prezentowane są macierze RAID, które oferowane są razem z dyskami, kontrolerami macierzowymi i obudowami, do których trzeba podłączać dyski. Należy zwrócić uwagę na macierze RAID gotowe do używania i rozważyć na następujące kwestie:

- Które opcje są dostępne?
- Ocena dostawców sprzętowych macierzy RAID.
- Możliwości oferowanych sprzętowych macierzy RAID.
- Które konfiguracje RAID można implementować za pomocą sprzętowych macierzy RAID? Czy system Windows Server 2003 obsługuje te konfiguracje?
- Jaki jest przedział cen zakupu sprzętowej macierzy RAID?
- Jaki jest koszt niektórych prostych macierzy RAID?

W okresie prac nad książką, koszt sprzętowego rozwiązania macierzy RAID umożliwiającego obsługę 720 GB pamięci dyskowej, czyli wartości znacznie przekraczającej pojemność jakiegokolwiek pojedynczego dysku większości serwerów, wynosił około 3000\$.

W jaki sposób należy przedstawić zarządowi firmy ocenę wartości sprzętowej macierzy RAID? Czy w porównaniu do konfiguracji wykorzystującej programową macierz RAID systemu Windows Servet 2003 warto rekomendować taki zakup macierzy sprzętowej? Dlaczego warto lub dlaczego nie warto?

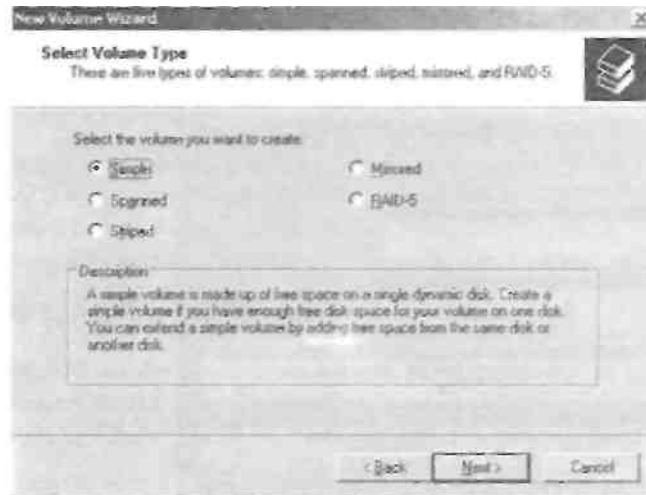
Rozwiązywanie problemów

Administrator firmy Contoso, Ltd. zajmuje się serwerem „odziedziczonym” po poprzedniku. Serwer zawiera szereg wewnętrznych dysków SCSI. Za pomocą konsoli Disk Management (Zarządzanie dyskami) administrator sprawdza konfigurację dysków i woluminów serwera. Konfiguracja ta została pokazana poniżej:



Prognoza pogody przewiduje nadejście silnych burz nazajutrz wcześniej rano. Administrator dla bezpieczeństwa rozpoczął wykonywanie kopii zapasowych serwera i opuścił pomieszczenie. Burza okazała się wyjątkowo silna, zmuszając przedsiębiorstwo do zamknięcia działalności na kilka dni. Długotrwały brak zasilania budynku spowodował całkowite wyczerpanie baterii zasilaczy awaryjnych, co spowodowało wyłączenie serwerów. W okresie przywracania zasilania budynku, podczas pierwszych kilku godzin wystąpiły wahania i zakłócenia w sieci zasilającej.

Po powrocie do serwerowni administrator uruchomił serwery. Opisywany serwer zgłosił wystąpienie błędów, a po uruchomieniu programu Disk Management (Zarządzanie dyskami) można było zobaczyć dość katastroficzny widok stanu dysków i woluminów serwera:



CKwa dyski serwera zostały uszkodzone. Jeden zawierał kopię woluminu systemowego (wolumin dublowany). Drugi zawierał kilka typów woluminów, wliczając w to część woluminu łączonego, rozłożonego oraz woluminu RAID-5.

Administrator miał zapasowy dysk o pojemności 80 GB. Wyłączył serwer i wyjął uszkodzone dyski, a następnie zainstalował nowy dysk i uruchomił serwer.

Ćwiczenie

Należy poświęcić pewien czas i na kartce papieru starannie zaplanować procedurę wymaganą do przywrócenia danych na każdym uszkodzonym woluminie. Należy uwzględnić kroki związane z „wyczyszczeniem” brakujących dysków i woluminów, a także z instalowaniem, konfigurowaniem oraz zastępowaniem danych na nowym dysku.

Po upewnieniu się, że procedura uwzględni wszystkie etapy, należy porównać ją z procedurą przedstawioną poniżej:

Procedura przywracania powinna zawierać następujące elementy:

1. Zaloguj się w systemie.
2. Zakończ instalowanie nowego dysku. Postępuj zgodnie z instrukcjami wyświetlanymi przez program Found New Hardware Wizard (Kreator wyszukiwania nowego sprzętu). Jeśli kreator nie został uruchomiony, otwórz program Device Manager (Menedżer urządzeń) i sprawdź, czy dysk został automatycznie wykryty i zainstalowany. Jeśli nie, należy otworzyć program Add Hardware (Dodaj sprzęt), aby zainstalować dysk.
3. Otwórz program Disk Management (Zarządzanie dyskami).
4. Wykryj i zainicjuj nowy dysk. Program Disk Management (Zarządzanie dyskami) prawdopodobnie wykryje nowy dysk i wyświetli program Initialize Disk Wizard (Kreator inicjowania dysku). Jeśli

kreator nie został uruchomiony, sprawdź czy dysk jest widoczny w programie Disk Management (Zarządzanie dyskami). Jeśli tak nie jest, kliknij prawym przyciskiem myszy węzeł programu Disk Management (Zarządzanie dyskami) i wybierz polecenie Rescan (Skanuj dyski ponownie). Po wyświetleniu dysku, kliknij dysk prawym przyciskiem myszy i wybierz polecenie Initialize (Zainicjuj).

5. Odtwarzanie woluminów (kolejność dowolna).

Odtwarzanie woluminu RAID-5

- a. Przekształć nowy dysk na dysk dynamiczny. Kliknij prawym przyciskiem myszy nowy dysk i wybierz polecenie Convert to Dynamic (Konwertuj na dysk dynamiczny).
- b. Kliknij prawym przyciskiem myszy działającą część woluminu RAID-5 i wybierz polecenie Repair Volume (Napraw wolumin). Zaznacz nowy dysk, który ma wystarczająco dużo przestrzeni, aby mógł stać się częścią zestawu rozłożonego. Wolumin RAID-5 zostanie utworzony i zsynchronizowany.

Odtwarzanie woluminu dublowanego

- a. Usuń dublowanie. Kliknij prawym przyciskiem myszy uszkodzony dysk i wybierz polecenie Remove Mirror (Usuń dublowanie). Sprawdź, czy jest zaznaczony fragment opisany jako Missing (Brak) i kliknij polecenie Remove Mirror (Usuń dublowanie). Pozostała część zestawu dublowanego przekształci się w wolumin prosty.
- b. Kliknij prawym przyciskiem myszy wolumin prosty i wybierz polecenie Add Mirror (Dodaj dublowanie). Zaznacz nowy dysk, który ma wystarczająco dużo przestrzeni, aby utworzyć zestaw dublowany i kliknij polecenie Add Mirror (Dodaj dublowanie). Zostanie utworzony i zsynchronizowany wolumin dublowany.

Odtwarzanie woluminu rozłożonego

- a. Usuń wolumin. Woluminy rozłożone nie są odporne na uszkodzenia. Wszystkie dane tego woluminu zostały utracone.
- b. Utwórz ponownie wolumin rozłożony. Kliknij prawym przyciskiem myszy nieprzydzieloną przestrzeń, gdzie istniał poprzednio wolumin rozłożony i wybierz polecenie New Volume (Nowy wolumin). Jako typ woluminu wybierz wolumin rozłożony i dodaj nowy dysk do zestawu rozłożonego. Wolumin rozłożony zostanie utworzony i sformatowany.
- c. Odtwórz dane woluminu rozłożonego na podstawie kopii zapasowej.

Odtwarzanie woluminu łączonego

- a. Usuń wolumin. Woluminy łączone nie są odporne na uszkodzenia. Wszystkie dane tego woluminu zostały utracone.
 - b. Utwórz ponownie wolumin łączony. Kliknij prawym przyciskiem myszy nieprzydzieloną przestrzeń, gdzie istniał poprzednio wolumin łączony i wybierz polecenie New Volume (Nowy wolumin). Jako typ woluminu wybierz wolumin łączony i dodaj nowy dysk do zestawu łączonego. Na nowym dysku wybierz odpowiednią wielkość przestrzeni, która ma być używana. Wolumin łączony zostanie utworzony i sformatowany.
 - c. Odtwórz dane woluminu łączonego na podstawie kopii zapasowej.
6. Usuń brakujące dyski. Kliknij prawym przyciskiem myszy brakujące dyski i kliknij polecenie Remove Volume (Usuń wolumin). Dopóki dublowanie nie zostanie usunięte, nie można usunąć

dysku zestawu, w którym brakuje drugiego dysku. Nie można usuwać dysków zawierających woluminy proste, łączone lub RAID-5 dopóki woluminy te nie zostaną usunięte lub naprawione.

7. Po ponownej synchronizacji i odtworzeniu wszystkich woluminów uruchom program CHKDSK.

Podsumowanie rozdziału

- System Windows Server 2003 obsługuje dwa typy pamięci dyskowych, podstawową i dynamiczną oraz kilka systemów plików, wliczając w to FAT, FAT32 oraz NTFS. Większość zaawansowanych funkcji zarządzania pamięcią dyskową dostępnych jest jedynie na dyskach dynamicznych sformatowanych za pomocą systemu NTFS.
- Dyski dynamiczne umożliwiają elastyczne i sprawne zarządzanie wielodyskowymi konfiguracjami dysków. Istnieje możliwość zainstalowania woluminów łączonych, dublowanych, rozłożonych oraz woluminów RAID-5 spełniających różne wymagania związane z pojemnością, wydajnością oraz odpornością na uszkodzenia systemu.
- Woluminy dyskowe mogą zostać uszkodzone, ulec fragmentacji lub (najczęściej) mogą zapęłnić się całkowicie. Programy narzędziowe Check Disk (Sprawdź dysk), Disk Defragmenter (Dcfragmentator dysku) oraz Disk Quotas (Przydziały dysku) są pomocne przy zarządzaniu istniejącymi woluminami.
- Nie wszystkie konfiguracje RAID są odporne na uszkodzenia. Woluminy dublowane oraz woluminy RAID-5 są odporne na uszkodzenia, natomiast woluminy rozłożone są nieodporne na uszkodzenia. Żaden z rodzajów woluminów systemu Windows Server 2003 nie zapewnia odporności na uszkodzenia, jeśli awarii ulega więcej niż jeden dysk woluminu.

Informacje dla zdających egzamin

Przed przystąpieniem do egzaminu należy zapoznać się z przedstawionymi poniżej najważniejszymi faktami i pojęciami, aby określić które tematy wymagają pogłębienia. Należy powrócić do lekcji, aby osiągnąć większą wprawę oraz przejrzeć działy znajdujące się w części 2 — „Materiały dodatkowe”. Informacje tu zawarte kierują do materiałów uzupełniających tematów objętych zadaniami egzaminacyjnymi.

Najważniejsze fakty

- Poznanie czynników decydujących o pojemności, wydajności i odporności na uszkodzenia każdego rodzaju woluminu dyskowego. Należy być przygotowanym na opracowanie zaleceń dotyczących wyboru konfiguracji dysków w oparciu o przedstawione wymagania.
- Poznanie sposobów wprowadzania przydziałów dysku dla użytkowników oraz działania obu rodzajów ustawień — domyślnych ustawień przydziału oraz określonych wpisów przydziału.
- Rozpoznawanie i naprawa woluminu, który był chwilowo odłączony (offline), a po pewnym czasie nastąpiło jego ponowne podłączenie: polecenia Rescan (Skanuj ponownie) i Reactivate Disk (Reaktywuj dysk) lub Reactive volumes (Reaktywuj woluminy) oraz program CHKDSK.
- Zapoznanie się ze sposobami odbudowy woluminów odpornych na uszkodzenia (woluminy dublowane i RAID-5) na dyskach zastępczych oraz z odpowiednimi poleceniami używanymi podczas

przywracania uszkodzonych woluminów: Rescan (Skanuj ponownie), Initialize (Zainicjuj), Convert to Dynamic Disk (Konwertuj na dysk dynamiczny), Break Mirror (Przerwij dublowanie), Remove Mirror oraz Repair Volume (Napraw wolumin).

Najważniejsze pojęcia

Wolumin prosty Ekwiwalentem partycji dysku podstawowego jest wolumin prosty dysku dynamicznego. Ponieważ woluminy proste istnieją tylko na dyskach fizycznych, nie są odporne na uszkodzenia.

Woluminy łączone Wolumin łączony zawiera przestrzeń dyskową co najmniej dwóch dysków fizycznych. Ze względu na fakt, że woluminy mają tendencję do zwiększania pojemności, a tym samym w zestawie stosowanych będzie coraz więcej dysków fizycznych, wzrasta ryzyko uszkodzenia.

Wolumin rozłożony Dane są zapisywane w takim samym tempie na co najmniej 2 dyskach. W zestawie mogą być maksymalnie 32 dyski. Wolumin zapewnia maksymalną wydajność i pojemność, ale nie jest odporny na uszkodzenia.

Wolumin dublowany Dwa dyski zawierają identyczną kopię danych. Jest to jedyna programowa konfiguracja macierzy RAID obsługiwana na woluminach systemowych. Wolumin dublowany zapewnia dobrą wydajność operacji odczytu i zapisu. Woluminy te są jednak drogie w kontekście oceny wykorzystania dysków, ponieważ 50% potencjalnej pojemności woluminu używane jest dla zapewnienia odporności na uszkodzenia.

Wolumin RAID-5 Dane są zapisywane w takim samym tempie na co najmniej 3 dyskach i dla zapewnienia odporności na uszkodzenia pojedynczego dysku, są przeplatane sumami kontrolnymi (parzystość). W zestawie mogą być zainstalowane maksymalnie 32 dyski. Charakteryzują się dobrą wydajnością operacji odczytu, dobrym wykorzystaniem pojemności dysku, są natomiast drogie w kontekście wykorzystania procesora oraz wydajności operacji zapisu, jako że podczas tych operacji muszą być obliczane sumy kontrolne.

Pytania i odpowiedzi

400 Pytania do lekcji 1

1. Administrator instaluje nowy dysk o pojemności 200 GB. Dysk ma być podzielony na pięć woluminów logicznych z przeznaczeniem dla systemu operacyjnego, aplikacji, katalogów macierzystych użytkowników, udostępnionych danych oraz punktu dystrybucji oprogramowania. Woluminy powinny mieć jednakową pojemność. 50 GB przestrzeni dyskowej powinno pozostać nieprzydzielone, aby można było w przyszłości rozszerzać wolumin logiczny. Biorąc pod uwagę dyski dynamiczne i podstawowe oraz obsługiwane przez nie rodzaje woluminów logicznych, jakie opcje konfiguracji należałoby zastosować?

Należy przydzielić 150 GB przestrzeni dyskowej, a 50 GB powinno pozostać nieprzydzielone. Oznacza to, że każdy z pięciu woluminów logicznych będzie miał 30 GB pojemności. Dysk może zostać skonfigurowany jako dysk podstawowy, który nie zawiera partycji podstawowych lub jako dysk podstawowy, który może zawierać do trzech takich partycji. Każda partycja podstawowa obsługuje jeden dysk logiczny (który jest woluminem logicznym dysku podstawowego). Pozostałe dwa do pięciu woluminów logicznych może zostać utworzonych jako dyski logiczne partycji rozszerzonej. Jeśli dysk zostanie skonfigurowany jako dysk dynamiczny, wszystkie pięć woluminów logicznych może zostać skonfigurowanych jako woluminy proste. Mimo, że opisane powyżej konfiguracje stanowią prawidłową odpowiedź na zadane pytanie, w tej sytuacji lepszym rozwiązaniem jest konfiguracja dysków w postaci dysków dynamicznych (uzasadnienie opisane jest w następnej lekcji).

2. Która z poniżej wymienionych konfiguracji umożliwia przywrócenie systemu po awarii pojedynczego dysku twardego?
 - a. Primary partition (Partycja podstawowa)
 - b. Extended partition (Partycja rozszerzona)
 - c. Logical drive (Dysk logiczny)
 - d. Simple volume (Wolumin prosty)
 - e. Spanned volume (Wolumin łączony)
 - f. Mirrored volume (Wolumin dublowany)

Striped volume (Wolumin rozłożony) g. RAID-5

volume (Wolumin RAID-5) Prawidłowe

odpowiedzi to f oraz h.

3. W systemie testowym używany jest rozruch dwóch systemów operacyjnych. Na pierwszej partycji podstawowej komputera zainstalowany został system Windows NT 4, a na drugiej partycji podstawowej system Windows Server 2003. Ponieważ w komputerze zaczyna brakować pamięci dyskowej, w systemie zainstalowany zostanie nowy napęd dyskowy. System uruchomiony został w oparciu o Windows Server 2003, a dysk skonfigurowany został jako dysk dynamiczny. Po rozruchu komputera w oparciu o system Windows NT 4 okazało się, że dysk nie jest widoczny. Dlaczego?

Dyski dynamiczne są obsługiwane jedynie w systemach Windows XP, Windows 2000 oraz Windows Server 2003.

4. W celu zagwarantowania odporności na uszkodzenia, maksymalnej wydajności oraz możliwości wymiany uszkodzonych dysków bez wyłączania systemu (hot-swap) administrator zakupił macierz

dyskową RAJD składającą się z siedmiu dysków. Po zainstalowaniu macierzy w systemie Windows Server 2003 widoczny był tylko jeden nowy dysk. Dlaczego?

Po skonfigurowaniu sprzętowy podsystem dyskowy przechwytuje lub maskuje dla systemu operacyjnego strukturę fizyczną dysków. Podsystem taki obsługuje operacje i funkcje we/wy dysków zainstalowanej macierzy, a operacje zapisu związane z dublowaniem lub z obliczaniem sum kontrolnych nie stanowią obciążenia dla systemu operacyjnego i nie mają wpływu na jego wydajność.

412 Pytania do lekcji 2

1. Niniejsze pytanie jest kontynuacją sytuacji opisanej w pytaniu pierwszym lekcji 1. W komputerze zainstalowany jest nowy dysk o pojemności 200 GB. Dysk skonfigurowany został jako podstawowy, a na dysku utworzone zostały trzy 30 GB partycje przeznaczone na system operacyjny, katalogi macierzyste użytkowników oraz dane udostępnione. Skonfigurowana została również partycja rozszerzona i dwa 30 GB dyski logiczne przeznaczone na instalowanie aplikacji oraz dla punktu dystrybucji oprogramowania. Na dysku pozostało 50 GB nieprzydzielonej przestrzeni. Kilka miesięcy później okazało się, że trzy woluminy są prawie całkowicie wypełnione. Administrator przygotowuje się do odpowiedniego zareagowania w sytuacji, kiedy jeden z woluminów trzeba będzie rozszerzyć. Jakie działania musi przedsięwziąć?

Należy przekształcić dysk na dysk dynamiczny. Partycja dysku podstawowego może być tylko rozszerzana na bezpośrednio przylegającą nieprzydzieloną przestrzeń ciągłą. Proces konwersji dysku na dysk dynamiczny przekształca każdą partycję podstawową oraz dysk logiczny na wolumin prosty. Woluminy proste mogą być rozszerzane o dowolną nieprzydzieloną przestrzeń.

2. Który rodzaj obszarów dysku obsługuje dyski logiczne?
 - a. Partycje podstawowa
 - b. Woluminy proste
 - c. Woluminy łączone
 - d. Partycje rozszerzone
 - e. Nieprzydzieloną przestrzeń

Prawidłowa odpowiedź to d.
3. Niedawno do komputera został dodany dysk. Dysk był poprzednio używany w systemie Windows 2000 Server. Dysk jest wyświetlany w programie Device Manager (Menedżer dysku), ale nie jest prawidłowo pokazywany w programie Disk Management (Zarządzanie dyskami). Jakie zadanie należy wykonać?
 - a. Import Foreign Disk (Zaimportuj obce dyski)
 - b. Format volume (Formatuj wolumin)
 - c. Rescan (Ponownie skanuj)
 - d. Change Drive Letter or Path (Zmień literę dysku i ścieżki)
 - e. Convert to Dynamic Disk (Konwertuj na dysk dynamiczny)

Prawidłowa odpowiedź to c.
4. Administrator próbuje przekształcić zewnętrzny dysk standardu FireWire z dysku podstawowego na dynamiczny, ale opcja umożliwiająca konwersję jest niedostępna. Jaka jest najbardziej prawdopodobna tego przyczyna?

Dyski wymienne nie mogą być przekształcane na dyski dynamiczne- Dyski zewnętrzne są traktowane jak dyski wymienne.

421 Pytania do lekcji 3

- 1- Administrator systemu Windows Server 2003 chce naprawić Wędy syatemu plików i odtworzyć uszkodzone sektory dysku twardego komputera- Które narzędzie powinien zastosować administrator?
 - a. Check Disk (Sprawdź dysk)
 - b. Disk Defragmenter (Defragmentator dysku)
 - c. DISKPART
 - d. Disk quotas (Przydziały dysku)

Prawidłowa odpowiedź to a.

2. Komputer działa pod kontrolą systemu Windows Server 2003- Dysk twardy komputera zawiera dwa woluminy danych: D oraz E. Administrator włączył przydziały dysku na woluminach D oraz E, które dla każdego użytkownika określają limit przestrzeni dyskowej równy 20 MB. Jednakże administrator chce ograniczyć wielkość folderów macierzystych użytkowników przechowywanych w ścieżce D:\Users do wartości 10 MB dla każdego użytkownika. Czy jest to możliwe? Dlaczego tak lub dlaczego nie? Gdzie można wprowadzać przydziały?
 - a. Na dowolnym serwerze dla wszystkich dysków
 - b. Na dowolnym dysku fizycznym dla wszystkich woluminów
 - c. Na dowolnym woluminie dla wszystkich folderów
 - d. Na dowolnym folderze

Prawidłowa odpowiedź to c. Przydziały wprowadzane są jedynie w odniesieniu do woluminu. Nie można skonfigurować przydziału dla foldera Users znajdującego się na woluminie D. Przydział stosowany jest do całego woluminu. Nie można również dla użytkownika definiować przydziału 20 MB przestrzeni rozmieszczonej na woluminach D i E. Można jednak skonfigurować limit 15 MB na woluminie D oraz 5 MB na woluminie E lub określić dowolnie inną kombinację przydziału, którego łączony limit to 20 MB.

- 3- Jaki jest wymóg minimalnej wielkości wolnej przestrzeni dyskowej, aby można było przeprowadzić defragmentację?
 - a. 5%
 - b. 10%
 - c. 15%
 - d. 25%
 - e. 50%

Prawidłowa odpowiedź to c.

431 Pytania do lekcji 4

1. Administrator instaluje programową macierz RAID w systemie Windows Server 2003 i zakłada, że partycje rozruchowa i systemowa mają być odporne na uszkodzenia. Która wersja macierzy RAID powinna zostać wykorzystana?

- a. RAID-0
- b. RAID-1
- c. RAID-5

d. Nic można użyć programowej macierzy RAID do ochrony partycji rozruchowej.

Prawidłowa odpowiedź to b. Wolumin dublowany może zawierać dowolne partycje, w tym partycje systemowe i rozruchowe.

2. Administrator konfiguruje system Windows Server 2003 i chce chronić dane dysku twardego. Administrator zakłada także, że wprowadzone zostanie rozwiązanie o najszybszym z możliwych systemie wc/wy oraz takie, które umożliwi wymianę dysków bez konieczności wyłączania komputera (hot swap). Która konfiguracja macierzy RAID powinna zostać zainstalowana?

- a. RAID-0
- b. RAID-1
- c. RAID-5
- d. Sprzętowa macierz RAID

Prawidłowa odpowiedź to d. Pomimo, że w porównaniu do programowej, sprzętowa macierz RAID jest droższym rozwiązaniem zapewniającym odporność na uszkodzenia, jednak operacje wc/wy przez nią realizowane są szybsze. Oprócz tego, sprzętowe rozwiązania mogą obsługiwać funkcje pozwalające wymieniać uszkodzone dyski bez wyłączania komputera (hot swap) oraz umożliwiają automatyczne zastępowanie dysku uszkodzonego przez podłączony dysk rezerwowy (hot spare).

3. Administrator konfiguruje macierz RAID-5 w systemie Windows Server 2003 i ma zamiar do jej zbudowania użyć pięciu dysków twardych o pojemności 20 GB każdy. Jaki procent nadmiarowości należy przewidzieć dla takiej konfiguracji?

- a. 20
- b. 25
- c. 33
- d. 50

Prawidłowa odpowiedź to a. Stosowanie woluminów RAID-5 ze względu na lepsze wykorzystanie dysków jest bardziej opłacalne. Im więcej dysków zainstalowanych jest w zestawie RAID-5, tym mniejszy jest koszt związany z nadmiarowością. Jeśli w konfiguracji RAID-5 używanych jest pięć dysków, przewidywana przestrzeń zarezerwowana dla zapewnienia odporności na uszkodzenia to 20% sumarycznej przestrzeni dysków.

4. Administrator konfiguruje programową macierz RAID w systemie Windows Server 2003, aby zapewnić odporność na uszkodzenia danych przechowywanych w tym systemie. Komputer jest wykorzystywany jako serwer bazy danych. Na serwerze wykonywanych jest wiele operacji odczytu i stosunkowo mało operacji zapisu. Po analizie administrator zdecydował, że zastosuje rozwiązanie, które jest odporne na uszkodzenia i zapewnia doskonałą wydajność dla operacji odczytu. Która konfiguracja macierzy RAID powinna zostać zainstalowana?

- a. RAID-0
- b. RAID-1
- c. RAID-5

Prawidłowa odpowiedź to c. Chociaż macierz RAID-5 charakteryzuje się średnią wydajnością dla operacji zapisu, ma znakomitą wydajność dla operacji odczytu. Macierz RAID-1 ma dobrą wydajność i dla odczytu i dla zapisu, ale wydajność operacji odczytu nie jest tak dobra, jak w przypadku macierzy RAID-5-

5. Komputer, na którym ma zostać zainstalowana macierz RAID jest wyposażony w trzy dyski, a każdy z nich ma 2 GB nieprzydzielonej przestrzeni. Administrator za pomocą przystawki Disk Management (Zarządzanie dyskami) uruchomił program New Volume Wizard (Kreator nowego woluminu), klikając prawym przyciskiem myszy obszar nieprzydzielonej przestrzeni dyskowej. Po wyświetleniu ekranu Select Volume Type (Wybieranie typu woluminu) okazało się, że opcja RAID-5 nie jest dostępna. Jaka jest najbardziej prawdopodobna tego przyczyna?
 - a. Została już zainstalowana sprzętowa macierz RAID-5.
 - b. Jeden lub dwa dyski są skonfigurowane jako dyski podstawowe.
 - c. Wszystkie trzy dyski są skonfigurowane jako dyski dynamiczne.
 - d. Wszystkie trzy dyski są skonfigurowane jako dyski podstawowe.
 - e. Została już zainstalowana programowa macierz RAID-5.

Prawidłowa odpowiedź to b. Aby skonfigurować wolumin RAID-5, co najmniej trzy dyski muszą być skonfigurowane jako dyski dynamiczne.

6. Awarii uległ dysk woluminu dublowanego. Administrator zdecydował się zastąpić uszkodzony dysk. Jak należy przygotować zestaw dublowany do wymiany dysku?

Należy sprawdzić, czy aktualnie żaden proces nie uzyskał dostępu do woluminu dublowanego oraz czy uszkodzenie woluminu dublowanego spowodowane jest awarią dysku czy uszkodzeniem kontrolera. Następnie, przy użyciu programu Diskpart lub przystawki Disk Management (Zarządzanie dyskami), należy zaznaczyć uszkodzony dysk i usunąć dublowanie. Po usunięciu dublowania, jeśli to konieczne, należy wyłączyć komputer i wymienić uszkodzony dysk. Po ponownym uruchomieniu komputera, przy użyciu programu Diskpart lub przystawki Disk Management (Zarządzanie dyskami), należy włączyć dublowanie pozostałego dysku zestawu. Dodanie dublowania utworzy kopię danych na nowym dysku.

12 Monitorowanie systemu Microsoft Windows Sewer 2003



Zadania egzaminacyjne omawiane w tym rozdziale:

- Monitorowanie bieżącej wydajności systemu
- Monitorowanie i analiza zdarzeń
- Monitorowanie i optymalizacja serwera pod kątem wydajności aplikacji
- Monitorowanie obiektów wydajności pamięci
- Monitorowanie obiektów wydajności sieci
- Monitorowanie obiektów wydajności procesu
- Monitorowanie obiektów wydajności dysku
- Monitorowanie wąskich gardeł urządzeń sprzętu serwera
- Monitorowanie zdarzeń

Cele rozdziału

Nowa instalacja komputera nie zapowiada kłopotów - system ma wystarczająco dużo zasobów, które jeszcze nie zostały zdegradowane długotrwałym wykorzystywaniem. Jednakże wraz z upływem czasu, wskutek dodawania aplikacji i użytkowników, problemy zaczynają narastać. Bez odpowiednich narzędzi monitorowania systemu oraz umiejętności odpowiedniego posługiwania się nimi, możemy tylko obserwować stopniowy spadek wydajności serwera poczynając od niewielkich zakłóceń a kończąc na znaczących problemach.

Pierwszy etap monitorowania nowego systemu Microsoft Windows Server 2003 powinien dotyczyć rzetelnego określenia danych o dostępności zasobów i wydajności. Dane te powinny być okresowo porównywane z danymi rzeczywistymi tak, aby powstające problemy aplikacji lub sprzętu mógł być rozwiązywany zanim staną się poważnym zagrożeniem. Szeroki wybór narzędzi dostępnych w systemie Windows Server 2003 sprawia, że żaden szanujący się administrator nie musi działać po omacku.

Lekcje rozdziału:

- Lekcja 1: Wykorzystywanie programu *Event Viewer* (Podgląd zdarzeń) 447
- Lekcja 2: Wykorzystywanie programu *Performance Console* (Wydajność) 453
- Lekcja 3: Wykorzystywanie programu *Task Manager* (Menedżer zadań).....463
- Lekcja 4: Wykorzystywanie usługi *WMI Event Logging Provider*
(Dostawcy protokolowania zdarzeń) 469

Wymagania

Aby przeprowadzić ćwiczenia omawiane w tym rozdziale trzeba przygotować:

- Komputer nazwany Server01, działający pod kontrolą systemu Windows Server 2003.
- Serwer Server01 powinien być kontrolerem domeny contoso.com.

Lekcja 1: Wykorzystywanie programu Event Viewer

System Windows Server 2003 został wyposażony w zestaw plików dziennika, które są konfigurowane i prezentowane w programie *Event Viewer* (Podgląd zdarzeń). Dzięki skonfigurowaniu opcji każdego dziennika zgodnie z wymaganiami środowiska, gromadzone będą odpowiednie dane dotyczące urządzeń sprzętu, aplikacji systemu oraz dostępu do zasobów.

Materiały omówione podczas lekcji pozwalają na

- Identyfikację typów dzienników programu *Event Viewer* (Podgląd zdarzeń)
- Konfigurowanie rejestrowania odpowiednich danych dziennika
- Wyświetlanie zaprotokołowanych danych przy użyciu filtra

Szacunkowy czas lekcji: 20 minut

Dostępne dzienniki programu Event Viewer (Podgląd zdarzeń)

Usługa systemu Windows Server 2003 — Event Log (Dziennik zdarzeń) jest uruchamiana automatycznie na wszystkich komputerach systemu Windows Server 2003. Usługa ta rejestruje zdarzenia w jednym z trzech wymienionych poniżej dzienników:

- **Application (Aplikacja)** Projektanci aplikacji mogą definiować, aby w tym dzienniku rejestrowane były zmiany konfiguracji, błędy lub inne zdarzenia związane z napisanym przez nich oprogramowaniem.
- **System** W tym dzienniku rejestrowane są zdarzenia związane z systemem operacyjnym Windows Server 2003 (uruchomienie usługi, nieprzewidziane wyłączenia, uszkodzenia urządzeń itp). Konfiguracja zdarzeń protokołowanych w tym dzienniku jest wstępnie zdefiniowana.
- **Security (Zabezpieczenia)** W dzienniku rejestrowane są zdarzenia dotyczące logowania i dostępu do zasobów (inspekcje). Konfiguracja większości tych zdarzeń określana jest przez administratora.



Informacja Pomimo, że dzienniki zdarzeń aplikacji i zabezpieczeń są określane odpowiednio przez programistów i system operacyjny, najpierw musi zostać skonfigurowany dziennik zabezpieczeń poprzez zdefiniowanie dla każdego z nich typu rejestrowanych zdarzeń (powodzenie lub niepowodzenie).

Jeśli wybrane zostały zdarzenia *File and Object Access* (Dostęp do plików i obiektów), właściwości zabezpieczeń każdego obiektu muszą zostać skonfigurowane tak, aby rejestrowały w dzienniku zabezpieczeń zdarzenia inspekcji.

Komputery systemu Windows Server 2003 będące kontrolerami domeny zawierają dwa dodatkowe dzienniki:

- **Directory Service (Usługa katalogowa)** Dziennik ten zawiera zdarzenia dotyczące usługi katalogowej Microsoft Active Directory, takie jak niezgodności replikacji obiektów lub istotne zdarzenia katalogu.

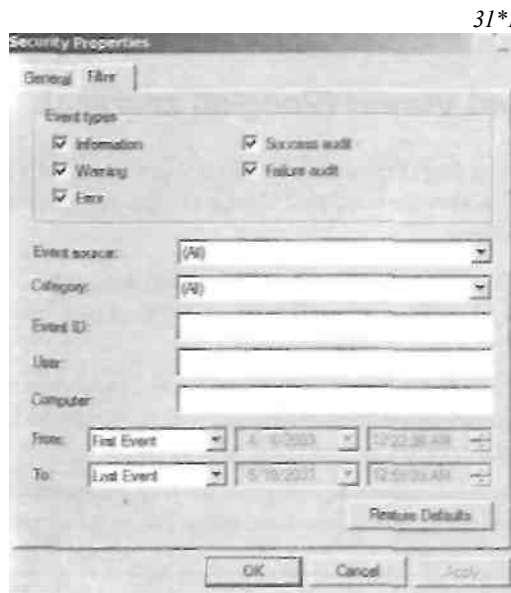
- **File Replication Service (Usługa replikacji plików)** Dziennik ten zawiera błędy i ważne zdarzenia odnotowane przez usługę *File Replication Service* (Usługa replikacji plików) związane z kopiowaniem informacji pomiędzy kontrolerami domeny w trakcie cyklu replikacji.

Z kolei komputer systemu Windows Server 2003 pełniący rolę serwera DNS (Domain Name System) będzie zawierał jeszcze jeden dziennik:

- **DNS Server (Serwer DNS)** Dziennik ten zawiera błędy lub ważne zdarzenia odnotowane przez serwer DNS.

Konfigurowanie dzienników programu Event Viewer

Podczas pierwszego uruchomienia programu *Event Viewer* (Podgląd zdarzeń), wyświetlane są wszystkie zdarzenia zarejestrowane w wybranym dzienniku. Lista taka może być długa i może zawierać wiele informacji lub ostrzeżeń. Zdarzenia można wyszukiwać według typu, przy użyciu polecenia **Filter** (Filtr) znajdującego się w menu **View** (Widok) przeglądane dziennika. Widok strony właściwości filtra dla dziennika *Security* (Zabezpieczenia) został pokazany na rysunku 12-1.



Rysunek 12-1 Ustawienia filtra dla dziennika *Security* (Zabezpieczenia)

W oknie właściwości dziennika, obok zakładki *Filter* (Filtr) znajduje się zakładka *General* (Ogólne), która umożliwia określanie następujących parametrów działania dziennika:

- Nazwa wyświetlana dziennika.
- Maksymalny rozmiar dziennika.
- Czy najstarsze zdarzenia zaprotokołowane w dzienniku mają być zastępowane, jeśli osiągnięty zostanie maksymalny rozmiar dziennika. Dostępne są trzy opcje:
 - » **Overwrite Events As Needed (default) (Zastąp zdarzenie w razie potrzeby)** Wybranie tej opcji spowoduje, że najstarsze zdarzenia zaprotokołowane w dzienniku będą zastępowane przez nowe, gdy zostanie osiągnięty maksymalny rozmiar dziennika.

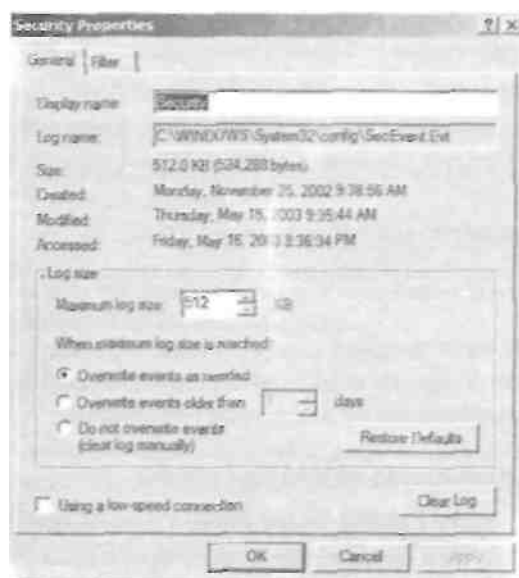
- » **Overwrite Events Older Than n Days (Zastąp zdarzenia starsze niż n dni)** Gdy osiągnięty zostanie maksymalny rozmiar dziennika, konfiguracja ta powoduje zastąpienie zdarzeń starszych niż wiek określony przez tę opcję.
- » **Do Not Overwrite Events (Clear Log Manually) [Nie zastępuj zdarzeń (Ręczne czyszczenie dziennika)]** Gdy osiągnięty zostanie maksymalny rozmiar dziennika, opcja ta powoduje zachowanie wcześniej zarejestrowanych zdarzeń.



Alert bezpieczeństwa Jeśli dziennik Security (Zabezpieczenia) nie jest często sprawdzany, to pozostawienie w nim opcji domyślnych ustawień *Overwrite Events As Needed* (Zastąp zdarzenia w razie potrzeby) może spowodować zastąpienie istotnych informacji dotyczących dostępu do zasobów lub innych danych związanych z zabezpieczeniami. Zalecany jest regularny harmonogram analiz dziennika. Jeśli zachodzi potrzeba zachowania niektórych rekordów lub ze względu na inne zadania administracyjne, pliki dziennika można archiwizować (to znaczy zapisywać na dysk).

Dla lepszego zabezpieczenia przed utratą wpisów dziennika *Security* (Zabezpieczenia) zasada grupy systemu Windows Server 2003 udostępnia ustawienie umieszczone w *Computer Configuration Policy/ Security Settings* (Zasada konfiguracji komputera/Ustawienia zabezpieczeń), które wymusza wyłączenie komputera, jeśli system nie mógł zapisać informacji inspekcji do dziennika *Security*. W praktyce ustawienie takie dyscyplinuje administratora, jeśli ustawienia dziennika *Security* określają jego ręczne czyszczenie.

Na rysunku 12-2 została pokazana zakładka *General* (Ogólne) dziennika *Security*.



Rysunek 12-2 Ustawienia na zakładce *General* (Ogólne) dziennika *Security* (Zabezpieczenia)

Zadanie kontrolne: Monitor zdarzeń

W zadaniu tym zostanie przeprowadzona konfiguracja dziennika *Security* (Zabezpieczenia) dla inspekcji *File and Object Access* (Dostęp do plików i obiektów) oraz zostanie pokazane działanie filtru wyświetlania danych tego dzienniku.

Ćwiczenie 1: Konfigurowanie dziennika Security (Zabezpieczenia)

W ćwiczeniu tym konfigurowana będzie inspekcja *File and Object Access* (Dostęp do plików i obiektów).

1. Zaloguj się jako administrator serwera Server01 i otwórz przystawkę **Active Directory Users And Computers** (Użytkownicy i komputery usługi Active Directory).
2. Kliknij prawym przyciskiem myszy jednostkę organizacyjną **Domain Controllers** (Kontrolery domeny), a następnie z menu skrótów wybierz polecenie **Properties** (Właściwości).
3. Na zakładce **Group Policy** (Zasada grupy) wybierz zasadę **Default Domain Controllers Policy**, a następnie kliknij przycisk **Edit** (Edytuj).
4. W węźle **Computer Configuration** (Konfiguracja komputera), rozwiń kolejno **Windows Settings** (Ustawienia systemu Windows), **Security Settings** (Ustawienia zabezpieczeń), **Local Policies** (Zasady lokalne), a następnie kliknij pozycję **Audit Policy** (Zasada inspekcji).
- 5- W oknie szczegółów kliknij prawym przyciskiem myszy opcję **Audit Object Access** (Przeprowadź inspekcję dostępu do obiektów), a następnie z menu skrótów wybierz polecenie **Properties** (Właściwości).
6. W oknie dialogowym *Audit Object Access Properties* (Właściwości: Przeprowadź inspekcję dostępu do obiektów) zaznacz opcje **Audit These Attempts: Failure** (Dokonaj inspekcji tych prób: Niepowodzenie), a następnie kliknij przycisk OK.
- 7- Zamknij program *Group Policy Object Editor* (Edytor obiektów zasady grupy), kliknij przycisk OK, aby zamknąć okno dialogowe *Domain Controllers Properties* (Właściwości: Kontrolery domeny), a następnie zamknij przystawkę *Active Directory Users And Computers* (Użytkownicy i komputery usługi Active Directory).
8. Otwórz okno wiersza poleceń i wpisz **gpupdate**, a następnie naciśnij ENTER.
- 9- Polecenie spowoduje odświeżenie zasad komputera (Computer Policy); po zakończeniu odświeżania zamknij okno wiersza poleceń.

Dzięki powyższej procedurze na serwerze Server01 (będącym częścią jednostki organizacyjnej Domain Controllers), włączona została inspekcja prób dostępu do obiektu zakończonych niepowodzeniem oraz odświeżona została zasada grupy tak, aby ustawienia zostały zastosowane bezzwłocznie.

Ćwiczenie 2: Określanie inspekcji dostępu do obiektów i plików

W ćwiczeniu tym konfigurowana będzie inspekcja foldera, który zostanie utworzony. Uprawnienia zostaną określone tak, aby zasymulować próbę nieautoryzowanego dostępu użytkownika do zasobu,

1. Na pulpicie swojego komputera utwórz/ folder **Data**.
2. Kliknij prawym przyciskiem myszy ten folder i z menu skrótów wybierz polecenie **Properties** (Właściwości).
3. Wybierz zakładkę **Security** (Zabezpieczenia), a następnie zaznacz konto użytkownika.

4. Dla tego konta użytkownika zaznacz pole wyboru oznaczające uprawnienia **Deny: Full Control** (Odmów: Pełna kontrola) i kliknij przycisk **Yes** (Tak) w oknie dialogowym ostrzeżenia.
- 5- Kliknij przycisk **Advanced** (Zaawansowane) i wybierz zakładkę **Auditing** (Inspekcja). Dodaj skonfigurowane wcześniej konto użytkownika do listy inspekcji **List Folder/Read Data: Failed** (Niepowodzenie: Wyświetlanie zawartości foldera/Odczyt danych), a następnie kliknij przycisk OK, aby zamknąć okna dialogowe *Properties*.
6. Dwukrotnie kliknij folder **Data**, aby go otworzyć. Powinien zostać wyświetlony komunikat ostrzeżenia o odmowie dostępu.

Ćwiczenie 3: Odczyt dziennika Security (Zabezpieczenia)

W ćwiczeniu tym sprawdzane będą wpisy inspekcji zakończonych niepowodzeniem prób dostępu do foldera Data.

1. W grupie programów **Administrative Tools** (Narzędzia administracyjne) otwórz konsolę **Computer Management** (Zarządzanie komputerem).
 2. Rozwiń węzeł **Event Viewer** (Podgląd zdarzeń), a następnie w oknie szczegółów kliknij dziennik **Security** (Zabezpieczenia).

Na początku listy zdarzeń powinno być widocznych kilka zdarzeń dotyczących inspekcji niepowodzeń **Failure Audit** (o identyfikatorze 560), które są związane z nieudanymi próbami dostępu do foldera Data.
 3. W oknie szczegółów kliknij prawym przyciskiem myszy dziennik **Security** (Zabezpieczenia), w menu skrótów wybierz polecenie **View** (Widok), a następnie kliknij opcję **Filter** (Filtruj).
 4. W oknie dialogowym *Filter* (Filtr) zaznacz następujące opcje:
 - » **Event Source** (Źródło zdarzenia): **Security** (Zabezpieczenia)
 - » **Category** (Kategoria): **Object Access** (Dostęp do obiektu)
 - » **Event Types** (Typy zdarzeń): zaznaczona opcja **Failure** (Niepowodzenie), pozostałe typy zdarzeń niezaznaczone
 - 5- Kliknij przycisk OK, aby filtr został zastosowany do dziennika *Security*.
- Obecnie w dzienniku *Security* (Zabezpieczenia) wyświetlane będą jedynie zdarzenia związane z nieudanymi próbami dostępu do obiektu.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Które dzienniki będą wyświetlane w programie *Event Viewer* (Podgląd zdarzeń) dla kontrolera domeny, na którym uruchomiony jest system DNS (przy założeniu, że obowiązują ustawienia domyślne)?

Administrator skonfigurował system Windows Server 2003 tak, aby przeprowadzana była inspekcja wszystkich nieudanych prób dostępu do obiektu, a inspekcja dla wszystkich plików i folderów określona została przez opcję List Folder/Read Data Failure (Niepowodzenie: Wyświetlanie zawartości foldera/Odczyt danych). Wszystkie inne ustawienia programu Event Viewer (Podgląd zdarzeń) oraz dziennika Security (Zabezpieczenia) są zgodne z ustawieniami domyślnymi. Co stanie się, jeśli plik wpisów dziennika Security (Zabezpieczenia) osiągnie 512 KB?

3. Jakie ustawienia należy skonfigurować na serwerze, aby dane dziennika *Security* (Zabezpieczenia) nie były zastępowane oraz aby w żadnym momencie system Windows Server 2003 nie zatrzymał obsługi sieci?

Podsumowanie lekcji

Program *Event Viewer* (Podgląd zdarzeń) systemu Windows Server 2003 zawiera szereg dzienników, które podczas operacji systemu rejestrują błędy oraz ważne zdarzenia. Dziennik System zawiera dane dotyczące usług i innych wewnętrznych funkcji systemu operacyjnego. Dziennik *Application* (Aplikacja) zawiera dane, które zostały zapisane przez programy. Dziennik *Security* (Zabezpieczenia) zawiera dane inspekcji zdarzeń związanych z powodzeniem lub niepowodzeniem operacji. Inaczej niż dla innych dzienników, dziennik *Security* jest konfigurowany przez administratora, który określa, jakie dane będą rejestrowane w dzienniku. Komputer będący kontrolerem domeny jest wyposażony w dodatkowe dzienniki: *Replication Services* (Usługi replikacji) oraz *Active Directory* (Usługa Active Directory). Serwery DNS mają jeszcze jeden odrębny dziennik - DNS.

Złożone i długie dzienniki mogą być filtrowane przy użyciu różnych kryteriów, wliczając w to zarejestrowane dane i typ danych, dzięki czemu odczyt informacji staje się prostszy. Dane dzienników mogą być przechowywane w plikach następujących typów:

- Plik Performance Monitor Binary (*.blg). Są to pliki służące do ciągłego zapisywania bez możliwości lub z możliwością zastępowania danych.
- Plik tekstowy (*.txt lub *.csv)
- Baza danych SQL

Po skonfigurowaniu ustawień dziennika, ustawienia programu *Performance Monitor* (Monitor wydajności) mogą zostać zapisane (poprzez wybranie w menu kontekstowym dziennika polecenia *Save Settings As* (Zapisz ustawienia jako)) jako plik HTML (Hypertext Markup Language). Plik taki może być później wykorzystywany przy użyciu opcji *New Log Settings From* (Ustawienia nowego dziennika z).

Dla wszystkich dzienników programu *Event Viewer* (Podgląd zdarzeń) można określać odrębne ustawienia maksymalnych rozmiarów pliku dziennika oraz odrębne działanie, jeśli maksymalny rozmiar pliku zostanie osiągnięty. Zachowanie po osiągnięciu maksymalnego rozmiaru dziennika określają trzy opcje: bezzwłoczne zastępowanie starszych danych, zastępowanie tylko tych wpisów, które mają określony wiek lub wymuszanie ręcznego czyszczenia dziennika i nie zastępowanie żadnych informacji. W konfiguracjach powiązanych może zostać włączona zasada grupy wymuszająca wyłączenie komputera, który nie potrafi zapisać do dziennika *Security* (Zabezpieczenia) informacji inspekcji.

Lekcja 2: Wykorzystywanie programu Performance Console (Wydajność)

Korzystając z programu *Performance Console* (Wydajność), użytkownik może mierzyć aktywność dowolnego komputera sieci. Przystawki *System Monitor* (Monitor systemu) oraz *Performance Logs And Alerts* (Dzienniki wydajności i alerty) zostały wbudowane jako część konsoli Performance (Wydajność) - *perfmon.msc*. Przystawka *System Monitor* umożliwia przeglądanie w czasie rzeczywistym gromadzonych przez liczniki danych o wydajności. Konfiguracja dzienników może być zmieniana. Przystawka *Performance Logs And Alerts* umożliwia rejestrowanie danych wydajności (dzienniki) oraz pozwala określać działania w sytuacji, kiedy progi liczników zostają przekroczone (alerty). Konsola *Performance* (Wydajność) umożliwia wykonywanie rozmaitych zadań, wliczając w to następujące:

- Gromadzenie i przeglądanie w czasie rzeczywistym danych o wydajności
- Przeglądanie zebranych w dzienniku informacji
- Przedstawianie danych w postaci wykresów, histogramów lub raportów
- Tworzenie stron HTML na podstawie widoków poprzez importowanie ustawień plików dziennika
- Zapis monitorowanych konfiguracji, które mogą być następnie w programie *System Monitor* (Monitor systemu) uruchamiane na innych komputerach

Materiały omówione podczas lekcji pozwalają na

- Monitorowanie w czasie rzeczywistym danych dotyczących wydajności
- Zapisywanie danych o wydajności w pliku dziennika
- Konfigurowanie alertów danych dotyczących wydajności systemu

Szacunkowy czas lekcji: 20 minut

Konfigurowanie programu System Monitor (Monitor systemu)

Wykorzystując program *System Monitor* użytkownik może gromadzić i przeglądać dane. W tym celu należy skonfigurować liczniki, które tworzą raporty dotyczące aktywności urządzeń sprzętu, aplikacji oraz usług dowolnego komputera sieci. Aby dane były gromadzone, użytkownik musi określić trzy rodzaje ustawień.

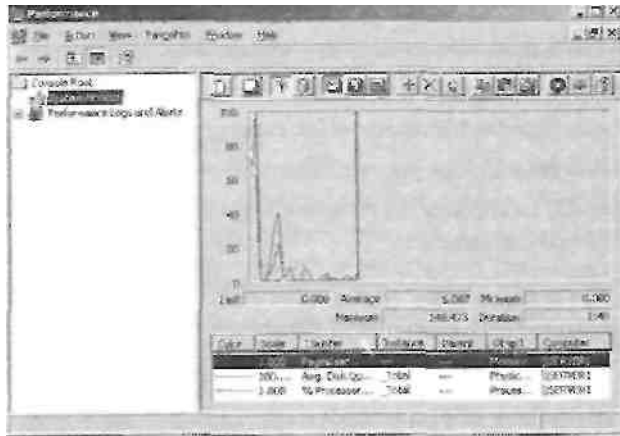
- **Typ danych** Należy określić jedną lub kilka instancji obiektów monitorowania wydajności, których dane mają być odnotowywane.
- **Źródło danych** Licznik może zbierać informacje o komputerze lokalnym lub zdalnym. Aby gromadzić dane, użytkownik musi być administratorem lub członkiem grupy Performance Log Users (Użytkownicy dzienników wydajności) wybranego komputera.
- **Parametry próbkowania** Dane mogą być rejestrowane ręcznie w czasie rzeczywistym lub użytkownik może określić okres zapisu danych.

Przeglądanie danych

Pierwsze uruchomienie programu *System Monitor* uruchamia trzy liczniki, które rozpoczynają odnotowywanie danych w czasie rzeczywistym:

- Memory: Pages/Second (Pamięć: Strony/s)
- Physical Disk(_Total): Average Disk Queue Length (Dysk fizyczny: Średnia długość kolejki dysku)
- Processor(_Total): % Processor Time (Procesor: Czas procesora%)

Rysunek 12-3 przedstawia widok programu System Monitor (Monitor systemu), w którym uruchomione zostały liczniki domyślne.

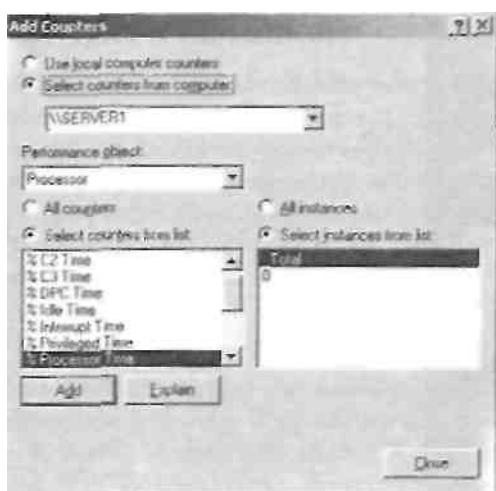


Rysunek 12-3 Program System Monitor konsoli Performance (Wydajność)

Liczniki mogą być dodawane lub usuwane poprzez naciśnięcie na pasku narzędzi ikony **Add** (Dodaj) (CTRL+I) lub poprzez kliknięcie prawym przyciskiem myszy dowolnego miejsca okna i wybranie z menu skrótów polecenia **Add Counters** (Dodaj liczniki). W oknie dialogowym *Add Counters* (Dodawanie liczników) dla komputera lokalnego lub dowolnego komputera zdalnego sieci, użytkownik może wybrać każdy dostępny licznik. Liczniki są dostępne i pogrupowane według typu obiektu, kategorii obiektu oraz instancji licznika.

- **Obiekt** Logiczny zbiór liczników zasobu, usługi lub aplikacji.
- **Licznik** Element odnotowujący dane. Rodzaj rejestrowanych danych zależy od typu licznika.
- **Instancja** Odnosi się do jednego lub wielokrotnego wystąpienia licznika indeksowana liczbą dostępnych wystąpień w danym komputerze. Na przykład dla komputera z dwoma procesorami „instancja 0” będzie dotyczyła pierwszego procesora, „instancja 1” drugiego, a parametr „Total” dotyczy sumarycznych danych obu instancji. W przypadku występowania pojedynczej instancji licznika dostępne są tylko wystąpienia „0” oraz „Total”.

Na rysunku 12-4 został przedstawiony licznik %Processor Time (Czas procesora %) dla komputera Server01, w którym zainstalowany został pojedynczy procesor.



Rysunek 12-4 Licznik %Processor Time (Czas procesora %) — pojedynczy procesor



Wskazówka egzaminacyjna Warto zapamiętać, że wystąpienie „JTotal” przedstawia łączne dane pochodzące z kilku instancji licznika, jeśli w komputerze dostępnych jest kilka instancji.

Alerty i protokolowanie

Program *Performance Logs And Alerts* (Dzienniki wydajności i alerty) umożliwia automatyczne gromadzenie danych o wydajności komputerów lokalnych lub zdalnych. Dane -zarejestrowane przez dziennik można przeglądać za pomocą programu *System Monitor* lub dane te mogą zostać wyeksportowane do arkusza kalkulacyjnego lub bazy danych, aby za ich pomocą opracowywać raporty i analizy. Poniżej wymienione zostały opcje, za pomocą których można konfigurować dostępne liczniki programu *System Monitor* wykorzystywane następnie w narzędziu *Performance Logs And Alerts*:

- Gromadzenie danych w formacie CSV lub rozdzielanym znakami tabulacji w celu wyeksportowania danych.
- Przeglądanie danych dziennika liczników (*Counter Log*) podczas rejestrowania oraz po zgromadzeniu danych.
- Określanie ustawień dla dzienników *Trace Logs* (Dzienniki śledzenia) w oparciu o dostępnych dostawców.
- Definiowanie parametrów plików dziennika, wliczając w to czas rozpoczęcia i zakończenia rejestrowania oraz maksymalny rozmiar pliku.
- Definiowanie alertu dziennika, który powoduje, że po przekroczeniu wartości progowej dziennika będzie wysłany komunikat, uruchomiony program lub uruchomiony dziennik.

Na rysunku 12-5 przedstawione zostało okno dialogowe konfiguracji alertu dla komputera Server01 w przypadku, kiedy wartość parametru *Free Disk Space* (Wolna przestrzeń dysku) spadnie poniżej 20%.



Rysunek 12-5 Konfiguracja alertu dla parametru Disk Free Space (Wolna przestrzeń dysku)



W praktyce Monitorowanie danych wydajności

Aby podczas monitorowania serwera lub sieci określić, gdzie występuje wąskie gardło, należy sprawdzać wydajność uruchamiając najpierw konfigurację o szerszym zakresie poprzez obserwację takich liczników jak *% Processor Time* (Czas procesora %), *Disk and Processor Queue Length* (Długość kolejki procesora i dysku), *Memory Use* (Wykorzystanie pamięci) oraz *Network I/O* (Interfejs sieciowy). Po określeniu obszaru występowania problemu, można przyjrzeć się poszczególnym usługom i aplikacjom, które korzystają z tego zasobu oraz w razie potrzeby przyjrzeć się poziomom protokołu i wątku. Najczęściej przyczyną problemu jest pojedyncze urządzenie bądź pojedyncza aplikacja lub ogólny brak zasobów w systemie. Pojedyncze urządzenia mogą zostać ponownie skonfigurowane lub zastąpione, a zasoby globalne mogą zostać powiększone (dodanie pamięci, szybszy procesor i tak dalej).

Jednakże rezultaty takiego monitorowania mogą być niejasne, jeśli nie dysponujemy materiałem porównawczym wydajności systemu. Dlatego po skonfigurowaniu nowego komputera, zalecaną praktyką jest możliwie szybkie przeprowadzenie monitorowania aktywności ważnych obiektów takich jak Processor (Procesor), Memory (Pamięć), Network (Sieć) oraz Process (Application and Services) (Procesy (aplikacja i usługi)), aby określić wydajność komputera w zwykłych warunkach. Ten *punkt odniesienia* powinien dotyczyć trzech stanów — normalny, bezczynność oraz szczyt wydajności. Występujące później problemy lub wąskie gardła będzie łatwiej wyszukać oraz łatwiej będzie znaleźć rozwiązanie problemu.

Wybór obiektów i liczników

Wybór liczników obiektu, dokonywamy w celu monitorowania serwera dla sprawdzenia wydajności odniesienia bądź wydajności bieżącej, może być przeprowadzany w dwojaki sposób. Jedną metodą monitorowania serwera sprawdza rolę, jaką spełnia serwer w środowisku oraz związane z nią zapytania przesyłane do serwera przez użytkowników. Innym podejściem monitorowania serwera jest sprawdzanie kategorii obiektów liczników takich jak *Processor* (Procesor), *Memory* (Pamięć), *Network Interface* (Interfejs sieciowy) oraz *PhysicalDisk* (Dysk fizyczny) przy zwracaniu mniejszej uwagi na pełnioną przez serwer rolę, a w zamian skupienie się na spójnych standardach monitorowania.

Role serwera

Monitorowanie serwera pod kątem roli jest przydatne, jeśli serwery spełniają w środowisku sieci pojedynczą rolę. Role te są definiowane poprzez usługi lub zasoby udostępniane użytkownikom przez serwer. Przykładami takich ról mogą być kontrolery domeny, serwery plików czy serwery sieci Web. Żądania serwera dotyczące zasobów mogą być porównywane (podczas monitorowania wydajności) z licznikami odpowiednich obiektów, które mierzą zasoby intensywnie wykorzystywane przez serwer danej roli. Dane bieżące dotyczące monitorowanej wydajności mogą być porównywane z danymi odniesienia i na tej podstawie można optymalizować serwer danej roli. Tabela 12-1 wymienia obiekty, które są najczęściej wykorzystywane podczas analizowania serwera w kontekście pełnionej przez niego roli.

Tabela 12-1. Role serwera oraz obiekty przeznaczone do monitorowania

Rola serwera	Używane zasoby	Obiekty i liczniki
Serwer aplikacji	Pamięć, sieć, pamięć podręczna procesora	Pamięć, Procesor, Interfejs sieciowy oraz System
Serwer kopii zapasowych Serwer baz danych	Procesor i sieć	System, Serwer, Procesor oraz Interfejs sieciowy
Kontroler domeny	Dyski, sieć i procesor	Dysk fizyczny. Dysk logiczny, Procesor, Interfejs sieciowy oraz System
Serwer plików i drukarek Serwer poczty	Pamięć, dysk i komponenty sieciowe	Pamięć, Procesor, System, Interfejs sieciowy, obiekty protokołów (zależne od sieci, ale mogą zawierać protokoły TCPv4, UDPv4, ICMP, IPv4, NBT Connection, NWLink IPX, NWLink NetBIOS oraz NWLink SPX), Dysk fizyczny i Dysk logiczny
Serwer sieci Web	Procesor, dysk, sieć i pamięć	Pamięć, Interfejs sieciowy, Dysk fizyczny, Dysk logiczny oraz Kolejka drukowania
	Dysk, bufor i komponenty sieciowe	Pamięć, Bufor, Procesor, System, Dysk fizyczny, Interfejs sieciowy oraz Dysk logiczny
		Bufor, Interfejs sieciowy, Dysk fizyczny oraz Dysk logiczny

Dla każdej roli serwera, przy użyciu odpowiednich liczników należy utworzyć wzorzec odniesienia dla danej roli, a następnie okresowo sprawdzać, czy nie nastąpiły istotne zmiany wartości liczników.

Kategorie obiektów

W środowisku sieci, w którym serwer pełni wiele ról, monitorowanie oparte na roli serwera może nie wychwycić istotnych informacji. W takim przypadku bardziej pełne dane powinny być gromadzone w oparciu o każdą kategorię obiektu podstawowego.

Licznik pamięci

Po utworzeniu wzorca odniesienia określającego wykorzystanie pamięci, powinno być przeprowadzane okresowe monitorowanie, które wykaże odchyłki od wzorca. Poniżej wymienione zostały liczniki, które są przydatne podczas monitorowania pamięci systemu komputerowego:

- **Niedobór pamięci:** **Memory (Pamięć)\Available Bytes (Dostępne bajty), Available Kbytes (Dostępna pamięć kB) lub Available MBytes (Dostępna pamięć MB)** - pamięć wyrażana w megabajtach; **Process (All processes) [Proces]\Working Set {Zestaw roboczy}; Memory (Pamięć)\Pages/sec (Strony/s); Memory (Pamięć)\Cache Bytes (Bajty pamięci podręcznej).** Liczniki te pokazują ile pamięci zajmują wszystkie procesy oraz ile pamięci pozostaje dostępnej.
- **Częste sprzętowe błędy stron:** **Memory (Pamięć)\Pages/sec (Strony/s); Process (All processes) [Proces]\Working Set (Zestaw roboczy); Memory (Pamięć)\Pages Input/sec (Strony wchodzące/s); Memory (Pamięć)\Pages Output/sec (Strony wychodzące/s).** Sprzętowe błędy stron występują, jeśli potrzebna strona pamięci została umieszczona w pamięci wirtualnej. Nadmierna wymiana (swapping) zmniejsza wydajność komputera, a rozwiązaniem problemu jest zmniejszenie liczby żądań lub zwiększenie wielkości pamięci fizycznej.

Liczniki sieci

Liczniki sieci odnotowują dane dotyczące zainstalowanych w komputerze kart sieciowych (NIC) oraz segmentów, z którymi karty te komunikują się. Poniżej wymienione zostały liczniki, które są przydatne podczas monitorowania wydajności komputera w sieci:

- **Network Interface (Interfejs sieciowy)\Output Queue Length (Długość kolejki wyjściowej); Bytes Total/sec (Całkowita liczba bajtów/s).** Wartość określająca długość kolejki powinna być nieduża, natomiast wysoka powinna być wartość określająca całkowitą liczbę bajtów, co oznacza, że karta sieciowa przesyła pakiety szybko i bez opóźnień.
- **Network Interface (Interfejs sieciowy): Bytes Sent/Sec (Bajty wysłane/s); Current Bandwidth (Bieżąca przepustowość); Bytes Received/Sec (Bajty odebrane/s).** Stała lub okresowa wysoka wartość tych liczników wskazuje, że ruch w sieci przekracza wartości optymalne. Podział sieci na segmenty lub zwiększenie jej przepustowości będzie zmniejszać szansę na występowanie wąskich gardeł podczas intensywnego ruchu.



Informacja Różne typy konfiguracji sieci udostępniają odmienne poziomy wydajności sieci. Przykładowo, podczas monitorowania licznika %Network Utilization (Wykorzystanie sieci%), jego wartość 30% określa maksimum zalecane dla sieci Ethernet, w której nie są używane przełączniki (tylko koncentratory). Oznacza to, że 10-megabitowa sieć Ethernet stanie się wąskim gardłem, jeśli przepustowość przekroczy 3 MB/s. Jeśli wartość licznika przekracza 40%, kolizje w sieci zaczynają obniżać jej wydajność.

Liczniki procesu

Żądanie zasobu systemu związane jest często z procesem, który wywołał to żądanie. Przy użyciu liczników procesu można przeglądać poszczególne procesy (wliczając w to usługi systemowe), które wykorzystują zasoby systemu. Poniżej wymienione zostały ważne liczniki używane podczas zbierania danych wydajności dotyczących procesów:

- **Wycieki pamięci; aplikacje intensywnie wykorzystujące pamięć:** **Memory (Pamięć)\Pool Nonpaged Allocs** (Przydziały w puli niestronicowanej); **Memory\Pool Nonpaged Bytes** (Bajty w puli niestronicowanej); **Memory\Pool Paged Bytes** (Bajty w puli stronicowanej); **Process(process_name)[Proces (nazwa_procesu)]\Pool Nonpaged Bytes** (Bajty w puli niestronicowanej); **Process(process_name)\Handle Count** (Licznik dojsć); **Process(process_name)\Pool Paged Bytes** (Bajty w puli stronicowanej); **Process(process_name)Wirtual Bytes** (Bajty wirtualne); **Process(process_name)\Private Bytes** (Bajty prywatne). Liczniki te pokazują wykorzystanie pamięci przez poszczególne procesy, co umożliwia przeniesienie na inne komputery aplikacji, które silnie obciążają pamięć (lub izolowanie tych aplikacji w celu przeciwdziałaniu wyciekom pamięci).



Informacja Wyciek pamięci aplikacji można wykryć uruchamiając aplikację na serwerze testowym, a następnie monitorując wykorzystanie pamięci, które zwiększa się wraz z upływem czasu bez zmian w zakresie liczby żądań usług. Taki nieuzasadniony wzrost wykorzystania pamięci świadczy o jej wycieku.

Liczniki dysku

Liczniki obiektu *PhysicalDisk* (Dysk fizyczny) udostępniają dane dotyczące aktywności każdego urządzenia pamięci dyskowej, natomiast liczniki obiektu *LogicalDisk* (Dysk logiczny) zawierają informacje o zdefiniowanych w systemie woluminach (C:\, D:\ itd). Monitorowanie liczników wolnej przestrzeni obiektu *LogicalDisk* (Dysk logiczny) oraz wydajności obiektu *PhysicalDisk* (Dysk fizyczny) dostarcza przydatne informacje. Poniżej wymienione zostały istotne liczniki używane do monitorowania obiektu dysku fizycznego i logicznego:

- **LogicalDisk (Dysk logiczny)\% Free Space (Wolne miejsce %)**. Licznik ten odnotowuje procentowy udział nieprzydzielonej pamięci dyskowej w stosunku do całkowitej przestrzeni użytkowej wolumenu logicznego. Licznik nie jest dostępny dla dysków fizycznych.



Informacja Podczas obliczania instancji *_Total*, liczniki *%Free Space (Wolne miejsce %)* ponownie przeliczają sumy wyrażając je jako procent w odniesieniu do każdego dysku.

- **PhysicalDisk (Dysk fizyczny)\Avg. Disk Bytes/Transfer** (Średnia liczba bajtów dysku/ Transfer); **\Avg. Disk sec/Transfer** (Średni czas dysku/Transfer; **\Avg. Disk Queue Length** (Średnia długość kolejki dysku; **\% Disk Time** (Czas dysku %). Liczniki te mierzą w czasie wielkość operacji wejściowych i wyjściowych oraz stopień zajętości dysku podczas wykonywania żądań. Dysk jest wydajny, jeśli przesyła dużą liczbę danych w relatywnie krótkim czasie, a dla każdego napędu wartość określająca długość kolejki jest mniejsza od 2.

Zadanie kontrolne: Wykorzystanie programu Performance Console

W zadaniu tym rejestrowane będą dane o wydajności, przeprowadzona zostanie ich analiza w programie *System Monitor* (Monitor systemu) oraz dane te zostaną wyeksportowane do arkusza kalkulacyjnego programu Excel.

Ćwiczenie 1: Rejestrowanie danych wydajności

W ćwiczeniu tym utworzony zostanie plik dziennika zawierający dane o obiektach *LogicalDisk* (Dysk logiczny), *PhysicalDisk* (Dysk fizyczny) oraz *Server Work Queue* (Kolejka robocza serwera).

1. Zaloguj się jako administrator w komputerze Server01 i uruchom konsolę **Performance** (Wydajność).
2. W oknie folderów rozwiń węzeł **Performance Logs And Alerts** (Dzienniki wydajności i alerty), a następnie zaznacz pozycję **Counter Logs** (Dzienniki liczników).
3. W oknie szczegółów kliknij prawym przyciskiem myszy i z menu skrótów wybierz polecenie **New Log Settings** (Ustawienia nowego dziennika).
4. Utwórz plik dziennika o nazwie **Test** i dodaj do niego obiekty **LogicalDisk** (Dysk logiczny), **PhysicalDisk** (Dysk fizyczny) oraz **Server Work Queue** (Kolejki robocze serwera). Dla okresu próbkowania należy przyjąć wartość 8 sekund. Zanotuj nazwę pliku i jego lokalizację, a następnie, aby uruchomić dziennik, kliknij przycisk OK.
5. W okresie kiedy działa rejestrowanie, przy użyciu innych aplikacji wykonaj pewne czynności na komputerze. Po około 30 sekundach przerwij rejestrowanie danych (w programie Dzienniki wydajności i alerty).
6. W programie *System Monitor* (Monitor systemu) kliknij przycisk **View Log Data** (Wyświetl dane dziennika) i otwórz plik dziennika utworzonego podczas testu. Funkcję Wyświetl dane dziennika można również uruchomić naciskając CTRL+L.

Wykres wyświetlony w programie *System Monitor* ilustruje dane zarejestrowane w trakcie sesji dziennika. Dane mogą być prezentowane za pomocą trzech rodzajów widoku — wykres, histogram oraz raport. Utworzony plik dziennika posiada format domyślny (plik binarny), wykorzystywany tylko w programie *Performance* (Wydajność).

Ćwiczenie 2: Importowanie zaprotokołowanych informacji

W ćwiczeniu tym dane zarejestrowane w ćwiczeniu 1 będą zapisywane w formacie umożliwiającym import do programu Microsoft Excel.

1. Jeśli konieczne, ponownie uruchom konsolę **Performance** (Wydajność).
2. Kliknij prawym przyciskiem myszy plik dziennika Test i wybierz polecenie **Properties** (Właściwości).
3. W oknie dialogowym *Properties* (Właściwości) dla pliku Test kliknij zakładkę **Log Files** (Pliki dziennika), a następnie zmień typ pliku dziennika z **Binary File** (Plik binarny) na **Text File (Comma Delimited)** (Plik tekstowy rozdzielany przecinkami).
4. Kliknij przycisk OK, a następnie rozpocznij rejestrowanie w pliku dziennika. Wykonaj przez około pół minuty pewne zadania związane z działaniem dysku, a następnie zatrzymaj rejestrowanie danych.

Utworzony plik dziennika ma format CSV i może być otwierany, przeglądany bądź analizowany za pomocą programu Excel.



Informacja Aby plik CSV mógł być otwarty za pomocą programu Excel, narzędzie *Performance Logs And Alerts* (Dzienniki wydajności i alerty) nie może być uruchomione, ponieważ Excel podczas otwierania pliku wymaga wyłącznego dostępu.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Zadaniem administratora jest monitorowanie wszystkich serwerów platformy Windows Server 2003 tak, aby defragmentacja przeprowadzana była na tych komputerach regularnie i możliwie wydajnie. Wykorzystywany program do prawidłowego przeprowadzenia defragmentacji dysku wymaga 20% wolnego miejsca na każdym wolumenie. W jaki sposób administrator powinien wykonać to zadanie?

2. Ze względu na słabą wydajność sieci monitorowane są systemy Windows Server 2003- Poniżej przedstawione zostały wyniki monitorowani komputerów:

» Processor: % Processor Time:	High
» Physical Disk: % Disk Time:	Low
» Memory: Pages/sec:	Low
» Processor: Interrupts/sec:	High
» Process: % Processor Time (for non-service processes):	Low
» Process: % Processor Time (for system processes):	Low

 Jakie jest najbardziej prawdopodobne wyjaśnienie problemu?

- 3- Serwer używany do monitorowania innych serwerów sieci jest zbyt przeciążony, należy więc zmniejszyć zakres zadań związanych z monitorowaniem. Co należy zrobić, aby uzyskać największy wpływ w odniesieniu do monitorowanej wydajności komputera przy założeniu, że rejestrowana jest możliwie największa ilość danych?

Podsumowanie lekcji

Konsola *Performance* (Wydajność) pozwala konfigurować dwie przystawki: *System Monitor* (Monitor systemu) oraz *Performance Logs And Alerts* (Dzienniki wydajności i alerty). Program *System Monitor* został zaprojektowany w celu rejestrowania danych czasu rzeczywistego prezentowanych na konsoli interfejsu programu. Dane mogą być wyświetlane w postaci wykresu, histogramu lub raportu. Przystawka *Performance Logs And Alerts* umożliwia zapis danych do pliku dziennika oraz odnotowuje wartości liczników po przekroczeniu wartości progowych (alerty). Dzienniki utworzone przez przystawkę *Performance Logs And Alerts* mogą być pobierane przez program *System Monitor* i poddawane analizie, jak również mogą być wyeksportowane w różnych formatach plików, takich jak *CSV* czy *HTML*, celem późniejszych analiz.

Lekcja 3: Wykorzystywanie programu Task Manager (Menedżer zadań)

Program *Task Manager* (Menedżer zadań) udostępnia informacje o programach i procesach uruchomionych na komputerze. W programie wyświetlanych jest także kilka charakterystycznych dla procesu liczników wydajności.

Materiały omówione podczas lekcji pozwalają na

- Konfigurowanie programu Task Manager w celu wyświetlenia danych o wydajności
- Wykorzystywanie programu Task Manager do uruchamiania i zatrzymywania aplikacji i procesów

Szacunkowy czas lekcji: 15 minut

Omówienie programu Task Manager

Program *Task Manager* (Menedżer zadań) można uruchomić poprzez kliknięcie prawym przyciskiem myszy obszaru paska narzędzi, a następnie wybranie polecenia **Task Manager** (Menedżer zadań) lub poprzez naciśnięcie CTRL+ALT+DEL, a następnie naciśnięcie przycisku **Task Manager** (Menedżer zadań). Domyślnie w systemie Windows Server 2003 interfejs programu *Task Manager* wyświetla pięć zakładek, na których prezentowane są następujące kategorie danych: aplikacje, procesy, wydajność, sieć oraz użytkownicy.

Zakładka Applications (Aplikacje)

Na zakładce *Applications* (Aplikacje) prezentowany jest status uruchomionych na komputerze programów poziomu użytkownika. Nie są wyświetlane usługi i aplikacje systemowe uruchomione w kontekście innym niż dla zalogowanego użytkownika. Oprócz tego, na zakładce *Applications* użytkownik może uruchomić nowy program klikając przycisk **New Task** (Nowe zadanie), może zakończyć zadanie klikając przycisk **End Task** (Zakończ zadanie) lub może przełączyć na inną aplikację przy użyciu przycisku **Switch To** (Przełącz na). Kliknięcie prawym przyciskiem myszy aplikacji umożliwia wybranie z menu skrótów polecenia **Go To Process** (Przejdź do procesu), co powoduje wyświetlenie odpowiedniego procesu na zakładce *Process* (Proces). Na rysunku 12-6 został przedstawiony przykładowy widok zakładki *Applications* programu *Task Manager*.

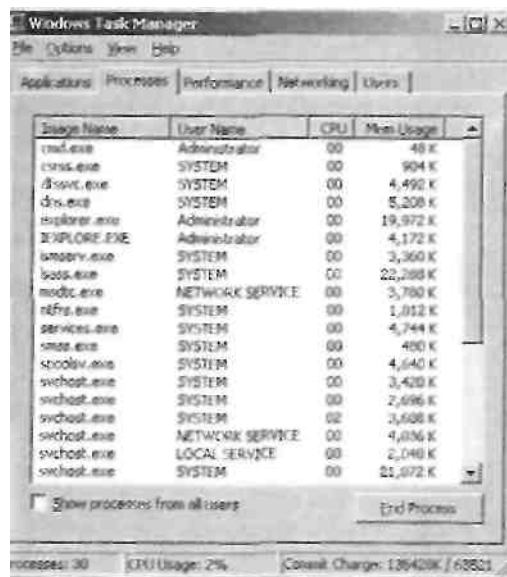


Rysunek 12-6 Zakładka Applications (Aplikacje) programu Task Manager (Menedżer zadań)

Zakładka Processes (Procesy)

Na zakładce *Processes* (Procesy) prezentowane są informacje o wszystkich procesach uruchomionych na komputerze, wliczając w to aplikacje poziomu użytkownika, usługi i inne procesy systemowe. W menu View (Widok) umieszczone zostało polecenie **Select Columns** (Wybierz kolumny), które umożliwia wybór kolumn danych wyświetlanych w oknie programu, wliczając w to zmiany wykorzystania pamięci (przyrosty), identyfikatory procesów czy wykorzystanie procesora. Kliknięcie nagłówka kolumny powoduje porządkowanie wyświetlanej całej listy według informacji pokazywanych w wybranej kolumnie.

Poprzez kliknięcie prawym przyciskiem myszy procesu użytkownik może zakończyć proces, może zmienić dla procesu priorytet uzyskiwania czasu procesora, a w przypadku komputerów wieloprocessorowych, może dla procesu określać koligacje. Użytkownik może zakończyć procesy, które mają procesy podrzędne lub powiązane wybierając polecenie **End Process Tree** (Zamknij drzewo procesu). Przykładowo, aby zamknąć aplikację pocztową, trzeba również zamknąć bufor MAPI. W takim przypadku wystarczy kliknąć prawym przyciskiem myszy aplikację pocztową i wybrać polecenie **End Process Tree** (Zamknij drzewo procesu). Zakładka *Processes* została pokazana na rysunku 12-7.



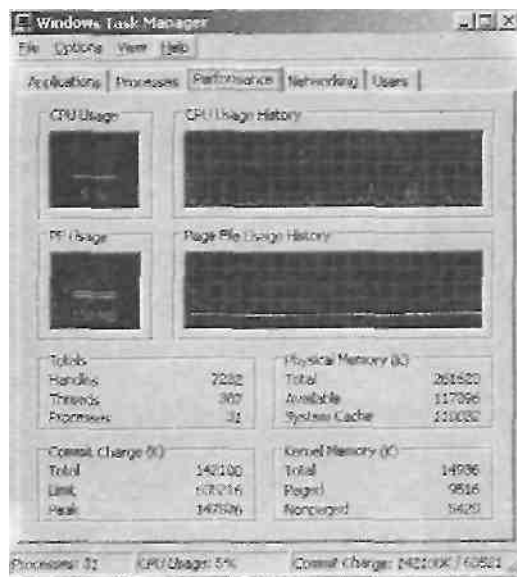
Rysunek 12-7 Zakładka Processes (Procesy) programu Task Manager (Menedżer zadań)



Informacja Zmiana ustawień procesu takich jak priorytet lub koligacje procesora może mieć odwrotny skutek w odniesieniu do wydajności innych aplikacji uruchomionych na komputerze. Zakończenie procesu, a w szczególności drzewa procesu, powinno być przeprowadzane jedynie, jeśli zawiódły normalne procedury zamykania. System Windows Server 2003 na szczęście zabezpiecza swoje procesy przed zamknięciem za pomocą programu Task Manager (Menedżer zadań), ale w dalszym ciągu są one wrażliwe na braki zasobów powstałe wskutek nieodpowiedniego przydziału priorytetu innych procesów.

Zakładka Performance (Wydajność)

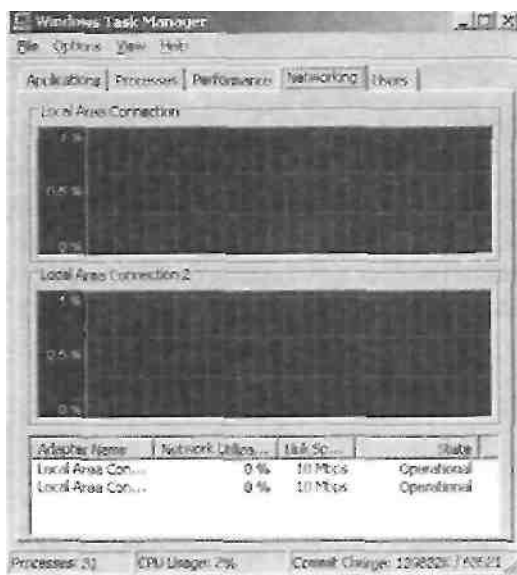
Na zakładce *Performance* (Wydajność) wyświetlane są w czasie rzeczywistym najważniejsze elementy wydajności komputera. Wykresy są prezentowane dla każdego procesora systemu oraz pokazują wykorzystanie pamięci. Wyświetlane są również informacje tekstowe o pamięci fizycznej, pamięci jądra i pamięci zadeklarowanej, a także o liczbie dojsć i wątków używanych przez aktywne procesy. Zakładka *Performance* została przedstawiona na rysunku 12-8.



Rysunek 12-8 Zakładka Performance (Wydajność) programu Task Manager (Menedżer zadań)

Zakładka Networking (Sieć)

Na zakładce *Networking* (Sieć) wszystkie aktywne połączenia sieciowe pokazywane są według nazwy, prędkości połączenia, wykorzystania pasma oraz statusu. Zakładka *Networking* została pokazana na rysunku 12-9.



Rysunek 12-9 Zakładka Networking (Sieć) programu Task Manager (Menedżer zadań)

Zakładka Users (Użytkownicy)

Na zakładce *Users* (Użytkownicy) wyświetlana jest lista zalogowanych użytkowników. Zakładka umożliwia wylogowanie użytkownika oraz wymuszenie odłączenia od komputera. Dotyczy to zarówno użytkowników zalogowanych na konsoli, jak i poprzez sieć. Komunikaty ostrzegawcze mogą być wysyłane do użytkowników (należy poinformować użytkownika sieci, że jego połączenie zostanie zamknięte). W tym celu trzeba kliknąć sesję użytkownika, a następnie przycisk **SendMessage** (Wyślij wiadomość). Zakładka *Users* została pokazana na rysunku 12-10.



Rysunek 12-10 Zakładka Users (Użytkownicy) programu Task Manager (Menedżer zadań)

Zadanie kontrolne: program Task Manager (Menedżer zadań)

W zadaniu tym za pomocą programu *Task Manager* uruchamiana będzie aplikacja oraz wyszukiwany proces.

1. Kliknij prawym przyciskiem myszy pustą część paska narzędzi i wybierz z menu skrótów polecenie **Task Manager** (Menedżer zadań).
2. Na zakładce *Applications* (Aplikacje) kliknij przycisk **New Task** (Nowe zadanie). Wpisz **explorer**, a następnie naciśnij przycisk OK.

Uruchomiony zostanie program Windows Explorer (Eksplorator Windows) i wyświetlony zostanie jego domyślne okno (najczęściej jest to folder *Moje dokumenty*). W oknie programu *Task Manager* na zakładce *Applications* wyświetlona zostanie nazwa aplikacji *Moje dokumenty* (lub innej wybranej aplikacji).

- 3- Kliknij prawym przyciskiem myszy nazwę uruchomionej aplikacji i wybierz polecenie **Go To Process** (Przejdź do procesu).

Wyświetlona zostanie zakładka *Processes* (Procesy) i podświetlony proces **Explorer.exe**. W tym miejscu można, jeśli sytuacja daje ku temu podstawy, zmienić priorytet procesu lub go zakończyć.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Jakie informacje dotyczące wydajności aplikacji udostępnia program Task Manager (Menedżer zadań)?
2. Komputer ulega awarii prawie dokładnie po godzinie pracy licząc od momentu uruchomienia. Prawdopodobną przyczyną tego problemu jest wyciek pamięci aplikacji. W jaki sposób można wykorzystać program Task Manager (Menedżer zadań) do określenia, która aplikacja wywołuje ten problem?
3. Na dwuprocessorowym komputerze uruchomiona jest baza danych. Należy określić, aby aplikacja bazy danych pracowała na drugim procesorze. Jak zrealizować to zadanie za pomocą programu Task Manager (Menedżer zadań)?

Podsumowanie lekcji

Program *Task Manager* (Menedżer zadań) umożliwia podgląd bieżącej wydajności komputera w odniesieniu do uruchomionych procesów i aplikacji. Program prezentuje informacje o wydajności procesora, pamięci i operacji we/wy, przy czym użytkownik może konfigurować okres aktualizacji danych i wybierać kolumny danych. Na zakładce *Applications* (Aplikacje) użytkownik może uruchomić lub zakończyć program, a na zakładce *Processes* (Procesy) można zmieniać priorytet procesów lub proces może zostać zakończony (również razem z procesami podrzędnymi). Zakładka *Performance* (Wydajność) prezentuje sumaryczne dane o wykorzystaniu procesora i pamięci komputera. Podobnie na zakładce *Networking* (Sieć) użytkownik może przeglądać dane o wykorzystaniu sieci oraz o jej podstawowej konfiguracji. Jeśli dostępna jest zakładka *Users* (Użytkownicy), można za jej pomocą rozłączać sesje lokalne lub zdalne. W przypadku sesji zdalnych istnieje również możliwość wysyłania komunikatu do przyłączonych użytkowników.

Lekcja 4: Wykorzystywanie usługi WMI Event Logging Provider (dostawcy protokołowania zdarzeń)

Usługa WMI (Windows Management Instrumentation) firmy Microsoft to implementacja WBEM (Web Based Enterprise Management Initiative), inicjatywy ustanowienia standardów tworzenia, odczytu oraz modyfikowania informacji dotyczących zarządzania. Usługa WMI jest zgodna z inicjatywą WBEM i zapewnia zintegrowaną obsługę modelu danych CIM (Common Information Model), który opisuje obiekty istniejące w środowisku zarządzania. Usługa WMI zawiera repozytorium obiektów, które jest bazą danych definicji obiektów oraz program WMI Object Manager (menedżer obiektów WMI), który obsługuje obiekty zbierając informacje wejściowe od dostawców WMI. Dostawcy usługi WMI mogą w szerokim zakresie odbierać informacje od usług, aplikacji oraz elementów systemu.

Materiały omówione podczas lekcji pozwalają na

- Korzystanie z usługi WMI oraz z usługi WMIC (wiersz poleceń usługi WMI) do monitorowania uruchomionych usług
- Korzystanie z usługi WMI oraz WMIC do identyfikowania zainstalowanych programów
- Korzystanie z usług WMI oraz WMIC do odnotowywania danych dotyczących zdarzeń

Szacunkowy czas lekcji: 30 minut

Działanie usługi WMI

Opisując skrótowo, źródła informacji usługi WMI (dostawcy) dostarczają dane o swoich komponentach (urządzenia, usługi, aplikacje itd.) do menedżera obiektów usługi WMI (WMI Object Manager), który wprowadza te informacje do bazy danych usługi WMI (repozytorium). W zależności od tego, co zostało zaakceptowane przez każdego dostawcę jako informacja wejściowa oraz co może być wysyłane jako informacja wyjściowa, administratorzy mogą używać metod do obsługi komponentów, ustawiania właściwości oraz określania zdarzeń, które mogą alarmować o zmianach w składnikach. Dostęp do repozytorium usługi WMI (WMI Repository) może być uzyskiwany przez narzędzia zarządzania dostarczane przez system, aplikację lub dostawcę urządzenia. Dostęp ten uzyskiwany jest poprzez interfejsy API (Application Programming Interfaces), narzędzia skryptowe (na przykład Windows Scripting Host) lub przy użyciu wiersza poleceń za pomocą usługi WMIC (Windows Management Interface Command-line).



Nieoficjalnie Administrator nie musi być ekspertem od tworzenia skryptów, aby stosować usługę WMI, a właściwie używa jej nie zdając sobie z tego sprawy. Wiele narzędzi korzysta z usługi WMI do odnotowywania i konfigurowania obiektów dostawcy WMI. Dla przykładu, narzędziami systemu Windows Server 2003, które wykorzystują usługę WMI, są programy System Information (Informacje o systemie), System Properties (Właściwości systemu) oraz Services (Usługi).

Usługa Windows Management Interface Command-line (WMIC)

Usługa WMIC udostępnia interfejs wiersza poleceń dla usługi WMI i może być wykorzystywana do zdalnego lub lokalnego zarządzania dowolnym komputerem, w którym może zarejestrować się użytkownik korzystający z usługi WMIC. Aby za pomocą usługi WMIC zarządzać komputerem zdalnym wystarczy uruchomienie usługi WMI na komputerze lokalnym, na którym realizowane będzie zadanie monitorowania. Usługa WMIC nie musi być dostępna na zdalnie zarządzanym komputerze. Usługa WMIC jest wykorzystywana do wykonywania następujących zadań:

- **Zarządzanie komputerem lokalnym** Użytkownik komputera wykorzystuje usługę WMIC do zarządzania tym komputerem.
- **Zarządzanie komputerem zdalnym** Użytkownik komputera wykorzystuje usługę WMIC do zarządzania innym komputerem.
- **Zarządzanie wieloma komputerami zdalnymi** Użytkownik komputera wykorzystuje usługę WMIC do zarządzania wieloma komputerami za pomocą pojedynczego polecenia.
- **Skrypty administracyjne** Usługa WMIC może być wykorzystywana do tworzenia skryptów zarządzania (pliki wsadowe) w celu zautomatyzowania zarządzania komputerów lokalnych bądź zdalnych lub zarządzania jednocześnie wieloma komputerami.

Administracja przy użyciu usługi WMIC

Pomimo, że pełne omówienie usług WMIC i WMI nie mieści się w zakresie tego rozdziału (temu tematowi poświęconych zostało kilka obszernych książek), potrzebne jest przedstawienie niektórych zagadnień, aby było możliwe udzielanie odpowiedzi na kwestie związane ze sprawnym monitorowaniem przy użyciu usługi WMI i WMIC. W niniejszym rozdziale zostało przyjęte założenie (o ile nie zostało to inaczej określone), że usługa WMIC jest używana w trybie interakcyjnym, dzięki czemu istnieje możliwość wprowadzenia pojedynczych poleceń i przeglądania rezultatów ich działania w środowisku usługi WMIC.



Wskazówka egzaminacyjna Wszystkie odniesienia do usługi WMIC w trybie interakcyjnym, w porównaniu do trybu automatycznego, nie mają wpływu na strukturę poleceń lub sposób ich używania. Różnica między tymi trybami dotyczy ilości poleceń, które mają być wykonane oraz tego, czy polecenia te mają być wprowadzane ręcznie lub za pośrednictwem pliku wsadowego. Aby uruchomić tryb interakcyjny usługi WMIC, należy w wierszu poleceń wpisać **wmic** i nacisnąć ENTER, natomiast opuszczenie tego trybu to wpisanie poleceń **exit** lub **quit**. Tryb automatyczny to pojedynczy wiersz komendy zaczynający się od WMIC i umieszczony w wierszu polecenia lub w pliku wsadowym.

Usługa WMI działa w kontekście obszarunazw, którym jest domyślnie główny katalog systemowy root\cli (MSFT_cli w arkuszu stylów XSL) i kontroluje, które właściwości, metody (zlecenia) i zastępcze nazwy (alias) są dostępne w usłudze WMI. Jeśli zachodzi taka potrzeba, nazwy zastępcze, metody i właściwości mogą być dodawane, ale dla większości zadań dotyczących monitorowania ich lista jest wystarczająca.

Zabezpieczenia usługi WMI są konfigurowane za pomocą przystawki konsoli MMC *WMI Control* (Sterowanie usługą WMI) (Wmimgmt.msc). Ustawienia domyślne określają, że poprzez usługę WMIC użytkownicy mają uprawnienia do odczytu informacji dostawcy WMI komputera lokalnego, ale nie mają uprawnień, aby połączyć się zdalnie lub zapisać informacje poza kontekstem dostawcy.

Administratorzy, którzy chcą przydzielić użytkownikom lub grupom dodatkowe uprawnienia, muszą je przydzielać poprzez przystawkę *WMI Control*.

AliasymMIC

Pierwszym parametrem w wierszu poleceń usługi WMIC jest alias. Nazwa zastępcza, alias, musi być unikatowa w schemacie przestrzeni nazw usługi WMI i umożliwia dostęp do informacji usługi WMI bez konieczności pamiętania bardziej złożonego schematu obiektów i właściwości. W tabeli 12-2 wymienione zostały właściwości skojarzone z każdą instancją aliasu. Pełne listy aliasów i przestrzeni nazw oraz inne szczegółowe informacje dotyczące aliasów WMIC można znaleźć w programie *Help and Support* (Centrum pomocy i obsługi techniczne) systemu Windows Server 2003 wyszukując temat: *Alias Namespaces and Classes* (Obszary nazw i klasy aliasów).

Tabela 12-2. Aliasym usługi WMIC

Właściwość	Opis
FriendlyName	Określa nazwę aliasu. Nazwa musi być unikatowa
Description	Opis aliasu. Jest to tekst opisowy wyświetlany po wpisaniu polecenia <code>/?</code> w wierszu polecenia aplikacji WMIC.
Formats	Lista formatów. Każdy format ma określoną nazwę i listę właściwości (obiektów klasy MSFT_CliProperty), które powinny być dla niego wyświetlane. Wszystkie formaty są obiektami klasy MSFT_CHFormat
Verbs	Lista zleceń, czyli różnych zachowań dostępnych za pośrednictwem danego aliasu. Istnieją dwie formy zachowań: • Zlecenia standardowe, które są bezpośrednio obsługiwane przez narzędzie. • Zlecenia definiowane przez użytkownika, które muszą odwoływać się do określonej metody zdefiniowanej dla obiektu docelowego aliasu. Wszystkie zlecenia są obiektami klasy MSFT_ChiVerb.
Qualifiers	Lista przypominająca listę kwalifikatorów WMI. Wszystkie kwalifikatory są obiektami klasy MSFT_CliQualifier.
Target PWhere	Lista przypominająca listę kwalifikatorów WMI. Wszystkie kwalifikatory są obiektami klasy MSFT_CliQualifier.
clause	Opcjonalna klauzula WHERE ograniczająca zakres właściwości Target. Dla tego warunku mogą istnieć wartości zastępcze, które są parametrami aliasu. Wartości zastępcze są oznaczane symbolem <code>#</code> . Jeśli konieczne jest użycie wielu parametrów, to są one kolejno oznaczane symbolem <code>#</code> .
Connection	Szczegóły dotyczące komputera, z którym ma być nawiązywane połączenie, szczegóły używanych zabezpieczeń itp. Jeśli połączenie nie jest określone, komputery, do których ma być uzyskiwany dostęp, są określone parametrem <code>/NODE</code> , a obszar nazw jest wyznaczony wartością parametru <code>/NAMESPACE</code> . Jeśli nie zostanie podana nazwa użytkownika i hasło, zostaną użyte wartości <code>/USER</code> i <code>/PASSWORD</code> , o ile są dostępne (w przeciwnym razie zostanie użyte bieżące konto).
View an alias schema	Wyświetla schemat aliasu przy użyciu metaaliasu Alias. Na przykład: <code>ALIAS OS</code>

WMIC Verbs (Zlecenia usługi WMIC)

Większość aliasów jest związana z wykonywanymi operacjami: czynności te są rozpoczynane przez umieszczenie zlecenia po nazwie aliasu. W połączeniu z parametrami i przełącznikami, zestaw alias-zlecenie sprawdza, jaka konfiguracja została określona dla aplikacji lub jakie informacje są odczytywane z repozytorium WMI (WMI Repository). W tabeli 12-3 została zamieszczona lista używanych do monitorowania najważniejszych zleceń wraz z ich opisem. Pełną listę zleceń oraz inne szczegółowe informacje dotyczące zleceń usługi WMIC można znaleźć w programie Help and Support (Centrum pomocy i obsługi techniczne) systemu Windows Server 2003 wyszukując temat: WMIC Verbs (Zlecenia usługi WMIC).

Tabela 12-3. Zlecenia WMIC

Zlecenie	Czynność	Parametry	Przykład
CALL	Wykonuje metody	Lista metod i parametrów, jeśli istnieje. Listy parametrów są rozdzielane przecinkami. Aby wyświetlić listę metod i ich parametrów dostępnych dla bieżącego aliasu, należy użyć polecenia SERVICE CALL /? Nazwa właściwości lub przełącznik.	SERVICE WHERE CAPTION=-TELNET' CALL STARTSERVICE
GET	Pobiera informacje na temat określonych właściwości.		PROCESS GET NAME
LIST	Pokazuje dane	Jest to polecenie domyślne. Łącznie z poleceniem LIST można używać wiele przełączników i parametrów (na przykład: BRIEF)	PROCESS LIST BRIEF

Monitorowanie przy użyciu usługi WMIC

Jeśli usługa WMI jest uruchomiona na komputerze, a użytkownik, który uruchomił usługę WMIC, ma wystarczające uprawnienia administracyjne, to może z wiersza poleceń monitorować komputer zdalny lub lokalny. W trybie automatycznym, w pliku wsadowym można zamieszczać wiele poleceń, które są uruchamiane ręcznie lub zgodnie z harmonogramem. Te polecenia usługi WMIC można zapisywać w pliku CSV, w pliku tekstowym lub jako stronę HTML, dzięki czemu mogą być przeglądane i analizowane. Poniżej przedstawione zostały przykłady często spotykanych sytuacji oraz dane wyjściowe, które ilustrują wykorzystanie usługi.

- **PRODUCT**

Polecenie to wyświetla na konsoli rezultaty zapytania dotyczącego wszystkich programów zainstalowanych na komputerze lokalnym.

- /OUTPUT:c:\applog.htm NTEVENT WHERE „eventtype<3 AND logfile='Application'” GET Logfile, SourceName, Eventtype, Message, TimeGenerated/FORMAT:hhtable:"sortby=EventType"

Polecenie to zapisuje w pliku HTML (C:\applog.htm) każde zdarzenie typu 0, 1 lub 2 znajdujące się w dzienniku aplikacji (Application) lokalnego komputera. Lista zostanie sformatowana w postaci tabeli HTML (przy użyciu arkusza stylów XML - htable.xml) i posortowana według parametru EventType (typ zdarzenia).

- /OUTPUT:c:\applog.csv/NODE:@ "c:\serverlist.txt" NTEVENT WHERE „eventtype<3 AND logfile=Application" GET Logfile, SourceName, Eventtype, Message, TimeGenerated/FORMAT: csv:"sortBy=EventType"

Polecenie to zapisuje w pliku CSV (c:\applog.csv) każde zdarzenie typu 0, 1 lub 2 znajdujące się w dziennikach aplikacji (Application) komputerów, których lista zawarta została w pliku serverlist.txt. Lista zostanie sformatowana w postaci listy rozdzielanej przecinkami (przy pomocy arkusza stylów XML — csv.xml) i posortowana według parametru Event Type (typ zdarzenia).

- OSASSOC

Polecenie to wyświetla informacje dotyczące zainstalowanych poprawek i uzupełnień systemu operacyjnego.

Zadanie kontrolne: Dane usługi WMI dostępne w programie Event Viewer (Podgląd zdarzeń)

W zadaniu tym pobrane zostaną dane z programu Event Viewer (Podgląd zdarzeń) i opublikowane na stronie sieci Web.

1. Zaloguj się jako administrator na w komputerze Server01, otwórz okno wiersza poleceń, wpisz polecenie **wmic** i naciśnij ENTER. Polecenie to wprowadza usługę WMIC w tryb interakcyjny.
2. W wierszu poleceń usługi WMIC wpisz następującą komendę, za pomocą której można uzyskać dostęp do danych dziennika *Security* utworzonego podczas lekcji 1 w ćwiczeniu 3:

NTEVENT WHERE "EVENTTYPE=5 AND LOGFILE='SECURITY'" GET LOGFILE, SOURCENAME, EVENTTYPE, MESSAGE, TIMEGENERATED

Polecenie to wyświetli na konsoli wpisy inspekcji dotyczącej niepowodzenia (Failure Audit).

- 3- W wierszu poleceń usługi WMC wpisz następującą komendę, aby te same informacje umieścić na stronie sieci Web nazwanej C:\seclog.htm.

/OUTPUT:C:\seclog.htm NTEVENT WHERE "EVENTTYPE=5 AND LOGFILE='SECURnT'" GET LOGFILE, SOURCENAME, EVENTTYPE, MESSAGE, TIMEGENERATED/FORMAT:htable

4. Dwukrotnie kliknij plik C:\Seclog.htm, aby otworzyć go za pomocą przeglądarki Internet Explorer.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Z kilku serwerów sieci należy pobrać zdalnie informacje o poprawkach i uzupełnieniach. W jaki sposób wykorzystać usługę WMI do zrealizowania tego zadania?
2. Z 17 komputerów działu projektowego należy zdalnie pobrać informacje o wszystkich zainstalowanych aplikacjach. W jaki sposób wykorzystać usługę WMI do zrealizowania tego zadania?
- 3- Administrator chce niewielkiej grupie inżynierów umożliwić wykorzystywanie usługi WMI tak, aby mogli pobierać informacje z niektórych serwerów w dziale, bez konieczności przydzielania im uprawnień administracyjnych do tych serwerów. Co można zrobić, aby inżynierowie uzyskali dostęp do serwerów?

Podsumowanie lekcji

W systemie Windows Server 2003 usługa WMI jest programem narzędziowym zgodnym z inicjatywą WBEM, która wykorzystuje bazę danych standardu CIM do gromadzenia informacji dotyczących zarządzania. Usługa WMIC jest interfejsem wiersza poleceń usługi WMI, która używa wielu zleceń, aliasów, przełączników i parametrów do zmiany konfiguracji lub pobierania informacji systemu komputerowego. Usługa WMIC może podłączać się zdalnie do dowolnego komputera, pod warunkiem, że użytkownik nawiązujący połączenie posiada wystarczające uprawnienia. Administrator lokalny ma uprawnienia umożliwiające połączenie zdalne, jak również administrator domeny może przy użyciu usług WMI i WMIC przeprowadzać administrację zdalną. W celu archiwizacji lub analizy, dane zebrane przez usługę WMI mogą być zapisywane w pliku CSV lub HTML. Podczas zarządzania wieloma komputerami komendy są wprowadzane z wiersza poleceń lub na podstawie pliku tekstowego. W obu trybach, automatycznym i interakcyjnym, polecenia są takie same, z wyjątkiem konieczności dołączenia w trybie automatycznym na początku każdej linii polecenia WMIC.

Zadanie praktyczne

Zadaniem nowego administratora jest, lepsze niż było to poprzednio, zorganizowanie administracji sieci przedsiębiorstwa. Uszkodzenia sprzętu serwera zdarzają się często, a użytkownicy nie są zadowoleni z poziomu usług sieci. Na podstawie rozmów z personelem działu IT można wywnioskować, że w ostatnich kilku latach bardzo niewiele czasu poświęcone zostało planowaniu i bezpieczeństwu działania sieci.

Zadanie postawione przez szefa firmy to szybka poprawa istniejącej sytuacji oraz przeprowadzenie działań zmniejszających jego obawy wynikające z braku zasad zabezpieczeń, dotyczące wydostawania się ważnych informacji na zewnątrz firmy. Powinna także wzrosnąć wydajność użytkowników, czyli wszystkich aplikacji, które są zainstalowane na komputerach użytkowników w odniesieniu do zasady przedsiębiorstwa.

Poniżej została zamieszczona lista zadań, które należy przedsięwziąć, aby poprawić środowisko sieci:

- Należy wykorzystać usługę WMI oraz inne pliki narzędziowe do utworzenia pełnej listy zasobów opartych na plikach przechowywanych na serwerach sieci. Należy utworzyć opis struktury uprawnień do tych zasobów i skonsultować ją z kierownikami działów, aby uzyskać pewność, że przyjęta struktura jest prawidłowa.
- Należy wykorzystać program Event Viewer (Podgląd zdarzeń) oraz konsolę Performance (Wydajność) do uzyskania wiernego obrazu wszystkich ostatnich problemów wąskich gardeł spowodowanych awariami urządzeń, błędną konfiguracją usługi lub niezgodnościami aplikacji. Następnie, jeśli zachodzi taka potrzeba, należy wymienić urządzenia sprzętu, prawidłowo skonfigurować usługi i zaktualizować aplikacje, aby poprawić ten fragment działającego środowiska.
- Po zdefiniowaniu uprawnień należy uruchomić inspekcję Failure Access Auditing (niepowodzenia dostępu), aby zostali wyszukani użytkownicy, którzy próbują uzyskać nieuprawniony dostęp, i należy odpowiednio zareagować na takie zdarzenia.
- Należy wykorzystać program Performance Logs And Alerts (Dzienniki wydajności i alerty), aby po usunięciu wąskich gardeł utworzyć wzorzec odniesienia dla serwerów. Następnie należy regularnie monitorować zmiany wydajności w odniesieniu do wzorca.

Rozwiązywanie problemów

Użytkownicy działu wsparcia technicznego utworzyli własne strony sieci Web, na których publikowane są dane techniczne dla pozostałych grup użytkowników oraz wiele programów narzędziowych używanych okresowo do testowania aplikacji w kontekście funkcjonalności i stabilności. Niedawno do działu dotarła prośba o pomoc w określeniu przyczyn nagłego, znaczącego spadku wydajności komputera.

Korzystając z konsoli Performance (Wydajność) należy zbudować wzorzec odniesienia dla następujących liczników:

- Cache\Data Map Hits % (Pamięć podręczna\Trafienia mapowania danych %)
- Cache\Fast Reads/sec (Pamięć podręczna\Odczyty szybkie/s)
- Cache\Lazy Write Pages/sec (Pamięć podręczna\Zapis z opóźnieniem/s)
- Logical Disk\% Free Space (Dysk logiczny\ Wolne miejsce %)
- Memory\Available Bytes (Pamięć\Dostępne bajty)
- Memory\ Pool Nonpaged Allocs (Pamięć\Przydziały w puli niestronicowanej)
- Memory\ Pool Nonpaged Bytes (Pamięć\Bajty w puli niestronicowanej)
- Memory\ Pool Paged Allocs (Pamięć\Przydziały w puli stronicowanej)
- Memory\ Pool Paged Bytes (Pamięć\Bajty w puli stronicowanej)
- Processor(_Total)\% Processor Time [Procesor(_Total)\Czas procesora %]
- System\Context Switches/sec (System\Przełączniki kontekstu/s)
- System\Processor Queue Length (System\Długość kolejki procesora)
- Processor(_Total)\Interrupts/sec [Procesor(_Total)\Przerwania/s]

Wszystkie „podejrzane” komputery należy monitorować w okresie jednego tygodnia normalnej aktywności, rejestrując wyniki dla każdego komputera w oddzielnych plikach. Do monitorowania należy użyć komputera zdalnego tak, aby nie zafałszować wyników tworzonego wzorca odniesienia.

Dane należy przeanalizować próbując określić, czy nie występują wąskie gardła. Utworzony wzorzec odniesienia liczników w szczególności dotyczy wydajności pamięci, dyskowych operacji we/wy oraz procesora każdego komputera. Po określeniu wąskich gardeł, należy sprawdzić, które aplikacje (procesy) są odpowiedzialne za powstawanie problemu. W następnym kroku można zaktualizować aplikacje (jeśli są przesłanki, że może to pomóc), można usunąć aplikację lub można dodać zasobów do komputera, aby ich wystarczająca ilość pozwalała na wykonywanie zadań.

Podsumowanie rozdziału

- Program *Event Viewer* (Podgląd zdarzeń) prezentuje dane w formie dzienników. Na każdym serwerze systemu Windows Server 2003 przechowywane są dzienniki *Application* (Aplikacja), *System* oraz *Security* (Zabezpieczenia). Kontrolery domeny mają dodatkowe dwa dzienniki dotyczące usługi Active Directory, a inne serwery aplikacji (takie jak DNS) mają swój własny zestaw dzienników.
- Na konsolę *Performance* (Wydajność) (perfmon.msc) składają się dwie przystawki: *System Monitor* (Monitor systemu) oraz *Performance Logs And Alerts* (Dzienniki wydajności i alerty). Program *System Monitor* prezentuje w czasie rzeczywistym dane w oparciu o liczniki obiektów oraz może wyświetlać dane dzienników zarejestrowanych przez przystawkę *Performance Logs And Alerts* w postaci dzienników liczników (okresowe próbkowanie) lub w postaci dzienników śledzenia (*Trace*), które są skupione na rejestrowaniu zdarzeń.
- Program *Task Manager* (Menedżer zadań) jest używany do przeglądania w czasie rzeczywistym danych wydajności związanych z procesami i aplikacjami. Za pomocą programu *Task Manager* procesy mogą być rozpoczynane lub kończone. Istnieje możliwość zmiany priorytetu procesu dotyczącego czasu dostępu do procesora, a w systemach wieloprocessorowych dla procesu można określać koligacje dotyczące wybranego procesora.
- Usługa WMI jest systemem zarządzania, który zbiera informacje o systemach komputerowych. Interfejs przystawki *WMI Control* (Sterowanie usługą WMI) umożliwia także dostosowanie uprawnień, poza domyślnymi uprawnieniami administratora lokalnego, aby możliwe było zarządzanie komputerami sieci. Chociaż za pomocą usługi WMI można konfigurować wiele różnych rodzajów zachowania się systemu, w tym użytkowników, grup i usług, to lekcje niniejszego rozdziału skupiały się na przedstawieniu sposobów pobierania informacji z bazy danych usługi — *WMI Repository* (Repozytorium WMI). Dane można uzyskiwać korzystając z usługi WMIC, czyli usługi będącej interfejsem wiersza poleceń usługi WMI. Za pomocą usługi WMIC można odnotować, które usługi są uruchomione, które aplikacje są zainstalowane oraz można publikować dane programu *Event Viewer* (Podgląd zdarzeń) w plikach CSV lub HTML, dzięki czemu dystrybucja i analiza tych informacji staje się prosta.

Informacje dla zdających egzamin

Przed przystąpieniem do egzaminu, należy zapoznać się z przedstawionymi poniżej najważniejszymi faktami i pojęciami, aby określić które tematy wymagają pogłębienia. Należy powrócić do lekcji, aby osiągnąć większą wprawę oraz przejrzeć działy znajdujące się w części 2 — „Materiały dodatkowe”. Informacje tu zawarte, kierują do materiałów uzupełniających tematy objęte zadaniami egzaminacyjnymi.

Najważniejsze fakty

- Program Event Viewer (Podgląd zdarzeń) nie służy do konfigurowania, ale do gromadzenia danych przesyłanych przez różnych dostawców. Odnotowywane dane są zbierane w odpowiednich dziennikach, a dla łatwiejszej analizy mogą być filtrowane, sortowane oraz eksportowane.
- Program Task Manager (Menedżer zadań) jest narzędziem wykorzystywanym jedynie na komputerze lokalnym. Program ten nie umożliwia konfiguracji pamięci, procesora bądź innych ustawień. Program Task Manager (Menedżer zadań) jest używany wyłącznie do uruchamiania, zatrzymywania oraz określania priorytetu i koligacji dotyczących aplikacji.
- Przystawka Performance Logs And Alerts (Dzienniki wydajności i alerty) nie służy do konfigurowania, a jedynie do protokolowania danych w dziennikach liczników (Counter Logs) odnotowywanych (w definiowanych okresach) przez dostawców, czyli przez liczniki obiektów lub służy do rejestrowania danych w dziennikach śledzenia (Tracę Logs) odnotowywanych przez dostawców skupiających się na występowaniu zdarzeń.
- Usługa WMI wymaga uprawnień administracyjnych dla uzyskania dostępu do komputera zdalnego i przeprowadzenia konfiguracji ustawień.
- Usługa WMIC nie jest narzędziem schematu zarządzania usługi Active Directory (Active Directory Schema Management Tool). Usługa WMI obsługuje swój własny schemat.

Najważniejsze pojęcia

Windows Management Instrumentation (WMI) Usługa ta jest implementacją firmy Microsoft inicjatywy WBEM (Web-Based Enterprise Management Initiative), dotyczącej między innymi ustanowienia standardów zarządzania danymi w przedsiębiorstwie.

Windows Management Instrumentation Control (WMIC) Jest to interfejs wiersza poleceń dla obsługi repozytorium usługi WMI (WMI Repository), dzięki któremu możliwe jest zarządzanie zadaniami związanymi z konfigurowaniem i monitorowaniem.

Task Manager (Menedżer zadań) Jest to narzędzie obsługi procesów.

System Monitor (Monitor systemu) Jest to element konsoli *Performance* (Wydajność), podobnie jak przystawka *Performance Logs And Alerts* (Dzienniki wydajności i alerty). Program Monitor systemu nie powinien być mylony z programem *System Properties* (Właściwości systemu)

Pytania i odpowiedzi

451 Pytania do lekcji 1

1. Które dzienniki będą wyświetlane w programie Event Viewer (Podgląd zdarzeń) dla kontrolera domeny, na którym uruchomiony jest system DNS (przy założeniu, że obowiązują ustawienia domyślne)?
 - » **Application (Aplikacja)** W tym dzienniku mogą być odnotowywane zmiany konfiguracji, błędy lub inne zdarzenia zgodnie z tym, co przewidział projektant aplikacji.
 - » **System** W tym dzienniku system operacyjny Windows Server 2003 odnotowuje zdarzenia (uruchomienie usługi, nietypowe zamknięcia, awarie urządzeń itp). Lista zdarzeń protokołowanych w dzienniku jest wstępnie skonfigurowana.
 - » **Security (Zabezpieczenia)** W dzienniku tym rejestrowane są zdarzenia logowania i dostępu do zasobów (inspekcje). Konfiguracja większości tych zdarzeń jest określana przez administratora.
 - » **Directory Service (Usługa katalogowa)** Dziennik ten zawiera zdarzenia dotyczące usługi Active Directory, takie jak niezgodności replikacji obiektów czy istotne zdarzenia w katalogu.
 - » **File Replication Service (Usługa replikacji plików)** Dziennik ten zawiera informacje o błędach lub istotnych zdarzeniach odnotowanych przez usługę replikacji plików (File Replication Service) dotyczących kopiowania informacji pomiędzy kontrolerami domeny w trakcie cykli replikacji.
 - » **DNS Server (Serwer DNS)** Dziennik ten zawiera informacje o błędach lub ważnych zdarzeniach odnotowywanych przez serwer DNS.
2. Administrator skonfigurował system Windows Server 2003 tak, aby przeprowadzana była inspekcja wszystkich nieudanych prób dostępu do obiektu, a inspekcja dla wszystkich plików i folderów określona została przez opcję List Folder/Read Data Failure (Niepowodzenie: Wyświetlanie zawartości foldera/Odczyt danych). Wszystkie inne ustawienia programu Event Viewer (Podgląd zdarzeń) oraz dziennika Security (Zabezpieczenia) są zgodne z ustawieniami domyślnymi. Co się stanie, jeśli plik wpisów dziennika Security (Zabezpieczenia) osiągnie 512 KB?

Ustawienia domyślne konfiguracji określają maksymalny rozmiar pliku dziennika jako 512 KB oraz zezwalają na zastępowanie danych. Tak więc po przekroczeniu wielkości 512 KB, starsze dane będą zastępowane kolejnymi wpisami.

3. Jakie ustawienia należy skonfigurować na serwerze, aby dane dziennika Security (Zabezpieczenia) nie były zastępowane oraz aby system Windows Server 2003 nie zatrzymał obsługi sieci w żadnym momencie?

We właściwościach dziennika Security (Zabezpieczenia) należy zaznaczyć opcję Do Not Overwrite Events (Clear Log Manually) [Nie zastępuj zdarzeń (ręczne czyszczenie dziennika)]. Nie można zaznaczyć opcji zabezpieczeń zasady grupy (Security Option): Audit: Shut Down System Immediately If Unable To Log Security Audits (Inspekcja: Zamknij system natychmiast, jeśli nie można zapisywać wyników inspekcji), jako że opcja ta spowoduje wyłączenie serwera po zapelnieniu pliku dziennika. Zalecaną praktyką administracyjną jest zaplanowanie regularnego analizowania dziennika Security (Zabezpieczenia), ale częstotliwość musi być odpowiednia, aby nie doszło do wyłączenia serwera z powodu zbyt rzadkiego czyszczenia dziennika.

Pytania do lekcji 2

1. Zadaniem administratora jest monitorowanie wszystkich serwerów platformy Windows Serw 2003 tak, aby defragmentacja przeprowadzana była na tych komputerach regularnie i możliwie wydajnie. Wykorzystywany program wymaga do prawidłowego przeprowadzenia defragmentacji dysku 20% wolnego miejsca na każdym wolumenie. W jaki sposób administrator powinien wykonać to zadanie?

Na stacji roboczej (lub mniej obciążonym serwerze) należy skonfigurować przystawkę Configure Performance Logs And Alerts (Dzienniki wydajności i alerty) tak, aby dla wszystkich serwerów zdalnych monitorowany był licznik obiektu LogicalDisk (Dysk logiczny) % Free Space (Wolne miejsce %) dla każdej instancji danego komputera. Oprócz tego, należy skonfigurować każdy licznik tak, aby po przekroczeniu progu 20% wolnego miejsca generowany był alert. Na koniec należy określić, że każdy alert ma powodować wysłanie wiadomości do administratora (lub innego konta użytkownika, które ma odbierać to powiadomienie).

2. Ze względu na słabą wydajność sieci monitorowane są systemy Windows Server 2003- Poniżej przedstawione zostały wyniki monitorowania komputerów:

» Processor: % Processor Time:	High
» Physical Disk: % DiskTime:	Low
» Memory: Pages/sec:	Low
» Processor: Interrupts/sec:	High
» Process: % Processor Time (for non-service processes):	Low
» Process: % Processor Time (for system processes):	Low

Jakie jest najbardziej prawdopodobne wyjaśnienie problemu?

Prawdopodobnie problemy występują na poziomie urządzenia, na karcie sieciowej (lub innym urządzeniu). Wysoka wartość parametru Przerwania/s może powodować zajęcie procesora obsługą żądań usług interfejsu sieciowego. Ponieważ inne liczniki mają niskie wartości, jest mało prawdopodobne, że uszkodzona jest aplikacja bądź inna usługa systemowa.

3. Serwer używany do monitorowania innych serwerów sieci jest zbyt przeciążony, należy więc zmniejszyć zakres zadań związanych z monitorowaniem. Co należy zrobić, aby uzyskać największy wpływ w odniesieniu do monitorowanej wydajności komputera przy założeniu, że rejestrowana jest możliwie największa ilość danych?

Należy zwiększyć okres próbkowania rejestrowania danych komputerów zdalnych. Zmniejszenie częstotliwości pobierania danych i skrócenie czasu rejestrowania (niejednokrotnie długiego), spowoduje, że większość danych będzie w dalszym ciągu monitorowana, a jednocześnie zmniejszy się obciążenie monitorowanego komputera.

Pytania do lekcji 3

1. Jakie informacje dotyczące wydajności aplikacji udostępnia program Task Manager (Menedżer zadań)?

Program Task Manager (Menedżer zadań) udostępnia informacje o wydajności procesora, wykorzystaniu pamięci (wliczając w to plik stronicowania) oraz podstawowe informacje we/wy. Informacje te prezentowane są w odniesieniu do każdego procesu.

2. Komputer ulega awarii prawie dokładnie po godzinie pracy licząc od momentu uruchomienia. Prawdopodobną przyczyną tego problemu jest wyciek pamięci aplikacji. W jaki sposób można wykorzystać program Task Manager (Menedżer zadań) do określenia, która aplikacja wywołuje ten problem?

Wszystkie aplikacje należy uruchomić w normalnym trybie. W programie Task Manager (Menedżer zadań), dla widoku Select Columns (Wybierz kolumny), należy zaznaczyć kolumnę Memory Usage Delta (Zmiana użycia pamięci), a następnie należy kliknąć nagłówek kolumny. Jeśli komputer zostanie bezczynny, wykorzystanie pamięci przez wszystkie uruchomione procesy powinno się ustabilizować. Jeśli w systemie znajduje się aplikacja z wyciekiem pamięci, będzie pokazywana na początku listy uruchomionych procesów komputera, a wartość w kolumnie Memory Usage Delta (Zmiana użycia pamięci) powinna się stale zwiększać, pomimo braku aktywności systemu.

3. Na dwuprocesorowym komputerze uruchomiona jest baza danych. Należy określić, aby aplikacja bazy danych pracowała na drugim procesorze. Jak zrealizować to zadanie za pomocą programu Task Manager (Menedżer zadań)?

Na zakładce Applications (Aplikacje) należy kliknąć prawym przyciskiem myszy aplikację bazy danych, a następnie nacisnąć przycisk Go To Process (Przejdź do procesu). W kolejnym kroku należy kliknąć prawym przyciskiem myszy proces i na podstawie opcji w menu skrótów określić koligacje z procesorem.

Pytania do lekcji 4

1. Z kilku serwerów sieci należy pobrać zdalnie informacje o poprawkach i uzupełnieniach. W jaki sposób wykorzystać usługę WMI do zrealizowania tego zadania?

Na każdym komputerze należy użyć aliasu OS ASSOC i przełącznika /node: do zdalnego uruchomienia polecenia WMIC. W celu przeprowadzenia analiz w innym terminie, dane wyjściowe mogą być również zapisywane w pliku CSV lub HTML przy użyciu aliasu /output oraz przełącznika /format. Na przykład, jeśli dla usługi WMIC, komputery Server01 i Server02 byłyby komputerami docelowymi, polecenie będzie miało następującą postać /NODE : "SERVER01" , "SERVER02" OS ASSOC.

2. "LXI komputerów działu projektowego należy zdalnie pobrać informacje o wszystkich zainstalowanych aplikacjach. W jaki sposób wykorzystać usługę WMI do zrealizowania tego zadania?

Nazwy komputerów należy wpisać w pliku tekstowym (na przykład computers.txt). Aby utworzyć listę zainstalowanych aplikacji każdego komputera, należy użyć aliasu WMIC PRODUCT i przełącznika node/node:@ switch. W celu przeprowadzenia analiz w innym terminie, dane wyjściowe mogą być również zapisywane w pliku CSV lub HTML przy użyciu aliasu /output oraz przełącznika /format. Na przykład:/NODE :@C: \computers.txt PRODUCT.

3. Administrator chce niewielkiej grupie inżynierów umożliwić wykorzystywanie usługi WMI, aby mogli pobierać informacje z niektórych serwerów działu, bez konieczności przydzielania im uprawnień administracyjnych do tych serwerów. Co można zrobić, aby inżynierowie uzyskali dostęp do serwerów?

W konsoli MMC, za pomocą przystawki WMI Control (Sterowanie usługą WMI) (Wmimgmt.msc), należy przydzielić każdemu inżynierowi lub grupie wszystkich inżynierów uprawnienia dla przestrzeni nazw usługi WMI.

13 Odzyskiwanie systemu po awarii



Zadania egzaminacyjne omawiane w tym rozdziale:

- Wykorzystywanie funkcji ASR (Automated System Recovery)
- Przeprowadzanie odzyskiwania systemu serwera

Cele rozdziału

Pomimo, że system Microsoft Windows Server 2003 zapewnia znakomitą stabilność i niezawodność, inne elementy komputera takie jak zasilacze, wentylatory, układy scalone, a nawet kod programów mogą spowodować awarię komputera. Skutki awarii serwera lasu domeny odczuwają wszyscy użytkownicy sieci. W niniejszym rozdziale omówione zostały sposoby implementacji i obsługi serwera minimalizujące ryzyko awarii. Oprócz tego opisane zostały metody odzyskiwania systemu po awarii poszczególnych usług, sterowników czy konfiguracji urządzeń sprzętu oraz umiejętności wymagane do przywrócenia serwera w sytuacji, kiedy uszkodzenie lub brak dostępu do systemu operacyjnego spowodowane jest poważnymi awariami.

Lekcje rozdziału:

- Lekcja 1: Odzyskiwanie systemu po awarii 484

Wymagania

W rozdziale omawiane są pojęcia i umiejętności dotyczące przywracania systemu uszkodzonego serwera. Aby przeprowadzić ćwiczenia zamieszczone w rozdziale, należy przygotować:

- Komputer działający pod kontrolą systemu Windows Server 2003. Zamieszczone przykłady zakładają, że komputer nazywa się Server01 i może być kontrolerem domeny lub serwerem członkowskim. Wykonywanie kopii zapasowych tworzonych podczas ćwiczeń będzie trwało krócej, jeśli komputer będzie serwerem członkowskim.
- Potrzebny będzie drugi dysk fizyczny do przeprowadzenia ćwiczenia ilustrującego działanie usługi Automated System Recovery (automatyczne odzyskiwanie systemu).
- Podczas przeprowadzania ćwiczenia dotyczącego automatycznego odzyskiwania systemu zostaną usunięte wszystkie dane na dysku zawierającym wolumen systemowy i dlatego, jeśli dysk zawiera istotne dane, nie należy na nim przeprowadzać tego ćwiczenia.

Lekcja 1: Odzyskiwanie systemu po awarii

Najgorszy scenariusz awarii zakłada, że uszkodzenie, jakiemu ulegają urządzenia sprzętu serwera, jest nieodwracalne. Aby przywrócić działanie serwera, trzeba dysponować pełną kopią zapasową serwera, która zostanie odtworzona na nowej części komputera. Pełna kopia zapasowa to dane przechowywane na serwerze, aplikacje oraz sam system operacyjny. W rozdziale 7 zostały omówione sposoby wykorzystywania programu *Backup Utility* (Kopia zapasowa) oraz programu wiersza poleceń *Ntbackup* do utworzenia kopii zapasowych danych serwera. Podczas niniejszej lekcji opisane zostaną metody korzystania z tych samych narzędzi tworzenia kopii zapasowych systemu tak, aby przywracanie działania systemu było możliwe krótkie nawet w przypadku „najgorszego” scenariusza. Oprócz tego omówione zostanie posługiwanie się programem *Recovery Console* (Konsola odzyskiwania) do przeprowadzania „chirurgicznych” napraw dotyczących specyficznych problemów, takich jak uszkodzenie usługi lub sterownika.

Materiały omówione podczas lekcji pozwalają na

- Tworzenie kopii zapasowej stanu systemu
- Przygotowanie kopii zapasowej dla usługi ASR i naprawę komputera przy pomocy programu ASR (Automated System Recovery)
- Instalowanie i wykorzystywanie programu *Recovery Console* (Konsola odzyskiwania) systemu Windows Server 2003

Szacunkowy czas lekcji: 60 minut

Przegląd opcji związanych z odzyskiwaniem

W niniejszej książce metody używane do naprawy i przywracania łączone były z określonymi typami uszkodzeń:

- **Brak danych lub ich uszkodzenie:** W rozdziale 7 omówione były sposoby tworzenia kopii zapasowej i odtwarzania danych, jak również opisana została nowa funkcja systemu Volume Shadow Copy Service (kopiowanie w tle), która umożliwia użytkownikom odtworzenie lub dostęp do poprzednich wersji plików przechowywanych w udostępnionych folderach na serwerze.
- **Aktualizacje sterowników powodujące niestabilność systemu:** W rozdziale 10 opisana została nowa funkcja systemu Windows Server 2003 pozwalająca na przywrócenie poprzedniej (działającej) wersji sterownika. Jeśli sterownik został zaktualizowany, a system zaczął pracować niestabilnie, sterownik oraz wszystkie ustawienia, jakie zostały zmienione podczas aktualizacji, mogą zostać przywrócone do poprzednio zainstalowanej wersji i stanu. Funkcja ta nie działa w odniesieniu do sterowników drukarek. Inna prosta metoda przywracania to wyłączanie sterownika powodującego niestabilność. Metoda została umieszczona w programie Device Manager (Menedżer urządzeń). Jeśli aplikacja lub obsługiwane oprogramowanie powoduje niestabilność, można wykorzystać program Add Or Remove Programs (Dodaj lub usuń programy) do usunięcia niezgodnego komponentu.
- **Uniemożliwienie uruchomienia systemu spowodowane instalacją lub aktualizacją usługi bądź sterownika:** W rozdziale 10 omówione zostało użycie funkcji *Last Known Good Configuration*

(Ostatnia znana dobra konfiguracja), która przywraca ustawienia rejestru systemu ControlSet sprzed ostatniego pomyślnego zalogowania w systemie. Jeśli po instalacji lub aktualizacji usługi bądź sterownika system uległ awarii lub nie można go ponownie uruchomić do momentu wyświetlenia ekranu logowania, funkcja Last Known Good Configuration (Ostatnia znana dobra konfiguracja) skutecznie przywróci działanie systemu sprzed instalacji sterownika lub usługi. W rozdziale omówiona została również opcja trybu Safe (tryb awaryjny), która umożliwia uruchomienie systemu przy wyłączonych określonych usługach i sterownikach. Tryb awaryjny często pozwala uruchomić komputer, kiedy nie udaje się to przy użyciu innych metod. Uruchomienie trybu awaryjnego umożliwia zastosowanie programu Device Manager (Menedżer urządzeń) do wyłączenia, odinstalowania lub przywrócenia poprzednio używanych usług bądź sterowników.

- **Uszkodzenia podsystemu dyskowego:** W rozdziale 11 zostały opisane etapy wymagane do skonfigurowania nadmiarowości dysku, którą tworzy się budując woluminy dublowane (RAID-1) lub RAID-5. Rozdział ten opisywał także sposoby przywracania woluminu odpornego na uszkodzenia po awarii pojedynczego dysku.

Wymienione powyżej procesy naprawy bądź odzyskiwania zakładają, że system można częściowo uruchomić. Jeśli system nie może być uruchomiony, przywrócenie działania systemu przeprowadzane jest przy użyciu funkcji *System State* (Stan systemu), *AutomatedSystem Recovery* (Automatyczne odzyskiwanie systemu) oraz *Recovery Console* (Konsola odzyskiwania).

System State

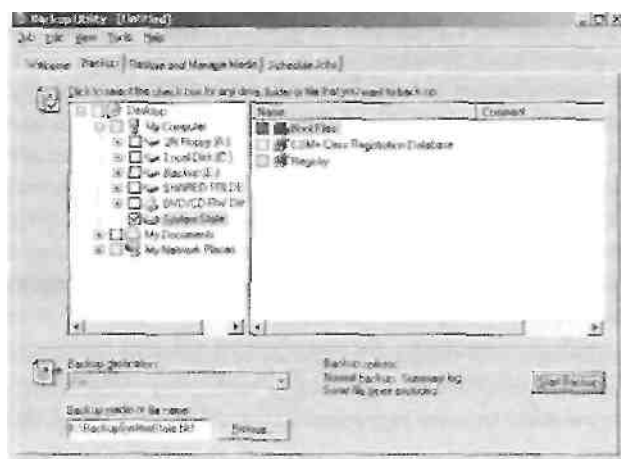
W systemach Windows 2000 oraz Windows Server 2003 do procesu wykonywania kopii zapasowej wprowadzone zostało pojęcie *System State* (Stan systemu). Dane o stanie systemu zawierają najważniejsze elementy konfiguracji systemu:

- Rejestr systemu
- Baza danych COM+ Class Registration
- Pliki rozruchowe, wliczając w to boot.ini, [ntdetect.com](#), ntldr, bootsect.dos oraz ntbootdd.sys
- Pliki systemowe, które są chronione działaniem usługi Windows File Protection (Ochrona plików systemu Windows)

Oprócz pozycji wymienionych powyżej, do listy *System State* dołączane są następujące elementy, pod warunkiem, że na komputerze zostały zainstalowane odpowiednie usługi:

- Baza danych Certificate Services dla serwera certyfikatów
- Usługa Active Directory oraz folder Sysvol dla kontrolera domeny
- Informacje usługi klastra dla serwera klastra
- Metabaza programu IIS (Internet Information Services) dla serwera, na którym zainstalowane zostały usługi IIS

Aby w programie *Backup Utility* (Kopia zapasowa) wykonać kopię zapasową danych o stanie systemu, należy dołączyć węzeł *System State* do listy kopiowanych pozycji. Węzeł *System State* oraz jego elementy zostały pokazane na rysunku 13-1.



Rysunek 13-1 Węzeł *System State*

Jeśli używany jest program narzędziowy wiersza poleceń Ntbackup, wprowadzana komenda powinna mieć następującą składnię:

```
Ntbackup backup systemstate /J „backup job name” ...
```

Polecenie musi zostać uzupełnione przełącznikiem /F, jeśli kopia zapasowa utworzona zostanie w pliku, lub odpowiednio przełącznikami /T, /G, /N albo /P, powodującymi wykonanie kopii na taśmie. Przełączniki programu Ntbackup opisane zostały w rozdziale 7.

Poniżej wymienione zostały istotne uwagi dotyczące tworzenia kopii zapasowej danych o stanie systemu (System State):

- Nie można kopiować pojedynczych elementów węzła *System State*. Na przykład nie można wykonać kopii zapasowej samej bazy danych COM+ Class Registration. Ze względu na wzajemne zależności pomiędzy elementami węzła *System State*, można wykonać jedynie kopię zapasową całości, to znaczy jednocześnie wszystkich danych o stanie systemu.
- Nie można używać programu Ntbackup lub *Backup Utility* (Kopia zapasowa) do tworzenia kopii zapasowej danych o stanie systemu komputera zdalnego. Programy Ntbackup lub *Backup Utility* mogą być uruchamiane w systemach, dla których wykonywana jest kopia zapasowa. Jednakże można skierować plik kopii zapasowej do serwera zdalnego, a ten prześle plik na inny nośnik kopii lub też można zaopatrzyć się w inny program archiwizacji danych, który umożliwia zdalne wykonywanie kopii zapasowych.
- Węzeł *System State* (Stan systemu) zawiera wiele elementów konfiguracji systemu, ale nie muszą to być wszystkie elementy potrzebne do przywrócenia działania wszystkich funkcji systemu. Dlatego, podczas tworzenia kopii zapasowej danych o stanie systemu zaleca się również kopiowanie wszystkich woluminów — rozruchowego, systemowego, danych oraz aplikacji. Kopia stanu systemu jest podstawowym elementem pełnej kopii zapasowej, ale trzeba pamiętać, że jest tylko jej częścią.
- Zaznaczenie węzła *System State* jako składnika kopii zapasowej automatycznie powoduje wybranie typu kopii — Kopia, chociaż interfejs może nie odnotowywać tego faktu. Warto o tym pamiętać, jeżeli oprócz stanu systemu do wyborów kopii zapasowej dołączane są inne elementy.

Aby odtworzyć kopię danych o stanie systemu (System State) na działającym komputerze, należy wykorzystać program *Backup Utility* (Kopia zapasowa), a na zakładce *Restore And Manage Media* (Przywracanie i zarządzanie nośnikiem) zaznaczyć pole wyboru System State. Jeśli natomiast komputer nie działa, trzeba prawdopodobnie najpierw powrócić do programu *Automated System Recovery* (Automatyczne odzyskiwanie systemu), aby przywrócić działanie systemu.

Stan systemu kontrolera domeny

Węzeł System State (stan systemu) kontrolera domeny zawiera usługę katalogową Microsoft Active Directory oraz folder Sysvol. Kopia zapasowa na kontrolerze domeny wykonywana jest dokładnie tak samo, jak na innych systemach — przy użyciu programów *Backup Utility* (Kopia zapasowa) lub Ntbackup. Tak samo jak dla wszystkich nośników kopii zapasowych, sprawą pierwszorzędnej wagi jest fizyczne zabezpieczenie nośników kopii zapasowej usługi Active Directory.

Aby odtworzyć dane o stanie kontrolera domeny, należy wyłączyć, a następnie ponownie uruchomić komputer, nacisnąć F8 i wybrać opcję rozruchową **Directory Services Restore Mode** (Tryb przywracania usług katalogowych). Tryb ten jest odmianą trybu *Safe* (Tryb awaryjny) opisanego w rozdziale 10. W trybie *Directory Services Restore Mode* (Tryb przywracania usług katalogowych) kontroler domeny uruchamia się, ale nie uruchamia usługi Active Directory. W komputerze należy zalogować się jako administrator lokalny wykorzystując hasło trybu *Directory Services Restore Mode*, które zostało użyte w programie Depromo podczas desygnowania serwera do roli kontrolera domeny.

Kontroler domeny w trybie *Directory Services Restore Mode* nie dokonuje uwierzytelnienia lub replikacji usługi Active Directory, dzięki czemu baza danych usługi Active Directory i obsługiwane pliki nie są narażone na zablokowanie, co pozwala na odtwarzanie stanu systemu za pomocą programu *Backup Utility* (Kopia zapasowa).

Podczas odtwarzania danych o stanie systemu kontrolera domeny należy określić, czy przywracanie usługi Active Directory i foldera Sysvol ma być nieautorytatywne (normalne) lub autorytatywne. Po odtworzeniu stanu systemu za pomocą programu *Backup Utility* (Kopia zapasowa) należy zakończyć procedurę, uruchamiając ponownie kontroler domeny w normalnym trybie. Ponieważ odtworzone zostały starsze dane, kontroler domeny musi aktualizować swoją replikę usługi Active Directory i foldera Sysvol. Proces pobierania danych z serwerów będących partnerami replikacji przeprowadzany jest poprzez standardowe mechanizmy replikacji.

Czasami kontroler domeny, na którym zostały odtworzone dane, nie powinien być synchronizowany z pozostałymi działającymi kontrolerami domeny, a przeciwnie, wszystkie kontrolery domeny powinny mieć stan zgodny z odtworzoną repliką. Taka sytuacja ma miejsce, jeśli przykładowo obiekty zostały **usunięte w** usłudze Active Directory, a kontroler domeny odtwarzany jest na podstawie kopii utworzonej przed usunięciem obiektów. Wtedy trzeba przeprowadzić przywracanie autorytatywne, które zaznacza wybrane obiekty jako autorytatywne i wymusza ich replikację z odtworzonego kontrolera domeny do jego partnerów replikacji.

Aby wykonać przywracanie autorytatywne, należy najpierw za pomocą programu *Backup Utility* przeprowadzić przywracanie nieautorytatywne danych o stanie systemu kontrolera domeny. Po zakończeniu odtwarzania należy w programie *Backup Utility* (Kopia zapasowa) kliknąć przycisk **Close** (Zamknij), a program będzie podpowiadał ponowne uruchomienie komputera. W tym momencie należy odpowiedzieć NIE. Nie można zezwolić, aby kontroler domeny został ponownie uruchomiony. Należy otworzyć okno wiersza poleceń i używając programu Ntdsutil zaznaczyć całą przywracaną bazę

danych lub wybrane obiekt jako autorytatywne. Więcej informacji o programie Ntdsutil i przywracaniu autorytatywnym można uzyskać wpisując w wierszu poleceń **ntdsutil /?** lub korzystając z programu *Help And Support Center* (Centrum pomocy i obsługi technicznej). Szczegółowe omówienie procesu przywracania kontrolera domeny zawiera pozycja **MCSE Training Kit (Egzamin 70-294): Planowanie, wdrażanie i obsługa infrastruktury Active Directory Windows Server 2003**.

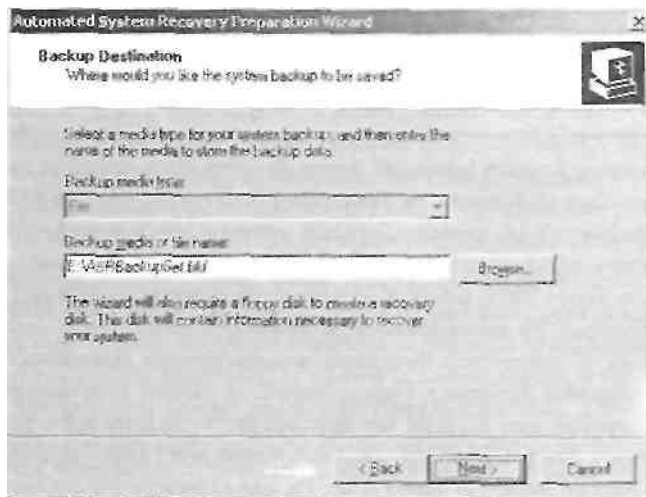


Wskazówka egzaminacyjna Najważniejsze informacje, o których warto pamiętać w kontekście egzaminu 70-290 to fakt, że dane o stanie systemu (System State) kontrolera domeny mogą być tylko przywracane poprzez uruchomienie kontrolera w trybie **Directory Services Restore Mode** (Tryb przywracania usług katalogowych). Warto także pamiętać, że za pomocą programu Ntdsutil przywracane zostają usunięte obiekty usługi Active Directory poprzez zaznaczenie tych obiektów jako autorytatywnych, przy czym wcześniej trzeba przeprowadzić przywracanie normalne lub nieautorytatywne danych o stanie systemu, przy użyciu programu Backup Utility (Kopia zapasowa).

Automated System Recovery (Automatyczne odzyskiwanie systemu)

Odtwarzanie uszkodzonego serwera jest zazwyczaj nużącym zajęciem, związanym z ponowną instalacją systemu operacyjnego, zainstalowaniem i uporządkowaniem taśm kopii zapasowych serwera, a następnie przeprowadzaniem pełnego przywracania systemu. Usługa automatycznego odzyskiwania systemu (ASR) znacznie upraszcza ten proces. Usługa wymaga utworzenia zestawu ASR, na który składają się najważniejsze pliki systemowe, rejestr oraz dyskietka zawierająca listę plików systemu Windows zainstalowanych na komputerze. W przypadku awarii serwera wystarczy po prostu uruchomić dysk CD-ROM systemu Windows Server 2003 i wybrać opcję **Automated System Recovery** (Automatyczne odzyskiwanie systemu). Proces korzysta z listy plików dysku ASR do odtworzenia z dysku CD-ROM standardowych sterowników i plików, a pozostałe pliki będzie odtwarzał na podstawie kopii zapasowej ASR.

Aby utworzyć zestaw ASR, należy uruchomić program **Backup Utility** (Kopia zapasowa) znajdujący się w grupie programów **Accessories** (Akcesoria) lub klikając menu **Start, Run** (Uruchom), a następnie wpisując polecenie **Ntbackup.exe**. Po wyświetleniu ekranu *Backup And Restore Wizard* (Kreator kopii zapasowych i przywracania) należy kliknąć opcję **Advanced Mode** (Tryb zaawansowany). Następnie w oknie programu należy wybrać przycisk **ASR Wizard** (Kreator automatycznego odzyskiwania systemu) lub w menu **Tools** (Narzędzia) wybrać polecenie **ASR Wizard**. Należy postępować zgodnie z instrukcjami programu kreatora przygotowania do automatycznego odzyskiwania. Procedura wymaga dyskietki 1.44 MB, aby na niej utworzyć dysk ASR. Okno programu Kreator ASR pokazane zostało na rysunku 13-2.



Rysunek 13-2 Strona *Backup Destination* (Miejsce docelowe kopii zapasowej) programu *ASR Wizard* (Kreator *ASR*)

Kopia zapasowa utworzona przez program kreatora ASR zawiera informacje o konfiguracji każdego dysku komputera, kopię zapasową danych o stanie systemu oraz kopię zapasową plików, w tym bufora sterownika. Zestaw kopii zapasowej może mieć pokaźne rozmiary. W przypadku standardowej instalacji systemu Windows Server 2003 wielkość kopii zapasowej ASR może przekroczyć 1 GB.

Dyskietka ASR zostaje utworzona przez program *Automated System Recovery Preparation Wizard* (Kreator przygotowania do automatycznego przywracania systemu) oraz jest ściśle związana z systemem i czasem, w którym zestaw ASR został utworzony. Dyskietka ASR oraz zestaw kopii zapasowej powinny być starannie oznaczone i przechowywane razem.

Dyskietka ASR zawiera dwa pliki katalogów: *Asr.sif* oraz *Asrnp.sif*. Jeśli komputer nie jest wyposażony w napęd dysków elastycznych, dyskietkę można utworzyć po uruchomieniu kreatora. Pliki te można skopiować z foldera `%Systemroot%\repair` do innego komputera, który ma napęd dyskietek i tam skopiować je na dyskietkę. Jeśli dyskietka ASR została zgubiona, pliki można odtworzyć z foldera `%Systemroot%\repair` zestawu kopii zapasowej ASR. Dyskietka ASR *jest potrzebna* do wykonania automatycznego odzyskiwania systemu, tak więc jeśli komputer nie ma napędu dyskietek, przed rozpoczęciem przywracania systemu trzeba podłączyć napęd dyskietek.

Wskazówka Zestaw ASR zawiera pliki potrzebne do uruchomienia systemu i nie jest kopią zapasową całego systemu. Dlatego, podczas tworzenia zestawu ASR zalecane jest utworzenie pełnej kopii zapasowej, wliczając w to dane o stanie systemu, wolumin systemowy, aplikacje, a być może także dane użytkownika.

Do przeprowadzenia automatycznego odzyskiwania systemu będzie potrzebny:

- Dysk instalacyjny CD-ROM systemu Windows Server 2003
- Zestaw kopii zapasowej ASR
- Dyskietka ASR utworzona w tym samym czasie, co zestaw kopii zapasowej ASR



Wskazówka Potrzebne będą również wszystkie sterowniki urządzeń pamięci masowej, które nie zostały umieszczone w standardowym zestawie sterowników systemu Windows Server 2003. Aby ułatwić proces odzyskiwania systemu, można skopiować te sterowniki na dyskietkę ASR.

Aby przywrócić system za pomocą funkcji *Automated System Recovery* (Automatyczne odzyskiwanie systemu), należy ponownie uruchomić komputer w oparciu o instalacyjny dysk CD-ROM systemu Windows Server 2003, dokładnie tak jak podczas instalacji systemu operacyjnego. Jeśli instalacja komputera wymaga sterowników urządzeń pamięci dyskowych, które nie są dołączane do zestawu sterowników systemu Windows Server 2003, należy w odpowiednim momencie nacisnąć F6 i wskazać sterownik umieszczony na dyskietce. Po zainstalowaniu początkowych sterowników, system podpowiada, że naciśnięcie przycisku F2 rozpocznie procedurę automatycznego odzyskiwania systemu. Po naciśnięciu F2 należy postępować zgodnie z wyświetlanymi na ekranie instrukcjami. Program zażąda dyskietki ARS, która zawiera dwa katalogi lub listy plików wymaganych do uruchomienia systemu. Pliki te są instalowane z dysku CD-ROM. Pozostałe ważne pliki, takie jak rejestr systemu, są odtwarzane na podstawie zestawu kopii zapasowej ARS. Po zainstalowaniu plików wymagane jest ponowne uruchomienie komputera i jeśli system wymaga dodatkowych sterowników pamięci dyskowych dostarczanych przez producenta, podczas drugiego uruchamiania należy ponownie nacisnąć F6. Ponieważ komputer jest ponownie uruchamiany, należy wyjąć z napędu dyskietkę lub tak zdefiniować kolejność rozruchu, aby nie było próby uruchomienia systemu z dyskietki.

Program Recovery Console (Konsola odzyskiwania)

Program *Recovery Console* (Konsola odzyskiwania) jest interpreterem poleceń trybu tekstowego, który umożliwia dostęp do dysku twardego komputera systemu Windows Server 2003 w celu wykonania podstawowych zadań związanych z rozwiązywaniem problemów i konserwacją systemu. Jest to szczególnie przydatne narzędzie, jeśli nie można uruchomić systemu operacyjnego. W takiej sytuacji program *Recovery Console* może być używany do zadań diagnostycznych, wyłączania napędów i usług, zastępowania plików i przeprowadzania innych procedur związanych z odzyskiwaniem systemu.

Instalowanie programu Recovery Console (Konsola odzyskiwania)

Program *Recovery Console* (Konsola odzyskiwania) może być uruchomiony podczas rozruchu systemu z dysku instalacyjnego CD-ROM systemu Windows Server 2003 poprzez naciśnięcie na klawiaturze R, co powoduje wybranie opcji naprawy i odzyskiwania. Jednakże w trakcie awarii systemu najczęściej administratorowi zależy, aby przywrócić system możliwie jak najszybciej i będzie chciał uniknąć straty czasu wynikającej z dość długiego rozruchu bazującego na instalacyjnym dysku CD-ROM. Dlatego zalecana jest inna metoda instalacji programu *Recovery Console*.

Aby zainstalować program *Recovery Console*, należy umieścić w napędzie instalacyjny dysk CD-ROM systemu Windows Server 2003 i wpisać w wierszu poleceń `<>f<>_C£>:\i386\winnt32/cmdcons`. Kreator instalacji zainstaluje konsolę w ukrytym folderze o nazwie `Cmdcons` (o wielkości 8 MB) i zmodyfikuje plik `boot.ini`, aby podczas rozruchu komputera pojawiała się opcja umożliwiająca uruchomienie programu *Recovery Console* (Konsola odzyskiwania).

Usuwanie programu Recovery Console

Jeśli użytkownik zdecyduje się usunąć konsolę odzyskiwania, musi usunąć pliki i foldery, które są skutecznie ukryte. W programie *Windows Explorer* (Eksplorator Windows) należy wybrać z menu **Tools** (Narzędzia) polecenie **Folder Options** (Opcje folderów). Następnie należy kliknąć zakładkę **View** (Widok), zaznaczyć opcje **Show Hidden Files** (Pokaż ukryte pliki i foldery), usunąć zaznaczenie opcji **Hide Protected Operating System Files** (Ukryj chronione pliki systemu operacyjnego), kliknąć przycisk **Yes** (Tak) dla potwierdzenia operacji, a na koniec kliknąć przycisk **OK**.

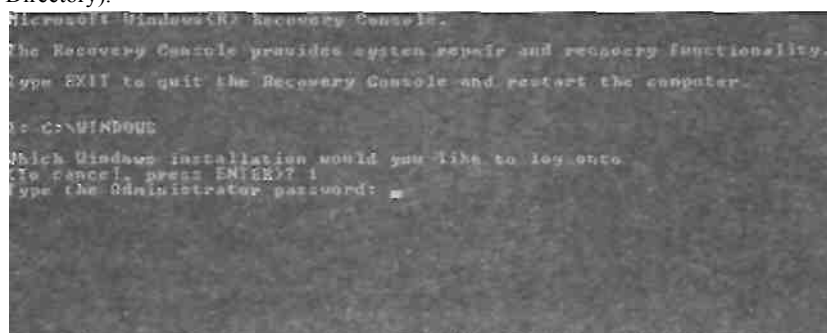
W kolejnym kroku należy usunąć folder *Cmdcons* i plik *Cmlldr*, które znajdują się w katalogu głównym dysku systemowego. Kolejnym krokiem jest usunięcie w pliku *Boot.ini* opcji rozruchowej programu *Recovery Console*. W tym celu należy uruchomić program *System* w folderze **Control Panel** (Panel sterowania), kliknąć zakładkę **Advanced** (Zaawansowane), w ramce *Startup And Recovery* (Uruchamianie i odzyskiwanie) kliknąć przycisk **Settings** (Ustawienia), a następnie w uruchomionym oknie dialogowym, w ramce *System Startup* (Uruchamianie systemu) należy nacisnąć przycisk **Edit** (Edytuj). Plik *Boot.ini* zostanie wyświetlony w oknie programu *Notepad* (Notatnik). Należy usunąć wpis dotyczący konsoli odzyskiwania, który będzie podobny do przedstawionego poniżej:

`c:\cmdcons\bootsect.dat="Microsoft Windows Recovery Console"/cmdcons` Po modyfikacji należy zapisać i zamknąć plik *Boot.ini*.

Korzystanie z programu Recovery Console (Konsola odzyskiwania)

Po zainstalowaniu programu *Recovery Console* (Konsola odzyskiwania) użytkownik może uruchomić komputer i z menu rozruchowego może wybrać polecenie uruchomienia konsoli. Jeśli konsola nie została zainstalowana lub jeśli nie uruchomiła się poprawnie, należy uruchomić komputer w oparciu o dysk CD-ROM systemu Windows Server 2003 i na powitalnym ekranie instalatora nacisnąć **R**, aby wybrać opcję **Repair** (Naprawa). Uruchamianie programu z dysku CD-ROM jest znacznie dłuższe, ale sam program *Recovery Console* (Konsola odzyskiwania) jest identyczny w porównaniu z programem zainstalowanym na systemie lokalnym.

Po uruchomieniu konsoli odzyskiwania (okno konsoli zostało pokazane na rysunku 13-3) użytkownik będzie poproszony o wybranie instalacji systemu Windows, w której będzie się logował oraz do wprowadzenia hasła administratora. Należy używać hasła konta administratora lokalnego, które zostało określone dla kontrolera domeny na stronie *Directory Services Restore Mode Password* (Hasło trybu przywracania usługi Active Directory) w programie *Active Directory Installation Wizard* (Kreator instalacji usługi Active Directory).



Rysunek 13-3 Program *Recovery Console* (Konsola odzyskiwania)

•

Wpisanie polecenia **help** po znaku zachęty konsoli spowoduje wyświetlenie listy dostępnych poleceń programu. Wprowadzone polecenie **help** wraz z nazwą komendy wyświetli informacje dotyczące konkretnego polecenia. Większość poleceń to standardowe polecenia środowiska wiersza poleceń, jednak kilka z nich wymaga zwrócenia szczególnej uwagi:

- **Listsvc** Wyświetlone zostają usługi i sterowniki, jak również ich ustawienia początkowe wymienione w rejestrze. Jest to przydatna funkcja, pozwalająca poznać skrótową nazwę usługi lub sterownika, zanim zastosowane zostanie polecenie **Enable** lub **Disable**.
- **Enable/Disable** Polecenie kontroluje status usługi lub sterownika po włączeniu komputera. Jeśli usługa lub sterownik uniemożliwia poprawne uruchomienie systemu operacyjnego, można użyć polecenia **Disable** programu *Recovery ConsoU* do wyłączenia komponentu, co pozwala po ponownym uruchomieniu komputera naprawić lub odinstalować komponent.
- **Diskpart** Polecenie umożliwia utworzenie lub usunięcie partycji za pomocą interfejsu podobnego do prezentowanego w części tekstowej programu instalacyjnego. W następnym kroku można korzystać z polecenia **Format** do skonfigurowania systemu plików wybranej partycji.
- **Bootcfg** Polecenie umożliwia zarządzanie rozruchowym menu komputera.

Program *Recovery ConsoU* (Konsola odzyskiwania) ma kilka ograniczeń wynikających z przyjętego poziomu zabezpieczeń. Ograniczenia te mogą być modyfikowane poprzez połączenie działania zmiennych środowiska programu konsoli oraz różnych zasad komputera lokalnego. Zasady te umieszczone są w węźle *Computer Configuration* (Konfiguracja komputera), *Windows Settings* (Ustawienia systemu), *Security Settings* (Ustawienia zabezpieczeń), *Local Policies* (Zasady lokalne), *Security Options* (Opcje zabezpieczeń).

- **Directory access** (Dostęp do katalogu) Użytkownik może przeglądać jedynie pliki katalogu głównego, w folderach `%Windir%` oraz `\Cmdcons`. Ograniczenie to można wyłączyć poprzez ustawienia zasady *Allow Floppy Copy And Access To Ali Drives And Ali Folders* (Zezwalaj na kopiowanie na dyskietkę oraz dostęp do wszystkich dysków i folderów) i polecenie **set AliowAllPaths = true**. Należy pamiętać, aby w poleceniu umieścić znak spacji przed i po znaku równości.
- **File copy** (Kopiowanie pliku) Użytkownik może jedynie kopiować pliki na lokalny dysk twardy. Kopiowanie plików z lokalnego dysku jest zabronione. Ograniczenie to można wyłączać za pomocą
 - zasady opisanej powyżej i polecenia **set AllowRemovableMedia = true**. Należy pamiętać, aby w poleceniu umieścić znak spacji przed i po znaku równości.
- **Wild cards** (Znaki zastępcze) Do usuwania plików użytkownik nie może wykorzystywać znaków zastępczych takich jak gwiazdka. Należy wprowadzić zasadę opisaną na poprzedniej stronie, a następnie w programie *Recovery Console* (Konsola odzyskiwania) wpisać polecenie **set AllowWildCards = true**. Należy pamiętać, aby w poleceniu umieścić znak spacji przed i po znaku równości.

Zadanie kontrolne: Przywracanie systemu po awarii

W zadaniu tym wykonana zostanie kopia zapasowa danych o stanie systemu (System State) oraz utworzony zostanie zestaw kopii zapasowej ASR (Automated System Recovery). Zainstalowany i wykorzystywany będzie również program *Recovery Console* (Konsola odzyskiwania) — do rozwiązywania problemów uszkodzonego sterownika lub usługi. Ostatnim zadaniem, o ile dysponujemy drugim dyskiem fizycznym, będzie uruchomienie funkcji *Automated System Recovery* (Automatyczne odzyskiwanie systemu) w celu przywrócenia uszkodzonego serwera.

Ćwiczenie 1: Wykonanie kopii zapasowej danych o stanie systemu (System State)

1. W komputerze Server01 zaloguj się jako administrator.
2. Uruchom program *Backup Utility* (Kopia zapasowa).
3. Jeśli wyświetlone zostaje okno *Backup And Restore Wizard* (Kreator kopii zapasowych lub przywracania), kliknij opcję **Advanced Mode** (Tryb zaawansowany).
4. Kliknij zakładkę **Backup** (Kopia zapasowa) i zaznacz pole wyboru obok foldera **System State**. Oprócz tego kliknij etykietę *System State*, aby w oknie szczegółów wyświetlić elementy foldera System State.
5. Wpisz nazwę pliku kopii zapasowej, na przykład C:\SystemState.bkf.
6. Uruchom tworzenie kopii zapasowej.
7. Po zakończeniu sprawdź wielkość pliku kopii zapasowej danych o stanie systemu (System State). Jakiej wielkości jest plik?

Ćwiczenie 2: Tworzenie zestawu ASR

Do przeprowadzenia ćwiczenia potrzebna będzie czysta dyskietka oraz około 1.5 GB wolnej przestrzeni dyskowej. Jeśli komputer Server01 wyposażony jest w drugi dysk fizyczny, należy kopię zapasową zapisać na tym właśnie dysku, aby w ćwiczeniu 4 możliwe było przeprowadzenie operacji automatycznego odzyskiwania systemu.

1. Uruchom program *Backup Utility* (Kopia zapasowa). Jeśli wyświetlone zostaje okno *Backup And Restore Wizard* (Kreator kopii zapasowych lub przywracania), kliknij opcję **Advanced Mode** (Tryb zaawansowany).
2. Kliknij przycisk **Automated System Recovery Wizard** (Kreator automatycznego odzyskiwania systemu) lub w menu **Tools** (Narzędzia) wybierz polecenie **ASR Wizard** (Kreator ASR).
- 3- Postępując zgodnie z instrukcjami wykonaj kopię zapasową do pliku nazwanego ASRBackup.bkf na dysku C lub jeśli dysponujemy drugim dyskiem fizycznym, na tym właśnie woluminie.
4. Po zakończeniu tworzenia kopii sprawdź wielkość pliku ASRBackup.bkf. Czy plik jest duży? Jaka jest wielkość tego pliku w porównaniu do kopii zapasowej danych o stanie systemu?

Ćwiczenie 3: Instalowanie i wykorzystywanie programu Recovery Console (Konsola odzyskiwania)

1. W napędzie umieść dysk systemu Windows Server 2003.
2. Kliknij menu Start, następnie Run (Uruchom) i w polu tekstowym wpisz następujące polecenie:
D: \i386\winnt32.exe/cmdcons
gdzie D: jest literą dysku napędu CD-ROM. Program *Recovery Console* (Konsola odzyskiwania) zostanie zainstalowany na lokalnym dysku twardym.
- 3- Aby zasymulować wystąpienie problemu dotyczącego usługi, w grupie programów **Administrative Tools** (Narzędzia administracyjne) otwórz konsolę Senders (Usługi). Wyszukaj usługę *Messenger* (Poślaniec). Dwukrotnie kliknij tę usługę i w ramce *Startup Type* (Typ uruchomienia) wybierz opcję **Automatic** (Automatyczny).
4. Ponownie uruchom serwer.

MCSE Training Kit: Egzamin 70-290

5. Podczas uruchamiania komputera z menu rozruchowego wybierz uruchomienie opcję **Microsoft Windows Recovery Console** (Konsola odzyskiwania).
6. Wpisz 1, aby wybrać instalację systemu Windows Server 2003-
7. Wpisz hasło konta administratora lokalnego.
8. Po wyświetleniu znaku zachęty (domyślnie jest to: C:\Windows>) programu *Recovery Console* wpisz **help**, aby wyświetlić listę poleceń.
9. Wpisz polecenie **listsvc**, aby wyświetlić listę usług i sterowników. Warto zapamiętać, że skróty nazw wielu usług są zupełnie inne niż pełne nazwy tych usług. W przypadku usługi *Messenger* (Posłaniec) skrót nazwy usługi jest taki sam, jak sama nazwa usługi. Sprawdź, czy typ uruchomienia usługi ustawiony jest jako Automatic (Automatyczny).
10. Wpisz polecenie **disable messenger**, aby wyłączyć usługę. Komunikat wyjściowy polecenia wskazuje powodzenie przeprowadzenia operacji dotyczącej polecenia i pierwotnej konfiguracji uruchomieniowej (w tym przypadku SERVICE_AUTO_START). Zawsze należy zanotować takie ustawienia, ponieważ po zakończeniu rozwiązywania problemów można będzie powrócić do pierwotnego stanu.
11. Aby zamknąć program *Recovery Console*, wpisz **exit** i naciśnij ENTER.

Ćwiczenie 4: Przywracanie systemu za pomocą usługi Automated System Recovery (automatyczne odzyskiwanie systemu)



Ostrzeżenie W trakcie tego ćwiczenia potrzebny będzie drugi dysk fizyczny, na którym zapisana została kopia zapasowa ASR wykonywana podczas ćwiczenia 2. Podczas tego ćwiczenia usuwane będą wszystkie dane dysku fizycznego, który zawiera partycję systemową i rozruchową. Jeśli dysk taki zawiera istotne informacje, nie należy wykonywać tego ćwiczenia.

1. Wyłącz zasilanie komputera.
2. Uruchom ponownie komputer i otwórz program BIOS. Upewnij się, że uruchomienie systemu będzie następowało z dysku CD-ROM.
3. Umieść w napędzie dysk instalacyjny systemu Windows Server 2003.
4. Ponownie uruchom komputer Server01. Na klawiaturze naciśnij odpowiedni przycisk, aby system uruchomił się z dysku CD-ROM.
5. W trakcie fazy tekstowego trybu instalacji, program podpowiada naciśnięcie klawisza F2 w celu uruchomienia funkcji *Automatic System Recovery* (Automatyczne odzyskiwanie systemu).
Naciśnij F2.
6. Program zażąda dyskietki ASR. Włóż dyskietkę utworzoną w trakcie ćwiczenia 2 i naciśnij dowolny klawisz, aby kontynuować operację.
7. Zostanie uruchomiony program instalacyjny trybu tekstowego dla usługi ASR (Automated System Recovery) oraz minimalna wersja systemu operacyjnego. Zakończenie tego etapu trwa dłuższą chwilę.
8. Na koniec procesu wyświetlony zostanie ekran programu instalacji systemu Windows Server 2003.

9. Program instalacyjny systemu Windows Server 2003 tworzy partycje i formatuje dyski, kopiuje pliki, określa początkową konfigurację systemu Windows i przygotowuje *system* do ponownego uruchomienia.
10. Usunąć z napędu dyskietkę i uruchomić ponownie komputer.
Instalacja będzie kontynuowana. Po jej zakończeniu powinien zostać przywrócony poprzedni stan komputera.

Pytania

Przedstawione poniżej pytania mają za zadanie ugruntować podstawowe informacje prezentowane podczas lekcji. Jeśli czytelnik nie potrafi udzielić odpowiedzi, powinien ponownie przejrzeć materiał lekcji i powrócić jeszcze raz do pytań. Odpowiedzi na te pytania można znaleźć w sekcji „Pytania i odpowiedzi”, znajdującej się pod koniec tego rozdziału.

1. Określany jest zestaw kopii zapasowej w systemie Windows Server 2003. Należy skopiować rejestr, pliki rozruchowe i bazę danych COM+ Class Registration. Którą opcję kopii zapasowej należy wybrać?
 - a. %Windir%
 - b. %Systemroot%
 - c. System State
 - d. Żadna z powyższych. Nie można utworzyć kopii zapasowej rejestru.
2. Użytkownik instalował skaner na komputerze działającym pod kontrolą systemu Windows Server 2003. Po instalacji system operacyjny nie uruchomił się ponownie. Która z wymienionych poniżej metod odzyskiwania systemu będzie najmniej inwazyjna i należy ją zastosować w pierwszej kolejności?
 - a. Automated System Recovery (Automatyczne odzyskiwanie systemu)
 - b. Recovery Console (Konsola odzyskiwania)
 - c. Safe mode (Tryb awaryjny)
 - d. Tryb Directory Services Restore (Odzyskiwanie usług katalogu)
- 3- Uszkodzony został dysk twardy systemu Windows Server 2003. Administrator wymienił dysk, uruchomił ponownie system, zainicjował dysk i na nowym dysku utworzył wolumin NTFS. Ostatnim zadaniem jest odtworzenie danych na podstawie ostatniej kopii zapasowej starego dysku. W jaki sposób należy odzyskać dane?
 - a. Do skopiowania danych na dysk należy użyć programu Recovery Console (Konsola odzyskiwania).
 - b. Należy użyć narzędzia Backup (Kopia zapasowa) do uruchomienia programu Restore Wizard (Kreator przywracania).
 - c. Do odzyskania danych należy użyć kopii zapasowej ASR.
 - d. Należy zastosować opcję Last Known Good Configuration (Ostatnia znana dobra konfiguracja) trybu Safe (Tryb awaryjny) do skonfigurowania nowego dysku.
4. Serwer plików w sieci przestał się uruchamiać. Po wyczerpaniu innych metod, administrator do przywrócenia systemu zdecydował się zastosować usługę ASR (Automated System Recovery). Admini-

strator dysponuje dwoma kopiami zapasowymi ASR - jedna wykonana zaraz po instalacji nowego systemu Microsoft Windows Server 2003 oraz druga wykonana dwa miesiące później, po instalacji sterownika urządzenia. Pełna kopia zapasowa wykonywana jest raz na tydzień. Co zostanie odtworzone za pomocą usługi ASR? (wybierz wszystkie właściwe odpowiedzi)

- a. Plik danych sprzed dwóch miesięcy
- b. Plik danych ostatniej kopii zapasowej
- c. Konfigurację dysku
- d. System operacyjny
- e. Dane o stanie systemu (System State) sprzed dwóch miesięcy
- f. Dane o stanie systemu (System State) z okresu ostatniej kopii zapasowej

Posumowanie lekcji

- Dane o stanie systemu (System State) zawierają rejestr, pliki rozruchowe, bazę danych COM+ Class Registration oraz inne ważne pliki dotyczące specyficznych usług. Zalecaną praktyką jest planowanie wykonywania kopii zapasowych, które uwzględniają kopiowanie danych o stanie systemu razem z woluminem systemowym i rozruchowym.
- Usługa ASR (Automated System Recovery) korzysta z procesu podobnego do instalacji systemu, aby przywrócić działanie komputera, a następnie uruchamia procedury odzyskiwania, aby odtworzyć pliki na podstawie zestawu kopii zapasowej ASR. Ten proces przywracania systemu powinien być używany, jeśli zawiodły inne, mniej inwazyjne metody, takie jak tryb awaryjny (Safe) lub program *Recotierey Console* (Konsola odzyskiwania).
- Program *Recovery Console* (Konsola odzyskiwania) jest interpreterem poleceń trybu tekstowego, który umożliwia dostęp do dysku twardego komputera działającego pod kontrolą systemu Windows Server 2003.

Informacje dla zdających egzamin

Przed przystąpieniem do egzaminu należy zapoznać się z przedstawionymi poniżej najważniejszymi faktami i pojęciami, aby określić które tematy wymagają pogłębienia. Należy powrócić do lekcji, aby osiągnąć większą wprawę oraz przejrzeć działy znajdujące się w części 2 — „Materiały dodatkowe”. Informacje tu zawarte kierują do materiałów uzupełniających tematy objęte zadaniami egzaminacyjnymi.

Najważniejsze fakty

- Dane o stanie systemu (System State) mogą być archiwizowane za pomocą programu *Backup Utility* (Kopia zapasowa) lub przy użyciu wiersza poleceń. Wykonywana może być tylko kopia danych o stanie systemu komputera lokalnego, natomiast nic nie jest możliwe zdalne wykonywanie takiej kopii. Istnieje jednak możliwość wykonania kopii zapasowej danych o stanie systemu lokalnego do pliku umieszczonego na komputerze zdalnym, a następnie przesłanie tego pliku na inne medium kopii zapasowej.
- Aby przywrócić dane o stanie systemu (System State) kontrolera domeny, należy uruchomić komputer w trybie *Directory Services Restore* (Przywracanie usług katalogowych). Zestaw danych o stanie

systemu zawiera informacje o usłudze Active Directory. Wykonując odtworzenie danych o stanie systemu (System State) kontrolera domeny, użytkownik wykonuje przywracanie nieautorytatywne, a następnie kontroler domeny będzie wykorzystywał standardowe metody replikacji do aktualizacji swojej bazy. Jeśli w przywróconych danych znajdują się obiekty, które użytkownik chce replikować do innych kontrolerów domeny, musi użyć programu **Ntdsutil**, aby przeprowadzić przywracanie autorytatywne, zanim kontroler domeny zostanie uruchomiony w normalnym trybie.

- Podczas przywracania plików z dysku CD-ROM systemu Windows Server 2003 usługa ASR (Automated System Recovery) bazuje na liście plików systemowych przechowywanych na dyskiecie ASR oraz na pełnej kopii zapasowej ASR. Zestaw kopii zapasowej ASR oraz dyskietka ASR jest przygotowana za pomocą narzędzia *ASR Wizard* (Kreator automatycznego przywracania systemu), które jest częścią programu *Backup Utility* (Kopia zapasowa). Aby wykonać automatyczne odzyskiwanie systemu, należy uruchomić komputer z dysku CD-ROM systemu Windows Server 2003, a następnie w odpowiednim momencie nacisnąć klawisz F2.
- * Program *Recovery Console* (Konsola odzyskiwania) umożliwia wykonanie napraw niektórych awarii systemu. Za pomocą tego programu można zastępować pliki systemowe, wyłączać nieprawidłowo działające usługi lub sterowniki, a także wykonywać inne zadania związane z konserwacją systemu. Konsola odzyskiwania może być uruchamiana z dysku CD-ROM systemu Windows Server 2003 CD lub poprzez zainstalowanie na dysku twardym serwera za pomocą polecenia **winnt32 /cmdcons**.

Najważniejsze pojęcia

System State Zestaw istotnych dla systemu komponentów wliczając W to rejestr, bazę danych COM+ Class Registration oraz pliki rozruchowe. Komponenty danych o stanie systemu (System State) mogą być archiwizowane za pomocą programu Backup Utility (Kopia zapasowa) lub polecenia Nibackup. Komponenty te nie mogą być archiwizowane oddzielnie.

Automated System Recovery (ASR) Jest to nowa cecha, która zastąpiła proces Emergency Repair obsługiwany przez wcześniejsze wersje systemu Windows. Usługa automatycznego odzyskiwania systemu (ASR) przywraca działanie systemu poprzez ponowne zainstalowanie systemu operacyjnego i odtworzenie danych o stanie systemu (System State) na podstawie zestawu kopii zapasowej ASR.

Recovery Console Program Konsola odzyskiwania jest narzędziem, które umożliwia dostęp do plików systemu z okna wiersza poleceń oraz udostępnia zestaw poleceń, za pomocą których można przeprowadzać precyzyjne naprawy uszkodzonego systemu.

Pytania i odpowiedzi

495 Pytania do lekcji 1

1. Określany jest zestaw kopii zapasowej w systemie Windows Server 2003. Należy skopiować rejestr, pliki rozruchowe i bazę danych COM+ Class Registration. Którą opcję kopii zapasowej należy wybrać?
 - a. `%Windir%`
 - b. `%Systemroot%`

- c. System State
 - d. Żadna z powyższych. Nie można utworzyć kopii zapasowej rejestru.
- Prawidłowa odpowiedź to c.

2. Użytkownik instalował skaner na komputerze działającym pod kontrolą systemu Windows Server 2003. Po instalacji system operacyjny nie uruchomił się ponownie. Która z wymienionych poniżej metod odzyskiwania systemu będzie najmniej inwazyjna i należy ją zastosować w pierwszej kolejności?
- a. Automated System Recovery (Automatyczne odzyskiwanie systemu)
 - b. Recovery Console (Konsola odzyskiwania)
 - c. Safe mode (Tryb awaryjny)
 - d. Tryb Directory Services Restore (Odzyskiwanie usług katalogu)

Prawidłowa odpowiedź to c.

3. Uszkodzony został dysk twardy systemu Windows Server 2003- Administrator wymienił dysk, uruchomił ponownie system, zainicjował dysk i na nowym dysku utworzył wolumin NTFS. Ostatnim zadaniem jest odtworzenie danych na podstawie ostatniej kopii zapasowej starego dysku. W jaki sposób należy odzyskać dane?
- a. Do skopiowania danych na dysk należy użyć programu Recovery Console (Konsola odzyskiwania).
 - b. Należy użyć narzędzia Backup (Kopia zapasowa) do uruchomienia programu Restore Wizard (Kreator przywracania).
 - c. Do odzyskania danych należy użyć kopii zapasowej ASR.
 - d. Należy zastosować opcję Last Known Good Configuration (Ostatnia znana dobra konfiguracja) trybu Safe (Tryb awaryjny) do skonfigurowania nowego dysku.

Prawidłowa odpowiedź to b.

4. Serwer plików w sieci przestał się uruchamiać. Po wyczerpaniu innych metod, administrator do przywrócenia systemu zdecydował się zastosować usługę ASR (Automated System Recovery). Administrator dysponuje dwoma kopiami zapasowymi ASR — jedna wykonana zaraz po instalacji nowego systemu Microsoft Windows Server 2003 oraz druga wykonana dwa miesiące później, po instalacji sterownika urządzenia. Pełna kopia zapasowa wykonywana jest raz na tydzień. Co zostanie odtworzone za pomocą usługi ASR? (wybierz wszystkie właściwe odpowiedzi)
- a. Plik danych sprzed dwóch miesięcy
 - b. Plik danych ostatniej kopii zapasowej
 - c. Konfigurację dysku
 - d. System operacyjny
 - e. Dane o stanie systemu (System State) sprzed dwóch miesięcy
 - f. Dane o stanie systemu (System State) z okresu ostatniej kopii zapasowej

Prawidłowe odpowiedzi to c, d oraz e.

Część II

Przygotowanie do egzaminu



L4 Zarządzanie oraz konserwacja fizycznych i logicznych urządzeń (1.0)



Podstawowe zadanie administratora systemu to prawidłowe zarządzanie i konserwacja fizycznych oraz logicznych urządzeń serwera. Najczęściej przyłączanymi fizycznymi urządzeniami sprzętowymi są: karty sieciowe, karty grafiki i dyski twarde SCSI. Urządzenia logiczne są tworzone przez system operacyjny, a przykładami urządzeń logicznych mogą być partycje, woluminy czy dyski rozłożone.

Konsola zarządzania dyskami umożliwia administratorowi zarządzanie oraz konserwację fizycznych i logicznych dysków systemu Microsoft Windows Server 2003. Konsolę tę można odszukać jako węzeł innej konsoli - *Computer Management* (Zarządzanie komputerem) lub używać jej jako odrębnej konsoli poprzez dodanie odpowiedniej przystawki niestandardowej konsoli MMC (Microsoft Management Console). Konsola zarządzania dyskami umożliwia administratorowi systemu przekształcanie dysków podstawowych na dynamiczne, formatowanie dysków za pomocą systemów plików NTFS, FAT lub FAT32, rozszerzanie woluminów na kilka dysków, konfigurowanie dublowania dysków, jak również instalowanie woluminów rozłożonych i RAID-5-

Wraz z upływem czasu fragmentacja dysku powoduje spadek wydajności nawet najszybszych dysków twardych. Powodem fragmentacji jest dodawanie i usuwanie plików na dysku. Na nowym dysku zapisywane pliki zajmują ciągłą przestrzeń. Jeśli na dysku jest dużo usuwanych i dodawanych plików, pliki zapisywane są we wszystkich dostępnych miejscach na dysku, często w obszarach, które ze sobą nie sąsiadują. Plik przechowywany w kilku różnych obszarach dysku twardego nazywany jest plikiem, który uległ fragmentacji. Odczyt takiego pliku trwa dłużej niż pliku zapisanego na ciągłym obszarze dysku. Proces defragmentacji porządkuje pliki dysku twardego tak, aby były zapisane na ciągłych obszarach dysku. Program defragmentujący uruchamiany jest w węźle konsoli *Computer Management* (Zarządzanie komputerem), jako niestandardowa przystawka MMC lub za pomocą programu narzędziowego wiersza poleceń Defrag.

Program *DeviceManager* (Menedżer urządzeń) umożliwia administratorowi systemu zarządzanie i konfigurację innych urządzeń sprzętu. Nową i ważną cechą systemu Windows Server 2003 jest możliwość przywracania poprzedniej, prawidłowo funkcjonującej w'crsji sterownika. We wcześniejszych wersjach systemu usunięcie nieprawidłowo działającego sterownika było bardzo trudne. Trudne było również zainstalowanie starszego sterownika w miejsce nowszego, który okazał się niestabilny. Program *Device Manager* (Menedżer urządzeń) może być także używany do sprawdzania, jakie zasoby wykorzystują poszczególne urządzenia oraz do rozwiązywania konfliktów zainstalowanych urządzeń.

Sprawdzanie umiejętności i sugerowane ćwiczenia praktyczne

Poniżej przedstawiono umiejętności potrzebne do opanowania tematu „Zarządzanie i obsługa dostępu do zasobów” objętego egzaminem 70-290 -Zarządzanie i obsługa środowiska Window Server2003'-

- Prawidłowe przekształcanie dysków podstawowych na dynamiczne oraz prawidłowa instalacja woluminów
 - » Zadanie kontrolne 1: Dodanie drugiego dysku twardego do systemu Windows Server 2003. Przekształcenie tego dysku z podstawowego na dynamiczny za pomocą programu *Disk Initialization and Configuration Wizard* (Kreator konfiguracji i inicjowania dysku) lub przy użyciu odpowiedniej opcji *menu Action* (Akcja).
 - » Zadanie kontrolne 2: Utworzenie trzech pustych folderów na woluminie System — Templ, Temp2 oraz Temp3. Utworzenie trzech jednakowej wielkości woluminów na nowym dynamicznym drugim dysku fizycznym. Sformatowanie woluminów za pomocą systemu NTFS i zainstalowanie na pierwszym woluminie foldera Templ, na drugim foldera Temp2, a na trzecim foldera Temp3-
- Monitorowanie urządzeń sprzętu serwera za pomocą programu *Device Manager* (Menedżer urządzeń) i innych narzędzi
 - » Zadanie kontrolne 1: Wyszukiwanie urządzeń niezgodnych z trybem Plug and Play poprzez przeglądanie właściwości urządzenia w programie *Device Manager* (Menedżer urządzeń) i zaznaczenie opcji *Show Hidden Devices* (Pokaż ukryte urządzenia). Warto zapamiętać, że w zależności od tego, czy włączona lub wyłączona jest opcja *Show Hidden Devices* (Pokaż ukryte urządzenia) wyświetlana jest inna lista urządzeń.
 - » Zadanie kontrolne 2: Wykorzystanie programu *Device Manager* (Menedżer urządzeń) do wydrukowania raportu - najpierw raportu dotyczącego poszczególnych klasy urządzeń systemu, a następnie raportu o wszystkich urządzeniach zainstalowanych w systemie Windows Server 2003-
- Prawidłowa optymalizacja wydajności dysku
 - » Zadanie kontrolne 1: Dodanie drugiego dysku fizycznego do systemu Window Server 2003 tak, aby w systemie były zainstalowane dwa dyski. Za pomocą menedżera dysków należy utworzyć systemowy wolumin dublowany. Po zakończeniu synchronizacji woluminu należy przerwać dublowanie i sprawdzić zawartość nowego dysku fizycznego.
 - » Zadanie kontrolne 2: Dodanie trzech dodatkowych dysków fizycznych do systemu Windows Server 2003 tak, aby w systemie były zainstalowane cztery dyski. Utworzenie woluminu RAID-5 w oparciu o nowe dyski.
 - » Zadanie kontrolne 3: Analiza i defragmentacja każdego woluminu systemu Windows Server 2003. Podczas analizy, należy zwrócić uwagę, jakimi kolorami oznaczane są poszczególne typy plików. Przeprowadzenie defragmentacji woluminu i porównanie różnic kolorów, służących do oznaczania dysków, wyświetlanych przez program analizujący wolumin.
- Prawidłowa instalacja i konfiguracja urządzeń sprzętu serwera
 - » Zadanie kontrolne 1: Wyszukanie urządzeń, które mogą być zainstalowane w skonfigurowanym systemie Window Server 2003- Przykładem może być kolejna karta sieciowa komputera. Należy wyłączyć komputer i zainstalować kartę. Po ponownym uruchomieniu komputera należa¹

przeprowadzić cały proces instalacji sterownika i konfiguracji karty tak, aby mogła prawidłowo funkcjonować w sieci.

- » Zadanie kontrolne 2: Wykorzystanie programu *Device Manager* (Menedżer urządzeń) do przeglądania listy zainstalowanych elementów systemu, uporządkowanej według zasobów wykorzystywanych przez te urządzenia.

Lektura uzupełniająca

Przed przystąpieniem do egzaminu należy przestudiować przedstawione poniżej dodatkowe źródła informacji.

Zadanie 1.1

Rozdział 11, lekcje 1, 2 oraz 3: „Omówienie opcji dotyczących pamięci dyskowych”, „Konfigurowanie dysków i woluminów” oraz „Obsługa woluminów pamięci dyskowej”. Rozdział ten opisuje szczegółowo zarządzanie i konfigurację opcji dotyczących pamięci dyskowych systemu Windows Server 2003.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat „Konwertowanie dysku podstawowego na dynamiczny”.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat „Inicjowanie nowych dysków”.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat „Zarządzanie dyskami”.

Zadanie 1.2

Rozdział 12, „Monitorowanie systemu Microsoft Windows Server 2003”. Rozdział ten dokonuje przeglądu kilku narzędzi, które mogą być używane do monitorowania różnych aspektów systemu operacyjnego Windows Server 2003.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat „Przeglądanie przydziałów energii dla koncentratorów USB”.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat „Przeglądanie przydziałów przepustowości dla kontrolera hosta USB”.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat „Drukowanie informacji o określonym urządzeniu”.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat „Przeglądanie ukrytych urządzeń”.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat „Menedżer urządzeń”.

Zadanie 1.3

Rozdział 11, lekcja 4, „Implementacja macierzy dyskowych RAID”. Rozdział ten przedstawia szczegółowo sposoby wdrożenia programowych macierzy RAID w systemie Windows Server 2003.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat „Defragmentator dysku”.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat „Zarządzanie dyskami”.

Zadanie 1.4

Rozdział 10, lekcje 1 oraz 2: „Instalowanie urządzeń sprzętu i sterowników” oraz „Konfigurowanie urządzeń sprzętu i sterowników”. Lekcje te dokonują przeglądu zagadnień i procesów, z których administrator powinien zdawać sobie sprawę podczas instalowania i konfigurowania urządzeń sprzętu.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat „Podpisywanie sterowników”.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat „Menedżer urządzeń”.

Zadanie 1.1

Zarządzanie dyskami podstawowymi i dynamicznymi

Różnice pomiędzy dyskami fizycznymi a dynamicznymi mają bezpośredni związek z opcjami zarządzania pamięciami dyskowymi serwera dostępnymi dla administratora. Dyski dynamiczne udostępniają więcej opcji niż dyski podstawowe. Dyski dynamiczne mogą być wykorzystywane do zbudowania woluminów dublowanych (RAID-1), dysków łączonych, woluminów rozłożonych (RAID-0) oraz woluminów RAID-5. Dyski podstawowe mogą zostać skonfigurowane jedynie jako proste lub rozszerzone partycje.

Zarządzanie dyskami może być wykonywane w dwojaki sposób — poprzez konsolę zarządzania dyskami lub poprzez interfejs wiersza poleceń. Obie metody mogą być wykorzystywane do konwersji dysku podstawowego na dynamiczny lub odwrotnie.

Po zainstalowaniu nowego dysku w serwerze automatycznie uruchamiany jest program *Initialize And Convert Disk Wizard* (Kreator inicjowania i konwersji dysku). Program ten może być używany do inicjowania dysku twardego i konwersji dysku podstawowego na dynamiczny.

Konwersję dysku podstawowego na dynamiczny lub dysku dynamicznego na podstawowy mogą przeprowadzać jedynie użytkownicy posiadający uprawnienia administracyjne oraz członkowie grupy Backup Operators (Operatorzy kopii zapasowych).

Wszystkie dyski mogą być przekształcane z podstawowych na dynamiczne. Jeśli na dysku podstawowym znajdują się dane, to na taki dysk nie można rozciągnąć innego dysku, tak jak jest to możliwe w przypadku rodzimych dysków dynamicznych. Jednakże dysk, który został przekształcony na dynamiczny, może być dublowany, co oznacza, że wolumin systemu operacyjnego może być odporny na uszkodzenia.

Jeśli serwer ma zainstalowanych kilka systemów operacyjnych, administrator nie powinien przekształcać partycji systemowej lub rozruchowej na dyski dynamiczne. Przekształcenie takie oznacza, że serwer będzie mógł być uruchomiony tylko w oparciu o system, przy użyciu którego konwersja została wykonana.

Inna ważna metoda zarządzania dyskami twardymi to wykorzystywanie sprzętowej macierzy RAID. Sprzętowe kontrolery RAID obsługują wiele dysków twardych i kontrolują procesy macierzy RAID. Kontrolery sprzętowe są zazwyczaj znacznie szybsze niż programowe rozwiązania RAID, takie jak zastosowane w systemie Windows Server 2003. Oprócz tego, sprzętowe kontrolery obsługują większą liczbę konfiguracji macierzy RAID niż oprogramowanie systemu Windows Server 2003-

Instalowanie (montowanie) woluminu powoduje przyłączenie foldera umieszczonego na innym woluminie. Wolumin zainstalowany może być utrzymywany na dysku podstawowym lub dynamicznym. Poprzez zainstalowanie woluminu w ścieżce foldera można zwiększać jego pojemność ponad rzeczywistą pojemność fizyczną. Cecha ta oznacza, że foldery, które muszą mieć dużą pojemność, mogą być instalowane na oddzielnych dużych dyskach i nie muszą zapełnić całego pierwotnego woluminu.

Pytania do zadania 1.1

1. Rooslan jest administratorem sieci w firmie średniej wielkości, która posiada pojedynczą domenę systemu Windows Server 2003. Zespół administratorów firmy jest odpowiedzialny za instalowanie i konserwację sześciu systemów Windows Server 2003. Każdy serwer został skonfigurowany jako serwer autonomiczny i nie jest członkiem domeny serwera 2003. Na każdym z tych serwerów członkowskich będą instalowane po dwa nowe dyski. Rooslan polecił to zadanie stażystce o imieniu Alex, który przebywa w firmie od miesiąca. Rooslan za pomocą obiektu zasady grupy GPO (Group Policy Object) skonfigurował dla Alexa proste konto użytkownika, które ma uprawnienia logowania lokalnego na każdym z serwerów. Zasada obowiązująca w przedsiębiorstwie wymaga, aby pod żadnym warunkiem konto użytkownika Alex nie mogło być członkiem grupy Administratorzy na żadnym z serwerów systemu Windows Server 2003. Następnie Rooslan poprosił Alexa, aby przekształcił nowo zainstalowane dyski podstawowe na dynamiczne. Alex próbował wykonać to zadanie, ale okazało się to niemożliwe. Co może zrobić Rooslan, aby Alex mógł wykonać powierzone zadanie, zakładając, że konto użytkownika Alex nie może być członkiem grupy Administratorzy na żadnym z autonomicznych serwerów systemu Windows Server 2003?
 - A. Na każdym serwerze Rooslan powinien dodać konto użytkownika Alex do grupy Backup Operators (Operatorzy kopii zapasowych).
 - B. Rooslan powinien w domenie dodać konto użytkownika Alex do grupy Backup Operators (Operatorzy kopii zapasowych).
 - C. Rooslan powinien w domenie dodać konto użytkownika Alex do grupy Power Users (Użytkownicy zaawansowani).
 - D. Na każdym serwerze Windows Server 2003 Rooslan powinien zmodyfikować lokalny obiekt GPO przydzielając kontu Alex uprawnienia użytkownika: Perform Volume Maintenance Tasks (Wykonywanie zadań konserwacji woluminu).
 - E. Na każdym serwerze Windows Server 2003 Rooslan powinien zmodyfikować lokalny obiekt GPO przydzielając kontu Alex uprawnienia użytkownika Take Ownership Of Files And Other Objects (Przejmowanie własności plików lub innych obiektów).
2. Rooslan jest administratorem systemu Windows Server 2003. W serwerze są zainstalowane dwa napędy dyskowe. Na pierwszym dysku, który ma 30 GB pojemności, przechowywane są wszystkie pliki systemu operacyjnego. Na drugim dysku o pojemności 80 GB przechowywane są dane użytkowników w pięciu udziałach. Każdy udział odpowiada określonemu działowi przedsiębiorstwa. Każdy udział jest podzielony na trzy odrębne foldery. W pierwszym folderze przechowywane są dokumenty działu, drugi folder służy do współpracy, a w trzecim przechowywane są dane poszczególnych użytkowników. Użytkownicy mogą odczytywać folder dokumentów działu, mogą odczytywać i zapisywać w folderze służącym do współpracy, a każdy użytkownik ma pełną kontrolę nad swoim własnym, unikatowym folderem. Użytkownik może odczytywać lub zapisywać wyłącznie swój własny folder i nie ma dostępu do folderów innych użytkowników. Działanie tych pięciu udostępnionych systemów sprawdziło się, a każdy pracownik rozumie, gdzie powinien zapisywać bądź wyszukiwać odpowiednie dokumenty. Problem polega na tym, że część dotycząca danych użytkowników w każdym z pięciu udziałów bardzo szybko zapełnia się i wkrótce dysk przechowujący dane użytkowników zapełni się całkowicie. Ważna uwaga dotyczy stanowiska menedżerów firmy, którzy nie dopuszczają rozwiązania zwiększającego liczbę udziałów (do których pracownicy muszą uzyskiwać dostęp).

- Rooslan musi zrealizować następujące zadania:

Główny cel: Dodać więcej przestrzeni do każdego udziału tak, aby nie zapełnił się dysk przechowujący foldery udostępnione.

Cele pomocnicze:

Pozostawić jedynie pięć udziałów oraz przechowywać dane użytkowników jako folder w każdym udziale danego departamentu.

Zapewnić odporność na uszkodzenia dla plików udziału.

Pozostawić bieżący schemat zabezpieczeń określający, że danych użytkowników ma pełną kontrolę nad swoim własnym katalogiem, natomiast inni użytkownicy nie mają dostępu do tego katalogu.

Rooslan wykonał następujące czynności. W zaplanowanym okresie po północy, kiedy żaden użytkownik nie jest podłączony do serwera, Rooslan wyłączył serwer i zainstalował pięć dysków twardych o pojemności 100 GB. Następnie sformatował dyski w postaci pojedynczych woluminów z systemem NTFS. Kolejnym krokiem było utworzenie foldera nazwanego Temp w każdym z folderów przechowujących każdy udział danego departamentu. Każdy z pięciu dysków po kolei został zainstalowany w kolejnym folderze Temp tak, że obecnie każdy folder Temp przekierowuje do swojego zainstalowanego dysku twardego. Następnie, w każdym udziale Rooslan skopiował całą zawartość foldera użytkowników do foldera Temp i usunął pierwotne foldery użytkowników. Na koniec zmieniona została nazwa foldera Temp na nazwę foldera danych użytkowników.

Które cele zrealizował Rooslan?

- A. Rooslan nie zrealizował celu głównego. Cele pomocnicze zostały osiągnięte.
 - B. Rooslan zrealizował cel główny i jeden cel pomocniczy.
 - C. Rooslan zrealizował cel główny i dwa cele pomocnicze.
 - D. Rooslan zrealizował wszystkie cele.
 - E. Rooslan nie zrealizował żadnego celu.
- O. W kontrolerze domeny systemu Windows Server 2003 przechowywanych jest kilka folderów, które zajmują znaczącą część przestrzeni systemu dyskowego. Są to następujące foldery:

C:\Datastore\Compress

C:\Datastore\Encrypt

C:\Datastore\Indiperf

Folder Compress jest skompresowany, wszystkie pliki w nim przechowywane są również skompresowane. Folder Encrypt jest zaszyfrowany, również wszystkie pliki w nim przechowywane są zaszyfrowane. Folder Indiperf przechowuje dane użytkowników. Każdy katalog w folderze Indiperf ma uprawnienia połączone indywidualnie z każdym użytkownikiem.

Wykonane zostały następujące działania: zainstalowany został pojedynczy dysk o pojemności 100 GB, na tym dysku utworzone zostały trzy woluminy o pojemności 30 GB, a w katalogu Datastore utworzone zostały następujące foldery:

C:\Datastore\Comptemp

C:\Datastore\Encrtemp

C:\Datastore\Inditemp

Następnie pierwszy 30 GB wolumin został zainstalowany w katalogu Comptemp, drugi wolumin 30 GB w katalogu Encrtemp, a trzeci w katalogu Inditemp. Zawartość katalogu Compress została przeniesiona do katalogu Comptemp. Podobnie dane katalogu Encrypt zostały przeniesione do foldera Encrtemp, a dane katalogu Datastore do foldera Inditemp.

Następnie foldery Compress, Encrypt oraz Indiperf zostały usunięte. Na koniec nazwy katalogów Comptemp, Encrtemp oraz Inditemp zostały zmienione odpowiednio na Compress, Encrypt oraz Indiperf.

Które z poniższych stwierdzeń jest prawdziwe? (wybierz wszystkie właściwe odpowiedzi)

- A. Dane katalogu Compress będą skompresowane.
 - B. Dane katalogu Compress nie będą skompresowane.
 - C. Dane katalogu Encrypt będą zaszyfrowane.
 - D. Dane foldera Encrypt nie będą szyfrowane.
 - E. Dane katalogu Indiperf zachowają indywidualne przydziały uprawnień NTFS.
 - F. Dane katalogu Indiperf nie zachowają indywidualnych przydziałów uprawnień NTFS.
- *7. Lee odpowiada za administrację dwóch dysków SCSI o pojemności 100 GB podłączonych do systemu Windows Server 2003- Oprócz tego, w serwerze zainstalowany jest pojedynczy sprzętowy kontroler macierzy RAID, który obsługuje konfiguracje RAID-0, RAID-1 oraz RAID-5. Aktualnie używany jest 70 GB przestrzeni pierwszego dysku, natomiast drugi dysk jest pusty. Lee obawia się, że dysk twardy serwera może ulec awarii i w konsekwencji zostaną utracone wszystkie dane pierwszego dysku. Lee rozważał wykonywanie regularnych kopii zapasowych, ale nie posiada odpowiedniego sprzętu, by regularnie wykonywać kopie 70 GB danych i dlatego zamierza wprowadzić rozwiązanie, które zapewni odporność na uszkodzenia pierwszego dysku. Które z wymienionych poniżej rozwiązań powinien zastosować Lee uwzględniając bieżącą konfigurację systemu Windows Server 2003?
- A. Lee powinien skonfigurować usługi Volume Shadow Copy (Kopiowanie woluminu w tle) na drugim dysku twardym przy użyciu właściwości dysku.
 - B. Lee powinien skonfigurować usługi Volume Shadow Copy (Kopiowanie woluminu w tle) na pierwszym dysku twardym przy użyciu właściwości dysku.
 - C. Lee powinien utworzyć macierz dyskową RAID-5 za pomocą programu narzędziowego sprzętowego kontrolera RAID.
 - D. Lee powinien utworzyć macierz dyskową RAID-0 za pomocą programu narzędziowego sprzętowego kontrolera RAID.
 - E. Lee powinien utworzyć macierz dyskową RAID-1 za pomocą programu narzędziowego sprzętowego kontrolera RAID.
13. Administrator zainstalował niedawno w systemie Windows Server 2003 kontroler dysków SCSI oraz trzy dyski SCSI o pojemności 100 GB. Po zainstalowaniu urządzeń sprzętu, administrator zalogował się w systemie w oparciu o konto posiadające uprawnienia administracyjne i uruchomił konsolę Disk Management (Zarządzanie dyskami). Zaraz po uruchomieniu konsoli zostało wyświetlone okno programu Initialize And Convert Disk Wizard (Kreator inicjowania i konwertowania dysków). Jakie zadania, spośród wymienionych, można zrealizować za pomocą tego kreatora w odniesieniu do nowo zainstalowanych dysków SCSI? (wybierz wszystkie właściwe odpowiedzi)
- A. Inicjowanie nowego dysku.

- B. Konwersja dysku dynamicznego na podstawowy.
- C. Konwersja dysków podstawowych na dynamiczne.
- D. Utworzenie dublowanej pary dysków.
- E. Utworzenie zestawów rozłożonych.
- F. Utworzenie woluminów RAID-5.
- G. Utworzenie woluminów łączonych.
- H. Utworzenie partycji podstawowej.
- I. Utworzenie partycji rozszerzonej.

Odpowiedzi do zadania 1.1

1. Prawidłowe odpowiedzi: A oraz D

- A. Prawidłowo** Członkowie grupy Backup Operators (Operatorzy kopii zapasowych) mają uprawnienia do przeprowadzania konwersji dysków.
- B. Nieprawidłowo** Metoda taka nie zadziała, ponieważ serwery autonomiczne nie należą do domeny.
- C. Nieprawidłowo** Metoda taka nie zadziała, ponieważ serwery autonomiczne nie należą do domeny. Oprócz tego w domenie brak grupy Power Users (Użytkownicy zaawansowani). Grupa taka istnieje tylko na serwerach autonomicznych.
- D. Prawidłowo** Użytkownicy, którzy posiadają takie uprawnienia przydzielone poprzez obiekt GPO, mogą wykonywać zadania takie jak defragmentacja i konwersja.
- E. Nieprawidłowo** Uprawnienia pozwalające przejść na własność pliki lub foldery nie mają związku z uprawnieniami potrzebnymi do przeprowadzania konwersji dysku podstawowego na dynamiczny.

<L. Prawidłowa odpowiedź: B

- A. Nieprawidłowo** Rooslan zrealizował cel główny instalując nowe dyski twarde o pojemności 100 GB, a kopiując na nie dane użytkowników dodał przestrzeń dyskową do każdego udziału.
- B. Prawidłowo** Rooslan zrealizował cel główny instalując nowe dyski twarde o pojemności 100 GB, a kopiując na nie dane użytkowników dodał przestrzeń dyskową do każdego udziału. Pierwszy cel pomocniczy został również osiągnięty poprzez zainstalowanie dysków jako folderów danych użytkowników. Bieżąca hierarchia folderów w udziale nie zmusza do wprowadzania dodatkowych folderów udostępnionych. Skopiowane pliki nie zachowują swoich uprawnień NTFS i tym samym trzeci cel pomocniczy nie został osiągnięty. W opisanym działaniu brak jakiegokolwiek wzmianki na temat stosowania metod odporności na uszkodzenia, tak więc drugi cel pomocniczy również nie został zrealizowany.
- C. Nieprawidłowo** Pierwszy cel pomocniczy został osiągnięty poprzez zainstalowanie dysków jako folderów danych użytkowników w bieżącej hierarchii folderów udziału. Nie było powodów, aby wprowadzać dodatkowe foldery udostępnione. Skopiowane pliki nie zachowują swoich uprawnień NTFS i tym samym trzeci cel pomocniczy nie został osiągnięty. W opisanym działaniu brak jakiegokolwiek wzmianki na temat stosowania metod odporności na uszkodzenia, tak więc drugi cel pomocniczy również nie został zrealizowany.

- D. **Nieprawidłowo** Pierwszy cel pomocniczy został osiągnięty poprzez zainstalowanie dysków jako folderów danych użytkowników w bieżące hierarchii folderów udziału. Nie było powodów, aby wprowadzać dodatkowe foldery udostępnione. Skopiowane pliki nie zachowują swoich uprawnień NTFS i tym samym trzeci cel pomocniczy nie został osiągnięty. Nie została wprowadzona żadna metoda odporności na uszkodzenia, tak więc drugi cel pomocniczy również nie został zrealizowany.
- E. **Nieprawidłowo** Rooslan zrealizował cel główny instalując nowe dyski twarde o pojemności 100 GB, a kopiując na nie dane użytkowników dodał przestrzeń dyskową do każdego udziału.

■ó. **Prawidłowe odpowiedzi: B, C oraz F**

- A. **Nieprawidłowo** Patrz uzasadnienie dla odpowiedzi B.
- B. **Prawidłowo** Pliki kopiowane lub przenoszone pomiędzy woluminami będą dziedziczyć atrybut kompresji foldera docelowego, nawet jeśli są to woluminy zainstalowane. W opisywanym przykładzie, dla foldera docelowego, atrybut kompresji nie został ustawiony.
- C. **Prawidłowo** Pliki zaszyfrowane podczas kopiowania lub przenoszenia pomiędzy woluminami NTFS zachowują swój status szyfrowania, bez względu na zestaw atrybutów foldera docelowego.
- D. **Nieprawidłowo** Patrz uzasadnienie dla odpowiedzi C.
- E. **Nieprawidłowo** Patrz uzasadnienie dla odpowiedzi F.
- F. **Prawidłowo** Pliki przenoszone pomiędzy woluminami dziedziczą uprawnienia NTFS foldera docelowego. Wszystkie indywidualne przydziały uprawnień NTFS zostaną utracone. Aby zachować uprawnienia, należy wykonać kopię zapasową plików, a następnie ją odtworzyć.

4. **Prawidłowa odpowiedź: E**

- A. **Nieprawidłowo** Usługi Vblume Shadow Copy (Kopiowanie woluminu w tle) nie zapewniają odpornej na uszkodzenia kopii zapasowej wszystkich danych pierwszego dysku.
- B. **Nieprawidłowo** Patrz uzasadnienie dla odpowiedzi A
- C. **Nieprawidłowo** Konfiguracja RAID-5 zapewnia odporność na uszkodzenia, ale w omawianym przykładzie do dyspozycji są tylko dwa dyski, natomiast do zbudowania macierzy RAID-5 potrzebne są co najmniej trzy dyski.
- D. **Nieprawidłowo** Konfiguracja RAID-0 zapewnia lepszą wydajność, nie zapewnia jednak odporności na uszkodzenia.
- E. **Prawidłowo** Lee powinien zbudować macierz dyskową RAID-1, nazywaną również dublowaniem dysków. Konfigurację należy przeprowadzić za pomocą programu narzędziowego sprzętowego kontrolera RAID. Fakt, że dysk już zawiera dane wpływa na również na to, które opcje można wykorzystywać. Pomimo, że istnieje możliwość dublowania dysku, na którym są dane, konwersja dysku do macierzy RAID-5 lub RAID-0 bez usuwania danych nie jest rozwiązaniem.

O. **Poprawne odpowiedzi: A oraz C**

- A. **Prawidłowo** Program Initialize And Convert Disk Wizard (Kreator inicjowania i konwertowania dysków) jest uruchamiany każdorazowo, jeśli do systemu został dodany nowy dysk i uruchamiana jest konsola zarządzania dyskami. Program pozwala jedynie na inicjowanie dysków oraz przeprowadzanie konwersji dysku podstawowego na dynamiczny.
- B. **Nieprawidłowo** Funkcja ta nie może być zrealizowana za pomocą programu Initialize And Convert Disk Wizard (Kreator inicjowania i konwertowania dysków).

- C. **Prawidłowo** Program Initialize And Convert Disk Wizard (Kreator inicjowania i konwertowania dysków) jest uruchamiany każdorazowo, jeśli do systemu został dodany nowy dysk i uruchamiana jest konsola zarządzania dyskami. Program pozwala jedynie na inicjowanie dysków oraz przeprowadzanie konwersji dysku podstawowego na dynamiczny.
- D. **Nieprawidłowo** Funkcja ta nie może być zrealizowana za pomocą programu Initialize And Convert Disk Wizard (Kreator inicjowania i konwertowania dysków).
- E. **Nieprawidłowo** Patrz uzasadnienie dla odpowiedzi D.
- F. **Nieprawidłowo** Patrz uzasadnienie dla odpowiedzi D.
- G. **Nieprawidłowo** Patrz uzasadnienie dla odpowiedzi D.
- H. **Nieprawidłowo** Patrz uzasadnienie dla odpowiedzi D.
- I. **Nieprawidłowo** Patrz uzasadnienie dla odpowiedzi D.

Zadanie 1.2

Monitorowanie urządzeń sprzętu serwera

Monitorowanie urządzeń sprzętu serwera zasadniczo jest realizowane za pomocą przystawki MMC — programu *Device Manager* (Menedżer urządzeń). Monitorowanie urządzeń przyłączonych do serwera może być również przeprowadzane za pomocą przystawek programu *Control Panel* (Panel sterowania) lub odrębnych programów narzędziowych takich jak WINMSD.

Program *Device Manager* (Menedżer urządzeń), który można znaleźć w konsoli MMC lub jako oddzielną konsolę w grupie programów *Administrative Tools* (Narzędzia administracyjne), jest podstawowym narzędziem zarządzania sprzętem. Za pomocą programu można wyświetlić stan określający funkcjonowanie wszystkich urządzeń sprzętu podłączonych do systemu. Urządzenia niezgodne z normą Plug and Play mogą być przeglądane poprzez wybranie w menu *View* (Widok) opcji *Show Hidden Devices* (Pokaż ukryte urządzenia).

Program WINMSD jest uruchamiany w oknie wiersza poleceń lub w oknie programu *Run* (Uruchom) i umożliwia przegląd urządzeń sprzętu zainstalowanego w danym systemie Windows Server 2003.

Niektórymi urządzeniami, takimi jak modemy czy karty grafiki, łatwiej jest zarządzać za pomocą ich specjalizowanych aplikacji umieszczonych w grupie programów *Control Panel* (Panel sterowania) niż za pomocą programu *Device Manager* (Menedżer urządzeń).

Pytania do zadania 1.2

1. Użytkownik pracuje w systemie Windows Server 2003, który został zaktualizowany z wersji serwera Windows 2000. Serwer ten jest wyposażony w starszy kontroler RAID SCSI, który nie jest zgodny z trybem PnP (Plug and Play). Urządzenie pracuje bardzo dobrze, ale nie jest uwidaczniane w programie Device Manager (Menedżer urządzeń). Co należy zrobić, aby urządzenie było widoczne w programie Device Manager (Menedżer urządzeń)?
 - A. W programie Device Manager (Menedżer urządzeń) widoczne są jedynie urządzenia zgodne z trybem PnP.
 - B. Należy aktualizować sterownik urządzenia tak, aby obsługiwany był tryb PnP (Plug and Play).
 - C. Dyski i kontrolery macierzy RAID nie są widoczne w programie Device Manager (Menedżer urządzeń).
 - D. W programie Device Manager (Menedżer urządzeń), w menu View (Widok) należy zaznaczyć opcję Show Hidden Devices (Pokaż ukryte urządzenia).
- 2., Rooslan zarządza systemem Windows Server 2003, w którym wykorzystuje kilka zewnętrznych dysków twardych USB (Universal Serial Bus) jako dodatkową opcję pamięci dyskowej. Oprócz tego, używany jest zewnętrzny napęd USB nagrywarki CD, Microsoft USB IntelliMouse oraz klawiatura USB. Niedawno Rooslan zauważył, że wydajność niektórych dysków twardych USB stała się zmienna

i dlatego chce wygenerować raport dotyczący bieżącego pasma i poboru mocy różnych urządzeń USB przyłączonych do systemu Windows Server 2003. Która z wymienionych poniżej metod umożliwi zrealizowanie tego zadania? (wybierz wszystkie właściwe odpowiedzi)

- A. Rooslan powinien uruchomić program narzędziowy urządzeń USB znajdujący się w grupie programów Control Panel (Panel sterowania). Ten program narzędziowy tworzy listę podłączonych do systemu urządzeń USB wraz z wykorzystywanym przez nie pasmem i poborem mocy.
- B. Rooslan powinien uruchomić program narzędziowy Power (Opcje Zasilania) znajdujący się w grupie programów Control Panel (Panel sterowania). W programie tym należy wybrać zakładkę USB, aby wyświetlić informacje o profilu poboru mocy różnych urządzeń przyłączonych do systemu.
- C. Rooslan powinien uruchomić program Device Manager (Menedżer urządzeń) i przejść do węzła USB Root Hub (Główny koncentrator USB), kliknąć węzeł prawym przyciskiem myszy i wybrać polecenie Properties (Właściwości). Następnie powinien kliknąć zakładkę Power (Zasilanie), która wyświetla informacje o poborze mocy przyłączonych urządzeń.
- D. Rooslan powinien uruchomić program Device Manager (Menedżer urządzeń) i przejść do węzła USB Root Hub (Główny koncentrator USB), kliknąć węzeł prawym przyciskiem myszy i wybrać polecenie Properties (Właściwości). Następnie powinien kliknąć zakładkę Advanced (Zaawansowane), na której wyświetlane są informacje o paśmie, jakie zajmują używane urządzenia.
- E. Rooslan powinien uruchomić program narzędziowy Bandwidth (Pasma) znajdujący się w grupie programów Control Panel (Panel sterowania). W programie tym powinien przejść do zakładki USB, na której wyświetlane są informacje o paśmie, jakie zajmują podłączone urządzenia.
- F. Rooslan powinien uruchomić program Task Manager (Menedżer zadań) i wybrać zakładkę USB Devices (Urządzenia USB). Na tej zakładce wyświetlane są informacje o zajmowanym paśmie i poborze mocy każdego podłączonego do systemu urządzenia USB.

ó* Przedsiębiorstwo przeprowadza inspekcję wszystkich urządzeń podłączonych do używanych serwerów systemu Windows Server 2003, którymi opiekuje się Orin. Inspektorzy prosili o wydrukowanie podsumowania zawierającego listę wszystkich urządzeń zainstalowanych w systemie. Podsumowanie powinno zawierać numer wersji produktu, typ magistrali oraz informacje o zasobach.

Orin musi zrealizować następujące zadania:

Główny cel: Wydrukować zestawienie zawierające listę wszystkich urządzeń zainstalowanych w systemie.

Cele pomocnicze:

Zapewnić, aby w raporcie znalazły się informacje zasobu dotyczące żądań przerwania (IRQ).

Dane wyjściowe raportu zapisać w pliku, a nie wydrukować.

Orin wykonał następujące operacje: W grupie programów Administrative Tools (Narzędzia administracyjne), w programie Computer Management (Zarządzanie komputerem) uruchomił program Device Manager (Menedżer urządzeń), zaznaczył węzeł systemu Windows Server 2003 i Serwer menu Action (Akcja) wybrał polecenie Print (Drukuj). Następnie określił typ raportu jako All Devices And System Summary (Wszystkie urządzenia i podsumowanie raportu), a na koniec kliknął polecenie Print (Drukuj).

Które cele zrealizował Orin?

- A. Orin osiągnął wszystkie cele.
- B. Orin zrealizował cel główny i jeden cel pomocniczy.

- C." Orin zrealizował cci główny, natomiast cele pomocnicze nic zostały osiągnięte.
 - D. Orin nie zrealizował celu głównego, natomiast osiągnięte zostały wszystkie cele pomocnicze.
 - E. Orin nie zrealizował celu głównego, natomiast zrealizowany został jeden cel pomocniczy.
 - F. Orin nie zrealizował żadnego celu.
4. Administrator jest odpowiedzialny za zespół systemów Windows Server 2003 używanych jako serwery sieci Web średniej wielkości dostawcy usług internetowych (ISP). Administrator ma przygotować raport dotyczący kart sieciowych zainstalowanych w każdym serwerze. W raporcie powinny znaleźć się informacje o typie adaptera oraz za-sobach urządzenia takich jak IRQ. Ponieważ musi być zapewniony nieprzerwany dostęp do obsługiwanych stron sieci Web, w każdym serwerze zainstalowanych zostało kilka kart sieciowych. Zadanie komplikuje fakt, że karty były dodawane w różnych okresach i nie są tego samego typu, jak również wytworzone zostały przez różnych producentów. Która z poniżej wymienionych metod pozwoli wygenerować taki raport? (wybierz wszystkie właściwe odpowiedzi)
- A. W każdym systemie Windows Server 2003 należy uruchomić Device Manager (Menedżer urządzeń). Następnie należy zaznaczyć węzeł Network Adapters (Karty sieciowe) i z menu Action (Akcja) wybrać polecenie Print (Drukuj). Należy wybrać opcję Selected Class or Device (Wybrana klasa lub urządzenie) i kliknąć przycisk Print (Drukuj).
 - B. W każdym systemie Windows Server 2003, w grupie programów Control Panel (Panel sterowania) należy uruchomić program Network Connections (Połączenia sieciowe). Następnie, na zakładce Advanced (Zaawansowane) należy wybrać opcję Network Hardware (Sprzęt sieciowy) i kliknąć przycisk Generate Report (Generuj raport).
 - C. Należy w wierszu poleceń uruchomić program WINMSD. W węźle Components (Składniki) należy wybrać węzeł Network (Sieć), a następnie Adapters (Karty). W menu File (Plik) należy wybrać polecenie Print (Drukuj).
 - D. W menu Run (Uruchom) należy uruchomić program Winipcfg. Na zakładce Adapters (Karty) należy zaznaczyć opcję Generate Hardware Report (Generuj raport o urządzeniach) i kliknąć przycisk Print (Drukuj).
 - E. W wierszu poleceń należy wpisać komendę Ipconfig/Adapter. Uzyskane w ten sposób informacje należy skopiować do pliku tekstowego za pomocą programu Notepad, a następnie plik ten wydrukować.
5. Rooslan jest głównym administratorem w przedsiębiorstwie średniej wielkości. Kilka miesięcy temu zakupione i zainstalowane zostały trzy systemy Windows Server 2003, które zostały skonfigurowane jako kontrolery domeny. Po tygodniu testowania każdy serwer został przesłany do lokalizacji zdalnej jako element wprowadzania w sieć przedsiębiorstwa systemu Windows Server 2003. Z jednej z tych lokalizacji zadzwonił administrator informując, że podczas uruchamiania kontrolera domeny pojawił się komunikat o błędzie. Z komunikatu wynika, że podczas rozruchu nie mógł zainstalować się sterownik urządzenia. Administrator w lokalizacji zdalnej za pomocą programu Device Manager (Menedżer urządzeń) sprawdzał, czy wyświetlone zostały informacje wskazujące, że jakiegokolwiek urządzenie nie funkcjonuje prawidłowo, ale w tym przypadku nic takiego nie miało miejsca. Rooslan zapytał, czy zaznaczona została opcja umożliwiająca pokazywanie ukrytych urządzeń. Okazało się, że administrator nie wiedział o takiej możliwości. Serwer był uruchamiany 20 razy i w trzech przypadkach wystąpił błąd. Błąd wystąpił ponownie dzisiaj rano, co skłoniło administratora do powiadomienia Rooslana o rym fakcie. Co prawda, tuż przed telefonem serwer był ponownie uruchamiany i błąd ten nie pojawił się. Rooslan rozpoczął nawiązywanie z serwerem połączenia pulpitu zdalnego, aby przeanalizować

działanie serwera. Która z wymienionych poniżej metod powinna być zastosowana celem wykrycia przyczyny błędu?

- A. Po połączeniu zdalnym z kontrolerem domeny Rooslan powinien uruchomić program Device Manager (Menedżer zadań) i w menu View (Widok) powinien zaznaczyć opcje Show Hidden Devices (Pokaż ukryte urządzenia).
- B. Po połączeniu zdalnym z kontrolerem domeny Rooslan powinien sprawdzić dziennik systemu analizując wpisy wygenerowane przez wadliwy sterownik urządzenia.
- C. Po połączeniu zdalnym z kontrolerem domeny Rooslan powinien sprawdzić dziennik zabezpieczeń analizując wpisy wygenerowane przez wadliwy sterownik urządzenia.
- D. Po połączeniu zdalnym z kontrolerem domeny Rooslan powinien sprawdzić dziennik urządzeń analizując wpisy wygenerowane przez wadliwy sterownik urządzenia.
- E. Po połączeniu zdalnym z kontrolerem domeny Rooslan powinien sprawdzić dziennik aplikacji analizując wpisy wygenerowane przez wadliwy sterownik urządzenia.
- F. Po połączeniu zdalnym z kontrolerem domeny Rooslan powinien uruchomić program WINMSD i sprawdzić listę sterowników, aby przekonać się, czy nie zostało zanotowane jakiegokolwiek nieprawidłowe uruchomienie.

Odpowiedzi do zadania 1.2

-L. Prawidłowa odpowiedź: D

- A. **Nieprawidłowo** Jest to nieprawdziwe twierdzenie. Urządzenie niezgodne z trybem PnP (Plug and Play) może być przeglądane za pomocą programu Device Manager (Menedżer urządzeń), jeśli wybrana zostanie opcja Show Hidden Devices (Pokaż ukryte urządzenia).
- B. **Nieprawidłowo** Specyfikacja PnP (Plug and Play) dotyczy urządzeń sprzętu, a nie oprogramowania. Tak więc aktualizacja sterownika nie uwidoczni urządzenia w programie Device Manager (Menedżer urządzeń).
- C. **Nieprawidłowo** Urządzenia te są widoczne w programie Device Manager (Menedżer urządzeń).
- D. **Prawidłowo** Ustawienia domyślne określają, że urządzenia sprzętu niezgodne z trybem PnP (Plug and Play) nie są pokazywane w programie Device Manager (Menedżer urządzeń). Aby je uwidocznić, należy zaznaczyć opcję Show Hidden Devices (Pokaż ukryte urządzenia). Wybranie tej opcji powoduje, że wyświetlone zostaną wszystkie „ukryte” urządzenia, wliczając w to starsze urządzenia, takie jak kontroler RAID SCSI, który nie jest zgodny ze specyfikacją PnP.

2.. Prawidłowe odpowiedzi: C oraz D

- A. **Nieprawidłowo** W grupie programów Control Panel (Panel sterowania) nie został umieszczony żaden program narzędziowy dla urządzeń USB.
- B. **Nieprawidłowo** Program Power (Opcje zasilania) kontroluje urządzenia takie jak UPS oraz okresy nieaktywności, natomiast nie są wyświetlane informacje o poborze mocy urządzeń USB.
- C. **Prawidłowo** W oknie właściwości węzła USB Root Hub (Główny koncentrator USB) umieszczonego w programie Device Manager (Menedżer urządzeń) wyświetlane są informacje o poborze mocy przyłączonych urządzeń USB.

- D. Prawidłowo** Uniwersalny kontroler hosta USB tworzy listę wykorzystania pasma dla tych urządzeń, które je zajmują, a następnie przekazuje te informacje do systemu. Nie wszystkie urządzenia USB pobierają zasilanie z systemu, niektóre mają niezależne źródła zasilania. Urządzenia takie jak klawiatura czy mysz są jednak zasilane z systemu. Podobnie, nie wszystkie urządzenia zajmują pasmo USB. Jeśli w systemie zostało zainstalowanych kilka urządzeń, które zajmują pasmo, należy monitorować jego wykorzystanie, żeby urządzenia działały sprawnie.
- E. Nieprawidłowo** W grupie programów Control Panel (Panel sterowania) nie został umieszczony program narzędziowy Bandwidth (Pasma).
- E Nieprawidłowo** W programie Task Manager (Menedżer zadań) brak zakładki USB Devices (Urządzenia USB).

O • Prawidłowa odpowiedź: B

- A. Nieprawidłowo** Wybór typu raportu Ali Devices And System Summary (Wszystkie urządzenia i podsumowanie raportu) spowoduje wydrukowanie raportu dla każdego urządzenia zainstalowanego w systemie, wliczając w to informacje o zasobach, jak również spowoduje wydrukowanie podsumowania informacji o systemie. W ten sposób zostanie osiągnięty cel główny oraz pierwszy cel pomocniczy. Ponieważ w opisie brak uwag o zaznaczeniu opcji Print To File (Drukuj do pliku), drugi cel pomocniczy nie zostanie zrealizowany.
- B. Prawidłowo** Wybór typu raportu Ali Devices And System Summary (Wszystkie urządzenia i podsumowanie raportu) spowoduje wydrukowanie raportu dla każdego urządzenia zainstalowanego w systemie, wliczając w to informacje o zasobach, jak również spowoduje wydrukowanie podsumowania informacji o systemie. W ten sposób zostanie osiągnięty cel główny oraz pierwszy cel pomocniczy.
- C. Nieprawidłowo** Patrz uzasadnienie dla odpowiedzi **B**.
- D. Nieprawidłowo** Wybór typu raportu Ali Devices And System Summary (Wszystkie urządzenia i podsumowanie raportu) spowoduje wydrukowanie raportu dla każdego urządzenia zainstalowanego w systemie, wliczając w to informacje o zasobach, jak również spowoduje wydrukowanie podsumowania informacji o systemie. W ten sposób zostanie osiągnięty cel główny oraz pierwszy cel pomocniczy. Ponieważ, w opisie brak uwag o zaznaczeniu opcji Print To File (Drukuj do pliku), drugi cel pomocniczy nie zostanie zrealizowany.
- E. Nieprawidłowo** Patrz uzasadnienie dla odpowiedzi **B**.
- E Nieprawidłowo** Patrz uzasadnienie dla odpowiedzi **B**.

4. Prawidłowe odpowiedzi: A oraz C

- A. Prawidłowo** Do wydrukowania raportu można użyć dwóch programów — Device Manager (Menedżer urządzeń) oraz WINMSD. Przy użyciu opisanej metody można szybko utworzyć listę zawierającą wszystkie istotne informacje, o które pytał menedżer.
- B. Nieprawidłowo** W ten sposób nie można wygenerować potrzebnych informacji.
- C. Prawidłowo** Patrz uzasadnienie dla odpowiedzi **A**.
- D. Nieprawidłowo** W ten sposób nie można wygenerować potrzebnych informacji.
- E. Nieprawidłowo** W ten sposób nie można wygenerować potrzebnych informacji.

5. Prawidłowa odpowiedź: B

- A. **Nieprawidłowo** Pomocnik administratora komunikował, że zaznaczył tę opcję, chociaż wcześniej nie wiedział, w jaki sposób wyświetlić ukryte urządzenia. Być może błąd związany jest z ukrytym urządzeniem, ale ponieważ przy ostatnim uruchomieniu błąd nie pojawił się, w tym miejscu nie będzie można znaleźć informacji o jego przyczynie.
- B. **Prawidłowo** Ponieważ przed telefonem do Rooslana system został uruchomiony prawidłowo, w programie Device Manager (Menedżer urządzeń) nie będzie można znaleźć żadnych informacji o przyczynach problemu. Rooslan będzie mógł przeanalizować dziennik systemu, w którym rejestrowane było ostatnich kilka uruchomień komputera i tym samym zarejestrowane będą zdarzenia związane z wadliwym sterownikiem.
- C. **Nieprawidłowo** Ten typ zdarzeń będzie zapisywany w dzienniku systemu, a nie w dzienniku zabezpieczeń.
- D. **Nieprawidłowo** Ten typ zdarzeń będzie zapisywany w dzienniku systemu, a nie w dzienniku urządzenia..
- E. **Nieprawidłowo** Ten typ zdarzeń będzie zapisywany w dzienniku systemu, a nie w dzienniku aplikacji.
- F. **Nieprawidłowo** Ponieważ ostatnie uruchomienie systemu było prawidłowe, program WINMSD nie będzie mógł wyświetlić przyczyny problemu.

Zadanie 1.3 Optymalizacja wydajności dysków serwera

Jednym z ważnych zadań administratora jest utrzymanie optymalnej wydajności podsystemu dyskowego serwera. Niejednokrotnie serwery obsługują intensywne operacje odczytu i zapisu na dyskach i nawet niewielki wzrost prędkości działania dysków może przynieść znaczne korzyści.

W systemie Windows Server 2003 istnieją trzy sposoby zwiększania wydajności operacji zapisu i odczytu dysków. Pierwszy to zainstalowanie dysków rozłożonych (RAID-0). Dysk rozłożony wykorzystuje dwa lub kilka dysków. W tej konfiguracji dane zapisywane są jednocześnie na kilku dyskach. Początek pliku może być zapisany na jednym dysku, część środkowa pliku na drugim dysku, a na trzecim dysku zapisana zostanie końcowa część pliku. Podobnie podczas odczytu, część początkowa, środkowa i końcowa pliku może być odczytywana jednocześnie. Równoległe wykonywanie tych operacji daje duży wzrost wydajności. Wadą macierzy dyskowej RAID-0 jest utrata wszystkich danych w konsekwencji awarii jednego z dysków zestawu rozłożonego. Na tego typu woluminach powinny być przechowywane jedynie dane, dla których nie jest wymagana odporność na uszkodzenia, natomiast potrzebne jest szybkie wykonywanie operacji zapisu i odczytu.

Drugi sposób zwiększania wydajności dysków to wprowadzenie dysków rozłożonych z parzystością, nazywanych również macierzą RAID-5. W przeciwieństwie do poprzednio omawianej, konfiguracja taka jest odporna na uszkodzenia. Jeśli awarii ulega jeden z dysków woluminu RAID-5, dane w dalszym ciągu są dostępne, dzięki informacjom sumy kontrolnej (parzystość) przechowywanej na pozostałych dyskach. Macierz RAID-5 jest bezpieczną metodą zwiększenia wydajności operacji zapisu i odczytu dysków. Konsola zarządzania dyskami umożliwia prosty sposób wprowadzenia tej konfiguracji w oparciu o co najmniej trzy dyski dynamiczne.

Ostatnim sposobem zwiększania wydajności operacji odczytu i zapisu dysków jest przechowywanie plików w obszarach dysku w miarę możliwości pozbawionych fragmentacji. Przyczyną fragmentacji dysków jest zapisywanie i usuwanie plików. Ponieważ przestrzeń na dysku twardym przydzielana jest w kolejności takiej, jak jest ona dostępna na dysku, to nowe pliki mogą być zapisywane w kilku odrębnych lokalizacjach dysku. Im bardziej plik jest podzielony, tym więcej czasu potrzeba do jego odczytu lub zapisu. Defragmentacja jest procesem odwrotnym, dzięki któremu pliki dysku twardego zostają uporządkowane i są zapisywane w ciągłych obszarach dysku. Zadanie to wykonywane jest za pomocą konsoli Disk Defragmenter (Defragmentator dysku) lub za pomocą narzędzia wiersza poleceń DEFRAG.

Pytania do zadania 1.3

- X. Sprawdzana jest wydajność kilku systemów Windows Server 2003. W szczególności dotyczy to wydajności operacji zapisu i odczytu dysków w różnych konfiguracjach wliczając w to woluminy dublowane, rozłożone, łączone i RAID-5. Wszystkie konfiguracje zbudowane w oparciu o oprogramowanie systemu Windows Server 2003. Wykonane zostały pewne testy, które miały przekonać o zaletach i wadach tych konfiguracji w porównaniu do woluminów prostych. Które z wymienionych poniżej

twierdzeń dotyczących różnych konfiguracji dyskowych i ich wydajności są prawdziwe? (wybierz wszystkie właściwe odpowiedzi)

- A. Dyski dublowane mają podobną wydajność operacji odczytu i zapisu, co woluminy proste.
- B. Dyski rozłożone w porównaniu do macierzy RAID-5 mają lepszą wydajność operacji odczytu i zapisu 5.
- C. Dyski rozłożone (RAID-0) w porównaniu do dysków łączonych mają lepszą wydajność operacji odczytu i zapisu.
- D. Dyski łączone w porównaniu do dysków rozłożonych mają lepszą wydajność operacji odczytu i zapisu.
- E. W porównaniu do woluminów prostych dyski rozłożone mają lepszą wydajność operacji odczytu i zapisu.

<£. Rooslan jest konsultantem poproszonym przez średniej wielkości przedsiębiorstwo o poradę dotyczącą optymalizacji wydajności dysków trzech nowo zakupionych systemów Windows Server 2003. Są to trzy różne systemy, natomiast platforma sprzętowa serwerów jest taka sama. Każdy serwer wyposażony jest w sześć 120 GB dysków i w żadnym z nich nie jest zainstalowany sprzętowy kontroler macierzy. Rooslan zapoznał się ze specyfikacjami zespołów, które będą wykorzystywały każdy z tych systemów.

Zespół pierwszego serwera ma jeden cel - potrzebny jest im drugi duży wolumin o pojemności około 600 GB, który będzie zawierał wszystkie dane. Pierwszy wolumin o pojemności 120 GB powinien zawierać pliki systemu operacyjnego i pliki programów. Prędkość i odporność na uszkodzenia dysków nie jest wymagana przez ten zespół.

Zespół, który będzie wykorzystywał drugi serwer, wyznaczył trzy cele. Pierwsze wymaganie określa, że pierwszy wolumin o pojemności 120 GB będzie odporny na uszkodzenia oraz że będzie przechowywać pliki systemu operacyjnego i programów. Drugi cel to utworzenie odpornego na uszkodzenia woluminu o pojemności 120 GB, na którym przechowywane będą dane programów. Natomiast trzeci cel to utworzenie woluminu o pojemności 240 GB, który zapewni najszybsze z możliwych operacje zapisu i odczytu.

Zespół trzeciego serwera wyznaczył postawił dwa wymagania. Pierwsze wymaganie określa, że pierwszy wolumin o pojemności 120 GB będzie odporny na uszkodzenia oraz że przechowywać będzie pliki systemu operacyjnego i programów. Natomiast drugi cel to utworzenie woluminu o pojemności około 480 GB, który zapewni najszybsze z możliwych operacje zapisu i odczytu.

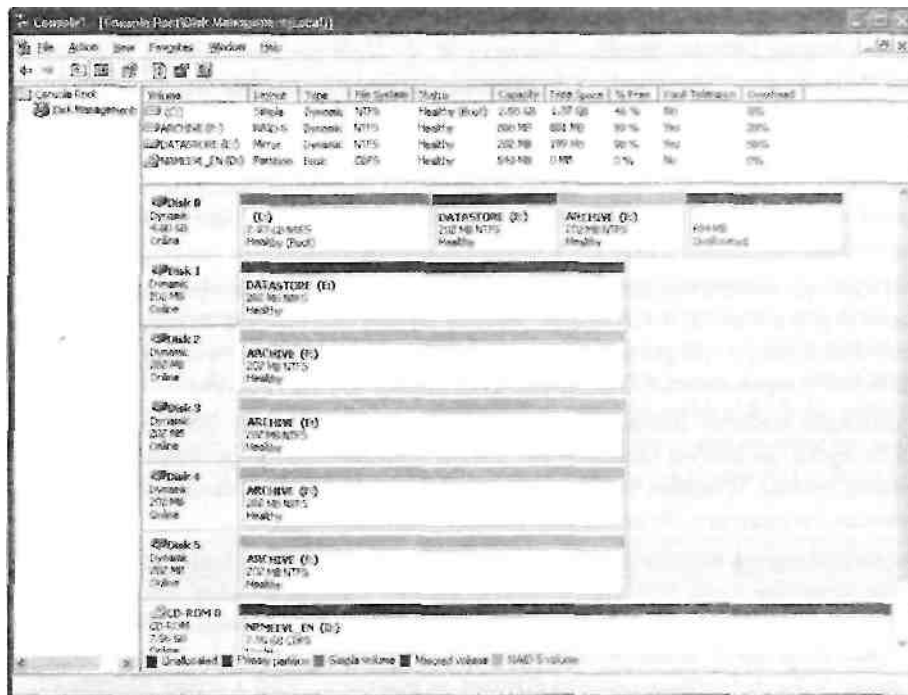
Na pierwszym serwerze Rooslan instaluje system Windows Server 2003 tworząc jedną partycję na całym dysku, na którym zainstalowane zostaną pliki systemu operacyjnego i programów. Po zainstalowaniu systemu Windows Server 2003, pozostałe pięć dysków zostanie przekształconych na dyski dynamiczne i w oparciu o nie utworzony zostanie wolumin łączony.

Na serwerze drugiego zespołu Rooslan zainstalował system Windows Server 2003 wykorzystując całą dostępną przestrzeń dysku 120 GB. Po skonfigurowaniu systemu, Rooslan utworzył dublowanie dysku systemowego w oparciu o drugi dysk o pojemności 120 GB. Na tym woluminie zainstalowane zostały ważne pliki programów. W kolejnym kroku Rooslan z pozostałych dysków utworzył dwie pary dysków dublowanych, każda o pojemności 120 GB.

Na serwerze trzeciego zespołu Rooslan zainstalował system Windows Server 2003 wykorzystując całą dostępną przestrzeń dysku 120 GB. Po skonfigurowaniu systemu Rooslan utworzył dublowanie dysku systemowego w oparciu o drugi dysk o pojemności 120 GB. Na tym woluminie zostały zainstalowane

ważne pliki programów. Następnie, w oparciu pozostałe cztery 120 GB dyski, Rooslan utworzył wolumin RAID-5. Które z przytoczonych poniżej twierdzeń dokładnie podsumowują zrealizowane przez Rooslana cele?

- A. Rooslan zrealizował wymagania wszystkich trzech zespołów.
 - B. Rooslan zrealizował wymagania pierwszego zespołu, dwa wymagania postawione przez drugi zespół oraz wszystkie wymagania trzeciego zespołu.
 - C. Rooslan zrealizował cele pierwszego zespołu, wszystkie wymagania drugiego zespołu oraz jedno z trzech wymagań postawionych przez trzeci zespół.
 - D. Rooslan nie zrealizował wymagania pierwszego zespołu, osiągnął wszystkie wymagania drugiego zespołu oraz zrealizował jedno z trzech wymagań postawionych przez zespół trzeci.
 - E. Rooslan nie zrealizował wymagania pierwszego zespołu, osiągnął dwa wymagania postawione przez drugi zespół oraz zrealizował jedno z trzech wymagań postawionych przez zespół trzeci.
 - E Rooslan zrealizował wymagania pierwszego zespołu, osiągnął dwa wymagania postawione przez drugi zespół oraz zrealizował jedno z trzech wymagań postawionych przez zespół trzeci.
3. Zamieszczony niżej rysunek przedstawia konfigurację dysków systemu Windows Server 2003- Bazując na zaprezentowanej konfiguracji należy określić, które z poniższych twierdzeń dotyczących woluminów tego systemu Windows Server 2003 są prawdziwe? (wybierz wszystkie prawidłowe odpowiedzi)



- A. Jeśli awarii ulegnie dysk 1, wszystkie dane zostaną zachowane.
- B. Jeśli awarii ulegnie dysk 0, wszystkie dane zostaną zachowane.
- C. Jeśli awarii ulegnie dysk 2, wszystkie dane zostaną zachowane.

- D. Prędkość operacji odczytu i zapisu woluminu Datastore będzie mniejsza niż dla woluminu Archive.
 - E. Prędkość operacji odczytu i zapisu woluminu Archive będzie mniejsza niż dla woluminu Data store.
 - F. Jeśli awarii ulegnie dysk 3, dane zostaną utracone.
4. Oksana przegląda raport wygenerowany przez program defragmentatora dysku. W systemie zainstalowane są dwa woluminy. Pierwszy wolumin ma pojemność 100 GB i jest woluminem dublowanym z drugim dyskiem o tej samej pojemności. Drugi wolumin o pojemności 400 GB zbudowany jest w oparciu o pięć dysków 100 GB w konfiguracji RAID-5- Raport, który analizuje Oksana, dotyczy wydajności drugiego woluminu. Oksana jest zdziwiona, ponieważ kilka sekcji drugiego woluminu jest zaznaczonych kolorem zielonym. Kolor zielony oznacza pliki, które nie mogą być przenoszone. Zaskoczenie Oksany wynika z przekonania, że pliki, które nie mogą być przenoszone przez program defragmentatora dysku znajdują się jedynie na woluminach systemowych lub rozruchowych. Jakie są przyczyny, dla których pliki drugiego woluminu nie mogą być przenoszone? (wybierz wszystkie właściwe odpowiedzi)
- A. Oksana przez pomyłkę analizuje raport dotyczący pierwszego woluminu, który zawiera pliki systemowe i rozruchowe.
 - B. Plik stronicowania został umieszczony na drugim woluminie.
 - C. Na drugim woluminie Oksana przechowywała pliki szyfrowane.
 - D. Na drugim woluminie Oksana przechowywała pliki skompresowane.
 - E. Plik dziennika zmian NTFS, przechowywany na każdym woluminie NTFS, jest plikiem, który nie może być przenoszony.
5. Dla wszystkich serwerów lokacji Oksana zaplanowała wykonywanie zadania wiersza poleceń dotyczącego defragmentacji dysku na godzinę 1:00 każdej niedzieli. Pora przeprowadzenia zadania jest doskonale dobrana, ponieważ w tym okresie aktywność serwerów jest minimalna. Sprawdzając w poniedziałek rano dzienniki, Oksana zauważyła, że defragmentacja nie została wykonana na jednym z woluminów jednego z systemów Windows Server 2003- Oksana zalogowała się na tym serwerze ' za pomocą połączenia pulpitu zdalnego i zaznaczyła program konsoli MMC — Disk Defragmenter (Defragmentator dysku). Oksana zdecydowała się poczekać na zakończenie dnia roboczego i dopiero następnie uruchomić ponownie proces defragmentacji tego woluminu. O godzinie 18:30 zalogowała się ponownie przy użyciu pulpitu zdalnego i spróbowała rozpocząć defragmentację woluminu. Proces ponownie zakończył się niepowodzeniem. Co może być tego przyczyną i które z wymienionych poniżej czynności powinna przedsięwziąć Oksana, aby przeprowadzić defragmentację woluminu?
- A. Dla woluminu nie można przeprowadzić defragmentacji, ponieważ jest prawie całkowicie zapelniony. Wolumin musi mieć co najmniej 15% wolnego miejsca, aby mógł rozpocząć się proces defragmentacji.
 - B. Wolumin został zaznaczony jako „zmieniony”. Oksana powinna najpierw w oknie wiersza poleceń uruchomić program Chkdsk, a dopiero następnie rozpocząć proces defragmentacji dysku.
 - C. Aby wykonać defragmentację dysku, Oksana musi ręcznie zmienić tryb pracy dysku na „offline”. Po zakończeniu tej operacji proces defragmentacji będzie przebiegał normalnie.
 - D. Aby przeprowadzić defragmentację, Oksana powinna odinstalować dysk, który obsługuje wolumin. Po zakończeniu tej operacji proces defragmentacji będzie przebiegał normalnie.

6. Administrator obsługuje kilka niewielkich przedsiębiorstw. Jedno z nich powiadomiło, że wydajność wykorzystywanego w firmie serwera znacznie spadła. Konfiguracja serwera została przedstawiona poniżej:

Wolumin	Typ	System plików	Odporność na uszkodzenia	Fragmentacja
Dysk C	Dynamiczny	NTFS	Dublowany	9%
Dysk D	Podstawowy	NTFS	Brak	13%
Dysk E	Dynamiczny	NTFS	Rozłożony	23%
Dysk F	Dynamiczny	NTFS	RAID-5	32%
Dysk G	Dynamiczny	NTFS	RAID-5	41%

Dla którego woluminu systemu Windows Server 2003 zalecane jest przeprowadzenie defragmentacji? (wybierz wszystkie właściwe odpowiedzi)

- A. Dysk C
- B. Dysk D
- C. Dysk E
- D. Dysk F
- E. Dysk G

Odpowiedzi do zadania 1.3

1. Prawidłowe odpowiedzi: A, B, C oraz E

- A. Prawidłowo** Dyski dublowane nie przyspieszają operacji odczytu i zapisu, ale zapewniają odporność na uszkodzenia.
- B. Prawidłowo** Podczas zapisu macierz RAID-5 musi obliczyć informacje sumy kontrolnej (parzystość), natomiast dyski rozłożone (RAID-0) nie wykonują tych operacji. Wynikające stąd opóźnienia są przyczyną wolniejszego działania w porównaniu do dysków rozłożonych.
- C. Prawidłowo** Dyski łączone mają podobną wydajność jak woluminy proste, a dyski rozłożone są najszybszą metodą odczytu i zapisu woluminu.
- D. Nieprawidłowo** Dyski łączone mają podobną wydajność jak woluminy proste, a dyski rozłożone są najszybszą metodą odczytu i zapisu woluminu.
- E. Prawidłowo** W przypadku dysków rozłożonych operacje zapisywania i odczytywania danych mogą być przeprowadzane jednocześnie na kilku dyskach. W przypadku woluminu prostego, w danym momencie może być zapisywany lub odczytywany tylko jeden dysk.

£. Prawidłowa odpowiedź: F

- A. Nieprawidłowo** Rooslan zrealizował cele pierwszego zespołu. W przypadku drugiego zespołu, zrealizował pierwsze i drugie wymaganie. Utworzenie konfiguracji dublowania zamiast dysków rozłożonych przesądza, że rzecy wolumin nie będzie woluminem o pojemności 240 GB charakteryzującym się najszybszymi operacjami odczytu i zapisu. Wolumin będzie miał pojemność 120 GB, a jego wydajność nie będzie znacząco lepsza od wydajności woluminu prostego. Rooslan zrealizował

jedno wymaganie postawione przez trzeci zespół. Osiągnął pierwszy cel, ale stosując macierz RAID-5 zamiast woluminu rozłożonego nie zrealizował wymagania drugiego. Drugi wolumin będzie miał pojemność 360 GB, a nie 480 GB jak określone zostało w wymaganiach. Różnica wynika z tego, że pojemność jednego z dysków jest przeznaczona na przechowywanie sum kontrolnych.

- B. Nieprawidłowo** Patrz uzasadnienie do odpowiedzi **A**.
- C. Nieprawidłowo** Patrz uzasadnienie do odpowiedzi **A**.
- D. Nieprawidłowo** Patrz uzasadnienie do odpowiedzi **A**.
- E. Nieprawidłowo** Patrz uzasadnienie do odpowiedzi **A**.
- F. Prawidłowo** Patrz uzasadnienie do odpowiedzi **A**.

6. Prawidłowe odpowiedzi: A, C oraz D

- A. Prawidłowo** Dysk 1 razem z dyskiem 0 tworzą wolumin dublowany. Jeśli jeden z dysków ulega awarii, wszystkie dane zostaną zachowane.
- B. Nieprawidłowo** Jeśli awarii ulega dysk 0, utracone zostaną dane woluminu rozruchowego, który nie jest chroniony.
- C. Prawidłowo** Dysk 2 jest częścią macierzy RAID-5 i dlatego, jeśli nastąpi jego uszkodzenie, informacje sum kontrolnych (parzystość) mogą być wykorzystane do odtworzenia danych.
- D. Prawidłowo** Datastore jest woluminem dublowanym, a wolumin Archive to macierz RAID-5. Konfiguracja RAID-5 jest szybsza niż RAID-1 (dublowanie).
- E. Nieprawidłowo** Datastore jest woluminem dublowanym, a wolumin Archive to macierz RAID-5. Konfiguracja RAID-5 jest szybsza niż RAID-1 (dublowanie).
- F. Nieprawidłowo** Dysk 3 jest częścią macierzy RAID-5 i dlatego w przypadku jego uszkodzenia dane zostaną zachowane.

4. Prawidłowe odpowiedzi: B oraz E

- A. Nieprawidłowo** W pytaniu zostało zaznaczone, że problem dotyczy drugiego woluminu. Oksana nie pomyliła się.
- B. Prawidłowo** Plików stronicowania nie można przenosić i dlatego przedstawiane są przez program analizy defragmentatora dysku za pomocą koloru zielonego. Podobnie dziennik zmian systemu plików NTFS (na woluminach NTFS) jest przedstawiany za pomocą koloru zielonego, jako plik, którego nie można przenosić.
- C. Nieprawidłowo** Pliki skompresowane i szyfrowane mogą być przenoszone.
- D. Nieprawidłowo** Pliki skompresowane i szyfrowane mogą być przenoszone.
- E. Prawidłowo** Plików stronicowania nie można przenosić i dlatego przedstawiane są przez program analizy defragmentatora dysku za pomocą koloru zielonego. Podobnie dziennik zmian systemu plików NTFS (na woluminach NTFS) jest przedstawiany za pomocą koloru zielonego, jako plik, którego nie można przenosić.

>3. Prawidłowa odpowiedź: B

- A. Nieprawidłowo** Jeśli na dysku jest mniej niż 15 % wolnej przestrzeni, proces defragmentacji zakończy się, natomiast defragmentacja dysku nie będzie pełna.
- B. Prawidłowo** Defragmentacja dysku nie powiedzie się jedynie, jeśli na dysku zostały wykryte błędy. Jeśli na dysku występują błędy, system operacyjny kwalifikuje dysk jako „zmieniony”. Jed-

- nym sposobem zmiany tego stanu jest uruchomienie sprawdzania dysku za pomocą programu Chkdsk i wykonanie wymaganych napraw.

- C. Nieprawidłowo** Dyski nie mogą być poddawane defragmentacji, jeżeli są w trybie „offline”.
- D. Nieprawidłowo** Woluminy nie mogą być poddawane defragmentacji, jeżeli są w trybie „offline”.

6. Prawidłowe odpowiedzi: B, C, D oraz E

- A. Nieprawidłowo** Poziom fragmentacji jest poniżej 10-procentowego progu i w takim przypadku nie jest zalecane przeprowadzanie defragmentacji.
- B. Prawidłowo** Poziom fragmentacji jest powyżej 10-procentowego progu i w takim przypadku zalecane jest przeprowadzanie defragmentacji.
- C. Prawidłowo** Patrz uzasadnienie do odpowiedzi **B**.
- D. Prawidłowo** Patrz uzasadnienie do odpowiedzi **B**.
- E. Prawidłowo** Patrz uzasadnienie do odpowiedzi **B**.

Zadanie 1.4

Instalowanie i konfigurowanie urządzeń sprzętu serwera

Sterownik podpisany ma cyfrowy certyfikat firmy Microsoft, który gwarantuje, że sterownik został przetestowany w rozmaitych konfiguracjach i uważany jest za niezawodny. System Windows Server 2003 może zostać tak skonfigurowany, aby sprawdzał podpis cyfrowy i odmawiał instalacji sterownika, który nie został zatwierdzony przez firmę Microsoft.

W systemie może jednak zachodzić potrzeba używania innych sterowników niż takie, które zostały zatwierdzone przez firmę Microsoft. Administratorzy mogą ręcznie określać ustawienia związane z podpisami cyfrowymi w programie *System Properties* (Właściwości systemu). Istnieje możliwość wyboru trzech opcji: *Block* (Blokuj), *Warn* (Ostrzegaj) oraz *Ignore* (Ignoruj). Blokowanie zabrania instalacji niepodpisanych sterowników. Opcja ostrzegania umożliwia przeprowadzenie instalacji, ale użytkownik musi w odpowiednim oknie komunikatu potwierdzić przeprowadzenie instalacji niepodisanego sterownika. Z kolei opcja *Ignore* (Ignoruj) powoduje, że system nie sprawdza podpisu i po prostu instaluje sterownik nie wysyłając nawet komunikatu ostrzegawczego.

Zasoby używane przez urządzenia sprzętu mogą być konfigurowane w programie *Device Manager* (Menedżer urządzeń) poprzez zaznaczenie danego urządzenia i wybranie w menu *Action* (Akcja) polecenia *Properties* (Właściwości). Czasami zainstalowanie nowego urządzenia sprzętu wywołuje konflikt z innym urządzeniem systemu. Konflikty takie najlepiej rozwiązywać dostosowując zasoby urządzeń, takie jak zakresy adresów we/wy czy przerwania IRQ.

Pytania do zadania 1.4

1. Niedawno Oksana zastąpiła Rooslana w funkcji administratora sześciu systemów Windows Server 2003. Te sześć serwerów to systemy autonomiczne, które nie należą do żadnej domeny. Kilka tygodni wcześniej Oksana otrzymała propozycję zakupu napędów taśmowych DAT (Digital Audio Tape) dla każdego systemu Windows Server 2003. W zaplanowanym okresie Oksana wyłączyła serwery i zainstalowała urządzenia. Po uruchomieniu serwerów zalogowała się na każdym z nich, aby przeprowadzić instalację nowego sprzętu za pomocą wywołanego przez system programu *Add New Hardware Wizard* (Kreator dodawania sprzętu). Oksana rozpoczęła instalację oprogramowania, ale zauważyła, że sterowniki nie zostały zainstalowane. Następnie w programie *System Properties* (Właściwości systemu) Oksana sprawdziła ustawienia dotyczące podpisu sterowników i okazało się, że wybrana jest opcja *Block* (Blokuj), przy czym pozostałe opcje są nieaktywne. Pomimo, że sterowniki nie są podpisane przez firmę Microsoft, Oksana zdecydowała się zainstalować te sterowniki i jeśli będą prawidłowo funkcjonowały w serwerach, Oksana zamierza je odpowiednio skonfigurować. Które z wymienionych czynności powinna przedsięwziąć Oksana, aby zezwolić na instalację niepodpisanych sterowników we wszystkich sześciu systemach Windows Server 2003? (wybierz wszystkie właściwe odpowiedzi)

- A. Oksana powinna ponownie skonfigurować obiekt GPO domeny i dla zasady Unsigned Driver Installation Behavior (Zachowanie przy instalacji niepodpisanych sterowników) wybrać opcję Warn But Allow Installation (Ostrzegaj, ale zezwalaj na instalację).
 - B. Oksana powinna ponownie skonfigurować lokalny obiekt GPO i dla zasady Unsigned Driver Installation Behavior (Zachowanie przy instalacji niepodpisanych sterowników) wybrać opcję Warn But Allow Installation (Ostrzegaj, ale zezwalaj na instalację).
 - C. Oksana powinna w programie System Properties (Właściwości systemu) zaznaczyć pole wyboru Administrator Option/Make This Action The System Default (Opcja administratora/Uczyń tę akcję domyślną dla systemu). Spowoduje to uaktywnienie pozostałych opcji i przełączenie z opcji Block (Blokuj) na opcję Warn (Ostrzegaj).
 - D. Oksana powinna ponownie skonfigurować obiekt GPO przydzielony do lokacji, w której znajdują się serwery i dla zasady Unsigned Driver Installation Behavior (Zachowanie przy instalacji niepodpisanych sterowników) powinna wybrać opcję Warn But Allow Installation (Ostrzegaj, ale zezwalaj na instalację).
 - E. Oksana powinna ponownie skonfigurować obiekt GPO dla jednostki organizacyjnej, w której znajdują się serwery i dla zasady Unsigned Driver Installation Behavior (Zachowanie przy instalacji niepodpisanych sterowników) powinna wybrać opcję Warn But Allow Installation (Ostrzegaj, ale zezwalaj na instalację).
- 2.. Administrator w średniej wielkości przedsiębiorstwie sprawdza w swoim laboratorium pięć systemów Windows Server 2003, które należą do jednej domeny przedsiębiorstwa. Ponieważ w przeszłości w firmie wystąpiły problemy spowodowane instalacją niepodisanego sterownika, którą przeprowadził użytkownik posiadający wystarczające uprawnienia, domyślny obiekt GPO domeny został tak skonfigurowany, aby blokował instalowanie niepodpisanych sterowników na wszystkich komputerach należących do domeny. Oprócz tego, obiekt GPO domeny blokuje dla wszystkich użytkowników dostęp do programu System Properties (Właściwości systemu) oraz ukrywa wszystkie ikony pulpitu. Jednakże niedawno administrator odebrał kilka kart sieciowych o wysokiej wydajności, które chce sprawdzić w swoim laboratorium. Sterownik tych kart nie jest podpisany przez firmę Microsoft. Ponieważ administrator nie ma dostępu do programu System Properties (Właściwości systemu), nie może zmienić ustawień obiektu GPO, które blokują instalację niepodisanego sterownika. Która z wymienionych metod pozwoli zastąpić domyślny obiekt GPO domeny i zmienić ustawienia serwerów testowych tak, aby wybrana została opcja Warn (Ostrzegaj), a jednocześnie aby dla pozostałych komputerów domeny ustawienia te nie zostały zmienione?
- A. Należy przeprowadzić edycję lokalnego obiektu GPO każdego serwera i dla zasady Unsigned Driver Installation Behavior (Zachowanie przy instalacji niepodpisanych sterowników) należy wybrać opcję Warn But Allow Installation (Ostrzegaj, ale zezwalaj na instalację).
 - B. Na każdym serwerze należy przeprowadzić edycję GPO stosowanego do lokacji i dla zasady Unsigned Driver Installation Behavior (Zachowanie przy instalacji niepodpisanych sterowników) należy wybrać opcję Warn But Allow Installation (Ostrzegaj, ale zezwalaj na instalację).
 - C. Należy utworzyć nową jednostkę organizacyjną nazwaną Mylab, a następnie przenieść konta komputerów systemów Windows Server 2003 do jednostki organizacyjnej Mylab. W kolejnym kroku należy utworzyć obiekt GPO, w którym dla zasady Unsigned Driver Installation Behavior (Zachowanie przy instalacji niepodpisanych sterowników) określona jest opcja Warn But Allow Installation (Ostrzegaj, ale zezwalaj na instalację) i zastosować obiekt do jednostki organizacyjnej Mylab.

- D. Należy przeprowadzić edycję obiektu GPO domeny i dla zasady Unsigned Driver Installation Behavior (Zachowanie przy instalacji niepodpisanych sterowników) należy wybrać opcję Warn But Allow Installation (Ostrzegaj, ale zezwalaj na instalację).
 - E. Należy utworzyć grupę, a następnie przenieść konta użytkowników do tej grupy. W kolejnym kroku należy utworzyć obiekt GPO, w którym dla zasady Unsigned Driver Installation Behavior (Zachowanie przy instalacji niepodpisanych sterowników) określona jest opcja Warn But Allow Installation (Ostrzegaj, ale zezwalaj na instalację) i zastosować obiekt do nowo utworzonej grupy.
3. Administrator zatrudniony w niepełnym wymiarze godzin opiekuje się przedsiębiorstwem komputerowego składu tekstu. W firmie zainstalowany jest autonomiczny system Windows Server 2003. Administrator niedawno wszedł w posiadanie starszej karty urządzenia umożliwiającego jednoczesne wysyłanie i odbieranie kilku faksów. Karta została zainstalowana w systemie Windows Server 2003, ale nie zadziałała. Administrator sprawdził kartę w programie Device Manager (Menedżer urządzeń) i zauważył, że obok ikony karty faksu został umieszczony znak ostrzegawczy w postaci żółtego wykrzyknika. Administrator podejrzewa, że wystąpił konflikt przerwań (IRQ) z innym urządzeniem zainstalowanym w systemie, a mianowicie ze starszego typu kontrolerem RAID. Która z wymienionych poniżej metod prawidłowo opisuje zmianę konfiguracji karty faksu tak, aby konflikty przerwań IRQ nie występowały pomiędzy kartą faksu a kontrolerem RAID?
- A. W programie Device Manager (Menedżer urządzeń) należy zaznaczyć kontroler RAID. W menu Action (Akcja) należy wybrać polecenie Properties (Właściwości). Następnie należy wybrać zakładkę Resources (Zasoby) i usunąć zaznaczenie z pola wyboru Use Automatic Settings (Użyj ustawień automatycznych). W kolejnym kroku należy kliknąć zasób IRQ, a następnie przycisk Change Settings (Zmień ustawienia). Przewijając listę należy wyszukać takie przerwanie, które nie jest w konflikcie z żadnym innym używanym w systemie. Na koniec należy kliknąć przycisk OK i ponownie uruchomić serwer.
 - B. W programie Device Manager (Menedżer urządzeń) należy zaznaczyć kartę faksu. W menu Action (Akcja) należy wybrać polecenie Properties (Właściwości). Następnie należy wybrać zakładkę Resources (Zasoby) i usunąć zaznaczenie z pola wyboru Use Automatic Settings (Użyj ustawień automatycznych). W kolejnym kroku należy kliknąć zasób IRQ, a następnie przycisk Change Settings (Zmień ustawienia). Przewijając listę należy wyszukać takie przerwanie, które nie jest w konflikcie z żadnym innym używanym w systemie. Na koniec należy kliknąć przycisk OK i ponownie uruchomić serwer.
 - C. W programie Device Manager (Menedżer urządzeń) należy zaznaczyć kontroler RAID. W menu Action (Akcja) należy wybrać polecenie Properties (Właściwości). Następnie należy wybrać zakładkę Resources (Zasoby) i usunąć zaznaczenie z pola wyboru Use Automatic Settings (Użyj ustawień automatycznych). W kolejnym kroku należy kliknąć zasób I/O Range (Zakres we/wy), a następnie przycisk Change Settings (Zmień ustawienia). Przewijając listę należy wyszukać taki zakres, który nie jest w konflikcie z żadnym innym używanym w systemie. Na koniec należy kliknąć przycisk OK i ponownie uruchomić serwer.
 - D. W programie Device Manager (Menedżer urządzeń) należy zaznaczyć kartę faksu. W menu Action (Akcja) należy wybrać polecenie Properties (Właściwości). Następnie należy wybrać zakładkę Resources (Zasoby) i usunąć zaznaczenie z pola wyboru Use Automatic Settings (Użyj ustawień automatycznych). W kolejnym kroku należy kliknąć zasób I/O Range (Zakres we/wy), a następnie przycisk Change Settings (Zmień ustawienia). Przewijając listę należy wyszukać taki zakres, który nie jest w konflikcie z żadnym innym używanym w systemie. Na koniec należy kliknąć przycisk OK i ponownie uruchomić serwer.

- E. W programie Device Manager (Menedżer urządzeń) należy zaznaczyć kontroler RAID. W menu Action (Akcja) należy wybrać polecenie Properties (Właściwości). Na zakładce General (Ogólne), na liście rozwijanej Device Usage (Użycie urządzenia) należy wybrać opcję Do Not Use This Device (Disable) [Nie używaj tego urządzenia (wyłącz)].
 - F. W programie Device Manager (Menedżer urządzeń) należy zaznaczyć kartę faksu. W menu Action (Akcja) należy wybrać polecenie Properties (Właściwości). Na zakładce General (Ogólne), na liście rozwijanej Device Usage (Użycie urządzenia) należy wybrać opcję Do Not Use This Device (Disable) [Nie używaj tego urządzenia (wyłącz)].
4. Administrator niedawno zainstalował trzy starsze karty sieciowe w serwerze członkowskim systemu Windows Server 2003- Dwie karty funkcjonują prawidłowo, natomiast ustawienia trzeciej kart)' są w konflikcie z innym ustawieniami innego urządzenia systemu. W jaki sposób można określić, z którym urządzeniem systemu karta sieciowa wywołała konflikt?
- A. Należy uruchomić program Device Manager (Menedżer urządzeń) i sprawdzić, które urządzenie zostało zaznaczone za pomocą ikony żółtego znaku wykrzyknika.
 - B. Należy przejrzeć dziennik aplikacji i wyszukać wpis opisujący urządzenie, które jest w konflikcie z kartą sieciową.
 - C. Należy uruchomić program Device Manager (Menedżer urządzeń) i zaznaczyć kartę sieciową, która jest zaznaczona za pomocą ikony żółtego znaku wykrzyknika. W menu Action (Akcja) należy wybrać polecenie Properties (Właściwości). Następnie na zakładce Resources (Zasoby) należy usunąć zaznaczenie pola wyboru Use Automatic Settings (Użyj ustawień automatycznych). Zostanie wyświetlone urządzenie, które używa zasobu powodującego konflikt.
 - D. Należy uruchomić program Hardware Troubleshooting Wizard (Kreator rozwiązywania problemów sprzętu) i wybrać opcję Resolve All Device Conflicts (Rozwiąż konflikty wszystkich urządzeń).
 - E. Należy uruchomić program Hardware Troubleshooting Wizard (Kreator rozwiązywania problemów sprzętu) i wybrać opcję Report On All Device Conflicts (Raport konfliktów wszystkich urządzeń).
5. Administrator chce utworzyć listę urządzeń przyłączonych do systemu Windows Server 2003 uporządkowanych według wartości określającej przerwanie (IRQ). Która z wymienionych poniżej metod pozwoli zrealizować to zadanie? (wybierz wszystkie właściwe odpowiedzi)
- A. Należy uruchomić program Device Manager (Menedżer urządzeń) i w menu View (Widok) wybrać opcję Resources By Connection (Zasoby według połączeń).
 - B. Należy uruchomić program Device Manager (Menedżer urządzeń) i w menu View (Widok) wybrać opcję Resources ByType (Zasoby według typu).
 - C. Należy uruchomić program Device Manager (Menedżer urządzeń) i w menu View (Widok) wybrać opcję Devices By Connection (Urządzenia według połączenia).
 - D. Należy uruchomić program Device Manager (Menedżer urządzeń) i w menu View (Widok) wybrać opcję Devices ByType (Urządzenia według typu).
 - E. Zadania tego nie można zrealizować.
6. Do systemu Windows Server 2003 przyłączone są dwa modemy używane do utworzenia wielokrotnego połączenia do lokacji zdalnej przy wykorzystaniu routingu z wybieraniem numerów „na żądanie”. Administrator zauważył, że jakość linii do lokalizacji zdalnej nie jest zbyt dobra i postanowił

zmodyfikować prędkość portów obu modemów. Które z wymienionych poniżej narzędzi administracyjnych można użyć do realizacji tego zadania?

- A. Należy użyć programu Device Manager (Menedżer urządzeń), aby wyszukać modemy i wybrać ich właściwości.
- B. W grupie programów Contro! Panel (Panel sterowania) należy wykorzystać program Phone And Modem Options (Opcje telefonu i modemu), aby dostosować prędkość modemu.
- C. Aby dostosować prędkość modemu, należy użyć konsoli Routing And Remote Access (Routing i dostęp zdalny).
- D. Należy kliknąć prawym przyciskiem myszy ikonę programu My Network Places (Moje miejsca sieciowe) i wybrać polecenie Properties (Właściwości). Następnie należy przeprowadzić edycję właściwości połączenia wielokrotnego i zmniejszyć prędkość połączenia.

7. Administrator opiekuje się siecią w szkole rolniczej. Studenci w swoich pokojach w akademiku instalują różne urządzenia w swoich stacjach roboczych systemu Windows XP Professional. Szkoła zezwala jedynie na to, aby wypożyczone stacje robocze Windows XP Professional mógł) łączyć się z siecią akademika. Zarządzenie to zezwala administratorowi ograniczać organizowanie niepożądanego działania, takiej jak udostępnianie plików w sieci P2P (peer-to-peer).

Grupa współpracowników administratora jest odpowiedzialna za konserwację stacji roboczych sieci szkoły. Analiza czasu poświęconego obsłudze stacji roboczych wykazała, że 30% tego czasu poświęcone jest uszkodzeniom spowodowanym przez zainstalowanie niepodpisanych sterowników urządzeń. Administrator postanowił uniemożliwić instalację niepodpisanych sterowników w pokojach akademika. Która z wymienionych poniżej metod pozwoli zrealizować to zadanie, przy założeniu, że ustawienia innych komputerów domeny nie ulegną zmianie?

- A. Należy przenieść wszystkie konta komputerów stacji roboczych w pokojach akademika do nowo utworzonej jednostki organizacyjnej nazwanej Dormwksn. Następnie należy utworzyć obiekt GPO, w którym zasada Unsigned Driver Installation Behavior zostanie określona poprzez opcję Warn But Allow Installation (Ostrzegaj, ale zezwalaj na instalację). Na koniec należy obiekt GPO przypisać do jednostki organizacyjnej Dormwksn.
- B. Należy utworzyć grupę nazwaną Dormwksn i do tej grupy dodać wszystkie konta komputerów stacji roboczych znajdujących się w pokojach akademika. Następnie należy utworzyć obiekt GPO, w którym zasada Unsigned Driver Installation Behavior zostanie określona poprzez opcję Warn But Allow Installation (Ostrzegaj, ale zezwalaj na instalację). Na koniec należy obiekt GPO przypisać do grupy Dormwksn.
- C. Należy utworzyć grupę nazwaną Dormwksn i do tej grupy dodać wszystkie konta użytkowników przydzielonych studentom w pokojach akademika. Następnie należy utworzyć obiekt GPO, w którym zasada Unsigned Driver Installation Behavior zostanie określona poprzez opcję Warn But Allow Installation (Ostrzegaj, ale zezwalaj na instalację). Na koniec należy obiekt GPO przypisać do grupy Dormwksn.
- D. Należy przenieść wszystkie konta komputerów stacji roboczych w pokojach akademika do nowo utworzonej jednostki organizacyjnej nazwanej Dormwksn. Następnie należy utworzyć obiekt GPO, w którym zasada Unsigned Driver Installation Behavior zostanie określona poprzez opcję Do Not Allow Installation (Nie zezwalaj na instalację). Na koniec należy obiekt GPO przypisać do jednostki organizacyjnej Dormwksn.

- E. Należy utworzyć grupę nazwaną Dormwksn i do tej grupy dodać wszystkie konta komputerów stacji roboczych znajdujących się w pokojach akademika. Następnie należy utworzyć obiekt GPO, w którym zasada Unsigned Driver Installation Behavior zostanie określona poprzez opcję Do Not Allow Installation (Nie zezwalaj na instalację). Na koniec należy obiekt GPO przypisać do grupy Dormwksn.

Odpowiedzi do zadania 1.4

■L. Prawidłowe odpowiedzi: B oraz C

- A. **Nieprawidłowo** Każdy z sześciu systemów jest serwerem autonomicznym i nie należy do żadnej domeny. Edycja obiektów GPO, które są stosowane do domeny, nie ma wpływu na te serwery.
- B. **Prawidłowo** Pozostałe opcje są nieaktywne, ponieważ nie zostało zaznaczone pole wyboru Administrator Option/Make This Action The System Default (Opcja administratora/Uczyń tę akcję domyślną dla systemu). Zaznaczenie tego pola wyboru oznacza, że każda zmiana ma natychmiastowe odzwierciedlenie w lokalnym obiekcie GPO. Aby uzyskać ten sam rezultat, można również przeprowadzić edycję lokalnego obiektu GPO.
- C. **Prawidłowo** Patrz uzasadnienie do odpowiedzi B.
- D. **Nieprawidłowo** Patrz uzasadnienie do odpowiedzi A.
- E. **Nieprawidłowo** Patrz uzasadnienie do odpowiedzi A.

2.. Prawidłowa odpowiedź: C

- A. **Nieprawidłowo** Ustawienia lokalnych obiektów GPO są zastępowane przez ustawienia obiektów GPO lokacji, domeny i jednostki organizacyjnej. Ponieważ obiekt GPO opisywany w pytaniu dotyczy poziomu domeny, jego ustawienia będą miały pierwszeństwo przed ustawieniami lokalnego obiektu GPO.
- B. **Nieprawidłowo** Ustawienia lokalnych obiektów GPO są zastępowane przez ustawienia obiektów GPO lokacji, domeny i jednostki organizacyjnej. Ponieważ obiekt GPO opisywany w pytaniu dotyczy poziomu domeny, jego ustawienia będą miały pierwszeństwo przed ustawieniami obiektu GPO stosowanego do lokacji.
- C. **Prawidłowo** Poprzez utworzenie jednostki organizacyjnej i przeniesienie określonych kont komputera środowiska testowego do tej jednostki organizacyjnej, zasada grupy zostanie zastosowana tylko do tych konkretnych systemów. Ustawienia zasady grupy zastosowanej na poziomie jednostki organizacyjnej zastępują ustawienia dotyczące poziomu lokacji lub domeny, tak więc zasada dotycząca podpisywania sterowników zastosowana na poziomie jednostki organizacyjnej zastąpi domyślny obiekt GPO domeny dla komputerów, które należą do tej jednostki organizacyjnej.
- D. **Nieprawidłowo** Działanie takie zmieni ustawienia dla wszystkich komputerów domeny, na co nie zezwalają założenia postawione w pytaniu.
- E. **Nieprawidłowo** Obiekt GPO nie może być zastosowany bezpośrednio do grupy. Obiekty GPO mogą być stosowane jedynie do lokacji, domeny, jednostki organizacyjnej oraz lokalnie. Grupy mogą być używane do modyfikowania ustawień określających, do których użytkowników stosują się obiekty GPO lokacji, domeny lub jednostki organizacyjnej.

3. Prawidłowa odpowiedź: B

- A. Nieprawidłowo** Działanie takie zmieni konfigurację kontrolera RAID, a nie konfigurację karty faksu. Pytanie dotyczy sposobu, w jaki powinna zostać zmieniona konfiguracja karty faksu.
- B. Prawidłowo** Pierwszą rzeczą jest upewnienie się, że dla karty faksu dostosowywane są ustawienia przerwań (IRQ), a nie adresów we/wy. Po określeniu ustawień wyświetlone zostanie okno dialogowe informujące, czy nie wystąpiły inne konflikty. Należy tak długo zmieniać ustawienia określające przerwanie, aż zostanie wyszukane przerwanie, które jest wolne. Nie można pozbyć się konfliktu przerwań pomiędzy kartą faksu a kontrolerem RAID, przy jednoczesnym występowaniu konfliktu tej karty i innego urządzenia.
- C. Nieprawidłowo** Działanie to konfiguruje niewłaściwe urządzenie i nieodpowiedni zasób (zakres we/wy zamiast IRQ).
- D. Nieprawidłowo** Działanie to konfiguruje nieodpowiedni zasób (zakres we/wy zamiast IRQ).
- E. Nieprawidłowo** Metoda ta po prostu wyłączy urządzenie, a nie rozwiąże występującego konfliktu. Wyłączenie kontrolera RAID nie jest również przydatnym rozwiązaniem związanym z obsługą sta bilnego działania serwera.
- F. Nieprawidłowo** Działanie to po prostu wyłączy urządzenie, a nie rozwiąże występującego konfliktu.

4. Prawidłowa odpowiedź: C

- A. Nieprawidłowo** Ponieważ inne urządzenie funkcjonuje, ma pierwszeństwo w stosunku do trzeciej karty sieciowej. Urządzenie to nie będzie zaznaczone jako takie, dla którego wystąpił problem.
- B. Nieprawidłowo** Jeśli informacja o konflikcie została zaprotokołowana, zostanie zapisana w dzienniku systemu, a nie w dzienniku aplikacji
- C. Prawidłowo** Dzięki zaznaczeniu zakładki Resources (Zasoby) w oknie dialogowym Device Properties (Właściwości urządzenia) wygenerowana zostanie lista wszystkich urządzeń, których ustawienia są w konflikcie z ustawieniami wybranego urządzenia. Na tym etapie można zdecydować, czy konfigurować urządzenie ręcznie tak, aby wykorzystywało inne zasoby lub jeśli to niemożliwe, sprawdzić zasoby drugiego urządzenia (będącego w konflikcie), aby przekonać się, czy nie można zmienić jego ustawień.
- D. Nieprawidłowo** W programie Hardware Troubleshooting Wizard (Kreator rozwiązywania problemów sprzętu) nie istnieje opcja, o której mowa w odpowiedzi.
- E. Nieprawidłowo** Patrz uzasadnienie do odpowiedzi D.

O. Prawidłowe odpowiedzi: A oraz B

- A. Prawidłowo** Lista urządzeń uporządkowana według przerwania (IRQ) może być wygenerowana w programie Device Manager (Menedżer urządzeń) poprzez wybranie polecenia przeglądania według zasobu lub według typu. Aby określić numer przerwania danego urządzenia w innych widokach programu, należy przejrzeć właściwości tego urządzenia.
- B. Prawidłowo** Patrz uzasadnienie do odpowiedzi A.
- C. Nieprawidłowo** Opcja ta nie sortuje urządzeń według przerwania (IRQ).
- D. Nieprawidłowo** Opcja ta nie sortuje urządzeń według przerwania (IRL).
- E. Nieprawidłowo** Patrz uzasadnienie do odpowiedzi A

O. Prawidłowa odpowiedź: B

- A. Nieprawidłowo** Prędkość portu modemu nie może być modyfikowana przy użyciu programu Device Manager (Menedżer urządzeń).
- B. Prawidłowo** Ponieważ prędkości modemu muszą być dostosowywane dla kilku połączeń, najlepszym rozwiązaniem jest edycja właściwości modemu przy użyciu programu Phone And Modem Options (Opcje telefonu i modemu) znajdującego się w grupie programów Control panel (Panel sterowania).
- C. Nieprawidłowo** Prędkość portu modemu nie może być modyfikowana przy użyciu konsoli MMC — Routing And Remote Access (Routing i dostęp zdalny).
- E. Nieprawidłowo** Program Network Connections (Połączenia sieciowe), znajdujący się w module My Network Places (Moje miejsca sieciowe), nie może być używany do modyfikowania prędkości portu modemu.

/. **Prawidłowa odpowiedź: D**

- A. Nieprawidłowo** Opcja ta umożliwia instalację niepodpisanego sterownika zamiast ją zablokować.
- B. Nieprawidłowo** Obiekty GPO nie mogą być stosowane do grup dystrybucji lub zabezpieczeń.
- C. Nieprawidłowo** Obiekty GPO nie mogą być stosowane do grup dystrybucji lub zabezpieczeń.
- D. Prawidłowo** Obiekty GPO mogą być stosowane do lokacji, domen i jednostek organizacyjnych. Istnieją również obiekty GPO, które mogą być edytowane i stosowane lokalnie. Zasada musi być określona poprzez opcję Do Not Allow Installation (Nie zezwalaj na instalację).
- E. Nieprawidłowo** Obiekty GPO nie mogą być stosowane do grup dystrybucji lub zabezpieczeń.

15 Zarządzanie użytkownikami, komputerami i grupami (2.0)



Podczas wykonywania swojej codziennej pracy użytkownicy potrzebują korzystać z zasobów sieci, ale dostęp do nich powinien być uwierzytelniony. Dostęp do zasobów uzyskiwany jest poprzez logowanie w komputerze, który ma dostęp do domeny, a następnie potwierdzenie członkostwa w grupie domeny. Uprawnienia do zasobów mogą być przypisywane tylko dla użytkowników, grup i komputerów rozpoznawanych przez domenę.

Tworzenie kont użytkowników, grup i komputerów może być przeprowadzane ręcznie za pomocą narzędzi interfejsu systemu Microsoft Windows Server 2003 lub automatycznie za pomocą narzędzi i skryptów wiersza poleceń. Znajomość metod tworzenia kont użytkowników, grup i komputerów jest ważnym elementem umożliwiającym pomyślne zdanie egzaminu.

Z metodami tworzenia oraz zarządzania kontami użytkowników, grup i komputerów powiązane jest przydzielanie uprawnień odpowiednich do wymaganego poziomu dostępu, a także zarządzanie danymi dotyczącymi kont, takimi jak skrypty logowania czy profile użytkowników.

Sprawdzanie umiejętności i sugerowane ćwiczenia praktyczne

Poniżej przedstawiono umiejętności potrzebne do opanowania tematu „Zarządzanie użytkownikami, komputerami i grupami” objętego egzaminem 70-290 - *Zarządzanie i obsługa środowiska Windows Server 2003*:

- Zarządzanie lokalnymi, mobilnymi oraz obowiązkowymi profilami użytkowników.
 - » Zadanie kontrolne 1: Skonfigurowanie profilu mobilnego o bezpiecznym dostępie. Określenie dla tego użytkownika uprawnień do indywidualnego foldera profilu. Zapewnienie, że pozostali użytkownicy nie będą mieli dostępu do danych oraz że ci użytkownicy mogą logować się i wykorzystywać dane swojego profilu.
 - » Zadanie kontrolne 2: Zmiana konfiguracji profilu z mobilnego na obowiązkowy. Grupy użytkowników współdzielących profil nie powinny posiadać uprawnień umożliwiających takie zmiany. W tym celu należy zmienić nazwę profilu współdzielonego Ntuser.dat na Ntuser.man. Korzystanie z profilu obowiązkowego nie powinno dla użytkowników współużytkujących profil ograniczać możliwości tworzenia, modyfikowania lub usuwania plików danych wewnątrz struktury foldera profilu.
- Tworzenie i zarządzanie kontami komputerów w środowisku usługi Active Directory.
 - » Zadanie kontrolne 1: Wykorzystywanie przystawki konsoli MMC, Active Directory User And Computers (Użytkownicy i komputery usługi Active Directory), do tworzenia w domenie nowych kont komputera.
 - » Zadanie kontrolne 2: Przyłączanie nowej stacji roboczej systemu Windows XP do domeny systemu Windows Server 2003. Sprawdzanie za pomocą przystawki Active Directory Users And

Computers (Użytkownicy i komputery usługi Active Directory), czy nowe konta komputerów zostały dodane do katalogu.

- Tworzenie grup oraz zarządzanie grupami.
 - » Zadanie kontrolne 1: Korzystanie z ręcznej metody tworzenia kont użytkowników, grup i komputerów. Korzystanie z przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) oraz narzędzi wiersza poleceń usługi katalogowej (Directory Service) do tworzenia kont użytkowników, grup i komputerów. Modyfikowanie właściwości kont użytkowników oraz testowanie rezultatów wprowadzonych zmian. Wykorzystywanie interfejsu System Properties (Właściwości systemu) na pulpicie komputera do przyłączenia komputerów do domeny.
 - » Zadanie kontrolne 2: Używanie automatycznych metod tworzenia kont użytkowników, grup i komputerów.
 - » Zadanie kontrolne 3: Rejestrowanie użytkowników, grup i komputerów jako członków grup za pomocą zarówno interfejsu systemu, jak i interfejsu wiersza poleceń.
 - » Zadanie kontrolne 4: Identyfikowanie członkostwa grupy w złożonej hierarchii grup. Wykorzystywanie narzędzi usługi katalogowej (Directory Service) interfejsu wiersza poleceń do całościowej analizy.
- Tworzenie i zarządzanie kontami użytkowników.
 - » Zadanie kontrolne 1: Utworzenie czterech różnych kont użytkowników za pomocą przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory).
 - » Zadanie kontrolne 2: Utworzenie pojedynczego konta użytkownika za pomocą przystawki Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory). Określanie dla użytkowników specyficznych godzin logowania i członkostwa w grupie. Utworzenie trzech podobnych kont przy użyciu polecenia kopiowania.
- Rozwiązywanie problemów dotyczących kont komputera.
 - » Zadanie kontrolne 1: Utworzenie konta komputera za pomocą przystawki Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory). Przeprowadzenie zmiany grupy, która może dodawać komputery do domeny (z grupy Administratorzy domeny na grupę Użytkownicy), w oknie dialogowym przystawki.
 - » Zadanie kontrolne 2: Lokalizowanie i sprawdzenie konta komputera systemu Windows XP, które zostało niedawno przyłączone do domeny, za pomocą przystawki Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory). Wyłączenie konta komputera przy użyciu menu Action (Akcja). Próba wykorzystania tego konta do uzyskania dostępu do domeny.
- Rozwiązywanie problemów kont użytkowników.
 - » Zadanie kontrolne 1: Modyfikowanie domyślnego obiektu GPO domeny oraz zmiana wartości progu Account Lockout (Blokowanie konta) tak, aby blokowanie następowało po trzech nieudanych próbach. Logowanie do domeny systemu Windows Server 2003 przy użyciu nieprawidłowego hasła, aż do momentu zablokowania konta. Wykorzystanie przystawki Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) do ponownego włączenia konta.
 - » Zadanie kontrolne 2: Wyzerowanie hasła konta użytkownika i skonfigurowanie konta tak, aby użytkownik musiał zmienić swoje hasło podczas następnego logowania w systemie.

- Rozwiązywanie problemów dotyczących uwierzytelnienia użytkownika.
 - » Zadanie kontrolne 1: Edycja domyślnej zasady GPO domeny w celu zmiany zasad hasła. Konfigurowanie zasady Account Lockout Threshold (Próg blokady konta) tak, aby blokada następowała po trzech nieudanych próbach logowania. Określenie wartości 30 minut dla zasady Account Lockout Duration (Czas trwania blokady konta).
 - » Zadanie kontrolne 2: Edycja domyślnej zasady GPO domeny w celu zmiany zasad hasła. Określenie wartości 10 (hasel) dla zasady Enforce Password History (Wymuszaj tworzenie historii hasel). Ustawienie wartości 2 (dni) dla zasady Minimum Password Age (Minimalny okres ważności hasła). Określenie wartości 10 (znaków) dla zasady Minimum Password Length (Minimalna długość hasła).

Lektura uzupełniająca

Przed przystąpieniem do egzaminu należy przestudiować przedstawione poniżej dodatkowe źródła informacji.

Zadanie 2.1

W rozdziale 3 „Konta użytkowników” omówione zostały metody tworzenia i zarządzania kontami i profilami użytkowników.

Rozdział 4 „Konta grup” zawiera dodatkowe informacje dotyczące automatycznego tworzenia grup, typów i zakresów grup oraz zagnieżdżania grup.

Pozycja Microsoft Corporation: *Microsoft Windows Server 2003 Deployment Kit*. Tom: *Designing a Managed Environment*. Redmond, Washington: Microsoft Press, 2003. umieszczona na witrynie Web firmy Microsoft pod adresem: <http://imvw.microsoft.com/windowsserver2003/tcchinfo/reskit/depltykit.mspix>.

Zadanie 2.2

Rozdział 5 „Konta komputerów” zawiera informacje dotyczące tworzenia kont komputerów przy wykorzystaniu metod automatycznych i ręcznych, opisuje różne metody podłączania kont komputerów do domeny oraz metod zerowania hasel kont komputerów.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat „Zarządzanie komputerami”.

Zadanie 2.3

W rozdziale 4 „Konta grup” omówione zostały metody tworzenia oraz zarządzania kontami i profilami użytkowników.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat „Zarządzanie użytkownikami i grupami domeny: Grupy”.

Zadanie 2.4

W rozdziale 3 „Konta użytkowników” omówione zostały zagadnienia związane z tworzeniem oraz zarządzaniem kontami i profilami użytkowników.

Microsoft Corporation- Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Zarządzanie użytkownikami i grupami domeny: Konta użytkowników i komputerów”.

Zadanie 2.5

Rozdział 5 „Konta komputerów” zawiera informacje dotyczące metod ręcznego i automatycznego tworzenia kont komputerów, różnych metod przyłączania konta komputera do domeny oraz metod zerowania haseł kont komputerów.

Artykuł 325850, opublikowany przez firmę Microsoft Corporation — Windows Server 2003 Knowledge Base: „How to Use netdom.exe to Reset Machine Account Passwords of a Windows Server 2003 Domain Controller”.

Zadanie 2.6

Rozdział 3 „Konta użytkowników” opisuje niektóre techniki rozwiązywania problemów dotyczących kont użytkowników i komputerów.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: Zarządzanie użytkownikami i grupami domeny: Konta użytkowników i komputerów.

Zadanie 2.7

W rozdziale 3 „Konta użytkowników” opisane zostały metody tworzenia oraz zarządzania profilami i kontami użytkowników.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: Zarządzanie użytkownikami i grupami domeny: Konta użytkowników i komputerów.

Zadanie 2.1

Zarządzanie lokalnymi, mobilnymi i obowiązkowymi profilami

Po zalogowaniu w systemie dla użytkownika pobierany jest pewien zestaw danych nazywany profilem użytkownika. Profil ten zawiera ustawienia aplikacji, pliki i ustawienia pulpitu oraz dla ustawień domyślnych inne foldery przeznaczone do przechowywania plików, takie jak My Documents (Moje dokumenty) czy My Pictures (Moje obrazy). Foldery te mogą zostać przekierowane za pomocą zasady grupy lub indywidualnie poprzez ustawienia konta użytkownika. Przekierowane profile mogą być przechowywane w dowolnej lokalizacji w sieci i jeśli lokalizacja profilu w sieci zostaje przypisana do użytkownika, profil traktowany jest jako profil mobilny. Dostęp do profili mobilnych może być uzyskiwany z dowolnego komputera, w którym użytkownik się zalogował, a profil ten zostanie pobrany i używany przez komputer lokalny. Jeśli profil mobilny zostanie skonfigurowany jako obowiązkowy, żadne zmiany poczynione przez użytkownika nie będą zapisywane w profilu. W praktyce cecha ta tworzy możliwość wykorzystywania profilu przez kilku użytkowników.

Pytania do zadania 2.1

1. Przedsiębiorstwo rozmieściło 35 komputerów w różnych miejscach budynku tak, aby pracownicy mogli w różnych miejscach uzyskiwać dostęp do informacji, nie tylko za pomocą pulpitu swojego komputera. Komputery te używane są do sprawdzania poczty elektronicznej, do czytania wiadomości rozsyłanych wewnątrz firmy oraz do zapoznawania się z informacjami o zasadach dostępu do intranetu przedsiębiorstwa.
 - . Zadaniem administratora jest zmiana ustawień pulpitu jednego z tych udostępnionych komputerów tak, aby spełnione zostały postawione wymagania oraz zastosowanie tych ustawień do pozostałych udostępnionych komputerów.

Co administrator powinien zrobić?

 - A. Skonfigurować profil obowiązkowy i przypisać go wszystkim użytkownikom domeny.
 - B. Skonfigurować profil obowiązkowy i przypisać go do wszystkich komputerów udostępnionych.
 - C. Skonfigurować profil mobilny i przypisać go każdemu użytkownikowi domeny.
 - D. Skonfigurować profil mobilny i przypisać go do każdego komputera udostępnionego.
- <Ł. Administrator jest odpowiedzialny za obsługę kont i profili użytkowników oraz poziomy dostępu do zasobów sieci. Obecnie wszyscy użytkownicy współdzielą w sieci pojedynczy profil, który pozwala na proste dodawanie i usuwanie obiektów pulpitu użytkowników, ale umożliwia również zapisywanie zmian pulpitu przeprowadzonych przez użytkownika. Administrator chce zachować możliwość centralnego zarządzania pulpitemi użytkowników, ale jednocześnie zabronić użytkownikom dokonywania zmian ustawień pulpitu.

Co administrator powinien zrobić?

- A. Na stronie właściwości foldera Security (Zabezpieczenia) dotyczącego profilu skonfigurować uprawnienia tak, aby zabraniały zapisu.
- B. Na stronie właściwości foldera Security (Zabezpieczenia) dotyczącego profilu skonfigurować uprawnienia tak, aby zezwolenie dotyczyło jedynie operacji odczytu.
- C. Zmodyfikować atrybuty foldera profilu tak, aby ustawiony został jedynie atrybut Read Only (Tylko odczyt).
- D. W folderze profilu zmienić nazwę pliku Ntuser.dat na Ntuser.man.

- O. W przedsiębiorstwie od 10 miesięcy używane są profile mobilne dla członków działu Sales oraz Information Technology. Dane profilu przechowywane są na członkowskim serwerze działającym pod kontrolą systemu Microsoft Windows Server 2003. System plików woluminu tego serwera to FAT32. Folder udostępniony przechowujący profile został nazwany Profshare. Ścieżki profili są prawidłowo skonfigurowane we właściwościach każdego użytkownika. Niedawno administrator zauważył, że niektórzy użytkownicy mogą uzyskiwać dostęp do danych zamieszczonych w profilach innych użytkowników. Administrator chce zabezpieczyć mobilne profile użytkowników sieci tak, aby jedynie użytkownik, który zalogował się do profilu, miał dostęp do danych zawartych w tym profilu.

Co administrator powinien zrobić? (wybierz dwie odpowiedzi, gdyż każda odpowiedź jest częścią całego rozwiązania)

- A. Należy przypisać uprawnienia Read (Odczyt) oraz Write (Zapis) do foldera, gdzie przechowywane są profile jedynie dla tych użytkowników, którzy przechowują profile mobilne.
- B. Należy włączyć podpisywanie bloku SMB (Server Message Block) na serwerach, które przechowują profil.
- C. Należy włączyć podpisywanie bloku SMB (Server Message Block) na każdym komputerze, który używa profilu mobilnego.
- D. Należy przeprowadzić konwersję systemu plików woluminu przechowującego profile do systemu NTFS.
- E. Należy skonfigurować system plików EFS (Encrypting Files System), aby zaszyfrować folder przechowujący profile.

4. W przedsiębiorstwie zdecydowano się umieścić w holu komputery umożliwiające uzyskanie dostępu do publicznych informacji o firmie. Członkowie działu Sales powinni logować się na tych komputerach i uzyskiwać dostęp zgodny z ich uprawnieniami określonymi w domenie (w celu przeprowadzania prezentacji dla swoich klientów), natomiast użytkownicy publiczni powinni używać konta Guest (Gość).

Członkowie działu Sales, których komputery i konta użytkowników znajdują się w jednostce organizacyjnej Sales, używają profili mobilnych. Komputery udostępnione w holu umieszczone są w jednostce organizacyjnej Lobby.

Administrator nie chce, aby podczas logowania w komputerach udostępnionych (w holu) używane były profile komputerów użytkowników grupy Sales. Wszyscy użytkownicy komputerów umieszczonych w holu powinni mieć taki sam pulpit bez możliwości zapisywania zmian.

Jakie zmiany konfiguracji musi przeprowadzić administrator? (wybierz trzy odpowiedzi, gdyż każda odpowiedź jest częścią całego rozwiązania)

- A. Należy skonfigurować profil lokalny po zalogowaniu się w jednym komputerów holu używając konta Guest (Gość). Skopiować profil do foldera Default User. Powtórzyć ten proces dla każdego komputera umieszczonego w holu.
- B. Należy skonfigurować profil lokalny na jednym z komputerów umieszczonych w holu. Skopiować profil do foldera Default User w katalogu na serwerze przechowującym profile mobilne.
- C. Należy utworzyć obiekt zasady grupy GPO (Group Policy Object) powiązany z jednostką organizacyjną Sales. W gałęzi w gałęzi Computer Configuration włączyć zasadę Only Allow Local User Profiles (Zezwalaj tylko na lokalne profile użytkowników).
- D. Należy utworzyć obiekt zasady grupy GPO (Group Policy Object) powiązany z jednostką organizacyjną Lobby. W gałęzi w gałęzi Computer Configuration włączyć zasadę Only Allow Local User Profiles (Zezwalaj tylko na lokalne profile użytkowników).
- E. W folderze Default User należy zmienić nazwę pliku Ntuser.dat na Ntuser.man dla każdego komputera umieszczonego w holu.
- F. W folderze Default User należy zmienić nazwę pliku Ntuser.dat na Ntuser.man w katalogu serwera przechowującego profile mobilne.
- G. Należy poinstruować każdego użytkownika działu sprzedaży (Sales), aby wylogowywał się z komputera umieszczonego w holu. Skopiować zawartość foldera Default User każdego komputera w holu do każdego katalogu profilu użytkownika.

Odpowiedzi do zadania 2.1

X. Prawidłowa odpowiedź: C

- A. **Nieprawidłowo** Profile obowiązkowe nie pozwalają na zachowywanie przeprowadzanych przez użytkownika zmian ustawień pulpitu.
- B. **Nieprawidłowo** Profil obowiązkowy nie pozwala na zapisywanie zmian ustawień. Poza tym, profile przypisywane są użytkownikom, a nie komputerom.
- C. **Prawidłowo** Użytkownik, do którego stosowany jest mobilny profil, korzysta ze swoich ustawień na każdym komputerze, na którym się zalogował.
- D. **Nieprawidłowo** Profile przypisywane są użytkownikom, a nie komputerom.

^ . Prawidłowa odpowiedź: D

- A. **Nieprawidłowo** Działanie takie spowoduje, że profil nie zostanie pobrany, ponieważ podczas pobierania profilu wymagany jest dostęp umożliwiający odczyt i zapis.
- B. **Nieprawidłowo** Patrz uzasadnienie do odpowiedzi A.
- C. **Nieprawidłowo** Patrz uzasadnienie do odpowiedzi A.
- D. **Prawidłowo** Działanie takie umożliwi prawidłowe otwieranie profilu, ale nie zezwala na zapis zmian ustawień dokonanych przez użytkownika w momencie wylogowania się z systemu.

O. Prawidłowe odpowiedzi: A oraz D

- A. **Prawidłowo** Działanie takie umożliwia odczyt danych zawartych w mobilnym profilu użytkownika tylko tym użytkownikom, dla których konfiguracja określa stosowanie takiego profilu (działy Sales oraz IT). Dostęp dla wszystkich pozostałych użytkowników zostanie zabroniony. Rozwiązanie takie może być zastosowane, jeśli system plików woluminu przechowującego dane profile zostanie

zmieniony na NTFS. Systemu FAT32 nie można skonfigurować tak, aby przydzielać indywidualne uprawnienia.

- B. **Nieprawidłowo** Działanie takie zabezpiecza w pewnym stopniu integralność każdego pakietu transmitowanego w sieci, ale nie zapobiega uzyskiwaniu nieuwierzytnionego dostępu pracownikom podczas zapisów na dysku.
- C. **Nieprawidłowo** Działanie takie zabezpiecza w pewnym stopniu integralność każdego pakietu transmitowanego w sieci, ale nie zapobiega uzyskiwaniu nieuwierzytnionego dostępu pracownikom podczas zapisów na dysku.
- D. **Prawidłowo** Działanie takie umożliwia kontrolę dostępu do profilu podczas zapisywania profilu na dysku. Istniejący system plików FAT32 nie zezwala na ustawianie takich uprawnień.
- E. **Nieprawidłowo** Dane profilu mobilnego nie mogą zostać zaszyfrowane przez system.

4. **Prawidłowe odpowiedzi: A, D oraz E**

- A. **Prawidłowo** Po zalogowaniu się za pomocą konta Guest (Gość), utworzony zostaje profil lokalny. Profil ten może zostać dowolnie skonfigurowany. Po skopiowaniu profilu do foldera Default User, profil ten będzie wykorzystywany początkowo, jeśli rejestrujący się w systemie użytkownik nie będzie używał profilu mobilnego.
- B. **Nieprawidłowo** Dane foldera Default User znajdujące się na serwerze profili są używane do utworzenia nowych profili mobilnych, które w tym miejscu nie będą wykorzystywane.
- C. **Nieprawidłowo** Ten obiekt GPO jest zasadą dotyczącą komputera, a w tej sytuacji obiektami są komputery w holu, a nie w dziale sprzedaży (Sales).
- D. **Prawidłowo** Ustawienia tego obiektu GPO uniemożliwią używanie na komputerze profilu mobilnego. Jeśli do komputerów znajdujących się w holu będzie stosowana ta zasada, zezwalała będzie jedynie na stosowanie profilu lokalnego i zabroni stosowania profilu mobilnego.
- E. **Prawidłowo** Konfiguracja taka nie zezwala na dokonywanie zmian profili lokalnych.
- F. **Nieprawidłowo** Działanie takie spowoduje, że nie będzie można zmieniać wszystkich nowych profili mobilnych, a nie to było celem wyznaczonym w pytaniu.
- G. **Nieprawidłowo** Działanie takie zastąpi jednorazowo mobilny profil użytkownika. Przy następnym zalogowaniu użytkownika zostanie przywrócone działanie profilu mobilnego.

Zadanie 2.2

Tworzenie i zarządzanie kontami komputerów w środowisku usługi Active Directory

Konta komputerów, będące jednym z trzech rodzajów podmiotów zabezpieczeń, mają właściwości bardzo podobne do użytkowników i grup. Komputery mogą posiadać zestaw uprawnień do zasobów oraz mogą być członkami grup. Do komputerów mogą stosować się obiekty GPO (Group Policy Objects), komputery mogą przetwarzać skrypty logowania i wylogowywania oraz wykonywać zadania w połączeniu z innymi obiektami sieci.

Administracja tych obiektów dotyczy tworzenia kont komputerów, nazywania i konfigurowania kont oraz zarządzania uprawnieniami. Zadania te mogą być realizowane za pomocą przystawki konsoli MMC - programu Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) lub przy użyciu szeregu narzędzi wiersza poleceń.

Pytania do zadania 2.2

1. W domenie systemu Windows Server 2003 nazwanej contoso.com, w jednostce organizacyjnej Pservers (Serwery druku) znajduje się serwer członkowski nazwany Pserver01. Serwer ten był odłączony przez dłuższy okres i nie komunikuje się z innymi komputerami domeny w celu realizowania zadań wydruku. Administrator zauważył, że hasło konta tego komputera w domenie powinno zostać wyzerowane.

Które polecenie prawidłowo wyzeruje konto komputera?

- A. dsmod CN=pserver01,CN=PSERVERS,DC=contoso,DC=com -reset
- B. dsmod computer pserver01 contoso.com -reset
- C. dsmod contoso\pserver01 -reset
- D. dsmod computer CN=pserver01,CN=PSERVERS,DC=contoso,DC=com -reset

- £.. Kontroler domeny działający pod kontrolą systemu Windows Server 2003 nie przeprowadza prawidłowo replikacji z innymi kontrolerami domeny contoso.com. W programie Event Viewer (Podgląd zdarzeń) administrator zauważył komunikat informujący o tym, że nastąpiła odmowa dostępu do tego kontrolera domeny. Administrator podejrzewa, że hasło kontrolera domeny nie zostało poprawnie zsynchronizowane z innymi kontrolerami domeny i powinno zostać wyzerowane.

Co administrator powinien zrobić?

- A. W przystawce Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) należy kliknąć prawym przyciskiem myszy obiekt komputera i wybrać polecenie Reset Account (Resetuj konto).

- B. Na kontrolerze domeny należy użyć narzędzia wiersza poleceń Dsmod do wyzerowania hasła komputera.
- C. Na kontrolerze domeny należy użyć narzędzia wiersza poleceń Netdom do wyzerowania hasła komputera.
- D. Należy ponownie uruchomić serwer w trybie programu Konsola odzyskiwania i za jego pomocą wyzerować konto komputera.

ó. Administrator zarządza domeną systemu Windows Server 2003 nazwaną contoso.com. Jako część restrukturyzacji domeny, do lasu zostały dodane dwie nowe domeny podrzędne: invest.contoso.com oraz cast.contoso.com. Trzy konta komputerów serwerów plików domeny contoso.com należy przenieść do domeny west.contoso.com. Wszystkie przenoszone serwery są serwerami członkowskimi działającymi pod kontrolą systemu Windows Server 2003.

Co administrator powinien zrobić?

- A. Do przeniesienia kont komputerów należy użyć przystawki Active Directory Domains And Trusts (Domeny i relacje zaufania usługi Active Directory).
- B. Do przeniesienia kont komputerów należy użyć przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory).
- C. Do przeniesienia kont komputerów należy użyć narzędzia wiersza poleceń Movetrec.
- D. Do przeniesienia kont komputerów należy użyć programu narzędziowego Dsmove.

4. Należy utworzyć plik wsadowy, który zautomatyzuje określanie atrybutów komputerów w usłudze Active Directory domeny contoso.com systemu Windows Server 2003. Plik wsadowy ma zmodyfikować wszystkie komputery w określonej jednostce organizacyjnej domeny. Do pliku wsadowego mogą być ręcznie wprowadzane informacje o jednostce organizacyjnej, atrybutach oraz ich nowych wartościach. Pozostałe informacje wejściowe oraz wyjściowe pliku wsadowego powinny być automatycznie dostarczane bądź wyprowadzane.

Które polecenie systemu Windows Server 2003 należy dołączyć do pliku wsadowego? (wybierz wszystkie właściwe odpowiedzi, które razem tworzą całe rozwiązanie)

- A. Dsget computer
- B. Dsmod computer
- C. Dsquery computer
- D. Dsadd computer
- E. Dsrm computer

Odpowiedzi do zadania 2.2

1. Prawidłowa odpowiedź: D

- A. **Nieprawidłowo** Polecenie to ma prawidłową składnię nazwy wyróżniającej, ale opuszczone zostało słowo kluczowe „computer”.
- B. **Nieprawidłowo** W poleceniu tym stosowane jest prawidłowe słowo kluczowe „computer”, nato miast niewłaściwa jest składnia nazwy wyróżniającej komputera, który ma zostać wyzerowany.

- C. **Nieprawidłowo** W poleceniu tym opuszczone zostało słowo kluczowe „computer”, jak również nie jest prawidłowa składnia nazwy wyróżniającej.
- D. **Prawidłowo** W poleceniu zostało prawidłowo użyte słowo kluczowe „computer” i zastosowana właściwa składnia nazwy wyróżniającej.

2.. **Prawidłowa odpowiedź: C**

- A. **Nieprawidłowo** Działanie to byłoby prawidłowe dla serwera członkowskiego, ale nie stosuje się dla kontrolera domeny. Hasła kontrolera domeny nie mogą być zerowane za pomocą przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory).
- B. **Nieprawidłowo** Stosowanie polecenia Dsmod byłoby właściwe w przypadku serwera członkowskiego, ale nie stosuje się do kontrolera domeny. Hasła kontrolera domeny nie mogą być zerowane za pomocą polecenia Dsmod.
- C. **Prawidłowo** Polecenie to, przy wprowadzeniu na konsoli kontrolera domeny polecenia Netdom/rcsetpwd, spowoduje wyzerowanie hasła kontrolera.
- D. **Nieprawidłowo** Konsola odzyskiwania nic może być używana do zerowania konta komputera domeny.

ó. **Prawidłowa odpowiedź: C**

- A. **Nieprawidłowo** Przystawka Active Directory Domains And Trusts (Domeny i relacje zaufania usługi Active Directory) jest używana do ustawiania takich właściwości domeny, jak poziomy funkcjonalności domeny bądź lasu oraz do zarządzania relacjami zaufania pomiędzy domenami, nie jest natomiast używana do zarządzania podmiotami zabezpieczeń znajdującymi się w domenie bądź lesie).
- B. **Nieprawidłowo** Przystawka Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) może być używana do przenoszenia obiektów jedynie wewnątrz tej samej domeny.
- C. **Prawidłowo** Narzędzie wiersza poleceń Movetree może być wykorzystywane do przenoszenia obiektów pomiędzy domenami.
- D. **Nieprawidłowo** Program Dsmove może być używany do przenoszenia obiektów jedynie wewnątrz tej samej domeny.

^r. **Prawidłowe odpowiedzi: B oraz C**

- A. **Nieprawidłowo** Polecenie Dsget zwraca wartości w postaci listy wszystkich obiektów danego typu. Może akceptować dane wejściowe generowane przez polecenie Dsqquery, ale nie może przekazywać swoich danych wyjściowych dla innego polecenia (przetwarzanie potokowe). Polecenie Dsget nie może przeprowadzić potrzebnych modyfikacji ani przekazać informacji do innych poleceń, które modyfikują atrybuty.
- B. **Prawidłowo** Polecenie Dsmmod może pobrać informacje na podstawie danych wyjściowych polecenia Dsqquery, a następnie zmodyfikować atrybuty obiektów usługi Active Directory.
- C. **Prawidłowo** Polecenie Dsqquery może przekazać dane wyjściowe dla polecenia Dsmmod, które może następnie zmodyfikować atrybuty obiektów usługi Active Directory.
- D. **Nieprawidłowo** Za pomocą polecenia Dsadd można dodawać obiekty do usługi Active Directory, ale nie można modyfikować ich atrybutów.
- E. **Nieprawidłowo** Za pomocą polecenia Dsrm można przenosić obiekty usługi Active Directory, ale nie można modyfikować ich atrybutów.

Zadanie 2.3

Tworzenie i zarządzanie grupami

]

Grupowanie kont użytkowników jest wygodnym sposobem organizowania poszczególnych użytkowników w logiczne jednostki, do których można następnie przydzielać uprawnienia. W odróżnieniu od jednostek organizacyjnych, grupy są podmiotami zabezpieczeń i w celu przypisywania uprawnień mogą być dodawane do listy DACL (Discretionary Access Control List) lub listy ACL zasobu.

Typy dostępnych grup, ich zakresy oraz połączenia grup zagnieżdżonych zależą od poziomu funkcjonalności domeny, w której znajdują się grupy. Podobnie, typ i zakres niektórych grup może być przekształcany, jeśli poziom funkcjonalności domeny jest odpowiednio wysoki. Aby obsługiwać wszystkie typy grup, zakresy, zagnieżdżanie oraz możliwości dotyczące konwersji, poziom funkcjonalności domeny musi być określony jako Windows 2000 Native (Windows 2000 macierzysty) lub Windows Server 2003. Poniżej poziomu funkcjonalności Windows 2000 Mixed (Windows 2000 mieszany) ograniczone jest zagnieżdżanie grup, a konwersja jest w ogóle niemożliwa.

Pytania do zadania 2.3

1. Administrator opiekuje się domeną systemu Windows Server 2003, której aktualny poziom funkcjonalności to Windows 2000 Mixed (Windows 2000 mieszany). Domena contoso.com systemu Windows 2003 ma ustanowione relacje zaufania z domeną contoso_north systemu Windows NT 4. Administrator planuje wykorzystywanie grup domeny oraz chce określić, jakie zakresy grup mogą być używane w dowolnej domenie tego lasu.

Jaki zakres grupy może być używany w tym kontekście jako podmiot zabezpieczeń?

- A. Lokalny domeny
- B. Globalny
- C. Uniwersalny
- D. Lokalny domeny wraz z zagnieżdżaniem grup globalnych.

rL= Poziom funkcjonalności lasu pojedynczej domeny contoso.com został podniesiony do poziomu Windows Server 2003- Administrator chce wykorzystać dostępne możliwości zagnieżdżania grup zabezpieczeń.

Jakie rodzaje zagnieżdżania są dostępne dla tego poziomu funkcjonalności domeny? (wybierz wszystkie właściwe odpowiedzi)

- A- Lokalne grupy domeny w lokalnych grupach domeny
- B. Grupy globalne w lokalnych grupach domeny
- C. Grupy uniwersalne w lokalnych grupach domeny
- D. Lokalne grupy domeny w grupach globalnych

- E. Grupy globalne w grupach globalnych
 - F. Grupy uniwersalne w grupach globalnych
 - G. Grupy uniwersalne w grupach uniwersalnych
 - H. Grupy globalne w grupach uniwersalnych
 - I. Lokalne grupy domeny w grupach uniwersalnych
- O. Poziom funkcjonalności lasu pojedynczej domeny **contoso.com** został podniesiony do poziomu Windows Server 2003. Administrator chce wykorzystać dostępne w systemie możliwości zagnieżdżania grup zabezpieczeń.
- Jakiego rodzaju przekształcenia grup są dostępne dla tego poziomu funkcjonalności domeny? (wybierz wszystkie właściwe odpowiedzi)
- A. Lokalna grupa domeny zawierająca użytkowników — konwersja na grupę globalną
 - B. Grupa globalna zawierająca członków - konwersja na grupę uniwersalną
 - C. Grupy globalne zawierające grupy globalne — konwersja na grupy uniwersalne
 - D. Grupy uniwersalne zawierające grupy uniwersalne — konwersja na lokalną grupę domeny
 - E. Grupy uniwersalne zawierające grupy uniwersalne — konwersja na grupę globalną
 - E Grupa globalna zawierająca użytkowników - konwersja na lokalną grupę domeny
 - G. Lokalna grupa domeny zawierająca użytkowników — konwersja na grupę uniwersalną
4. Administrator opiekuje się domeną *contoso.com* w systemie Windows Server 2003. Podczas migracji w sieci dla domeny ustawiony jest poziom funkcjonalności Windows 2000 Mixed (Windows 2000 mieszany). Administrator planuje wykorzystywanie grup w trakcie tego okresu przejściowego oraz chce określić, jakie grupy może tworzyć i jaki zakres mogą mieć te grupy.
- Jakie rodzaje grup i jakie zakresy są możliwe na tym poziomie funkcjonalności? (wybierz wszystkie właściwe odpowiedzi)
- A. Lokalna grupa domeny). Typ zabezpieczeń
 - B. Lokalna grupa domeny: Typ dystrybucji
 - C Grupy globalne: Typ zabezpieczeń
 - D. Grupy globalne: Typ dystrybucji
 - E. Grupy uniwersalne: Typ zabezpieczeń
 - F. Grupy uniwersalne: Typ dystrybucji

Odpowiedzi do zadania 2.3

1. Prawidłowa odpowiedź: B

- A. **Nieprawidłowo** Lokalne grupy domeny są dostępne jako podmioty zabezpieczeń jedynie na kontrolerach domeny w domenie *contoso.com* systemu 2003.
- B. **Prawidłowo** Grupom globalnym można przypisywać uprawnienia na dowolnej liście ACL lasu.

- ' **C. Nieprawidłowo** Grupy uniwersalne są dostępne jako grupy dystrybucji, a nie jako grupy zabezpieczeń, dla poziomu funkcjonalności Windows 2000 Mixed (Windows 2000 mieszany).
- D. Nieprawidłowo** Na tym poziomie funkcjonalności lokalne grupy domeny są dostępne jedynie na kontrolerach domeny w domenie contoso.com, bez względu na to, jakie grupy mogą zawierać. Jednakże zagnieżdżone grupy globalne umożliwiają przypisywanie uprawnień.

ż.. **Prawidłowe odpowiedzi: A, B, C, F, G oraz H**

- A- Prawidłowo** Lokalne grupy domeny mogą zawierać inne lokalne grupy tej samej domeny. **B. Prawidłowo** Ten sposób zagnieżdżania jest możliwy bez względu na poziom funkcjonalności. **C. Prawidłowo** Grupy uniwersalne mogą być umieszczane w lokalnych grupach domeny.
- D. Nieprawidłowo** Ten rodzaj zagnieżdżania nie jest możliwy na żadnym poziomie funkcjonalności.
- E. Prawidłowo** Grupy globalne mogą być umieszczane w grupach globalnych.
- F. Nieprawidłowo** Ten rodzaj zagnieżdżania nie jest możliwy na żadnym poziomie funkcjonalności.
- G. Prawidłowo** Grupy uniwersalne mogą być umieszczane w grupach uniwersalnych.
- H. Prawidłowo** Grupy globalne mogą być umieszczane w grupach uniwersalnych.
- I. Nieprawidłowo** Ten rodzaj zagnieżdżania nie jest możliwy na żadnym poziomie funkcjonalności.

ó. **Prawidłowe odpowiedzi: B, D oraz G**

- A. Nieprawidłowo** Lokalne grupy domeny nie mogą być przekształcane na grupy globalne, bez względu na poziom funkcjonalności.
- B. Prawidłowo** Grupy globalne, które nie zawierają innych grup globalnych, mogą zostać przekształcone na grupy uniwersalne.
- C. Nieprawidłowo** Konwersja grup tego rodzaju może tworzyć zamknięte pętle odniesień i dlatego jest zabroniona.
- D. Prawidłowo** Przy takim poziomie funkcjonalności, nie istnieją żadne ograniczenia dotyczące tego typu konwersji, bez względu na członkostwo grup uniwersalnych.
- E. Nieprawidłowo** Konwersja grup tego rodzaju może tworzyć zamknięte pętle odniesień i dlatego jest zabroniona.
- F. Nieprawidłowo** Ten rodzaj konwersji jest zabroniony.
- G. Prawidłowo** Konwersja lokalnej grupy domeny na uniwersalną jest dopuszczona, o ile lokalna grupa domeny nie zawiera żadnej innej lokalnej grupy domeny.

*T. **Prawidłowe odpowiedzi: A, B, C, D oraz F**

- A. Prawidłowo** Lokalne grupy domeny mogą być tworzone jako grupy zabezpieczeń, ale dostępne będą jedynie na kontrolerach domeny, na których zostały utworzone, chyba że zostanie zwiększony poziom funkcjonalności domeny.
- B. Prawidłowo** Lokalne grupy domeny mogą być tworzone jako grupy dystrybucji, ale dostępne będą jedynie na kontrolerach domeny, na których zostały utworzone, chyba że zostanie zwiększony poziom funkcjonalności domeny.

- D. Prawidłowo** Grupy globalne mogą być tworzone jako grupy typu zabezpieczeń bez względu na poziom funkcjonalności domeny.
- D. Prawidłowo** Grupy globalne mogą tworzone jako grupy typu dystrybucji bez względu na poziom funkcjonalności domeny.
- E. Nieprawidłowo** Grupy uniwersalne nie mogą być tworzone jako grupy typu zabezpieczeń, chyba że zostanie podniesiony poziom funkcjonalności domeny.
- F. Prawidłowo** Grupy uniwersalne mogą tworzone jako grupy typu dystrybucji bez względu na poziom funkcjonalności domeny.

Zadanie 2.4

Tworzenie i zarządzanie kontami użytkowników

Konta użytkowników mogą być dodawane indywidualnie za pomocą przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) lub za pomocą narzędzia wiersza poleceń usługi katalogowej Dsadd. Narzędzia te są zalecane i wystarczające w przypadku pojedynczych kont. Przystawka Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) lepiej nadaje się do zarządzania właściwościami kont użytkowników, jako że dla tych właściwości prezentuje wspólny i wygodny interfejs. Z kolei narzędzia wiersza poleceń usługi katalogowej lepiej nadają się do operacji grupowych modyfikujących właściwości istniejących zbiorów użytkowników takich jak grupy, jednostki organizacyjne lub całe domeny.

Jeśli dysponujemy katalogiem lub bazą danych użytkowników, może okazać się, że wydajniejszym sposobem importowania tych użytkowników do usługi Active Directory jest wykorzystywanie programów Ldifde lub Csvde.

Pytania do zadania 2.4

1. Które z wymienionych poniżej narzędzi umożliwiają tworzenie podmiotów zabezpieczeń usługi Active Directory (konta użytkowników, komputerów i grup) w oparciu o informacje wprowadzane przez użytkownika lub na podstawie pliku? (wybierz wszystkie właściwe odpowiedzi)
 - A. Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory)
 - B. Active Directory Domains And Trusts (Domeny i relacje zaufania usługi Active Directory)
 - C. Ntdsutil
 - D. Ldifde
 - E. Csvde
 - F. Dsadd
 - G. Dsquery
 - H. Dsmod

- ^ Administrator opiekuje się domeną systemu Windows Server 2003 nazwaną *contoso.com*. Przedsiębiorstwo wielu pracowników zatrudnia tymczasowo. Niektórzy z nich zatrudniani są jednorazowo, a niektórzy okresowo.

Zadaniem administratora jest automatyzacja procesu pozwalającego określić, które konta były nieużywane w ciągu ostatniego miesiąca i w konsekwencji wyłączyć te konta. Jeśli konto będzie znowu potrzebne, zostanie wtedy ponownie włączone.

Które narzędzie wiersza poleceń dotyczące usługi katalogowej jest odpowiednie do realizacji tego zadania?

- A. dsquery user domainroot -inactive 4 -disabled yes
 - B. dsquery user domainroot -inactive 4 | dsmod user -disabled yes
 - C. dsquery user domainroot -inactiw 4 | dsrm -q
 - D. dsquery user domainroot -inactive 4 | dsmove -newparent OU=disabIed,DC=contoso, DC=com -q
- ó. Administrator wykonuje 7.adania dotyczące kont użytkowników w domenie usługi Active Directory - contoso.com. Jednym z nich jest przeniesienie wszystkich kont grupy East umieszczonej w jednostce organizacyjnej Sales do nowo utworzonej jednostki East Sales.

Która procedura zrealizuje to zadanie?

- A. Za pomocą przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) należy przenieść grupę East do jednostki organizacyjnej East Sales.
 - B. Za pomocą programu Dsquery należy wygenerować listę członków grupy, a następnie wyniki (stdn) przekazać do polecenia Dsmode wskazując East Sales jako docelową jednostkę organizacyjną.
 - C. Za pomocą programu Dsquery należy wygenerować listę członków grupy, a następnie wyniki (stdn) przekazać do polecenia Dsmove wskazując East Sales jako docelową jednostkę organizacyjną.
 - D. Za pomocą programu Dsquery należy wygenerować listę członków grupy, a następnie wyniki (stdn) przekazać do polecenia Dsadd wskazując East Sales jako docelową jednostkę organizacyjną.
4. Administrator konfiguruje właściwości kont użytkowników jednostki organizacyjnej Sales w domenie contoso.com. Katalogi macierzyste użytkowników powinny być przechowywane na serwerze sieci nazwanym Server01. Katalogi te mają być przechowywane w folderze udostępnionym Home na dysku D:. Homedir jest nazwą udostępniania tego foldera.

W jaki sposób należy zdefiniować katalog macierzysty we właściwościach foldera Home każdego użytkownika?

- A. D:\Home\%Username%
- B. \\Server01\ds\Home\%Username%
- C. \\Server01\%Homedir%\%Username%
- D. \\Server01\Homedir\%Username%

Odpowiedzi do zadania 2.4

1. Prawidłowe odpowiedzi: A, D, E oraz F

- A. **Prawidłowo** Przystawka Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) jest podstawowym narzędziem tworzenia podmiotów zabezpieczeń.
- B. **Nieprawidłowo** Przystawka Active Directory Domains And Trusts (Domeny i relacje zaufania usługi Active Directory) jest używana do określania poziomu funkcjonalności domeny lub lasu oraz do tworzenia i zarządzania relacjami zaufania. Konta domeny nie są tworzone przy użyciu tego narzędzia.
- C. **Nieprawidłowo** Program Ntdsutil jest używany do przywracania danych, operacji na metadanych i do wykonywania innych funkcji usługi katalogowej. Program Ntdsutil nie jest używany do tworzenia obiektów zabezpieczeń w usłudze Active Directory.

- D. Prawidłowo** Za pomocą programu Ldifde można tworzyć obiekty w usłudze Active Directory wykorzystując jako informacje wejściowe pliki danych lub parametry wiersza poleceń.
- E. Prawidłowo** Za pomocą programu Csvde można tworzyć obiekty w usłudze Active Directory wykorzystując jako informacje wejściowe plik o wartościach rozdzielanych przecinkami.
- E. Prawidłowo** Program Dsadd jest narzędziem wiersza poleceń używanym do dodawania obiektów do usługi Active Directory.
- G. Nieprawidłowo** Program Dsquery jest używany do generowania informacji wyjściowych pobieranych z usługi Active Directory. Informacje wyjściowe tego programu mogą być wykorzystywane przez inne polecenia usługi katalogowej, ale za pomocą programu Dsquery nie można tworzyć obiektów katalogu.
- H. Nieprawidłowo** Program Dsmod jest używany do modyfikowania atrybutów istniejących obiektów usługi Active Directory.

***L. Prawidłowa odpowiedź: B**

- A. Nieprawidłowo** Polecenie to zwraca listę kont użytkowników, które były nieaktywne przez co najmniej cztery tygodnie i które są wyłączone. Polecenie Dsquery nie wykonuje żadnych działań.
- B. Prawidłowo** Polecenie to zwraca listę kont użytkowników nieaktywnych przez co najmniej cztery tygodnie, a następnie przekazuje dane wyjściowe do polecenia Dsmod, które będzie wyłączać konta.
- C. Nieprawidłowo** Polecenie to zwraca listę kont użytkowników nieaktywnych przez co najmniej cztery tygodnie, a następnie przekazuje dane wyjściowe do polecenia Dsrm, które usunie konta.
- D. Nieprawidłowo** Polecenie to będzie przenosić wszystkie konta, które były nieaktywne przez co najmniej cztery tygodnie, do jednostki organizacyjnej nazwanej „disabled”, ale nie będzie wyłączać kont.

O. Prawidłowa odpowiedź: C

- A. Nieprawidłowo** Działanie takie przeniesie grupę do jednostki organizacyjnej East Sales, ale konta użytkowników pozostaną w jednostce organizacyjnej Sales.
- B. Nieprawidłowo** Polecenie Dsmod może modyfikować właściwości konta użytkownika, ale jednostka organizacyjna (OU) nie jest właściwością konta użytkownika.
- C. Prawidłowo** Działanie takie prawidłowo przenosi konta do jednostki organizacyjnej.
- D. Nieprawidłowo** Wykonanie polecenia to próba utworzenia nowych kont w jednostce organizacyjnej East Sales i pozostawienie starych kont użytkownika w jednostce organizacyjnej Sales. Działanie takie nie powiedzie się. Pomimo, że jednostka organizacyjna i grupa są odrębne, to są częścią tej samej domeny i w związku z tym proces wywoła komunikat o błędzie.

4. Prawidłowa odpowiedź: D

- A. Nieprawidłowo** Definicja ta wskazuje dysk D komputera użytkownika.
- B. Nieprawidłowo** Ustawienia te wymagają uprawnień administratora do uzyskania dostępu do katalogu głównego dysku D, a takich uprawnień użytkownicy nie mają.
- C. Nieprawidłowo** Zmienna %Homedir% odnosi się do przydzielonego katalogu macierzystego, który jest określany przez wartość właściwości. W tym przypadku odniesienie to jest nieprawidłowe.
- D. Prawidłowo** Polecenie określi katalog macierzysty użytkownika jako folder znajdujący się w folderze udostępnionym Homedir. Nazwa foldera będzie określona przez nazwę logowania użytkownika.

Zadanie 2.5

Rozwiązywanie problemów kont komputerów

Konta komputerów są podmiotami zabezpieczeń usługi Active Directory takimi jak konta użytkowników lub grup. Podczas tworzenia kont komputerów przypisywane są im: identyfikator zabezpieczeń (SID), identyfikator względny (RID) oraz unikatowy globalny identyfikator (GUID). Identyfikator RID jest dostarczany przez kontroler domeny usługi Active Directory z puli identyfikatorów RID dystrybuowanych przez pojedynczy kontroler domeny, któremu przypisana została rola wzorca RID. Jeśli przez jakiś czas wzorec RID nie jest dostępny, pula identyfikatorów RID zostaje wyczerpana i tworzenie kont komputerów domeny staje się niemożliwie.

Do kont komputerów przypisane są również hasła, które są synchronizowane wewnętrznie z usługą Active Directory. Jeśli hasło nie jest zsynchronizowane, administrator powinien je wyzerować.

Pytania do zadania 2.5

X, Użytkownik po dłuższej nieobecności włączył swój komputer nazwany Desk249 i próbował zalogować się w domenę, ale rejestracja nie powiodła się. Również administrator, wykorzystując konto administratora domeny, nie potrafił zalogować się w komputerze użytkownika.

Następnie administrator próbował wyszukać komputer Desk249 w usłudze Active Directory i okazało się, że komputer o takiej nazwie nie istnieje w katalogu. Administrator zalogował się na komputerze jako administrator lokalny i wykrył, że konfiguracja komputera określa, iż należy on w dalszym ciągu do domeny. Administrator doszedł do wniosku, że musi ponownie utworzyć konto komputera. Umożliwienie użytkownikowi logowania na komputerze powinno być przeprowadzone najszybciej jak to możliwe oraz przy najmniejszym nakładzie pracy administracyjnej.

Co administrator powinien zrobić?

- A. Należy zalogować się na komputerze Desk249 jako administrator lokalny. W module System w panelu sterowania, na zakładce Computer Name (Nazwa komputera) należy kliknąć przycisk Change (Zmień) umieszczony obok tekstu „To rename this computer or join a domain, click Change” (Aby zmienić nazwę komputera lub przyłączyć się do domeny, kliknij przycisk Zmień). Następnie należy przyłączyć komputer Desk249 do grupy roboczej nazwanej TEST i ponownie go uruchomić. Kolejnym krokiem jest zalogowanie się na komputerze jako administrator lokalny i przejście do strony określania członkostwa w grupie roboczej lub domenie. Za pomocą konta o uprawnieniach administratora domeny należy ponownie przyłączyć komputer Desk249 do usługi Active Directory, a następnie ponownie go uruchomić.
- B. Za pomocą przysławki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) należy utworzyć nowe konto komputera o nazwie Desk249 w kontenerze Computers (Komputery). Następnie należy ponownie uruchomić komputer Desk249.

- C. Za pomocą polecenia Dsadd należy utworzyć nowe konto komputera o nazwie Desk249 w koncie nierz Computers (Komputery). Następnie należy ponownie uruchomić komputer Desk249.
- D. Za pomocą programu Ntdsutil należy odtworzyć konto komputera z kopii zapasowej usługi Active Directory zawierającej konto Desk249-
- 2.. Administrator próbuje wykorzystać przystawkę Computer Management (Zarządzanie komputerem) do zarządzania zdalnego serwerem plików sieci. Serwer plików jest członkiem domeny, a administrator jest członkiem grupy Domain Admins (administratorzy domeny).
- Administrator nie może podłączyć się do serwera plików za pomocą przystawki Computer Management (Zarządzanie komputerem), może natomiast przyłączać się zdalnie do innych serwerów sieci. Administrator posiada również dostęp do plików serwera, podobnie jak inni użytkownicy sieci.
- Na czym może polegać problem dotyczący serwera plików?
- A. Usługa Browser (Przeglądarka komputerowa) nie została uruchomiona.
- B. Usługa Remote Registry (Rejestr zdalny) nie została uruchomiona.
- C Program Routing and Remote Access (Routing i dostęp zdalny) nie został zainstalowany na serwerze plików.
- D. Konto komputera wymaga wyzerowania w usłudze Active Directory.
3. Administrator za pomocą programu narzędziowego Sysprep instaluje kilka systemów Windows Server 2003 w środowisku Windows NT 4. Po instalacji obrazu na wszystkich serwerach, administrator sprawdza połączenia sieci do każdego serwera, aby upewnić się, że rozmieszczanie systemów przeprowadzone zostało prawidłowo.
- Podczas próby zdalnego zalogowania się na serwerze Server03 wyświetlony został komunikat informujący, że relacje zaufania były nieprawidłowe (Trust relationship has failed), a administrator nie mógł połączyć się z serwerem. Co administrator powinien zrobić, aby rozwiązać problem? (wybierz wszystkie właściwe odpowiedzi)
- A. Za pomocą polecenia Dsmod należy wyzerować hasło serwera Server03-
- B. Należy użyć przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) do wyzerowania hasła serwera Server03.
- C. Należy przyłączyć serwer Server03 do grupy roboczej.
- D. Należy przyłączyć serwer Server03 do domeny.
- E. W domenie należy usunąć konto komputera Server03-
- F. W domenie należy wyłączyć konto komputera Server03-
- G. W domenie należy utworzyć konto komputera Server03-
- H. W domenie należy włączyć konto komputera Server03-
- nr. Administrator dodaje użytkowników, komputery i grupy do nowej domeny systemu Windows Server 2003- Po dodaniu kilku setek obiektów za pomocą importu z pliku wsadowego, administrator rozpoczął dodawanie ostatnich 24 komputerów, które muszą być wprowadzone ręcznie. Po dodaniu trzech kont komputerów system wyświetlił komunikat o błędzie, a administrator nie mógł już do domeny dodać więcej kont. Wszystkie inne połączenia sieci oraz funkcje serwera działały normalnie.

Co może być najbardziej prawdopodobną przyczyną problemu?

- A. Komputer pełniący rolę wzorca RID jest niedostępny.
- B. Komputer pełniący rolę emulatora PDC jest niedostępny.
- C. Komputer pełniący rolę infrastruktury domeny jest niedostępny.
- D. Komputer pełniący rolę wzorca schematu jest niedostępny.

Odpowiedzi do zadania 2.5

1. Prawidłowa odpowiedź: A

- A. **Prawidłowo** Zależności między kontem komputera usługi Active Directory a lokalną stacją roboczą, w tym przypadku komputerem Desk249, są zależnościami synchronizowanymi, które wymagają, aby ustawienia zabezpieczeń dla obu komputerach były określone w trakcie pojedynczego procesu. Należy więc ponownie utworzyć zależności po Stronie komputera Desk249, jak również utworzyć ponownie konto w usłudze Active Directory.
- B. **Nieprawidłowo** Działanie takie utworzy konto komputera, które jest zgodne tylko z nazwą komputera (Desk249). Dwie części zależności wzajemnych obiektów - obiekt usługi Active Directory i komputer lokalny - w takiej sytuacji nie będą w stanie synchronizować haseł i innych informacji o zabezpieczeniach.
- C. **Nieprawidłowo** Działanie takie utworzy konto komputera, które jest zgodne tylko z nazwą komputera (Desk249). Dwie części zależności wzajemnych obiektów - obiekt usługi Active Directory i komputer lokalny - w takiej sytuacji nie będą w stanie synchronizować haseł i innych informacji o zabezpieczeniach.
- D. **Nieprawidłowo** Pojedyncze konta komputerów nie mogą być odtwarzane na podstawie kopii zapasowych. Oprócz tego, proces usuwania zależności komputera klienta, a następnie ponowne utworzenie relacji pomiędzy klientem a kontem komputera w usłudze Active Directory jest znacznie prostszy.

2. Prawidłowa odpowiedź: B

- A. **Nieprawidłowo** Usługa Browser (**Przeglądarka** komputerowa) bierze udział w lokalizowaniu komputerów lub usług o określonych nazwach. Administrator może zlokalizować komputer.
- B. **Prawidłowo** Usługa Remote Registry (Rejestr zdalny) jest potrzebna do określenia, czy istnieją wystarczające uprawnienia dla połączenia zdalnego. Uruchomienie tej usługi prawdopodobnie rozwiąże problem.
- C. **Nieprawidłowo** Program Routing and Remote Access (Routing i dostęp zdalny) służy do zarządzania połączeniami telefonicznymi i prywatnych sieci wirtualnych (VPN) oraz do realizacji funkcji routingu w komputerze. Program nie jest potrzebny dla połączeń z komputerem dotyczących zarządzania.
- D. **Nieprawidłowo** Jeśli hasło byłoby niesynchronizowane, niemożliwy byłby również dostęp do plików.

o. Prawidłowe odpowiedzi: C, D, E oraz G

- A. **Nieprawidłowo** Polecenie Dismod (jak również wszystkie inne programy wiersza poleceń usługi katalogowej) jest dostępne jedynie w usłudze Active Directory.

- B. Nieprawidłowo** Przystawka Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) jest dostępna jedynie wraz z instalacją usługi Active Directory.
- C. Prawidłowo** Działanie takie na komputerze lokalnym usunie identyfikację komputera dla domeny.
- D. Prawidłowo** Działanie to zsynchronizuje konto komputera z jego odpowiednikiem w domenie.
- E. Prawidłowo** Działanie to usunie z domeny identyfikację komputera w domenie.
- F. Nieprawidłowo** Wyłączenie konta nie usuwa jego identyfikacji. Pomieszczenie identyfikatorów generuje kolejne problemy.
- G. Prawidłowo** Działanie to tworzy konto domeny, do którego komputer może przyłączać się i z którym może przeprowadzać synchronizację.
- H. Nieprawidłowo** Jeśli konto komputera zostało ponownie utworzone, już będzie włączone. Ponowne włączenie konta po uprzednim wyłączeniu nie usunie problemów relacji zaufania.

4. **Prawidłowa odpowiedź: A**

- A. Prawidłowo** Wzorzec RID jest potrzebny do przydziału identyfikatorów nowych obiektów katalogu. Brak identyfikatorów uniemożliwia tworzenie nowych obiektów.
- B. Nieprawidłowo** Obiekty mogą być zapisywane w dowolnym kontrolerze domeny, tak więc emulator PDC nie jest wymagany.
- C. Nieprawidłowo** Rola ta nie jest wymagana podczas tworzenia podmiotów zabezpieczeń domeny.
- D. Nieprawidłowo** Rola ta nie jest źródłem problemu, ponieważ do momentu wystąpienia problemu obiekty tworzone były prawidłowo.

Zadanie 2.6

Rozwiązywanie problemów kont użytkowników

Konta użytkowników umożliwiają użytkownikom uwierzytelnienie i dostęp do zasobów zarówno na komputerze lokalnym, jak i w sieci. Jeśli właściwości konta użytkownika są nieprawidłowo skonfigurowane, niemożliwy staje się dostęp do jednego typu lub kilku typów zasobów. Wiele problemów dotyczących zadań realizowanych przez użytkowników jest związanych z ustawieniami konta użytkownika.

Właściwości użytkownika dotyczące dostępu ogólnego do sieci odnoszą się do ustawień przydziału praw użytkownika (User Rights Assignments) dla logowania lokalnego i poprzez sieć, do uprawnień połączeń telefonicznych (Dial-in) oraz do uprawnień dostępu do usług terminalowych (Terminal Services).

Preferencje konfiguracji użytkownika dotyczą: katalogów macierzystych oraz ścieżek profili.

Konfiguracja logowania i ustawienia ograniczeń dotyczą okresu ważności hasła, zasad blokowania oraz okresów, w których użytkownik może logować się na wybranej stacji roboczej.

Pytania do zadania 2.6

1. Użytkownik powiadomił, że nie może zalogować się w sieci ze swojego komputera przenośnego działającego pod kontrolą systemu Windows 98. Użytkownik może zalogować się do sieci korzystając z komputera systemu Windows XP.

Środowisko sieci kontrolowane jest przez domenę usługi Active Directory systemu Windows Server 2003.

Komputer systemu Windows 98 nie ma zainstalowanego programu klienta usługi Active Directory.

Co jest najbardziej prawdopodobną przyczyną problemu?

- A. Konto komputera w domenie wymaga wyzerowania.
- B. Hasło użytkownika jest dłuższe niż 14 znaków.
- C. Konto użytkownika powinno być skonfigurowane tak, aby umożliwiała logowanie na wszystkich stacjach roboczych.
- D. Uszkodzony został katalog macierzysty użytkownika.

- £ ■ Użytkownik John powiadomił, że ustawienia jego profilu nie są prawidłowo przenoszone podczas logowania w różnych komputerach sieci. John może logować się na każdym komputerze w sieci, ale jego tapeta pulpitu, skróty oraz inne ustawienia preferencji na każdym komputerze są inne.

Administrator sprawdził ścieżkę profilu we właściwościach konta użytkownika i okazało się, że jest ona określona przez wyrażenie „D:\profiles\John”. Administrator upewnił się, że folder nazwany John

istnieje w folderze profili na dysku D: serwera ServerO 1 (jest to serwer, który przechowuje w sieci profile użytkowników). Folder udostępniony, w którym znajdują się foldery profili, nazywa się Profiles.

Inne profile użytkowników są przenoszone prawidłowo.

Co administrator powinien zrobić, aby rozwiązać problem?

- A. Wyzerować hasło użytkownika John.
 - B. Określić ścieżkę katalogu macierzystego dla użytkownika John jako D:\Profiles\%Username%.
 - C. Określić ścieżkę profilu dla użytkownika John jako \\Server01\Profiles\%Username%\o.
 - D. Skopiować profil, który chce wykorzystywać użytkownik John do foldera D:\Profiles\John na serwerze profili.
0. Użytkownik powiadomił, że nie może uzyskać dostępu do sieci stosując połączenie telefoniczne. W sieci lokalnej biura użytkownik loguje się prawidłowo.
- Administrator sprawdził, czy zasady dostępu zdalnego (Remote Access) zostały uruchomione na serwerze usługi Routing and Remote Access (Routing i dostęp zdalny). Wszystkie modemy zostały przetestowane i działały prawidłowo. Co jest najbardziej prawdopodobną przyczyną problemu?
- A. We właściwościach konta użytkownika nie został włączony dostęp do programu Terminal Srrwr (Serwer terminali).
 - B. We właściwościach konta użytkownika nie zostały włączone' uprawnienia dotyczące połączeń telefonicznych.
 - C. Użytkownik dla swojego komputera zdalnego nie posiada konta komputera w domenie.
 - I>. Podczas korzystania z dostępu telefonicznego użytkownik posługuje się nieodpowiednim poświadczeniem tożsamości.

Odpowiedzi do zadania 2.6

- 1. Prawidłowa odpowiedź: B
 - A. Nieprawidłowo Komputery systemu Windows 98 nie mają kont w domenie.
 - B. Prawidłowo Komputery systemu Windows 98 nie obsługują haseł użytkowników dłuższych niż 14 znaków. Można to poprawić instalując klienta usługi Active Directory Client.
 - C. Nieprawidłowo Komputery systemu Windows 98 nie są członkami domeny i nie mogą być kontrolowane poprzez działanie tego ustawienia.
 - D. Nieprawidłowo Katalog macierzysty jest magazynem plików i nie uniemożliwia logowania w przypadku uszkodzenia.
- JL. Prawidłowa odpowiedź: C
 - A. Nieprawidłowo John może logować się, tak więc hasło jest prawidłowe.
 - B. Nieprawidłowo Katalogi macierzyste i profile są obsługiwane przez różne konfiguracje i w tym przypadku nie muszą być takie same.
 - C. Prawidłowo Ścieżka profilu wskazywała literę dysku lokalnego, co odpowiada dyskowi każdego komputera, w którym użytkownik John się logował.

D. **Nieprawidłowo** Skopiowanie profilu nie rozwiąże problemu, jako że konfiguracja we właściwościach użytkownika nie wskazywała na lokalizację w sieci.

O. Prawidłowa odpowiedź: B

- A. **Nieprawidłowo** Ustawienia konfiguracji programu Terminal Server (Serwer terminali) nie są używane do określania uprawnień lub dostępu do połączeń telefonicznych.
- B. **Prawidłowo** Prawdopodobnie ustawienia konta użytkownika zostały tak określone, że nie zezwalały na dostęp do sieci przy użyciu połączenia telefonicznego.
- C. **Nieprawidłowo** Takie ustawienie nie powinno zabraniać dostępu zdalnego do sieci z wykorzystaniem połączenia telefonicznego.
- D. **Nieprawidłowo** Konto użytkownika jest takie samo dla połączeń zdalnych i dla połączeń lokalnych, tak więc pomieszczenie tożsamości jest nieprawdopodobne.

Zadanie 2.7

Rozwiązywanie problemów uwierzytelnienia użytkownika

Użytkownik nie uzyska dostępu do zasobów sieci, jeśli nie zostanie prawidłowo uwierzytelniony, a nawet w niektórych przypadkach nie będzie mógł zalogować się na swoim komputerze lokalnym. Podstawą uwierzytelnienia jest kombinacja nazwy użytkownika i hasła, która stanowi poświadczenie tożsamości użytkownika, jeśli informacje wprowadzone przez użytkownika nie są zgodne z tym, czego oczekuje system uwierzytelnienia, użytkownik nie będzie inogł podłączyć się do zasobu. Jeśli zasób ten znajduje się na komputerze lokalnym, użytkownik w ogóle nie będzie mógł się zalogować.

Pytania do zadania 2.7

X- Podróżujący użytkownik przebywał kilka miesięcy poza biurem. Konfiguracja komputera przenośnego użytkownika nie umożliwia uzyskania dostępu telefonicznego do sieci przedsiębiorstwa, ponieważ komputer używany jest najczęściej do prezentacji i dokumentowania kontaktów z klientami.

PO powrocie do biota i podłączeniu do sieci użytkownik nie mógł zalogować się na swoim kompulcize używając konia lokalnego, a na ekranie wyświetlane było okno dialogowe „I.ogon lailed” (nieprawidłowe logowanie).

Co administrator powinien zrobić?

- A. Należy wyzerować hasło użytkownika w usłudze Active Directory.
- B. Należy wyzerować konto komputera użytkownika w usłudze Active Directory.
- C. Dla tego użytkownika należy użyć dysku leserowania hasła, aby wyczyścić hasło na komputera lokalnym.
- D. Należy odłączyć komputer od sieci, a następnie ponownie go uruchomić.

^. Użytkownik powrócił z długiej podróży służbowej i podłączył komputer do sieci biura. Użytkownik mógł zalogować się, ale nie mógł podłączyć się do żadnego zasobu sieci.

Administrator sprawdził konta skojarzone z użytkownikiem w przystawce Active Dirccototy Users And Computers (Użytkownicy i komputery usługi Active Directory) i zauważył, że konto komputera prae-nośnego użytkownika zaznaczone jest przez ikonę czerwonego krzyżyka „X”. Co administrator powinien zrobić, aby rozwiązać problem?

- A. Należy wyzerować hasło użytkownika w usłudze Active Directory.
- B. Należy wyzerować konto komputera przenośnego w usłudze Active Directory.
- C Należy w domenie usunąć konto komputera przenośnego, przyłączyć komputer przenośny do gtupy roboczej, a następnie ponownie przyłączyć do domeny.
- D. Należy usunąć, a następnie ponownie utworzyć konto komputera przenośnego.

0. Administrator opiekuje się siecią w średniej wielkości przedsiębiorstwie, zorganizowaną jako pojedyncza domena systemu Windows Server 2003. Domyślny obiekt zasady domeny (Default Domain Group Policy) został określony za pomocą następujących ustawień:

Pamiętanych jest 10 haseł

Maksymalny okres ważności hasła to 10 dni

Minimalny okres ważności hasła to 2 dni

Minimalna długość hasła to 10 znaków

Grupa 40 programistów pracujących w jednym dziale naciska na zarząd, aby dla tego działu określone zostały odrębne zasady haseł, specyficzne dla członków tego działu. Programiści chcą, aby minimalny okres ważności hasła określony był wartością „0 dni”, a maksymalny okres ważności hasła ustawiony na „28 dni”. Która z wymienionych poniżej metod pozwoli zmienić zasadę haseł dla tej grupy programistów?

- A. Należy utworzyć **domenę podrzędną** w stosunku do domeny bieżącej i przenieść konta programistów do tej domeny. Przeprowadzić edycję domyślnego obiektu CIPO domeny podrzędnej i wprowadzić odrębne zasady haseł wymagane przez programistów.
- B. Należy utworzyć odrębną jednostkę organizacyjną i przenieść konta użytkowników (40 programistów) do tej jednostki organizacyjnej. Następnie należy utworzyć i **przeprowadzić** edycję nowego obiektu GP() i poprzez ten obiekt GPO wprowadzić odrębne zasady haseł wymagane przez programistów. Na koniec należy zastosować obiekt GPO do nowo utworzonej jednostki organizacyjnej, w której zostały umieszczone konta programistów.
- C. Należy ponownie podzielić sieć na podsieci i utworzyć w usłudze Active Directory nową lokację. Następnie należy umieścić stacje robocze 40 programistów w tej nowej podsieci. Następnie należy utworzyć i przeprowadzić edycję nowego obiektu GPO i poprzez ten obiekt GPO wprowadzić odrębne zasady haseł wymagane przez programistów. Na koniec należy zastosować obiekt GPO do nowo utworzonej lokacji, w której zostały umieszczone konta komputerów programistów.
- D. Na każdej stacji roboczej programistów należy przeprowadzić edycję lokalnego obiektu GPO i poprzez ten obiekt GPO wprowadzić odrębne zasady haseł wymagane przez programistów.

Odpowiedzi do zadania 2.7

1. Prawidłowa odpowiedź: C

- A. **Nieprawidłowo** Okno dialogowe "Logon Failed" (Nieprawidłowe logowanie) jest wyświetlane, jeśli dla konta na komputerze lokalnym został utworzony dysk resetowania hasła. Konto użytkownika domeny nie wywołuje tego problemu.
- B. **Nieprawidłowo** Okno dialogowe "Logon Failed" (Nieprawidłowe logowanie) jest wyświetlane, jeśli dla konta na komputerze lokalnym został utworzony dysk resetowania hasła. Konto użytkownika domeny nie wywołuje tego problemu.
- C. **Prawidłowo** Dysk resetowania hasła jest tworzony dla lokalnych kont użytkownika i może być używany, kiedy użytkownik próbuje uzyskać dostęp do komputera lokalnego przy użyciu nieprawidłowego poświadczenia tożsamości, tak jak miało to miejsce w tym przypadku.

- D. **Nieprawidłowo** Połączenie komputera do sieci lub dowolne inne interakcje sieciowe nie spowodują wyświetlenia okna dialogowego „Logon Failed” (Nieprawidłowe logowanie).

£.. **Prawidłowa odpowiedź: B**

- A. **Nieprawidłowo** Hasło użytkownika nie będzie wpływać na konto komputera w ten sposób, w jaki zostało to pokazane w usłudze Active Directory.
- B. **Prawidłowo** Hasło komputera przenośnego przestało być zsynchronizowane z kontem komputera w domenie i dlatego musi być wyzerowane.
- C. **Nieprawidłowo** Działanie takie rozwiąże problem, ale może spowodować inne problemy, jeśli zdefiniowany był zestaw uprawnień do zasobów dla tego komputera przenośnego. Poza tym, w porównaniu do wyzerowania konta, proces ten jest znacznie bardziej czasochłonny.
- D. **Nieprawidłowo** Działanie takie pogłębi problem, ponieważ oprócz niesynchronizowanych haseł pojawią się niezgodne identyfikatory SID.

O. **Prawidłowa odpowiedź: A**

- A. **Prawidłowo** Zasady haseł stosują się do domeny. Jedyną metodą, dzięki której użytkownicy mogą mieć odrębne zasady haseł, jest umieszczenie kont tych użytkowników w innych domenach. Domena podrzędna nie dziedziczy zasady hasła po domenie nadrzędnej.
- B. **Nieprawidłowo** Zasady haseł stosują się do domeny. Zasady haseł zastosowane na poziomie jednostki organizacyjnej nie zastępują zasad haseł używanych na poziomie domeny. Jeśli zastosowane zostanie działanie opisane w odpowiedzi, zasady haseł pozostaną niezmienione.
- C. **Nieprawidłowo** Zasady haseł stosują się do domeny. Zasady haseł zastosowane na poziomie lokalnej jednostki nie zastępują zasad haseł używanych na poziomie domeny. Jeśli zastosowane zostanie działanie opisane w odpowiedzi, zasady haseł pozostaną niezmienione.
- D. **Nieprawidłowo** Zasady haseł stosują się do domeny. Zasady haseł zastosowane na poziomie lokalnym nie zastępują zasad haseł używanych na poziomie domeny. Jeśli zastosowane zostanie działanie opisane w odpowiedzi, zasady haseł pozostaną **niezmienione**.

16 Zarządzanie i obsługa dostępu do zasobów (3.0)



Dostęp do zasobów wymaga prawidłowej identyfikacji i prawidłowych uprawnień. Aby uzyskać dostęp do plików poprzez sieć wymagane są dwie rzeczy - zasoby muszą być dostępne (udostępnione), a użytkownicy muszą mieć odpowiednie uprawnienia związane z wykonywanymi czynnościami (odczyt, zapis, usuwanie itp). Jest to transakcyjny proces analizy żetonu dostępu użytkownika powodujący odczyt wpisów kontrolnej listy dostępu (ACL) zasobu i porównanie ich z identyfikatorami zabezpieczeń (SID) żetonu. Jeśli usługi zabezpieczeń zarządzające procesem dostępu do zasobu określą, że kombinacja identyfikatorów Sii oraz ich uprawnień jest wystarczająca do wykonania żądanych zadań, uprawnienia zostają przydzielone, w przeciwnym razie dostęp do zasobów zostaje zabroniony.

Taki dostęp bazujący na uprawnieniach jest realizowany przez/ system operacyjny w oparciu o system plików, który jest zainstalowany na urządzeniu pamięci przechowującym zasób. Przykładowo dla systemu plików FAT32, nawet jeśli systemem operacyjnym jest system Windows Server 2003, uprawnienia nie mogą być definiowane na poziomie systemu plików. Dla tego rodzaju przydziału uprawnień wymagany jest system plików NTFS.

Uprawnienia do udziałów mogą być jednak określane bez względu na system plików, w którym zasoby są przechowywane. Sam system operacyjny kontroluje uprawnienia udziałów, określając które są ważne dla każdej jednostki próbującej uzyskać dostęp do zasobu poprzez sieć.

Program Terminal Services (Usługi terminalowe) umożliwia dostęp użytkownikowi innego rodzaju poprzez sieć prezentowane jest środowisko lokalne. Utworzenie i używanie tego wirtualnego środowiska lokalnego wymaga dodatkowych uprawnień i konfiguracji, ale dostęp do plików i folderów jest w dalszym ciągu zarządzany poprzez sieć (udziały) oraz uprawnienia systemu plików (NTFS). Rozumienie tych dodatkowych wymagań i możliwości i konfiguracji ma podstawowe znaczenie dla właściwego wykorzystywania programu Terminal Services (Usługi terminalowe).

Sprawdzanie umiejętności i sugerowane ćwiczenia praktyczne

Poniżej przedstawiono umiejętności potrzebne do opanowania tematu „Zarządzanie i obsługa dostępu do zasobów” objętego egzaminem 70-290 - *Zarządzanie i obsługa środowiska Windows Server 2003*:

- Konfigurowanie dostępu do folderów udostępnionych.
 - » Zadanie kontrolne 1: Określenie uprawnień dla poszczególnych użytkowników i grup. Tworzenie złożonych zestawów dotyczących członkostwa w grupie oraz przydziału uprawnień tak, aby zostały zbudowane dwu-, trójwarstwowe zestawy uprawnień wykorzystujące dla kont użytkownika członkostwo w wielu grupach oraz konfigurowanie zagnieżdżenia w grupach.
 - » Zadanie kontrolne 2: Konfigurowanie zestawów uprawnień w punktach udostępniania sieci. Konfigurowanie uprawnień NTFS dla tych samych zasobów, analiza uprawnień czynnych użytkownika.
- Rozwiązywanie problemów usług terminalowych.
 - » Zadanie kontrolne 1: Konfigurowanie w trybie Remote Desktop for Administration (Pulpit zdalny dla administracji) ustawień programu Terminal Services (Usługi terminalowe) takich jak zezwalanie bądź odmowa uprawnień dla różnych użytkowników. Określanie właściwości dla użytkowników, którzy uzyskują dostęp lokalny, aby mogli kontrolować swoje ścieżki profilu, katalogi macierzyste oraz to, czy ich sesje mogą być sterowane zdalnie za pomocą innej sesji programu Terminal Services (Usługi terminalowe).
 - » Zadanie kontrolne 2: Konfigurowanie zasady grupy dla użytkowników programu Terminal Services (Usługi terminalowe) tak, aby do sesji programu Terminal Services (Usługi terminalowe) zostały przekierowane drukarka lokalna i dane wyjściowe dysku. Poznanie przeznaczenia i funkcjonalności każdego z tych ustawień.
- Konfigurowanie uprawnień systemu plików.
 - » Zadanie kontrolne 1: Określanie uprawnień dla poszczególnych użytkowników i grup. Tworzenie złożonych zestawów dotyczących członkostwa w grupie oraz przydziału uprawnień tak, aby zostały zbudowane dwu-, trójwarstwowe zestawy uprawnień wykorzystujące dla kont użytkownika członkostwo w wielu grupach oraz konfigurowanie zagnieżdżenia w grupach.
 - » Zadanie kontrolne 2: Konfigurowanie zestawów uprawnień NTFS dla obiektów systemu plików. Konfigurowanie uprawnień udziału dla tych samych zasobów, analiza uprawnień czynnych użytkownika.
- Rozwiązywanie problemów dostępu do udostępnionych plików i folderów.
 - » Zadanie kontrolne 1: Dostęp do właściwości pliku, dla którego określony został zestaw złożonych uprawnień NTFS dotyczących kilku grup i użytkowników. Wybranie użytkownika będącego członkiem co najmniej jednej grupy, dla której przypisane zostały uprawnienia do pliku. Użycie przycisku Zaawansowane znajdującego się na zakładce zabezpieczeń celem uzyskania dostępu do zakładki „Uprawnienia czynne”. Wprowadzenie nazwy użytkownika w celu określenia jego uprawnień czynnych.
 - » Zadanie kontrolne 2: Dostęp do właściwości foldera, dla którego kilka grup ma przydzielone różne uprawnienia NTFS. Korzystanie z przycisku Zaawansowane znajdującego się na zakładce zabezpieczeń w celu uzyskania dostępu do zakładki „Uprawnienia czynne”. Wprowadzenie nazwy grupy celem przejrzenia uprawnień czynnych grupy do tego foldera.

Lektura uzupełniająca

Przed przystąpieniem do egzaminu należy przestudiować przedstawione poniżej dodatkowe źródła informacji.

Zadanie 3.1

W rozdziale 6 „Pliki i foldery” omówione zostały uprawnienia udziałów, uprawnienia NTFS oraz inspekcja dostępu do zasobu.

Artykuł Microsoft Corporation. *Frequently Asked Questions: Security Technologies* jest dostępny w sieci Web pod adresem: <http://www.microsoft.com/windowsserver2003/community/centers/security/securityfaq.asp>.

Zadanie 3.2

Rozdział 2, lekcja 3 „Administracja zdalna za pomocą programu Terminal Services (Usługi terminalowe)”. W trakcie lekcji omówione zostały zagadnienia konfiguracji i uprawnień dotyczące programów Terminal Services (Usługi terminalowe), Remote Desktop (Pulpit zdalny) oraz Remote Assistance (Pomoc zdalna).

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: Pomoc zdalna.

Zadanie 3.3

W rozdziale 6 „Pliki i foldery” omówione zostały uprawnienia udziałów, uprawnienia NTFS oraz inspekcja dostępu do zasobu.

Zasób sieci Web Microsoft Corporation. Technet; Script Center: Disks and File Systems — dostępny jest pod adresem URL: <http://www.microsoft.com/technet/scriptcenter/default.asp?url=/technet/scriptcenter/default.asp>.

Zadanie 3.4

W rozdziale 6 „Pliki i foldery” opisane zostały zagadnienia dotyczące rozwiązywania problemów związanych z uprawnieniami, wliczając w to przegląd uprawnień czynnych.

Warto zapoznać się z następującym artykułem działu Microsoft Technet: http://www.microsoft.com/technet/prodtechnol/windowsserver2003prod/standardacl_view_effective_permissions.asp.

Zadanie 3.1

Konfigurowanie dostępu do folderów udostępnionych

Uprawnienia udziału są określone w systemie operacyjnym Windows Server 2003 wewnątrz systemu plików w punktach dostępu do sieci, czyli udziałach. Uprawnienia udziału są przypisywane we właściwościach foldera (zakładka Udostępnianie) programu Windows Explorer (Eksplorator Windows). Pojedyncze pliki nie mogą być udostępniane.

Dla kilku jednostek związanych z użytkownikiem uprawnienia analizowane są dla każdego identyfikatora SID umieszczonego w żetonie dostępu użytkownika. Przydzielane są najbardziej liberalne uprawnienia. Wyjątkiem od tej liberalnej zasady jest sytuacja, kiedy w żetonie co najmniej jeden identyfikator SID na liście ACL zasobu ma przydzielone uprawnienie odmowy. W takim przypadku uprawnienia odmowy mają pierwszeństwo.

Jeśli w systemie plików używane są uprawnienia NTFS, uprawnienia czynne udziału są porównywane z czynnymi uprawnieniami NTFS, a najbardziej restrykcyjne uprawnienia są wybierane jako uprawnienia czynne użytkownika do danego zasobu.

Pytania do zadania 3.1

1. Komputer Server01 jest serwerem plików działającym pod kontrolą systemu Microsoft Windows Server 2003 i używany jest przez dział księgowości do Opracowywania kart czasu pracy i raportów kosztów dla pracowników. Administrator określa uprawnienia punktów udostępniania dla tych folderów, które muszą spełniać następujące wymagania:

- Formularze dotyczące pracowników przechowywane są w folderze Forms. Formularze te powinny być dostępne dla wszystkich pracowników.
- Tylko użytkownicy uwierzytelnieni (Authenticated Users) mogą uzyskiwać dostęp do formularzy.
- Pracownicy mogą zapisywać wypełnione formularze w folderze nazwanym Forms\Report.s\<username>.
- Użytkownicy powinni odczytywać jedynie swoje własne formularze, natomiast formularze wypełnione przez innych użytkowników powinny być dla nich niedostępne.
- Formularze dotyczące kierownictwa przechowywane są w folderze Forms\Supervisors i dostęp do nich mogą uzyskiwać wyłącznie kierownicy.

Folder Forms udostępniany jest jako „Forms”, folder Supervisors udostępniany jest jako „Supervisors”, a każdy folder użytkownika udostępniany jest w oparciu o nazwę użytkownika.

Kierownicy są członkami globalnej grupy Supervisors.

Uprawnienia NTFS dla wszystkich folderów dla członków grupy Authenticated Users (Użytkownicy uwierzytelnieni) zezwalają na modyfikacje (Modify).

Do folderów udostępnionych zostały przydzielone następujące uprawnienia:

Folder udostępniony	Uprawnienia do udziału
Forms	Everyone, Allow Read (Wszyscy, zezwalaj na odczyt)
Supervisors	Supervisors, Allow Read (Supervisor, zezwalaj na odczyt)
<username>	<username> Allow Change {<nazwa_użytkownika> zezwalaj na zmianę}

Które i wymienionych poniżej wymagań zostały spełnione? (wybierz wszystkie właściwe odpowiedzi)

- A. Wszyscy pracownicy mogą pobierać swoje formularze.
 - B. Wszyscy pracownicy mogą w swoich folderach zapisywać wypełnione formularze.
 - C. Pracownicy mogą odczytywać wyłącznie swoje własne formularze.
 - D. Jedynie członkowie grupy Authenticated Users (Użytkownicy uwierzytelnieni) mogą pobierać formularze.
 - E. Jedynie członkowie grupy Supervisors mogą pobierać formularze dotyczące członków tej grupy.
- £. Administrator na serwerze plików skonfigurował uprawnienia foldera udostępnionego. Konfiguracja powinna zezwalać członkom grupy Authenticated Users (Użytkownicy uwierzytelnieni) na zapisywanie plików w folderze, odczytywanie wszystkich plików foldera oraz modyfikowanie lub usuwanie plików, których są właścicielami,

Które uprawnienia należy określić dla foldera udostępnionego, aby zrealizować cele postawione w zadaniu? (wybierz wszystkie właściwe odpowiedzi)

- A. Authenticated Users Full Control (Użytkownicy uwierzytelnieni - pełna kontrola)
 - B. Authenticated Users - Change (Użytkownicy uwierzytelnieni - zmiana)
 - C. Authenticated Users - Read (Użytkownicy uwierzytelnieni - odczyt)
 - D. Creator/Owner Full Control (Twórca/właściciel - pełna kontrola)
 - E. Creator/Owner Change (Twórca/właściciel - zmiana)
 - F. Creator/Owner - Read (Twórca/właściciel - odczyt)
- ó. Administrator konfiguruje w sieci uprawnienia folderów udostępnionych. Członkowie grupy Authenticated Users (Użytkownicy uwierzytelnieni) powinni mieć możliwość odczytu plików przy podłączeniu do foldera poprzez sieć, a jedynie członkowie grupy Managers powinni mieć możliwość odczytu i zmiany plików przy logowaniu lokalnym na komputerze, na którym pliki są przechowywane.

Wszyscy użytkownicy mogą w komputerze logować się lokalnie.

Które uprawnienia należy określić dla foldera udostępnionego? (wybierz wszystkie właściwe odpowiedzi)

- A. NTFS — Interactive - Change (NTFS - Interakcyjni — Zmiana)
- B. NTFS - Interactive - Read (NTFS - Interakcyjni - Odczyt)
- C. NTFS - Authenticated Users - Change (NTFS — Użytkownicy uwierzytelnienie - Zmiana)
- D. NTFS - Managers - Change (NTFS - Managers - Zmiana)
- E. Share Permission - Network - Read (Uprawnienia udziału - Sieć - Odczyt)

E Share Permission - Interactive — Read (Uprawnienia udziału - Interakcyjni — Odczyt) G.
Share Permission — Managers — Change (Uprawnienia udziału — Managers — Zmiana)

4. Folder Documents znajdujący się na komputerze Server01 udostępniany jest jako DocsS. Uprawnienia foldera udostępnionego są następujące:
- Uprawnienia foldera udostępnionego Docs\$: Everyone - Full Control (Wszyscy — pełna kontrola)
 - Uprawnienia NTFS foldera Documents: Authenticated Users — Read, Write; Managers - Modify; Administrators - Full Control (Użytkownicy uwierzytelnieni - odczyt; Managers - modyfikacja; Administratorzy - pełna kontrola)

Które z wymienionych poniżej stwierdzeń są prawdziwe w odniesieniu do dostępu do zasobu? (wybiera wszystkie właściwe odpowiedzi)

- A. Tylko członkowie grupy Administratorzy mogą uzyskiwać dostęp do foldera udostępnionego.
- B. Wszyscy członkowie grupy Users (Użytkownicy) mogą poprzez sieć uzyskiwać dostęp do udziału.
- C. Członkowie grupy Authenticated Users (Użytkownicy uwierzytelnieni) mogą usuwać pliki foldera.
- D. Członkowie grupy Managers mogą usuwać pliki **foldera**.
- E. **Członkowie** grupy **Authenticated Users** (Użytkownicy uwierzytelnieni) mogą zapisywać pliki w folderze.
- F. Członkowie grupy Authenticated Users (Użytkownicy uwierzytelnieni) mogą zmieniać własność plików w folderze.
- G. Członkowie grupy Managers mogą zmieniać własność plików w folderze.

Odpowiedzi do zadania 3.1

1. Prawidłowe odpowiedzi: A, B oraz D

- A. **Prawidłowo** Wszyscy pracownicy mogą uzyskać dostęp do swoich formularzy poprzez folder udostępniony Forms jako członkowie grupy Everyone (Wszyscy).
- B. **Prawidłowo** Wszyscy pracownicy mogą uzyskać dostęp do swoich folderów poprzez przydzielone im uprawnienie zezwalające na zmiany.
- C. **Nieprawidłowo** Pomimo, że uprawnienie zezwalające na zmianę dotyczy foldera określonego przez nazwę użytkownika, każdy użytkownik może przechodzić do dowolnego foldera poprzez folder udostępniony Forms.
- D. **Prawidłowo** Ustawienia domyślne systemu Windows Server 2003 określają, że grupa Everyone (Wszyscy) nie zawiera tożsamości Anonymous Logon (Logowanie anonimowe).
- E. **Nieprawidłowo** Pomimo, że użytkownicy nie mogą bezpośrednio uzyskać dostępu do udostępnionego foldera Supervisors, mogą przejść do niego za pomocą foldera udostępnionego Forms.

2. Prawidłowe odpowiedzi: C oraz E

- A. **Nieprawidłowo** Przydzielając członkom grupy Authenticated Users (Użytkownicy uwierzytelnieni) uprawnienia pełnej kontroli zezwala się na modyfikację lub usuwanie każdego pliku w folderze, co określa zbyt duże uprawnienia niż te, które były wymagane.

- B. Nieprawidłowo** Przydzielając członkom grupy **Authenticated Users** (Użytkownicy uwierzytelnieni) uprawnienia umożliwiające zmiany zezwala się na modyfikacje każdego pliku w folderze, co określa zbyt duże uprawnienia niż te, które były wymagane.
- C. Prawidłowo** Przydzielając członkom grupy **Authenticated Users** (Użytkownicy uwierzytelnieni) uprawnienia umożliwiające odczyt zezwala się na odczyt każdego pliku w folderze, co w spełnia postawione w zadaniu wymagania.
- D. Nieprawidłowo** Przydzielając członkom grupy **Creator/Owner** (Twórca/właściciel) uprawnienia pełnej kontroli zezwala się na modyfikacje lub usuwanie swoich własnych plików w folderze, ale również umożliwia się im zmianę uprawnień tych plików. W takiej sytuacji członek grupy **Creator/Owner** (Twórca/właściciel) może określić uprawnienia tak, aby inni użytkownicy mogli modyfikować lub usuwać pliki.
- E. Prawidłowo** Przydzielając członkom grupy **Creator/Owner** (Twórca/właściciel) uprawnienia umożliwiające zmianę zezwala się użytkownikom, którzy utworzyli pliki, na modyfikacje lub usuwanie każdego plików, co spełnia postawione wymagania.
- F. Nieprawidłowo** Przydzielając członkom grupy **Creator/Owner** (Twórca/właściciel) Użytkownicy uwierzytelnieni) uprawnienia umożliwiające odczyt nie zezwala się użytkownikom na modyfikacje lub usuwanie żadnego pliku w folderze, co nie spełnia wymagań postawionych w zadaniu.

i. Prawidłowe odpowiedzi: !) oraz 1 ■'.

- A. Nieprawidłowo** Ustawienie to umożliwia zmianę plików każdemu użytkownikowi, który załogował się na komputerze. Uprawnienia NTFS dotyczą jedynie użytkowników, którzy **załogowali** się lokalnie, co z założenia dotyczy grupy **Interactive** (Interakcyjni).
- B. Nieprawidłowo** Ustawienie to umożliwia odczyt plików każdemu załogowanemu użytkownikowi, czyli jest niezgodne z wymaganiami. Uprawnienia NTFS dotyczą jedynie użytkowników, którzy załogowali się lokalnie, co z założenia dotyczy grupy **Interactive** (Interakcyjni).
- C. Nieprawidłowo** Ustawienie to umożliwia odczyt plików każdemu załogowanemu użytkownikowi, czyli jest niezgodne z wymaganiami. Uprawnienia NTFS dotyczą jedynie użytkowników, którzy załogowali się lokalnie, co z założenia dotyczy grupy **Interactive** (Interakcyjni).
- D. Prawidłowo** Ustawienie to umożliwia modyfikację plików członkom grupy **Managers**, o ile załogowali się lokalnie. Użytkownicy ci mają również uprawnienia modyfikacji przy logowaniu poprzez sieć, chyba że uprawnienia udziału są bardziej restrykcyjne.
- E. Prawidłowo** Ustawienie to umożliwia odczyt plików wszystkim użytkownikom, którzy uzyskują dostęp do foldera poprzez sieć. Jeśli nie zostały przypisane inne uprawnienia do udziału, członkowie grupy **Managers** nie będą uzyskiwali dodatkowego dostępu do plików poza kontekstem wynikającym z członkostwa w grupie **Network** (Sieć).
- F. Nieprawidłowo** Uprawnienia dotyczące grupy **Interactive** (Interakcyjni), nawet gdy są określone, nie mają wpływu na użytkowników przyłączających się poprzez sieć. Członkami grupy **Interactive** (Interakcyjni) są użytkownicy, którzy załogowali się lokalnie za pomocą konsoli komputera.
- G. Nieprawidłowo** Ustawienie to umożliwia zmianę plików członkom grupy **Managers**, którzy załogowali się poprzez sieć, czyli jest to niezgodne z wymaganiami: członkowie grupy **Managers** mogą jedynie odczytywać i modyfikować pliki, o ile załogowali się lokalnie.

4. Prawidłowe odpowiedzi: B, D oraz E

- A. Nieprawidłowo** Znak \$ powoduje, że nazwa udziału jest ukrywana na listach programów przeglądalających, ale nie ma wpływu na uprawnienia udziału dostępnego w sieci. Chociaż każdy udział utworzony przez system operacyjny jako udział ukryty, w katalogu głównym dysku jest skonfigurowany tak, że jedynie członkowie grupy Administratorzy mogą uzyskiwać do niego dostęp, to dla dowolnego udziału ukrytego utworzonego ręcznie określenie takich wymogów nie jest obowiązujące.
- B. Prawidłowo** Połączenie uprawnień pełnej kontroli dla foldera udostępnionego oraz uprawnień NTFS zezwalających na odczyt i zapis umożliwia dostęp z sieci dla członków grupy Authenticated Users (Użytkownicy uwierzytelnieni).
- C. Nieprawidłowo** Użytkownicy nie mają uprawnień Delete (Usuwanie) lub Modify (Modyfikacja), które są wymagane do usuwania plików.
- D. Prawidłowo** Uprawnienie NTFS zezwalające na modyfikacje umożliwia członkom grupy Managers usuwanie plików.
- E. Prawidłowo** Uprawnienie NTFS zezwalające na zapis umożliwia członkom grupy Authenticated Users (Użytkownicy uwierzytelnieni) zapis plików w folderze.
- F. Nieprawidłowo** Uprawnienia NTFS Zezwalające na odczyt i zapis nie są wystarczające do modyfikacji własności plików.
- G. Nieprawidłowo** Uprawnienia NTFS zezwalające na modyfikacje nie są wystarczające do modyfikacji własności plików.

Zadanie 3.2

Rozwiązywanie problemów dotyczących programu Terminal Services (Usługi terminalowe)

Program Terminal Services (Usługi terminalowe) w porównaniu do uprawnień do udziału, posiada Unikalną konfigurację i uprawnienia. Oprócz uprawnień bezpośrednio wymaganych do używania programu Terminal Services (Usługi terminalowe), wykorzystywanie tego programu wymaga praw użytkownika (przykładowo zalogowanego lokalnie) do komputera, na którym program Terminal Services (Usługi terminalowe) został uruchomiony. W systemie Windows Server 2003 wszystkie te uprawnienia związane z wykorzystywaniem programu Terminal Services (Usługi terminalowe) są przypisane do grupy Remote Desktop Users (Użytkownicy pulpitu zdalnego).

Ustawienia programu Terminal Services for Remote Control (Usługi terminalowe dla sterowania zdalnego), katalog macierzysty; uruchamiane aplikacje oraz ustawienia profilu nie powinny być mylone z uprawnieniami i prawami użytkownika wymaganymi do uzyskania dostępu do programu Terminal Services (Usługi terminalowe).

Pytania do zdania 3.2

1. Administrator dostosowuje konfigurację dla kilku użytkowników tak, aby mogli łączyć się z komputerem Server01 za pomocą programu Terminal Services (Usługi terminalowe) oraz modyfikuje domyślne ustawienia za pomocą konsoli Terminal Services (Usługi terminalowe) tak, aby umożliwić przekierowanie drukarek klienta. Celem jest, aby podczas sesji programu Terminal Services (Usługi terminalowe) każdy użytkownik mógł drukować, na drukarce skonfigurowanej na komputerze lokalnym.

Użytkownicy powiadomili jednak administratora, że nie mogą drukować na swoich lokalnych drukarkach.

Co należy zrobić, aby rozwiązać ten problem?

- A. Dla każdego komputera klienta korzystającego z programu Terminal Server (Usługi terminalowe) należy włączyć ustawienie Client/Server data redirection (Przekierowanie danych klienta/serwera) znajdujące się w zasadzie grupy.
- B. Dla komputera, na którym uruchomiony jest program Terminal Server (Serwer terminali), należy włączyć ustawienie zasady grupy Client/Server data redirection (Przekierowanie danych klienta/serwera).
- C. Poinstruować użytkowników, aby zainstalowali drukarkę lokalną podczas sesji programu Terminal Server (Serwer terminali).
- D. Należy użyć skryptu logowania dla sesji użytkownika programu Terminal Server (Serwer terminali), aby dodać drukarkę.

- 2.. Administrator skonfigurował dla kilku komputerów program klienta usług terminalowych (Terminal Service) - Remote Desktop Connection (Połączenie pulpitu zdalnego), przy czym program Terminal Server (Serwer terminali) został skonfigurowany w trybie domyślnym Remote Desktop for Administration (Pulpit zdalny dla administracji). Użytkownicy próbując połączyć się z programem Terminal Server (Serwer terminali) otrzymywali komunikat o błędzie informujący, że lokalna zasada systemu nie zezwala na logowanie interakcyjne.

Co należy zrobić, aby rozwiązać problem?

- A. Należy dodać użytkowników do grupy Remote Desktop Users (Użytkownicy pulpitu zdalnego).
 - B. Dla każdego użytkownika należy skonfigurować prawo zezwalające na logowanie lokalne (Log on locally) w programie Terminal Server (Serwer terminali).
 - C. Należy włączyć ustawienie zasady grupy Client/Server data redirection (Przekierowanie danych klienta/serwera).
 - D. Dla każdego użytkownika należy włączyć ustawienie Terminal Services Remote Control (Sterowanie zdalne usług terminalowych).
- O. Użytkownik wysłał do administratora prośbę (poprzez e-mail) o nawiązanie sesji programu Remote Assistance (Pomoc zdalna). Administrator próbował połączyć się do komputera użytkownika, aby ustanowić sesję programu Remote Desktop (Pomoc zdalna), ale nie mógł nawiązać połączenia sieciowego.

Administrator mógł połączyć się do komputera użytkownika uzyskując dostęp do systemu plików poprzez udział C\$.

Co jest najbardziej prawdopodobną przyczyną tego problemu?

- A. Konto administratora nie jest członkiem grupy administratorów lokalnych komputera użytkownika.
 - B. Na komputerze administratora nie został zainstalowany klient programu Terminal Services (Usługi terminalowe).
 - C. Nie został otwarty port 3389 zapory ogniowej pomiędzy segmentem sieci administratora a segmentem sieci użytkownika.
 - D. Konto użytkownika w usłudze Active Directory zostało tak skonfigurowane, że nie zezwala na sterowanie zdalne (Remote Control).
4. W przedsiębiorstwie wszyscy użytkownicy komputerów uzyskują dostęp do kilku aplikacji poprzez pojedynczy komputer — Server01, na który uruchomiony został program Terminal Server (Serwer terminali). Komputer ten umieszczony jest w tym samym segmencie sieci lokalnej LAN. Usługa Active Directory, system DNS oraz program Terminal Server (Serwer terminali) działają pod kontrolą systemu Windows Server 2003.
- Poprzedniego dnia, pod koniec pracy administrator zmienił nazwę serwera terminali (Terminal Server) na Appl. Następnie za pomocą programu Terminal Services (Usługi terminalowe) sprawdził, czy serwer jest dostępny poprzez jego nową nazwę przy użyciu konta administratora i konta zwykłego użytkownika. Dostępność została sprawdzona także za pomocą programu Windows Explorer (Eksplorator Windows).
- Rano wszyscy użytkownicy powiadomili, że nie mogą połączyć się do serwera terminali (Terminal Server). Administrator sprawdził i okazało się, że połączenie do programu Terminal Server (Serwer terminali) jest możliwe przy użyciu programu Windows Explorer (Eksplorator Windows), ale nie jest

możliwe poprz.cz program Terminal Services (Usługi terminalowe). Administrator w oparciu o swoje konto mógł połączyć się do programu Terminal Server (Serwer terminali).

Co jest najbardziej prawdopodobną przyczyną tego problemu?

- A. Wpis DNS dotyczący programu Terminal Server (Serwer terminali) powinien zostać odświeżony.
- B. Uprawnienia połączenia programu Terminal Server (Serwer terminali) powinny zostać odświeżone.
- C. Należy zainstalować i skonfigurować program Terminal Services Licensing Server (Serwer licencjonowania usług terminalowych).
- D. Należy ponownie uruchomić program Terminal Server (Serwer terminali).

Administrator próbuje połączyć się do komputera Server01 poprzez klienta programu Remote Desktop for Administration (Pulpit zdalny dla administracji), ale otrzymuje komunikat informujący, że przekroczona została liczba bieżących połączeń.

Administrator może połączyć się za pomocą klienta programu Remote Desktop for Administration (Pulpit zdalny dla administracji) do serwerów Server02, Server03 oraz Server04. Serwery te są serwerami członkowskimi tej samej domeny, a administrator posiada uprawnienia administracyjne do każdego z tych serwerów.

Komputer Server01 nie jest fizycznie dostępny dla administratora, ponieważ znajduje się w lokalizacji zdalnej.

Jakie kroki należy przedsięwziąć, aby rozwiązać ten problem? (wybierz wszystkie właściwe odpowiedzi)

- A. Należy połączyć się do komputera Server01 za pomocą klienta programu Remote Desktop for Administration (Pulpit zdalny dla administracji).
- B. Należy podłączyć się do komputera Server01 z sesji programu Terminal Services (Usługi terminalowe) na serwerze Server02 (za pomocą konsoli Terminal Services Manager). Należy *odłączyć* jedną z sesji zdalnych.
- C. Należy za pomocą klienta programu Remote Desktop for Administration (Pulpit zdalny dla administracji) połączyć się do serwera Server01 z sesji programu Terminal Services (Usługi terminalowe) ustanowionej na serwerze Server02. Należy odłączyć jedną z sesji zdalnych.
- D. W przystawce Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) należy otworzyć okno dialogowe właściwości komputera Server01. Następnie należy skonfigurować serwer Server01 tak, aby następowała odmowa połączeń usług terminalowych, a w kolejnym kroku należy skonfigurować komputer Server01 tak, aby zezwalał na połączenia programu Terminal Services (Usługi terminalowe).
- E. Za pomocą klienta programu Remote Desktop for Administration (Pulpit zdalny dla administracji) należy podłączyć się do serwera Server01 z sesji programu Terminal Services (Usługi terminalowe) na serwerze Server02. Następnie należy otworzyć stronę właściwości modułu System dla serwera Server01 i skonfigurować serwer tak, aby następowała odmowa połączeń pulpitu zdalnego (Remote Desktop Connections), a następnie ponownie skonfigurować Server01 tak, aby możliwe stały się połączenia programu Remote Desktop Connections (Połączenia pulpitu zdalnego).

Odpowiedzi do zadania 3.2

1. Prawidłowa odpowiedź: A

- A. Prawidłowo Pomimo, że domyślnie ustawienie to nie jest skonfigurowane (Not Configured), jeśli będzie określone jako Disabled (Wyłączone) ustawienie zasady grupy zastąpi ustawienia konsoli Terminal Server (Serwer terminali) uniemożliwiając prawidłowe przekierowanie danych. Zmiana tego ustawienia (z Wyłączone na Załączone) rozwiąże problem.
- B. Nieprawidłowo To ustawienie zasady grupy dotyczy działania komputera lokalnego podczas sesji programu Terminal Services (Usługi terminalowe) uruchomionej z tego komputera. Włączenie tego ustawienia dla komputera, na którym uruchomiony jest program Terminal Server (Serwer terminali), będzie kontrolować sesje wyjściowe konsoli programu Terminal Server (Serwer terminali), a nie wejściowe komputerów klienta, co jest wymagane w zadaniu.
- C. Nieprawidłowo Działanie takie skonfiguruje połączenie drukarki sieciowej do komputera lokalnego, co nie jest wymaganiem postawionym w zadaniu. Na komputerze lokalnym wymagane byłyby także dodatkowe działania związane z udostępnianiem i określaniem uprawnień dla drukarki.
- D. Nieprawidłowo Patrz uzasadnienie do odpowiedzi C.

2.. Prawidłowa odpowiedź: A

- A. Prawidłowo Grupa Remote Desktop Users (Użytkownicy pulpitu zdalnego) ma odpowiednią konfigurację i uprawnienia, aby jej członkowie uzyskiwali dostęp do programu Terminal Server (Serwer terminali).
- B. Nieprawidłowo Ustawienie to usunie jedną przeszkodę uniemożliwiającą użytkownikom połączenie z programem Terminal Services (Serwer terminali), ale poza tym muszą zostać określone uprawnienia dla połączenia do samego programu Terminal Server (Serwer terminali). Oprócz tego, działanie takie zezwoli użytkownikom na logowanie lokalne, co mogłoby być niepożądane.
- C. Nieprawidłowo Ustawienie to pozwala na kontrolowanie podczas sesji użytkownika sposobu realizowania przekierowywania danych drukarek i dysków, nie umożliwia natomiast konfiguracji dostępu logowania do samej sesji.
- D. Nieprawidłowo Ustawienie to kontroluje, w jaki sposób sterowanie zdalne (Remote Control) może być używane w ustanowionej sesji programu Terminal Services (Usługi terminalowe), a nie kontrola dostępu logowania do samej sesji.

o. Prawidłowa odpowiedź: C

- A. Nieprawidłowo W tym przypadku nie zachodzi taka sytuacja, gdyż administrator mógł podłączyć się do administracyjnego punktu udostępniania (C\$) komputera użytkownika.
- B. Nieprawidłowo Klient programu Terminal Services (Usługi terminalowe) nie jest wywoływany w sesji programu Remote Assistance (Pomoc zdalna). Za ustanowienie i wykorzystanie sesji programu Remote Assistance (Pomoc zdalna) jest odpowiedzialna aplikacja Windows Messenger Services.
- C. Prawidłowo Usługi Remote Assistance (Pomoc zdalna) wykorzystują do komunikacji port 3389. Jest to prawdopodobna przyczyna problemu, jeśli nie można nawiązać połączenia z komputerem użytkownika.

D. Nieprawidłowo Ustawienie to kontroluje, czy umożliwiające jest sterowanie zdalne dla użytkowników sesji programu Terminal Server (Serwer terminali), a nie programu Remote Assistance (Pomoc zdalna).

A. Prawidłowa odpowiedź: C

- A. Nieprawidłowo** Ponieważ komputer jest widoczny za pomocą programu Windows Explorer (Eksplorator Windows), rozwiązywanie nazwy działa prawidłowo.
- B. Nieprawidłowo** Uprawnienia połączenia zostały skonfigurowane prawidłowo, gdyż administrator sprawdził dostęp do programu Terminal Server (Serwer terminali) po zmianie nazwy serwera. Żadne mechanizmy odświeżania systemu DNS lub zasady grupy nie wpływają na te uprawnienia.
- C. Prawidłowo** Jest to prawdopodobna przyczyna problemu. Program Terminal Services (Usługi terminalowe) będzie zainstalowany i będzie pracował prawidłowo przez 120 dni. Po tym okresie program nie będzie zezwalał na ustanawianie połączeń dopóki serwer licencjonowania (License Server) nie zostanie skonfigurowany i udostępniony.
- D. Nieprawidłowo** Sama usługa nie jest prawdopodobnie przyczyną błędu, ponieważ administrator mógł się połączyć i usługa działała prawidłowo już po zmianie nazwy serwera.

O. Prawidłowe odpowiedzi: A oraz B

- A. Prawidłowo** Poprzez połączenie do innego serwera (terminali) administrator uzyska dostęp do konsoli Terminal Services Manager (Menedżer usług terminalowych), dzięki której administrator, będzie mógł odłączyć jedną z ustanowionych sesji programu Terminal Services (Serwer terminali) komputera Server01. W ten sposób administrator będzie mógł nawiązać inną sesję używając swojej tożsamości.
- B. Prawidłowo** Konsola Terminal Services Manager (Menedżer usług terminalowych) może łączyć się do dowolnego serwera domeny, na którym uruchomiony jest program Terminal Services (Usługi terminalowe). Za pomocą konsoli Terminal Services Manager (Menedżer usług terminalowych) administrator będzie mógł odłączyć jedną z sesji zdalnych i nawiązać inną sesję używając swojej tożsamości.
- C. Nieprawidłowo** Jeśli za pomocą klienta programu Remote Desktop (Pulpit zdalny) nie było możliwe połączenie do serwera Server01, odmowa połączenia wystąpi przy próbie jego nawiązania do każdego innego komputera, bez względu na to, czy komputer ten jest serwerem terminali, czy nim nie jest.
- D. Nieprawidłowo** To nie jest prawidłowa opcja. W oknie właściwości systemu w przystawce Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) nie można przeprowadzać konfiguracji programu Terminal Services (Usługi terminalowe).
- E. Nieprawidłowo** Zmiana polegająca na wyłączeniu i włączeniu możliwości realizowania połączeń nie zmienia żadnych konfiguracji komputera ani nie odłączy żadnej aktywnej sesji. Problem nie zostanie rozwiązany, ponieważ spowodowany był przekroczeniem limitu liczby sesji.

Zadanie 3.3

Konfigurowanie uprawnień systemu plików

W celu określenia uprawnień do obiektów (folderów i plików) systemu plików użytkownik musi mieć możliwość dodawania wpisów do listy kontroli dostępu (ACL) obiektu. Listy ACL są częścią systemu plików NTFS, tak więc system ten musi zostać zainstalowany na każdym komputerze, na którym znajdują się zasoby przewidziane do zabezpieczania za pomocą systemu plików.

Uprawnienia NTFS działają w taki sam sposób, jak uprawnienia do udziałów w odniesieniu do wyznaczania uprawnień czynnych. Wszystkie identyfikatory SID wymienione w żetonie użytkownika są porównywane z wpisami na liście ACL zasobu. Wszystkie uprawnienia związane z różnymi identyfikatorami są sortowane i przydzielane zostają najbardziej liberalne uprawnienia.

Wyjątkiem od tej liberalnej zasady jest sytuacja, kiedy co najmniej jeden identyfikator SID ma przydzielone uprawnienie odmowy. W takim przypadku uprawnienia odmowy mają pierwszeństwo.

Pytania do zadania 3.3

- X. Użytkownik Joe ma konto w domenie cuinoHi.com i jest członkiem {globalnej grupy Sales. Uprawnienia do foldera Documents znajdującego się na serwerze plików obliczone za pomocą programu Cads przedstawiają się następująco:

```
C:\>cacls documents
```

```
C:\Documents CONTOSONJoe: (01 MCI HDENYHspecial access:)
```

```
    READ_CONTROL
    FILE_READ_DATA
    FILE_READ_EA
    FILE_READ_ATTRIBUTES
```

```
CONTOSONSa 1 es:(01 HCI HDENYHspecial access:)
```

```
    FILE_WRITE_DATA FILE_APPEND_DATA
    FILE_WRITE_EA FILE_WRITE_ATTRIBUTES
```

```
BUILTIN\Administrators:F CONTOS0\Sales:(CI)R
```

```
CONTOS0\Sales:(01HCI)(special access:)
```

```
    READ_CONTROL
    SYNCHRONIZE
    FILE_GENERIC_READ
    FILE_READ_DATA
    FILE_READ_EA
```

FILE_READ_ATTRIBUTES

BUILTIN\Administrators:(OI)(CI)F NT
 AUTHORITY\SYSTEM:(OI)(CI)F CREATOR
 OWNER:(OI)(CI)(IO)F
 BUILTIN\Users:(OI)(CI)R
 BUILTIN\Users:(CI)(special access:)
 FILE_APPEND_DATA

BUILTIN\Users:(CI)(special access:)
 FILE_WRITE_ATTRIBUTES

Jakie są uprawnienia czynne użytkownika Joe do foldera Documents?

- A. Access Denied (odmowa dostępu)
- B. Read (Odczyt)
- C. Change (Zmiana)
- D. Full Control (Pełna kontrola)

A. Administrator konfiguruje uprawnienia dla foldera udostępnionego Finance znajdującego się na serwerze plików - Server(\\).

Dla grup Accounting oraz AccountingExec uprawnienia do foldera należy skonfigurować w następujący sposób:

Grupa Accounting powinna mieć dostęp zezwalający na odczyt zawartości foldera Finance.

Grupa AccountingFjccc powinna mieć uprawnienia zezwalające na zmianę (Change) danych w folderze Finance.

Wszyscy użytkownicy **muszą** mieć możliwość odczytu pliku nazwanego Summary.rpt umieszczonego w folderze Finance. Użytkownicy nie powinni mieć dostępu do żadnych innych plików w tym folderze.

W jaki sposób należy skonfigurować uprawnienia NTFS i udziału dla foldera Finance?

- A. Share: Accounting - Read; AccountingFjccc - Read; Users - Read (Udział: Accounting - Odczyt; AccountingExec - Odczyt; Users - Odczyt), NTFS: Accounting - Read; AccountingFjccc - Modify; Users - Read (NTFS: Accounting - Odczyt; AccountingExec - Modyfikacja; Users - Odczyt)
- B. Share: Accounting - Full Control; AccountingFjccc - Full Control; Users - Read (Udział: Accounting - Pełna kontrola; AccountingFjccc - Pełna kontrola; Users - Odczyt), NTFS: Accounting - Read; AccountingExec - Modify; Users - List, Read access on Summary.rpt (NTFS: Accounting - Odczyt; AccountingFjccc - Modyfikacja; Users - Wyświetlanie zawartości foldera, Odczyt dla pliku Summary.rpt)
- C. Share: Accounting - Read; AccountingExec - Modify; Users - Read (Udział: Accounting - Odczyt; AccountingExec - Modyfikacja; Users - Odczyt), NTFS: Accounting - Read; AccountingExec - **Full Control**; Users - Read (NTFS: Accounting - Odczyt; AccountingFjccc - Pełna kontrola; Users - Odczyt)
- D. Share: Accounting - Full Control; AccountingExec - Full Control; Users - Deny Read (Udział: Accounting - Pełna kontrola; AccountingExec - Pełna kontrola; Users - Odmowa odczytu), NTFS: Accounting - Read; AccountingExec - Read; Users - List, Read access on Summary.rpt (NTFS:

Odpowiedzi do zadania 3.3

1. Prawidłowa odpowiedź: A

- A. Prawidłowo Po konta użytkownika Joe zostało przypisane uprawnienie Deny — Read (Odmów odczytu), które przetwarzane jest na początku listy uprawnień i zastępuje wszystkie inne, blokując tym samym dostęp do zasobu.
- B. Nieprawidłowo Patrz uzasadnienie do odpowiedzi A.
- C. Nieprawidłowo Patrz uzasadnienie do odpowiedzi A.
- D. Nieprawidłowo Patrz uzasadnienie do odpowiedzi A.

2.. Prawidłowa odpowiedź: B

- A. Nieprawidłowo Ustawienia te umożliwiają użytkownikom odczyt wszystkich plików foldera Finance, co nie jest zgodne z wymaganiami zadania.
- B. Prawidłowo Ustawienia re umożliwiają użytkownikom odczyt plików realizowany poprzez punkt udostępniania, ale nie przypisują żadnych uprawnień poprzez NTFS, za wyjątkiem zezwolenia na odczyt pliku Summary.rpr, co jest zgodne z postawionymi wymaganiami.
- C. Nieprawidłowo Ustawienia te umożliwiają użytkownikom odczyt wszystkich plików foldera Finance, co nie jest zgodne z wymaganiami zadania.
- D. Nieprawidłowo Ustawienia te umożliwiają członkom grupy Users (Użytkownicy) odpowiedni dostęp do pliku Summary.rpi, ale ustawienia NTFS ograniczają użytkownikom grupy Accountin gl*.xc< odczyt wszystkich plików w folderze Finance. m nie jest zgodne z postawionymi wymaga niami.

O. Prawidłowe odpowiedzi: A, D oraz E

- A. Prawidłowo Uprawnienie Read (Odczyt), przydzielone pośrednio i bezpośrednio, umożliwia odczyt atrybutów. Istnieje możliwość ograniczania specyficznych ustawień umożliwiających odczyt atrybutów, ale w tym celu należy usunąć zaznaczenie pola wyboru na tym poziomie zestawienia uprawnień (a nie zaznaczać pole wyboru).
- B. Nieprawidłowo Uprawnienie zezwalające na zapis zasobu zostało przydzielone pośrednio dla grupy Salcs, ale odmowa /osrała określona w sposób bezpośredni. Bezpośrednie uprawnienia odmowy zastępują pośrednie uprawnienia zezwalające. Uprawnienia Wrire (Zapis) zawierają upraw nienia zapisu atrybutów.
- C. Nieprawidłowo Uprawnienie zezwalające na zapis zasobu zostało przydzielone pośrednio dla grupy Sales, ale odmowa została określona w sposób bezpośredni, co oznacza, że dla grupy Salcs przypisana została odmowa zapisu. Bezpośrednie uprawnienia odmowy zastępują pośrednie upraw nienia zezwalające. Uprawnienia Writc (Zapis) zawierają uprawnienia zezwalające na tworzenie plików.
- D. Prawidłowo Uprawnienie zezwalające na zapis zasobu zostało przydzielone pośrednio dla grupy Sales, ale odmowa została określona w sposób bezpośredni, co oznacza, że dla grupy Sales przypi sana została odmowa zapisu. Bezpośrednie uprawnienia odmowy zastępują pośrednie uprawnienia zezwalające. Uprawnienia Write (Zapis) zawierają uprawnienia zezwalające na tworzenie plików.
- E. Prawidłowo Uprawnienie Read (Odczyt), przydzielone pośrednio i bezpośrednio, umożliwia odczyt plików foldera.

F. Nieprawidłowo Uprawnienie Read (Odczyt), przydzielone pośrednio i bezpośrednio, umożliwia odczyt plików foldera.

4. Prawidłowa odpowiedź: B

A. Nieprawidłowo Uprawnienia takie umożliwiają użytkownikom dostęp do foldera Report, ale umożliwiają również wyświetlanie listy plików foldera i w związku z tym nie są to minimalne wymagane uprawnienia.

B. Prawidłowo Uprawnienie to umożliwia użytkownikom przechodzenie prze/, foldery Marketing i Summary w celu uzyskania dostępu do foldera Reports. W folderach Marketing lub Summary użytkownicy nie będą mogli uzyskać dostępu do żadnego pliku (a nawet przeglądania ich listy).

C. Nieprawidłowo Umożliwienie odczytu atrybutów rozszerzonych nie pozwala uzyskać dostępu do pod folderów.

D. Nieprawidłowo Umożliwienie odczytu atrybutów nie pozwala uzyskać dostępu do podfolderów.

Zadanie 3.4

Rozwiązywanie problemów związanych z dostępem do plików i folderów udostępnionych

Po określeniu uprawnień do zasobu, reguły dostępu są jednoznaczne. Jeśli uprawnienia czynne użytkownika nie pozwalają uzyskać dostępu do zasobu, zgodnie z regułą użytkownik nie uzyska dostępu. Takie jest oczekiwane działanie systemu.

Nieoczekiwany sposób działania systemu dostępu ma miejsce, jeśli wydaje się, że dostęp do zasobu został skonfigurowany prawidłowo, a tak nie jest w rzeczywistości. W przypadku błędnej konfiguracji, użytkownik nie może uzyskać dostępu do zasobu, do którego jest mu ten dostęp potrzebny, albo użytkownik uzyskuje dostęp do zasobów, do których dostępu nie powinien uzyskać. Oba przypadki są niepożądane.

Błędna konfiguracja zdarza się najczęściej w dwóch przypadkach: użytkownik nie jest członkiem grupy, która ma uprawnienia do zasobu lub występuje pierwszeństwo uprawnień udziału lub NTFS, którego administrator nie przewidział. W obu sytuacjach uważna analiza konfiguracji członkostwa grup i przydziału uprawnień powinna rozwiązać większość problemów związanych z uzyskiwaniem dostępu do zasobu.

Pytania do zadania 3.4

1. Użytkownik powiadomił dział pomocy technicznej informując, że nie może zalogować się w sieci. Przy użyciu przysławki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) administrator sprawdził usługę Active Directory i okazało się, że konto użytkownika nie istnieje w katalogu. Dalsza analiza dzienników zdarzeń usługi katalogowej pokazała, że konto zostało usunięte.
Administrator ponownie utworzył konto użytkownika za pomocą przysławki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory). Jakie czynności należy jeszcze wykonać, aby dostęp użytkownika do zasobów został w pełni odtworzony? (wybierz wszystkie właściwe odpowiedzi)
 - A. Należy umieścić konto użytkownika w odpowiednich grupach.
 - B. Należy wyzerować konto komputera.
 - C. Do konta użytkownika należy ponownie przypisać i zastosować odpowiednie zasady grupy.
 - D. Należy ponownie przydzielić uprawnienia do zasobów, do których uprawnienia te były przydzielone w oparciu o konto użytkownika.
 - E. Należy ponownie przydzielić uprawnienia do zasobów, do których uprawnienia te były przydzielone w oparciu o członkostwo grup.

2.. Użytkownik Joe ma być odpowiedzialny za realizację dodatkowych zadań związanych z administracją sieci działu Finance.

Administrator na komputerze użytkownika Joe (zalogowany jako Joe) wykonał polecenie Run As wykorzystując tożsamość administratora do uruchomienia przystawki Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory), a następnie dodał użytkownika Joe do grupy liadmin3, do której przydzielone zostały uprawnienia administracyjne dla kont użytkowników jednostki organizacyjnej Finance. Następnie administrator zamknął przystawkę Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory).

Podczas próby wyzerowania hasła użytkownika jednostki organizacyjnej Finance system odmówił dostępu użytkownikowi Joe.

Jakie dodatkowe czynności należy wykonać, aby użytkownik Joe mógł wykonywać powierzone mu Zadania administracyjne?

- A. Należy dodać konto użytkownika Joe do wbudowanej w domenie grupy Account Operators (Operatorzy kont).
- B. Należy dodać konto użytkownika Joe do jednostki organizacyjnej liadmin3.
- C. Należy wyzerować konto komputera użytkownika Joe.
- D. Należy poinstruować użytkownika Joe, aby wylogował się, a następnie ponownie zalogował na komputerze.

■i. Konto użytkownika Joe jest członkiem jednostki organizacyjnej Sales domeny contoso.com, a także należy do grupy globalnej Eniployccs.

Po przydzieleniu użytkownika Joe do działu Finance administrator zarejestrował konto użytkownika joe w grupie globalnej Finance. Kiedy użytkownik Joe zalogował się w swoim komputerze i chciał uzyskać dostęp na serwerze .Sciver()l do udostępnionego foldera Documents podczas próby zapisu plików w tym folderze, system wyświetlił komunikat informujący o odmowie dostępu.

Poniżej wymienione zostały uprawnienia udziału Documents.

Podmiot zabezpieczeń

Uprawnienia

Joe (konto użytkownika)	Allow: Read (Zezwalaj na odczyt)
Finance (grupa globalna)	Allow: Read (Zezwalaj na odczyt)
F.mployccs (grupa globalna)	Allow: Read (Zezwalaj na odczyt)

Poniżej wymienione zostały uprawnienia NTFS dla foldera Documents.

Podmiot zabezpieczeń

Uprawnienia

Joe (konto użytkownika)	Allow: Read (Zezwalaj na odczyt)
Finance (grupa globalna)	Allow: Read, Write (Zezwalaj na odczyt i zapis)
Employccs (grupa globalna)	Allow: Read (Zezwalaj na odczyt)
System	Allow: Full Control (Zezwalaj na pełną kontrolę)
Administratorzy	Allow: Full Control (Zezwalaj na pełną kontrolę)

Dlaczego użytkownik Joe nie może uzyskać dostępu do foldera Documents? A.

Uprawnienia udziału zastępują uprawnienia NTFS.

- B. Konto użytkownika Joe należy przenieść do jednostki organizacyjnej Finance.
- C. Dla konta użytkownika Joe należy usunąć uprawnienia NTFS, dzięki czemu zastosowane zostaną uprawnienia NTFS dotyczące grupy.
- D. Konto użytkownika Joe należy usunąć z grupy globalnej Employee.

Odpowiedzi do zadania 3.4

1. Prawidłowe odpowiedzi: A oraz D

- A. **Prawidłowo** Konto użytkownika powinno stać się członkiem tych samych grup, co konto usunięte. Jeśli konto użytkownika znajduje się na liście członków grupy, należy najpierw je usunąć z grupy, a następnie ponownie je do niej dodać. Pomimo, że poprzednie konto korzysta z tej samej nazwy, ma inny identyfikator (Sid). Uprawnienia zasobu dla danej grupy nie muszą być ponownie przypisywane, ponieważ jedyną informacją, która uległa zmianie, jest członkostwo tej grupy.
- B. **Nieprawidłowo** Konto komputera nie jest powiązane z konkretnym kontem użytkownika i dla tego nie musi być zerowane. Zerowanie konta komputera jest potrzebne jedynie wtedy, kiedy konto komputera nie jest zsynchronizowane z domeną.
- C. **Nieprawidłowo** Zasady grup stosują się do lokalacji, domen oraz jednostek organizacyjnych. Zawsze po umieszczeniu w jednostce organizacyjnej nowego użytkownika, zasady grupy tej jednostki oraz zasady grupy na poziomie domeny będą automatycznie stosowane i odświeżane w momencie logowania się użytkownika.
- D. **Prawidłowo** Każdy indywidualny przydział uprawnień do konta Użytkownika musi być ponownie utworzony, jeśli konto użytkownika znajduje się na liście członków grupy, należy najpierw je usunąć z grupy, a następnie ponownie je do niej dodać. Pomimo, że poprzednio konto korzysta z tej samej nazwy, ma inny identyfikator SID.
- E. **Nieprawidłowo** Uprawnienia dla grup nie zostały zmienione, tak więc nie są potrzebne żadne nowe uprawnienia dla grup w związku z zarejestrowaniem w grupie nowego członka. W momencie logowania się użytkownika, w jego żetonie do listy identyfikatorów (Sid) zostanie dodana lista wszystkich grup, których członkiem jest użytkownik.

2. Prawidłowa odpowiedź: D

- A. **Nieprawidłowo** Działanie takie rozszerzy uprawnienia użytkownika Joe daleko poza granice jednostki organizacyjnej Finance, które w takim przypadku obejmą całą domenę. Oprócz tego, do grupy Account Operators (Operatorzy kont) mogą być przydzielone dodatkowe uprawnienia, które nie powinny być przypisane grupie Itadmin3.
- B. **Nieprawidłowo** Członkostwo użytkownika Joe w jednostce organizacyjnej nie ma związku z jego uprawnieniami do administrowania kontami użytkowników jednostki organizacyjnej Finance. Odpowiednie uprawnienia przydzielane są poprzez członkostwo w grupie Itadmin3, a nie poprzez członkostwo w jakiegokolwiek jednostce organizacyjnej.
- C. **Nieprawidłowo** Zerowanie konta komputera jest potrzebne, jeśli komputer przestaje być zsynchronizowany z domeną i nie dotyczy uprawnień użytkownika, który w tym momencie loguje się na komputerze. Dopóki komputer może komunikować się z domeną, co ma miejsce w przypadku użytkownika Joe, uprawnienia użytkownika są podstawą do określenia, czy użytkownik może wykonywać konkretne zadania administracyjne.

D. Prawidłowo Zmiana członkostwa w grup nie będzie widoczna dopóki tożsamość użytkownika Joe nie zostanie ponownie sprawdzona i nie zostanie przypisany nowy żeton, który zawiera informacje o członkostwie w nowej grupie. Przydział żetonu następuje jedynie podczas logowania. Ponieważ Joe był zalogowany w komputerze w momencie dokonywania zmian członkostwa grupy, jego żeton nie zawiera identyfikatorów SID skojarzonych z członkostwem w nowej grupie.

»J. **Prawidłowa odpowiedź: A**

A. Prawidłowo Uprawnienia udziału dla konta użytkownika Joe oraz dla grupy globalnej Finance zezwalają na odczyt i dlatego uprawnienia dostępu dla użytkownika Joe zostały ograniczone do odczytu. Spośród uprawnień udziału i NTFS, uprawnieniami czynnymi stają się te, które są bardziej restrykcyjne.

B. Nieprawidłowo Lokalizacja konta użytkownika Joe w usłudze Active Directory nie ma związku z dostępem do zasobów. Obiekty użytkowników, grup i komputerów są jedynie obiektami katalogu będącymi podmiotami zabezpieczeń, do których można przypisywać uprawnienia do zasobu.

C. Nieprawidłowo Uprawnienia czynne NTFS użytkownika Joe to odczyt i zapis, co wynika z jego członkostwa w grupie globalnej Finance. **Ograniczenia** wynikają z upra. uprawnień udziału (odczyt), a nie z ograniczeń uprawnień NTFS.

D. Nieprawidłowo W tym przypadku usunięcie użytkownika Joe z grupy globalnej Finance nie spowoduje skutku, ponieważ ograniczenie zapisu wynika z uprawnień **udziału**, a nie z ograniczeń uprawnień NTFS. Po zwiększeniu uprawnień udziału dla konta użytkownika Joe lub dla grupy globalnej Finance, użytkownik Joe będzie mógł zapisywać pliki w folderze Documents.

17 Zarządzanie i obsługa środowiska serwera (4.0)



Do zarządzania systemem Microsoft Windows Server 2003 potrzebna jest wiedza o tym, jakie zdarzenia miały w miejsce w systemie. Informacje te najłatwiej uzyskać analizując dzienniki zdarzeń. System Windows Server 2003 został wyposażony w trzy główne dzienniki - System, Security (Zabezpieczenia) oraz Application (Aplikacja). Podczas przeglądania dzienników można korzystać z filtrów tak, aby wyświetlane były tylko te informacje, które są potrzebne.

Odrębnym fragmencem zagadnień związanych z zarządzaniem serwerem jest zapewnienie, aby w systemie były terminowo pobierane i stosowane istotne aktualizacje. Wiele spośród ważnych luk w zabezpieczeniach systemu zostało poprawionych przez firmę Microsoft, ale administratorzy systemów nie znaleźli czasu na zainstalowanie poprawek w serwerach. Gdyby administratorzy na czas zainstalowali poprawki, ich systemy byłyby odporne na różnego rodzaju programy wirusowe, takie jak Code Red czy Slammer. Usługa SUS (Software Update Services) uruchomiona w systemie Windows Server 2003 umożliwia przedsiębiorstwu wykorzystywanie tego serwera jako serwera aktualizacji, z którego można pobierać poprawki firmy Microsoft, zamiast korzystania z serwerów aktualizacji firmy Microsoft umieszczonych w Internecie.

Innym obszarem wymagającym poświęcenia uwagi jest licencjonowanie. Jeśli przedsiębiorstwo zostanie poddane inspekcji zgodności licencji, w sytuacji wykrycia niezgodności opłaty karne będą bardzo wysokie. Zrozumienie działania licencjonowania może również przyczynić się do zaoszczędzenia pieniędzy przedsiębiorstwa, ponieważ pozwala stosować najbardziej odpowiednie opcje licencjonowania, lepsze niż te, które są aktualnie wykorzystywane.

System Został wyposażony w kilka narzędzi umożliwiających zdalne zarządzanie serwerami. Są to programy Terminal Services (Usługi terminalowe), Remote Assistance (Pomoc zdalna), Computer Management Console (Konsola zarządzania komputerem) oraz narzędzia HTML dla administracji zdalnej. Każde może być używane w określonych sytuacjach, do wykonywania specyficznych grup zadań. Administratorzy powinni znać zalety i ograniczenia każdej postaci zarządzania zdalnego.

Istotnym zagadnieniem jest również obsługa niezawodności infrastruktury serwera plików i druku. Administratorzy systemów muszą diagnozować i rozwiązywać problemy dotyczące serwerów plików i druku, jak również muszą monitorować ich wydajność, dzięki czemu mogą przedsięwziąć działania poprawiające wydajność systemu.

Sprawdzanie umiejętności i sugerowane ćwiczenia praktyczne

Poniżej przedstawiono umiejętności potrzebne do opanowania tematu „Zarządzanie i obsługa środowiska serwera” objętego egzaminem 70-290 — *Zarządzanie i obsługa środowiska Windows Server 2003*:

- Monitorowanie i analiza zdarzeń.
 - » Zadanie kontrolne 1: Ustawianie filtra dla dziennika Security (Zabezpieczenia) tak, aby wyszukiwane były wszystkie zdarzenia wygenerowane przez konto administratora.
 - » Zadanie kontrolne 2: Ustawianie filtra dziennika System tak, aby wyszukiwane były wszystkie zdarzenia dotyczące awarii urządzeń, które wystąpiły w ostatnim tygodniu.
- Zarządzanie infrastrukturą aktualizacji oprogramowania.
 - » Zadanie kontrolne 1: Instalacja i konfiguracja dodatku SUS w celu wygenerowania listy aktualizacji zatwierdzonych oraz w celu pobrania tych aktualizacji do serwera usługi SUS. Wykorzystanie zasady grupy do skonfigurowania systemu Windows XP Professional tak, aby dla tego systemu serwer SUS był wykorzystywany jako serwer usługi Automatic Updates.
 - » Zadanie kontrolne 2: Instalowanie pakietu serwisowego w systemie Windows XP Professional przy użyciu zasady grupy.
- Zarządzanie licencjami oprogramowania lokacji.
 - » Zadanie kontrolne 1: Uruchomienie konsoli Licensing (Licencjonowanie) znajdującej się w grupie programów Control Panel (Panel sterowania) i zapoznanie się z informacjami modułu Help (Pomoc) dotyczącymi zmiany trybu licencjonowania Per Server na Per User/Per Device (Na serwer/Użytkownika lub urządzenie).
 - » Zadanie kontrolne 2: Instalowanie programu License Logging Service (Serwer rejestrowania licencji) w systemie Windows Server 2003.
- Zdalne Zarządzanie serwerami.
 - » Zadanie kontrolne 1: Instalowanie narzędzi HTML (Hypertext Markup Language) dla administracji zdalnej na serwerze członkowskim systemu Windows Server 2003 oraz wykorzystanie tych narzędzi do zmiany nazwy serwera.
 - » Zadanie kontrolne 2: Logowanie zdalne w systemie Windows Server 2003 za pomocą trybu usług terminalowych Remote Desktop or Administration (Pulpit zdalny dla administracji).
- Rozwiązywanie problemów zagadnień związanych z kolejkami wydruku.
 - » Zadanie kontrolne 1: Utworzenie dwóch współużytkowanych drukarek, które dotyczą tej samej drukarki fizycznej. Ustawianie priorytetów dla obu drukarek udostępnionych (dla jednej 99 oraz dla drugiej 1). Wygenerowanie pięciu zadań wydruku dla każdej drukarki i sprawdzenie, która drukarka współużytkowana szybciej zakończy zadania.
 - » Zadanie kontrolne 2: Wysłanie kilku zadań do drukarki. Wstrzymanie jednego z zadań i zamiana priorytetów drukarek celem sprawdzenia, w jaki sposób zmieniła się kolejność wydruku zadań.
- Monitorowanie zdarzeń.
 - » Zadanie kontrolne 1: Konfigurowanie inspekcji dla zdarzeń związanych z zarządzaniem kontami domeny za pomocą zasady grupy. Utworzenie pięciu kont użytkowników i dwóch grup. Zmiana

hasel dla trzech nowych kont użytkowników. Przeglądanie dziennika Security (Zabezpieczeń) kontrolera domeny w celu sprawdzenia, które zdarzenia zostały zarejestrowane.

- » Zadanie kontrolne 2: Konfigurowanie inspekcji dla zdarzeń związanych z dostępem do obiektów domeny. Edycja właściwości foldera udostępnionego tak, aby inspekcja dotyczyła grupy Every-one (Wszyscy). Korzystanie z kilku różnych kont celem uzyskania dostępu do foldera udostępnionego i następnie przeanalizowanie dziennika Security (Zabezpieczenia) serwera, na którym folder ten jest przechowywany.
- Monitorowanie bieżącej wydajności systemu.
 - » Zadanie kontrolne 1: Utworzenie widoku konsoli Performance (Wydajność) w celu wyświetlenia średniej wartości liczników % Processor Time (Czas procesora %), Current Disk Queue Length (Długość bieżącej kolejki dysku) oraz Available Memory (Dostępna pamięć) zarówno wyrażonej w kilobajtach, jak i megabajtach.
 - » Zadanie kontrolne 2: Utworzenie widoku konsoli Performance (Wydajność) w celu wyświetlenia średniej wartości licznika % Processor Time (Czas procesora %) dla kilku różnych aplikacji uruchomionych na serwerze.
- Monitorowanie serwerów plików i druku.
 - » Zadanie kontrolne 1: Włączenie przydziału dysku o wartości 10 MB dla wszystkich użytkowników woluminu za wyjątkiem administratora. Utworzenie na tym woluminie foldera udostępnionego. Otwarcie woluminu udostępnionego na stacji roboczej systemu Windows XP przy użyciu konta innego niż konto administratora. Próba skopiowania danych o wielkości przekraczającej wartość 10 MB do foldera udostępnionego.
 - » Zadanie kontrolne 2: Określenie zestawu indywidualnych przydziałów na woluminie systemu Windows Server 2003 (przydział dla jednego użytkownika to 10 MB, dla drugiego 15 MB, a dla trzeciego to 20 MB). Eksport tych wartości przydziałów do pliku, a następnie zaimportowanie ich do innego woluminu.
- Zarządzanie serwerem sieci Web.
 - » Zadanie kontrolne 1: Skonfigurowanie drugiego adresu IP karty sieciowej (Ethernet) w systemie Windows Server 2003, na którym zainstalowany jest program Internetowe usługi informacyjne — IIS (Internet Information Services). Skonfigurowanie jednej witryny sieci Web tak, aby odpowiadała na żądania HTTP pojawiające się na pierwszym adresie IP, a drugiej witryny, aby odpowiadała na żądania pojawiające się na drugim adresie IP.
 - » Zadanie kontrolne 2: Skonfigurowanie witryny sieci tak, aby jedynie komputery o określonych adresach IP mogły uzyskiwać dostęp do tej witryny sieci Web. Sprawdzenie, czy zabezpieczenia funkcjonują prawidłowo poprzez wykonanie próby dostępu z adresu dopuszczonego oraz z adresu zabronionego.
 - » Zadanie kontrolne 3: Skonfigurowanie dwóch witryn sieci Web do działania poza pojedynczym adresem IP, skierowanie do danych za pomocą nazw nagłówka hosta (Host Header).

Lektura uzupełniająca

Przed przystąpieniem do egzaminu należy przestudiować przedstawione poniżej dodatkowe źródła informacji.

Zadanie 4.1

Rozdział 12 „Monitorowanie systemu Microsoft Windows Server 2003” omawia wykorzystanie programu Event Viewer (Podgląd zdarzeń).

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Podgląd zdarzeń”.

Zadanie 4.2

Rozdział 9 „Obsługa systemu operacyjnego” omawia wykorzystanie usługi SUS (Software Update Services) oraz sposoby instalowania pakietów serwisowych.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Instalowanie aktualizacji oprogramowania”.

Zadanie 4.3

W rozdziale 9 „Obsługa systemu operacyjnego” została omówiona administracja licencjonowania oprogramowania.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Licencjonowanie”.

Zadanie 4.4

W rozdziale 7 „Administracja systemu Microsoft Windows Server 2003” zostały przedstawione informacje dotyczące zdalnego zarządzania serwerami przy użyciu konsoli MMC, administracji zdalnej przy użyciu programu Remote Desktop for Administration (Pulpit zdalny dla administracji) oraz przy użyciu programu Remote Assistance (Pomoc zdalna).

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Usługi terminalowe”, „Narzędzia HTML dla administracji zdalnej” oraz „Pomoc zdalna”.

Zadanie 4.5

W rozdziale 8 „Drukarki” zostały przedstawione informacje dotyczące obsługi, monitorowania oraz rozwiązywania problemów związanych z drukarkami.

Zadanie 4.6

Rozdział 12 „Monitorowanie systemu Microsoft Windows Server 2003” omawia wykorzystanie programu Event Viewer (Podgląd zdarzeń).

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Podgląd zdarzeń”.

Zadanie 4.7

Rozdział 12 „Monitorowanie systemu Microsoft Windows Server 2003” omawia wykorzystanie programu System Monitor (Monitor systemu).

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Wydajność”.

Zadanie 4.8

W rozdziale 8 „Drukarki” zostały przedstawione informacje dotyczące zaawansowanego konfigurowania i zarządzania drukarkami.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Drukarki udostępnione”.

Zadanie 4.9

Rozdział 6 „Liki i foldery” omawia administrację programu IIS.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej), temat: „Internetowe usługi informacyjne”.

Zadanie 4.1

Monitorowanie i analiza zdarzeń

Dziennik zdarzeń może zostać skonfigurowany tak, aby rejestrowane były ogromne ilości informacji dotyczących systemu i dlatego istotna staje się umiejętność odpowiedniego filtrowania wyświetlanych informacji, aby pokazywane były tylko te dane, które są użytkownikowi potrzebne.

Zdarzenia dziennika można filtrować stosując kilka metod. Pierwszy sposób polega na określeniu typu zdarzenia. Typem zdarzenia może być Informacja, Ostrzeżenie, Błąd, Inspekcja zdarzeń zakończonych powodzeniem lub niepowodzeniem. Innym sposobem filtrowania jest określenie źródła zdarzenia, które wygenerowało wpis dziennika, czyli może to być sam system Windows Server 2003 lub jego usługa. Zdarzenia grupowane są według kategorii określających, który podsystem wygenerował zdarzenie. Zdarzenia mogą być również filtrowane według identyfikatora zdarzenia (Evtnt. ID), nazwy użytkownika, nazwy komputera, a ich lista może być zawężana do określonego przedziału czasu. Umiejętne filtrowanie zdarzeń dziennika umożliwia administratorowi przegląd tylko tych zdarzeń, które mają znaczenie dla analizowanego problemu.

Pytania do zadania 4.1

1. Administrator chce przeglądać zdarzenia związane wyłącznie z komunikatami informacyjnymi i ostrzeżeniami w dzienniku Application (Aplikacja) wygenerowanymi przez moduł przydziału dysku. Które z wymienionych poniżej czynności należy wykonać, aby zrealizować to zadanie?
 - A. W programie Event Viewer (Podgląd zdarzeń) należy przeprowadzić edycję dziennika System. Na zakładce Filter (Filtr) należy upewnić się, że zaznaczone są pola wyboru Information (Informacje) oraz Warning (Ostrzeżenie), a usunięte są zaznaczenia pól wyboru odnoszących się do opcji Error (Błąd), Success Audit (Inspekcja sukcesów) oraz Failure Audit (Inspekcja niepowodzeń).
 - II. W programie Event Viewer (Podgląd zdarzeń) należy przeprowadzić edycję dziennika Application (Aplikacja). Na zakładce Filter (Filtr) należy upewnić się, że zaznaczone są pola wyboru Information (Informacje) oraz Warning (Ostrzeżenie), a usunięte są zaznaczenia pól wyboru odnoszących się do opcji Error (Błąd), Success Audit (Inspekcja sukcesów) oraz Failure Audit (Inspekcja niepowodzeń).
 - C. W programie Event Viewer (Podgląd zdarzeń) należy przeprowadzić edycję dziennika Application (Aplikacja). Na zakładce Filter (Filtr) należy upewnić się, że nie są zaznaczone pola wyboru Information (Informacje) oraz Warning (Ostrzeżenie), natomiast są zaznaczone pola wyboru odnoszące się do opcji Error (Błąd), Success Audit (Inspekcja sukcesów) oraz Failure Audit (Inspekcja niepowodzeń). Oprócz tego należy określić, że źródłem zdarzeń jest moduł Disk Quota (Przydział dysku).
 - D. W programie Event Viewer (Podgląd zdarzeń) należy przeprowadzić edycję dziennika Application (Aplikacja). Na zakładce Filter (Filtr) należy upewnić się, że zaznaczone są pola wyboru Information (Informacje) oraz Warning (Ostrzeżenie), natomiast nie są zaznaczone pola wyboru odnoszące się do opcji Error (Błąd), Success Audit (Inspekcja sukcesów) oraz Failure Audit (Inspekcja niepowodzeń). Oprócz tego należy określić, że źródłem zdarzeń jest program Chkdsk.

- E. W programie Event Viewer (Podgląd zdarzeń) należy przeprowadzić edycję dziennika Application (Aplikacja). Na zakładce Filter (Filtr) należy upewnić się, że zaznaczone są pola wyboru Information (Informacje) oraz Warning (Ostrzeżenie), natomiast nie są zaznaczone pola wyboru odnoszące się do opcji Error (Błąd), Success Audit (Inspekcja sukcesów) oraz Failure Audit (Inspekcja niepowodzeń). Oprócz tego należy określić, że źródłem zdarzeń jest program Disk Quota.
- F. W programie Event Viewer (Podgląd zdarzeń) należy przeprowadzić edycję dziennika System. Na zakładce Filter (Filtr) należy upewnić się, że zaznaczone są pola wyboru Information (Informacje) oraz Warning (Ostrzeżenie), natomiast nie są zaznaczone pola wyboru odnoszące się do opcji Error (Błąd), Success Audit (Inspekcja sukcesów) oraz Failure Audit (Inspekcja niepowodzeń). Oprócz tego należy określić, że źródłem zdarzeń jest program Disk Quota.
- 2.. Rooslan opiekuje się systemem Windows Server 2003, który pracuje niestabilnie. Ustawienia dla dziennika System określają, że jego maksymalny rozmiar to 50 MB, a w razie potrzeby starsze zdarzenia będą zastępowane nowymi. Rooslan chce przejrzeć zdarzenia związane z błędami zarejestrowane w dzienniku System, które miały miejsce w ostatnim tygodniu. W jaki sposób Rooslan może zrealizować to zadanie?
- A. Rooslan powinien uruchomić program Event Viewer Wizard (Kreator podglądu zdarzeń) i zaznaczyć pole wyboru Display Errors (Wyświetlaj błędy). Poza tym powinien określić daty wyświetlania tak, aby odnosiły się do ostatnich siedmiu dni.
- B. W programie Event Viewer (Podgląd zdarzeń) Rooslan powinien przeprowadzić edycję właściwości dziennika System. Na zakładce Filter (Filtr) powinien upewnić się, że zaznaczone jest jedynie pole wyboru odnoszące się do opcji Error (Błąd).
- C. W programie Event Viewer (Podgląd zdarzeń) Rooslan powinien przeprowadzić edycję właściwości dziennika Application (Aplikacja). Na zakładce Filter (Filtr) powinien upewnić się, że zaznaczone jest jedynie pole wyboru odnoszące się do opcji Error (Błąd) oraz że data pierwszego zdarzenia określona jest na siedem dni przed datą bieżącą. Data bieżąca wyznacza datę ostatniego zdarzenia.
- D. W programie Event Viewer (Podgląd zdarzeń) Rooslan powinien przeprowadzić edycję właściwości dziennika System. Na zakładce Filter (Filtr) powinien upewnić się, że zaznaczone jest jedynie pole wyboru odnoszące się do opcji Error (Błąd) oraz że data pierwszego zdarzenia określona jest na siedem dni przed datą bieżącą. Data bieżąca wyznacza datę ostatniego zdarzenia.
- E. W programie Event Viewer (Podgląd zdarzeń) Rooslan powinien przeprowadzić edycję właściwości dziennika System. Na zakładce Filter (Filtr) powinien upewnić się, że zaznaczone jest jedynie pole wyboru odnoszące się do opcji Information (Informacje) oraz że data pierwszego zdarzenia określona jest na siedem dni przed datą bieżącą. Data bieżąca wyznacza datę ostatniego zdarzenia.
- ó. Dyrektor polecił Rooslanowi, aby wygenerował raport dotyczący aktywności logowania się w systemie użytkownika Agim w ciągu ostatnich dwóch miesięcy. Dyrektor chce ustalić na podstawie zarejestrowanych zdarzeń logowania, w których dniach użytkownik Agim przychodził do pracy, ponieważ jego obecność w firmie stała się przypadkowa. Zdarzenia logowania były poddane inspekcji w domenie systemu Windows Server 2003 w ciągu ostatnich sześciu miesięcy. Rozmiary wszystkich plików dzienników zdarzeń zostały ograniczone do wartości 190,240 KB. Wszystkie zdarzenia ostatnich sześciu miesięcy są dostępne, ponieważ żaden dziennik jeszcze się nie zappełnił. Która z wymienionych poniżej metod jest najlepszym sposobem zrealizowania zadania powierzonego Rooslanowi?

- A. W dzienniku System należy utworzyć filtr. Powinny być wyszukiwane jedynie inspekcje sukcesów, a źródłem zdarzeń powinny być zabezpieczenia (Security). Datę pierwszego zdarzenia należy określić na dwa miesiące przed datą bieżącą. Data bieżąca wyznacza datę ostatniego zdarzenia.
- B. W dzienniku System należy utworzyć filtr. Powinny być wyszukiwane jedynie inspekcje sukcesów, a źródłem zdarzeń powinny być zabezpieczenia (Security). Ustawienia dotyczące pola User (Użytkownik) powinny być określone przez nazwę konta użytkownika: Agim. Datę pierwszego zdarzenia należy określić na dwa miesiące przed datą bieżącą. Data bieżąca wyznacza datę ostatniego zdarzenia.
- C. W dzienniku System należy utworzyć filtr. Powinny być wyszukiwane jedynie inspekcje sukcesów, a źródłem zdarzeń powinien być menedżer zabezpieczeń kont (Security Account Manager). Ustawienia dotyczące pola User (Użytkownik) powinny być określone przez nazwę konta użytkownika: Agim. Identyfikator zdarzenia (Event ID) powinien zostać określony przez wartość 538. Datę pierwszego zdarzenia należy określić na dwa miesiące przed datą bieżącą. Data bieżąca wyznacza datę ostatniego zdarzenia.
- D. W dzienniku Security (Zabezpieczenia) należy utworzyć filtr. Powinny być wyszukiwane jedynie inspekcje sukcesów, a źródłem zdarzeń powinny być zabezpieczenia (Security). Datę pierwszego zdarzenia należy określić na dwa miesiące przed datą bieżącą. Data bieżąca wyznacza datę ostatniego zdarzenia. Identyfikator zdarzenia (Event ID) powinien zostać określony przez wartość 538.
- E. W dzienniku Security (Zabezpieczenia) należy utworzyć filtr. Powinny być wyszukiwane jedynie inspekcje sukcesów, a źródłem zdarzeń powinien być menedżer zabezpieczeń kont (Security Account Manager). Ustawienia dotyczące pola User (Użytkownik) powinny być określone przez nazwę konta użytkownika: Agim. Identyfikator zdarzenia (Event ID) powinien zostać określony przez wartość 538. Datę pierwszego zdarzenia należy określić na dwa miesiące przed datą bieżącą. Data bieżąca wyznacza datę ostatniego zdarzenia.
- F. W dzienniku Security (Zabezpieczenia) należy utworzyć (i.e.). Powinny być wyszukiwane jedynie inspekcje sukcesów, a źródłem zdarzeń powinny być zabezpieczenia (Security). Ustawienia dotyczące pola User (Użytkownik) powinny być określone przez nazwę konta użytkownika: Agim. Identyfikator zdarzenia (Event ID) powinien zostać określony przez wartość 538. Datę pierwszego zdarzenia należy określić na dwa miesiące przed datą bieżącą. Data bieżąca wyznacza datę ostatniego zdarzenia.

4* Użytkownik Lee obawia się, że inna osoba w biurze próbuje zalogować się na jego stacji roboczej za pomocą jego konta.

Lee nie ma pewności, że takie zdarzenia miały miejsce, ale chce przejrzeć raport informujący ile razy w ciągu ostatniego miesiąca zarejestrowane zostały zdarzenia związane z niepowodzeniem logowania przy użyciu jego konta. W celu sprawdzenia swojej hipotezy Lee umieścił przy monitorze notatkę „Password » Gillian1948”. „Gillian1948” nie jest jego hasłem. Lee założył, że jeśli ktokolwiek próbuje zalogować się nielegalnie na jego komputerze, sprawdzi pozostawione na widoku hasło. Jedynie dla zdarzeń logowania w domenie określona została inspekcja zarówno sukcesów, jak i niepowodzeń. W jaki sposób wygenerować raport w programie Event Viewer (Podgląd zdarzeń), aby określić, czy miały miejsce nieudane próby logowania przy użyciu konta użytkownika Lee?

- A. Należy utworzyć filtr w dzienniku System. Wyszukiwane powinny być jedynie zdarzenia związane z inspekcją niepowodzeń, a źródłem zdarzeń powinny być zabezpieczenia (Security). Ustawienia dotyczące pola User (Użytkownik) powinny być określone przez nazwę konta użytkownika: Lee. Datę pierwszego zdarzenia należy określić na miesiąc przed datą bieżącą. Data bieżąca wyznacza datę ostatniego zdarzenia.
- B. Należy utworzyć filtr w dzienniku System. Wyszukiwane powinny być jedynie zdarzenia związane z inspekcją sukcesów, a źródłem zdarzeń powinny być zabezpieczenia (Security). Ustawienia

dotyczące pola User (Użytkownik) powinny być określone przez nazwę konta użytkownika: Lee. Datę pierwszego zdarzenia należy określić na miesiąc przed datą bieżącą. Data bieżąca wyznacza datę ostatniego zdarzenia.

- C. Należy utworzyć filtr w dzienniku System. Wyszukiwane powinny być jedynie zdarzenia związane z inspekcją sukcesów, a źródłem zdarzeń powinien być menedżer zabezpieczeń kont (Security Account Manager). Ustawienia dotyczące pola User (Użytkownik) powinny być określone przez nazwę konta użytkownika: Lee. Datę pierwszego zdarzenia należy określić na miesiąc przed datą bieżącą. Data bieżąca wyznacza datę ostatniego zdarzenia.
- D. Należy utworzyć filtr w dzienniku Security (Zabezpieczenia). Wyszukiwane powinny być jedynie zdarzenia /wiązane z inspekcją, sukcesów, a źródłem zdarzeń powinien być menedżer zabezpieczeń kont (Security Account Manager). Ustawienia dotyczące pola User (Użytkownik) powinny być określone przez nazwę konta użytkownika: Lec. Datę pierwszego zdarzenia należy określić na miesiąc przed datą bieżącą. Data bieżąca wyznacza datę ostatniego zdarzenia.
- E. Należy utworzyć filtr w dzienniku Security (Zabezpieczenia). Wyszukiwane powinny być jedynie zdarzenia związane z inspekcją niepowodzeń, a źródłem zdarzeń powinny być zabezpieczenia (Security). Ustawienia dotyczące pola User (Użytkownik) powinny być określone przez nazwę konta użytkownika: Lee. Datę pierwszego zdarzenia należy określić na miesiąc przed datą bieżącą. Data bieżąca wyznacza datę ostatniego zdarzenia.

Odpowiedzi do zadania 4.1

X. Prawidłowa odpowiedź: I'

- A. Nieprawidłowo Działanie takie wyświetli wszystkie /darzenia związane z komunikatami informacyjnymi i ostrzeżeniami zarejestrowanymi w dzienniku System, a nie w dzienniku Application (Aplikacja).
- B. Nieprawidłowo Działanie takie wyświetli wszystkie /darzenia związane z komunikatami informacyjnymi i ostrzeżeniami zarejestrowanymi w dzienniku Application (Aplikacja), a niewyłącznie zdarzenia wygenerowane przez moduł przydziału dysku.
- C. Nieprawidłowo Działanie takie wyświetli zdarzenia związane z błędami, inspekcją sukcesów i niepowodzeń, nie wyświetli natomiast zdarzeń związanych z komunikatami informacyjnymi i ostrzeżeniami, co było celem zadania.
- D. Nieprawidłowo Działanie takie wyświetli wszystkie zdarzenia związane z komunikatami informacyjnymi i ostrzeżeniami, których źródłem jest program Chckdisk, a nie moduł Disk Quota (Przydział dysku).
- E. Prawidłowo Ustawienia takie spowodują wygenerowanie prawidłowego raportu.
- F. Nieprawidłowo Działanie takie będzie dotyczyło dziennika System, a nie dziennika Application (Aplikacja), co było wymogiem podanym w pytaniu.

2-. Prawidłowa odpowiedź: D

- A. Nieprawidłowo Nie istnieje program Eveni Viewer Wizard (Kreator podglądu zdarzeń).
- B. Nieprawidłowo Działanie takie nie ograniczy raportu zdarzeń do okresu ostatniego tygodnia.
- C. Nieprawidłowo Zadanie dotyczyło dziennika System, a nie dziennika Application (Aplikacje).

D. Prawidłowo Działanie tego filtra spowoduje wyświetlenie zdarzeń odnoszących się do zarejestrowanych błędów, które wystąpiły w okresie ostatnich siedmiu **dni**.

E. Nieprawidłowo Działanie tego filtra spowoduje wyświetlenie zdarzeń odnoszących się do zarejestrowanych komunikatów informacyjnych, które wystąpiły w okresie ostatnich siedmiu dni, a nie do zdarzeń dotyczących błędów.

«J. **Prawidłowa odpowiedź: F**

A. Nieprawidłowo Należy analizować dziennik Security (Zabezpieczenia), a nie dziennik System.

B. Nieprawidłowo Należy analizować dziennik Security (Zabezpieczenia), a nie dziennik System.

C. Nieprawidłowo Należy analizować dziennik Security (Zabezpieczenia), a nie dziennik System.

D. Nieprawidłowo Raport ten będzie dotyczył zdarzeń logowania wszystkich użytkowników w okresie ostatnich dwóch miesięcy.

E. Nieprawidłowo Jako źródło zdarzeń powinna zostać wybrana opcja Security, a nie opcja Security Account Manager. Opcja dotycząca menedżera zabezpieczeń koni (Security Account Manager) jest używana dla zdarzeń związanych z zarządzaniem kontami, takich jak dodanie użytkownika czy zmiana hasła.

K. Prawidłowo Działanie takie wygeneruje prawidłowy raport. Pomimo że wszystkie identyfikatory zdarzeń wymienione w pytaniu określone są przez 538, to 538 jest identyfikatorem zdarzenia logowania. Jeśli pole User (Użytkownik) nie będzie określone przez nazwę konta użytkownika Agim, wyświetlone zostaną zdarzenia logowania dotyczące wszystkich użytkowników. Ustawienia prawidłowo wyznaczają daty, zawężając raport do wymaganego w pytaniu okresu.

nK **Prawidłowa odpowiedź: E**

A. Nieprawidłowo Należy analizować dziennik Security (Zabezpieczenia), a nie dziennik System.

B. Nieprawidłowo Należy analizować dziennik Security (Zabezpieczenia), a nie dziennik System.

C. Nieprawidłowo Należy analizować dziennik Security (Zabezpieczenia), a nie dziennik System.

D. Nieprawidłowo Źródłem zdarzeń powinny być zabezpieczenia (Security), a inspekcja powinna dotyczyć niepowodzeń.

E. Prawidłowo Ponieważ jedynie inspekcja zdarzeń logowania odnosi się zarówno do zdarzeń związanych z niepowodzeniem, jak i z udanymi próbami, a filtr dotyczy tylko nieudanych prób logowania za pomocą konta użytkownika Lee w okresie ostatniego miesiąca, to opisana metoda wygeneruje prawidłowy raport.

Zadanie 4.2

Zarządzanie infrastrukturą aktualizacji oprogramowania

Usługa SUS (Software Update Services) jest rozszerzeniem systemu Windows Server 2003, które nie jest instalowane w oparciu o nośnik instalacyjny systemu, lecz poprzez pobranie plików instalacyjnych z witryny sieci Web firmy Microsoft. Usługi SUS umożliwiają administratorom zbudowanie zatwierdzonej listy aktualizacji, która następnie służy do instalowania aktualizacji w całym przedsiębiorstwie.

Działanie usługi SUS można podzielić na dwie części. Pierwsza to serwer SUS, który przechowuje listę zatwierdzonych aktualizacji. Serwer usługi SUS może być również wykorzystywany do przechowywania aktualizacji, dzięki czemu klient usługi nie musi kłopotać się pobieraniem zatwierdzonych aktualizacji z serwerów usługi Windows Update firmy Microsoft. Druga część to klient, który musi być skonfigurowany tak, aby wykorzystywał serwet usługi SUS, a nie serwer programu Windows Update. Konfigurację taką można uzyskać jedynie poprzez zmianę ustawień zasady grupy, nie można w tym celu natomiast skorzystać z zakładki Automatyzacja aktualizacji (Automatyczne aktualizacje) konsoli System znajdującej się w grupie programów Control Panel (Panel sterowania). Konfiguracja realizowana jest za pomocą lokalnego obiektu (Group Policy Object), jak również za pomocą zasad stosowanych do lokalacji, domen oraz jednostek organizacyjnych.

Niektóre aktualizacje, takie jak dodatek Service Pack, mogą być również instalowane z pominięciem usługi SUS, po prostu przy użyciu ustawień instalacji oprogramowania zasady grupy. Odpowiedni obszar zasady grupy dotyczący tej instalacji znajduje się w węźle Computer Configuration\Software Settings (Konfiguracja komputera\Ustawienia oprogramowania). Pakiet serwisowy powinien być rozpakowany do postaci plików umieszczonych w udostępnionym folderze sieciowym, aby był dostępny dla wszystkich klientów sieci. W niektórych przypadkach, dla łączności sieciowej WAN o niskiej przepustowości, administratorzy mogą umieszczać folder udostępniony zawierający rozpakowane pakiety serwisowe na komputerach w każdej lokalizacji, a następnie wykorzystywać obiekty (GPO), które wskazują na te komputery. Dzięki temu pliki pakietu serwisowego będą pobierane z komputera danej lokalizacji, a nie z serwera w lokalizacji centralnej.

Pytania do zadania 4.2

1. Administrator sieci przedsiębiorstwa średniej wielkości ma zamiar za pomocą usługi SUS (Software Update Services) zarządzać aktualizacjami dostarczanych przez firmę Microsoft dla stacji systemu Windows XP Professional. W przedsiębiorstwie używany jest serwer proxy uruchomiony na innej platformie, który wymaga uwierzytelnienia bazującego na nazwie i hasle użytkownika. Baza danych użytkowników i haseł serwera proxy jest inna niż baza danych używana w domenie systemu Windows Server 2003. Uwzględniając opisaną sytuację, które z podanych opcji są dostępne podczas konfigurowania infrastruktury aktualizacji oprogramowania?

- A. Ponieważ usługa SUS nie może być skonfigurowana tak, aby przeprowadzała uwierzytelnienie wymagane przez serwer proxy, wszystkie aktualizacje muszą być przez administratora pobierane i umieszczane ręcznie na serwerze SUS. Stacje systemu Windows XP Professional powinny być skonfigurowane za pomocą zasady grupy tak, aby w celu pobierania aktualizacji łączyły się z serwerem SUS.
- B. Ponieważ usługa SUS nie może być skonfigurowana tak, aby przeprowadzała uwierzytelnienie wymagane przez serwer proxy, natomiast klient systemu Windows XP może realizować takie uwierzytelnienie, to klient systemu Windows XP w celu pobrania aktualizacji powinien łączyć się z firmą Microsoft.
- C. Usługa SUS może być skonfigurowana tak, aby przeprowadzała uwierzytelnienie wymagane przez serwer proxy i pobierała zatwierdzone przez administratora aktualizacje. Systemy Windows XP powinny być skonfigurowane tak, aby sprawdzały serwer SUS celem wyszukania listy zatwierdzonych aktualizacji, a następnie powinny automatycznie pobierać te aktualizacje z witryny sieci Web firmy Microsoft.
- D. Usługa SUS może być skonfigurowana tak, aby przeprowadzała uwierzytelnienie wymagane przez serwer proxy i pobierała zatwierdzone przez administratora aktualizacje. Systemy Windows XP powinny być skonfigurowane tak, aby sprawdzały serwer SUS celem wyszukania listy zatwierdzonych aktualizacji, a następnie powinny automatycznie pobierać te aktualizacje z serwera usługi SUS.

2.

Administrator sieci przedsiębiorstwa średniej wielkości ma zamiar wprowadzić w firmie usługę SUS dla wszystkich stacji roboczych Windows XP Professional oraz dla systemów Windows Server 2003. W celu wykonania leśiów zostało wybranych 10 stacji roboczych systemu Windows XP Professional, serwer członkowski systemu Windows Server 2003, na którym uruchomiona została usługa SUS, kontroler domeny systemu Windows Server 2003 oraz autonomiczny system Windows Server 2003. Z wyjątkiem serwera SUS, administrator chce, aby wszystkie systemy automatycznie sprawdzały, pobierały i instalowały aktualizacje codziennie o 7:00. Które z wymienionych poniżej czynności powinien wykonać administrator, aby zrealizować zadanie? (wybierz wszystkie właściwe odpowiedzi)

- A. Na każdej stacji roboczej systemu Windows XP Professional, za pomocą zakładki Automatic Updates (Aktualizacje automatyczne) w konsoli System umieszczonej w grupie programów Control Panel (Panel sterowania) należy zdefiniować serwer aktualizacji tak, aby ustawienia wskazywały na serwer SUS. Należy określić, aby codziennie o godzinie 7:00 stacje robocze Windows XP automatycznie pobierały i instalowały aktualizacje.
- B. Na każdym komputerze systemu Windows Server 2003 (za wyjątkiem serwera SUS), za pomocą zakładki Automatic Updates (Aktualizacje automatyczne) w konsoli System umieszczonej w grupie programów Control Panel (Panel sterowania) należy zdefiniować serwer aktualizacji tak, aby ustawienia wskazywały na serwer SUS. Należy określić, aby codziennie o godzinie 7:00 serwery te automatycznie pobierały i instalowały aktualizacje.
- C. Należy umieścić stacje robocze systemu Windows XP Professional i kontroler domeny systemu Windows Server 2003 w odrębnej jednostce organizacyjnej nazwanej Uptest. Następnie należy przeprowadzić edycję obiektów GPO właściwości aktualizacji (Windows Update) dla jednostki organizacyjnej Uptest wskazując jako serwer aktualizacji adres serwera usługi SUS. Ustawienie to znajduje się w zasadzie Intranet Microsoft Update Service Location (Określ lokalizację intranetową usługi aktualizującej firmy Microsoft). Zasada Configure Automatic Updates (Konfiguracja aktualizacji automatycznych) powinna być tak skonfigurowana, aby automatyczne pobieranie

i instalowanie aktualizacji było przeprowadzane codziennie o godzinie 7:00. Ten obiekt GPO należy powiązać z jednostką organizacyjną Uptest.

- D. Dla autonomicznego systemu Windows Server 2003 należy przeprowadzić edycję właściwości lokalnego obiektu GPO dotyczącego aktualizacji systemu Windows (Windows Update) wskazując jako serwer aktualizacji adres serwera usługi SUS. Ustawienie to znajduje się w zasadzie Intranet Microsoft Update Service Location (Określ lokalizację intranetową usługi aktualizującej firmy Microsoft). Zasada Configure Automatic Updates (Konfiguracja aktualizacji automatycznych) powinna być tak skonfigurowana, aby automatyczne pobieranie i instalowanie aktualizacji było przeprowadzane codziennie o godzinie 7:00.
- E. Dla serwera SUS należy przeprowadzić edycję właściwości lokalnego obiektu GPO dotyczącego aktualizacji systemu Windows (Windows Update), wskazując jako serwer aktualizacji adres serwera usługi SUS. Ustawienie to znajduje się w zasadzie Intranet Microsoft Update Service Location (Określ lokalizację intranetową usługi aktualizującej firmy Microsoft). Zasada Configure Automatic Updates (Konfiguracja aktualizacji automatycznych) powinna być tak skonfigurowana, aby automatyczne pobieranie i instalowanie aktualizacji było przeprowadzane codziennie o godzinie 7:00.

Rooslan pracuje w przedsiębiorstwie, którego pojedyncze biuro oddalone połączone jest z centralą poprzez łącze ISDN BRI (Integrated Services Digital Network Basic Rate Interface). Lokacja zdalna korzysta z łącza do Internetu o przepustowości 10 Mb. Centrala posiada łącze do sieci Internet o przepustowości 20 Mb. Łącze ISDN BRI najczęściej obsługuje macierze związane z replikacją usługi Active Directory i rozproszonego systemu plików (DFS). Przedsiębiorstwo zorganizowane jest w postaci pojedynczej domeny systemu Windows Server 2003. Ze względu na replikację centrala i biuro zdalne zostały skonfigurowane jako odrębne lokacje usługi Active Directory. W firmie są dwa systemy Windows Server 2003, na których została uruchomiona usługa SUS. Serwer znajdujący się w centrali przechowuje listę zatwierdzonych aktualizacji, jak również przechowywane są na nim lokalnie pliki aktualizacji. Drugi serwer SUS został umieszczony w lokacji zdalnej.

Cel główny:

Rooslan chce zapewnić, że stacje robocze Windows XP Professional oraz systemy Windows Server 2003 będą pobierały jedynie aktualizacje wymienione na liście aktualizacji zatwierdzonych przechowywanych na serwerze SUS. Cel pomocniczy:

Rooslan chce zapewnić, aby łącze ISDN BRI nie zostało przeciążone ruchem związanym z transferami aktualizacji z serwera SUS umieszczonego w centrali.

Cel trzeciordny:

Należy zminimalizować ilość aktualizacji pobieranych do centrali poprzez łącze o przepustowości 20 Mb. Które z wymienionych poniżej metod pozwolą Rooslanowi zrealizować poszczególne cele? (wybierz wszystkie właściwe odpowiedzi - połączenie prawidłowo wybranych odpowiedzi stanowi właściwe rozwiązanie)

- A. Rooslan powinien przeprowadzić edycję obiektu GPO i skonfigurować właściwości dotyczące aktualizacji (Windows Update). Ustawienia zasady Specify Intranet Microsoft Update Service Location (Określ lokalizację intranetową usługi aktualizującej firmy Microsoft) powinny określać drugi serwer SUS jako źródło wykrywania aktualizacji i statystyk. Ta zasada grupy powinna być zastosowana do lokacji zdalnej.

- ' B. Należy skonfigurować drugi serwer SUS tak, aby uzyskiwał listę zatwierdzonych aktualizacji z pierwszego serwera SUS. Poza tym, należy skonfigurować drugi serwer SUS tak, aby obsługiwał pliki aktualizacji serwera programu Windows Update firmy Microsoft.
- C. Należy skonfigurować pierwszy serwer SUS tak, aby przechowywał listę zatwierdzonych aktualizacji oraz aby pobierał i przechowywał pliki aktualizacji.
- D. Rooslan powinien przeprowadzić edycję obiektu GPO i skonfigurować właściwości dotyczące aktualizacji (Windows Update). Ustawienia zasady Specyficznego Intranetu Microsoft Update Service Location (Określ lokalizację intranetową usługi aktualizującej firmy Microsoft) powinny określać pierwszy serwer SUS jako źródło wykrywania aktualizacji i statystyk. Ta zasada grupy powinna być zastosowana do lokalizacji centrali.
- E. Rooslan powinien przeprowadzić edycję obiektu GPO i skonfigurować właściwości dotyczące aktualizacji (Windows Update). Ustawienia zasady Specyficznego Intranetu Microsoft Update Service Location (Określ lokalizację intranetową usługi aktualizującej firmy Microsoft) powinny określać pierwszy serwer SUS jako źródło wykrywania aktualizacji i statystyk. Ta zasada grupy powinna być zastosowana do lokalizacji zdalnej.
- F. Rooslan powinien przeprowadzić edycję obiektu GPO i skonfigurować właściwości dotyczące aktualizacji (Windows Update). Ustawienia zasady Specyficznego Intranetu Microsoft Update Service Location (Określ lokalizację intranetową usługi aktualizującej firmy Microsoft) powinny określać drugi serwer SUS jako źródło wykrywania aktualizacji i statystyk. Ta zasada grupy powinna być zastosowana do lokalizacji centrali.
4. Mick jest administratorem sieci przedsiębiorstwa, które posiada pięć biur rozmieszczonych w jednym mieście. Tylko biuro centrali ma łącze do sieci Internet oraz utrzymuje serwer proxy. W centrali rozmieszczonych jest 200 stacji roboczych Windows XP Professional oraz kilka systemów Windows Server 2003. Każde z pięciu biur oddziałowych ma 150 stacji roboczych Windows XP Professional i kilka systemów Windows Server 2003. Oddziały połączone są do centrali poprzez łącze ISDN BRI. Obecnie żaden z systemów Windows nie pobiera aktualizacji z serwera programu Windows Update firmy Microsoft, ponieważ systemy te nie potrafią przeprowadzić uwierzytelnienia wymaganego przez serwer proxy. Dyrektor poprosił Micka, aby w przedsiębiorstwie zainstalował usługę SUS, dzięki czemu zatwierdzone aktualizacje będą instalowane na stacjach roboczych i serwerach oraz, aby Mick zminimalizował ruch związany z aktualizacjami przesyłanymi poprzez łącza ISDN BRI. Która z wymienionych poniżej metod zrealizuje postawione zadania?
- A. W lokalizacji biura centrali należy skonfigurować serwer SUS tak, aby obsługiwał listę aktualizacji zatwierdzonych oraz aby przechowywał aktualizacje pobrane z serwerów programu Windows Update firmy Microsoft. Następnie należy skonfigurować zasadę grupy, która nakaze klientom korzystać z serwera SUS jako serwera aktualizacji. Ten obiekt GPO powinien być zastosowany do centrali oraz do lokalizacji oddziałów.
- B. W lokalizacji biura centrali należy skonfigurować serwer SUS tak, aby obsługiwał listę aktualizacji zatwierdzonych, ale by aktualizacje te były przechowywane na serwerach Windows Update firmy Microsoft. Następnie należy skonfigurować zasadę grupy, która nakaze klientom korzystać z serwera SUS jako serwera aktualizacji. Ten obiekt GPO powinien być zastosowany do centrali oraz do lokalizacji oddziałów.
- C. W lokalizacji biura centrali należy skonfigurować serwer SUS tak, aby obsługiwał listę aktualizacji zatwierdzonych oraz aby obsługiwał aktualizacje przy użyciu serwerów programu Windows Update firmy Microsoft. W każdej lokalizacji biura oddziału należy skonfigurować serwer SUS tak, aby

obsługiwał listę aktualizacji zatwierdzonych oraz aby obsługiwał aktualizacje przy użyciu serwerów programu Windows. Następnie należy utworzyć obiekt GPO i zastosować go do każdej lokacji. Obiekt GPO powinien określać taką zasadę grupy, która nakaże klientom korzystać z lokalnego serwera SUS jako serwera aktualizacji.

- D. W lokalizacji biura centrali należy skonfigurować serwer SUS tak, aby obsługiwał listę aktualizacji zatwierdzonych oraz aby przechowywał aktualizacje pobrane z serwerów programu Windows Update firmy Microsoft. Każdy serwer SUS w lokacjach oddziałowych należy skonfigurować tak, aby synchronizował się z serwerem SUS w centrali. Następnie należy skonfigurować taką zasadę grupy, która nakaże klientom korzystać z serwera SUS centrali jako serwera aktualizacji. Ten obiekt GPO powinien być zastosowany do centrali oraz do lokacji oddziałów.
- E. W lokalizacji biura centrali należy skonfigurować serwer SUS tak, aby obsługiwał listę aktualizacji zatwierdzonych oraz aby przechowywał aktualizacje pobrane z serwerów programu Windows Update firmy Microsoft. Każdy serwer SUS w lokacjach oddziałowych należy skonfigurować tak, aby synchronizował się z serwerem SUS w centrali. Następnie należy utworzyć obiekt GPO i zastosować go do każdej lokacji. Obiekt GPO powinien zawierać taką zasadę grupy, która nakaże klientom korzystać z lokalnego serwera SUS jako serwera aktualizacji.

5.

Orin jest administratorem systemu wydziału lokalnego uniwersytetu. Na wydziale zainstalowanych jest 40 stacji roboczych Windows XP Professional oraz dwa systemy Windows Server 2003. Jeden z tych serwerów jest kontrolerem domeny, a drugi serwerem plików i druku. Wszystkie komputery wydziału należą do pojedynczej domeny systemu Windows Server 2003. Firma Microsoft niedawno udostępniła pakiet serwisowy dla systemu Windows XP i po jego przetestowaniu Orin bez obaw postanowił zainstalować pakiet serwisowy na Stacjach roboczych wydziału. Orin rozpakował na serwerze plik pakietu serwisowego w katalogu nazwanym \\Fileshare\uewsvpk. Którą z poniżej wymienionych metod może Orin wykorzystać do zainstalowania pakietu serwisowego na wszystkich stacjach roboczych systemu Windows XP Professional? (wybierz wszystkie właściwe odpowiedzi)

- A. Orin może podejść do każdej stacji roboczej Windows XP Professional i zainstalować pakiet serwisowy z pliku umieszczonego w folderze udostępnionym.
- B. Orin może utworzyć grupę nazwaną Xpwkstn i umieścić w niej wszystkie konta komputerów stacji roboczych Windows XP Professional. Następnie może utworzyć obiekt GPO, w którym określony zostanie nowy pakiet instalacyjny. Pakiet zostanie określony w węźle Computer Configuration\Software Settings (Konfiguracja komputera/Ustawienia oprogramowania) w oparciu o lokalizację pliku pakietu serwisowego .msi umieszczonego w udziale \\Fileshare\uewsvpk. W oknie dialogowym Deploy Software (Rozmieszczanie oprogramowania) Orin powinien wybrać polecenie Assign (Przypisz), a następnie powinien zastosować ten obiekt GPO do grupy Xpwkstn.
- C. Orin może utworzyć grupę nazwaną Xpusrs i umieścić w niej wszystkich użytkowników stacji roboczych Windows XP Professional. Następnie może utworzyć obiekt GPO, w którym określony zostanie nowy pakiet instalacyjny. Pakiet zostanie określony w węźle Computer Configuration\Software Settings (Konfiguracja komputera/Ustawienia oprogramowania) w oparciu o lokalizację pliku pakietu serwisowego .msi umieszczonego w udziale \\Fileshare\uewsvpk. W oknie dialogowym Deploy Software (Rozmieszczanie oprogramowania) Orin powinien wybrać polecenie Assign (Przypisz), a następnie powinien zastosować ten obiekt GPO do grupy Xpusrs.
- D. Orin może utworzyć jednostkę organizacyjną nazwaną Xpwkstn i umieścić w niej wszystkie konta komputerów stacji roboczych Windows XP Professional. Następnie może utworzyć obiekt GPO, w którym określony zostanie nowy pakiet instalacyjny. Pakiet zostanie określony w węźle Computer

Configuration\Software Settings (Konfiguracja komputera/Ustawienia oprogramowania) w oparciu o lokalizację pliku pakietu serwisowego .msi umieszczonego w udziale \\Fileshare\newsrvpk. W oknie dialogowym Deploy Software (Rozmieszczanie oprogramowania) Orin powinien wybrać polecenie Assign (Przypisz), a następnie powinien zasrosować ten obiekt GPO do jednostki organizacyjnej Xpwkstn.

Odpowiedzi do zadania 4.2

X. Prawidłowa odpowiedź: D

- A. **Nieprawidłowo** Usługa SUS może być skonfigurowana tak, aby przeprowadzała uwierzytelnienie wymagane przez serwer proxy.
- B. **Nieprawidłowo** Usługa SUS może być skonfigurowana tak, aby przeprowadzała uwierzytelnienie wymagane przez serwer proxy.
- C **Nieprawidłowo** Aktualizacje oprogramowania systemu Windows XP nie mogą być skonfigurowane tak, aby przeprowadzały uwierzytelnienie wymagane przez serwer. W takiej sytuacji serwu SUS powinien być tak skonfigurowany, aby pobierał aktualizacje z witryny firmy Microsoft, natomiast systemy Windows XP powinny pobierać i instalować aktualizacje z serwera SUS.
- D. **Prawidłowo** Ponieważ mechanizmy aktualizacji oprogramowania systemu Windows XP nie mogą być skonfigurowane tak, aby przeprowadzały uwierzytelnienie wymagane przez serwer piosy, aktualizacje muszą być pobierane z lokalnego serwera SUS. Lisia pobieranych i instalowanych aktualizacji powsraje w oparciu o listę zatwierdzonych aktualizacji zbudowaną przez administratora serwera SUS.

2.. Prawidłowe odpowiedzi: C oraz I)

- A. **Nieprawidłowo** Komputery systemu Windows XP Professional za pomocą konsoli System nie mogą być konfigurowane tak, aby łączyły się z alternatywnym serwerem aktualizacji.
- B. **Nieprawidłowo** Komputery systemu Windows Server 2003 za pomocą konsoli System nie mogą być konfigurowane tak, aby łączyły się z alternatywnym serwerem aktualizacji.
- C. **Prawidłowo** Opisana metoda jest prawidłowym sposobem dla komputerów, które należą do domeny - dodanie wszystkich do jednostki organizacyjnej, a następnie zastosowanie zasady grupy, która ma odpowiednie ustawienia dotyczące aktualizacji.
- I). **Prawidłowo** Ponieważ serwer ten nie należy do domeny, ustawienia muszą być określone poprzez lokalny obiekt GPO.
- E. **Nieprawidłowo** Serwer SUS nie może aktualizować samego siebie, serwer ten powinien pobierać aktualizacje z witryny firmy Microsoft.

ó. Prawidłowe odpowiedzi: A, B, C oraz D

- A. **Prawidłowo** Opisane działanie stanowi drugą część realizacji celu pomocniczego oraz część realizacji celu głównego. Gdyby zasada grupy wskazywała na pierwszy serwer SUS, łącze ISDN BR] byłoby przeciążone pobieraniem aktualizacji z rego serwera.
- B. **Prawidłowo** Ustawienie takie oznacza, że klient, którego konfiguracja wskazuje na ten serwer SUS, będzie korzystał z listy zatwierdzonych aktualizacji tego serwera, ale same aktualizacje będzie pobierał z serwerów usługi Windows Update firmy Microsoft. Opisane rozwiązanie stanowi pierwszą część realizacji celu pomocniczego.

- C. Prawidłowo Pierwszy serwer będzie zapewniał usługi aktualizacji dla lokacji centrali, wliczając w to listę zatwierdzonych aktualizacji, jak również możliwość pobierania aktualizacji z serwera. Opisane rozwiązanie stanowi część realizacji trzeciorzędnego i głównego celu.
- D. Prawidłowo Opisane działanie stanowi uzupełnienie realizacji celu trzeciorzędnego oraz część realizacji celu głównego. Poprzez wykorzystywanie pierwszego serwera SUS, zamiast drugiego, klienci centrali będą uzyskiwać listę aktualizacji oraz same aktualizacje z pierwszego serwera SUS. Gdyby konfiguracja klienta wskazywała na drugi serwer SUS, aktualizacje byłyby pobierane z serwerów firmy Microsoft, co nie byłoby optymalnym wykorzystaniem łącza centrali do sieci Internet.
- E. Nieprawidłowo Rozwiązanie takie oznacza, że komputery w lokacji zdalnej będą pobierać aktualizacje z pierwszego serwera SUS, a nie z serwerów firmy Microsoft, co spowoduje przeciążenie łącza ISDN BRI. Jest to więc- niezgodne z realizacją celu pomocniczego.
- K Nieprawidłowo Przyjęcie tego rozwiązania spowoduje, że klienci centrali będą pobierać zawierające aktualizacje z serwerów firmy Microsoft, zamiast z pierwszego serwera SUS, co jest niezgodne z celem trzeciorzędnym.

Prawidłowa odpowiedź: E

4.

- A. Nieprawidłowo Pomimo, że opisane rozwiązanie pozwoli instalować aktualizacje w przedsiębiorstwie, to nastąpi przeciążenie linii ISDN BRI wynikające z przesyłania aktualizacji, ponieważ każda stacja robocza będzie pobierać swoje aktualizacje z centralnego serwera SUS.
- B. Nieprawidłowo Pomimo, że klienci będą mieli listę aktualizacji, nie będą mogli pobierać plików aktualizacji z serwerów programu Windows Update firmy Microsoft, ponieważ nie mają możliwości przeprowadzenia uwierzytelnienia wymaganego przez serwer proxy.
- C Nieprawidłowo Patrz uzasadnienie do odpowiedzi B.
- D. Nieprawidłowo) Pomimo, że opisane rozwiązanie pozwoli instalować aktualizacje w przedsiębiorstwie, to nastąpi przeciążenie linii ISDN BRI] wynikające z przesyłania aktualizacji, ponieważ każda stacja robocza będzie pobierać swoje aktualizacje z centralnego serwera SUS. Komputery oddziałów firmy muszą wykorzystywać lokalne serwery SUS.
- E. Prawidłowo Zastosowanie tego rozwiązania umożliwi instalowanie aktualizacji na każdym komputerze firmy, a oprócz tego, poprzez łącza ISDN BRI aktualizacje będą przesyłane tylko jeden raz. Rozwiązanie spełnia postawione w zadaniu wymagania.

Prawidłowe odpowiedzi: A OMZ D

5.

- A. Prawidłowo Metoda jest prawidłowa, chociaż nie jest najbardziej wydajną metodą przy wykonywaniu tego rodzaju operacji.
- B. Nieprawidłowo Zasady grupy nie mogą być stosowane do grup, a jedynie do lokacji, domen oraz jednostek organizacyjnych.
- C. Nieprawidłowo Zasady grupy nie mogą być stosowane do grup, a jedynie do lokacji, domen oraz jednostek organizacyjnych.
- D. Prawidłowo Zasada grupy będzie stosowana jedynie do tych stacji roboczych, które należą do jednostki organizacyjnej Xpwwstn. Ponieważ wszystkie stacje robocze, o których mowa w zadaniu zostały dodane do tej jednostki organizacyjnej, pakiet serwisowy zostanie zainstalowany przy następnym uruchomieniu komputerów.

Zadanie 4.3

Zarządzanie licencjami oprogramowania lokacji

Licencjonowanie jest zagadnieniem, które może wprawić w zakłopotanie większość, nawet doświadczonych administratorów. W systemie Windows Server 2003 zostały wprowadzone dwa sposoby licencjonowania - Per Server (Na serwer) oraz Per User/Per Device (Na użytkownika lub na urządzenie): Tryb licencjonowania Na serwer analizuje bieżące połączenia do pojedynczego serwera. Tryb Na użytkownika lub na urządzenie analizuje połączenia pojedynczego użytkownika lub urządzenia do wielu serwerów. Jeśli administrator nie jest pewny, co do wyboru trybu, powinien wybrać tryb Na serwer, ponieważ dla tego trybu licencjonowania istnieje możliwość bezpłatnej konwersji do trybu Na użytkownika lub na urządzenie.

Tryb licencjonowania Na serwer najlepiej nadaje się, jeśli w sieci istnieje kilka serwerów, do których dostęp jest możliwy z każdej stacji roboczej. Tryb licencjonowania Na użytkownika jest natomiast lepszy, jeśli użytkownicy pracują na wielu stacjach roboczych, z których uzyskują dostęp do pojedynczego serwera lub do wielu serwerów. Licencjonowanie trybu Na urządzenie sprawdza się najlepiej, jeśli wielu użytkowników pracuje na pojedynczym urządzeniu, z którego uzyskują dostęp do wielu serwerów.

Program Terminal Server (Serwer terminali) w trybie usług aplikacji wymaga licencji CAL (Client Access Licenses) dla klientów łączących się w celu wykorzystania usługi. Licencje CAL programu Terminal Services (Usługi terminalowe) są dołączane do systemów Windows 2000 oraz Windows XP Professional dla połączeń tych klienckich systemów operacyjnych.

Pytania do zadania 4.3

1. Czym różnią się licencje CAL urządzenia (Windows Device CAL) i licencje CAL użytkownika (Windows User CAL)? (wybierz wszystkie właściwe odpowiedzi)
 - A. Licencja CAL urządzenia (Windows Device CAL) umożliwia urządzeniu, takiemu jak stacja robocza, połączenie z serwerem bez względu na to, ile użytkowników wykorzystuje to urządzenie.
 - B. Licencja CAL urządzenia (Windows Device CAL) umożliwia pojedynczemu użytkownikowi połączenie do wielu serwerów, o ile użytkownik wykorzystuje pojedynczą stację roboczą.
 - C. Licencja CAL użytkownika (Windows User CAL) umożliwia pojedynczemu użytkownikowi dostęp do serwera z wielu urządzeń, takich jak stacja robocza.
 - D. Licencja CAL użytkownika (Windows User CAL) umożliwia pojedynczemu użytkownikowi dostęp do serwera z pojedynczej stacji roboczej.
2. Rooslan jest odpowiedzialny za licencjonowanie w przedsiębiorstwie średniej wielkości, w którym zainstalowane zostały trzy systemy Windows Server 2003. Systemy te zostały nazwane Server Alpha, Server Beta oraz Server Gamma. Licencjonowanie systemu Server Alpha określa tryb Per Server (Na serwer)

i zostało skonfigurowane dla 500 licencji CAL. Licencjonowanie systemu Server Beta określa tryb Per Server (Na serwer) i zostało skonfigurowane dla 700 licencji CAL. System Server Gamma jest również licencjonowany w trybie Na serwer, przy czym ilość licencji CAL została określona liczbą 600. Jaka liczba licencji CAL jest potrzebna w firmie Rooslana, jeśli w przedsiębiorstwie zainstalowanych jest 550 stacji roboczych, z których jednocześnie 500 uzyskuje dostęp do systemu Server Alpha, 525 z nich uzyskuje dostęp do systemu Server Beta, a 540 do systemu Server Gamma?

- A. 500
- B. 540
- C. 1565
- D. 1800

3.

W niewielkim przedsiębiorstwie administrator odpowiada za licencjonowanie oprogramowania. W firmie pracuje 17 projektantów i 22 pracowników działu handlowego. 13 projektantów wykorzystuje dwie stacje robocze systemu Windows XP Professional. Czterech programistów dodatkowo (oprócz, tych dwóch stacji Windows XP Professional) korzysta z komputerów typu Tablet PC. Zespół handlowców pracuje w parach, które korzystają z jednego komputera typu Tablet PC. Serwer plików firmy został skonfigurowany w trybie Per Device or Per User (Na urządzenie lub Na użytkownika). Jaka jest minimalna liczba licencji potrzebnych do spełnienia wymogów zgodności?

- A. 17 licencji Per Device (Na urządzenie) i 11 licencji Per User (Na użytkownika).
- B. 22 licencje Per Device (Na urządzenie) i 17 licencji Per User (Na użytkownika).
- C. 38 licencji Per User (Na użytkownika) i 22 licencje Per Device (Na urządzenie).
- D. 17 licencji Per User (Na użytkownika) i 11 licencji Per Device (Na urządzenie).

4.

W przedsiębiorstwie jest zainstalowany pojedynczy serwer terminali pracujący w trybie serwera aplikacji, który umożliwia wielu użytkownikom przyłączenie się do serwera w celu uruchomienia pewnego zestawu aplikacji. Spośród użytkowników, którzy łączą się do serwera, 17 wykorzystuje stacje robocze Windows XP Professional, 29 wykorzystuje stacje robocze Windows 2000 Professional, 31 stacje robocze Windows NT 4, a 15 z nich posiada stacje systemu Apple Macintosh OSX, na których zainstalowany został klient Microsoft RDP. W dowolnym momencie do serwera terminali w trybie aplikacji maksymalnie może być zrealizowanych 70 jednoczesnych połączeń. Zachowując zgodność z zasadami licencjonowania, ile licencji CAL Terminal Services jest wymaganych dla programu i opisywanego zestawu klientów, przy założeniu, że aktualnie zostało zakupionych 20 licencji?

- A. 92
- B. 70
- C. 56
- D. 53
- E. 20

5.

Usługa License Logging (Rejestrowanie licencji) analizuje tryb licencjonowania Per Device or Per User (Na urządzenie lub na użytkownika) według nazwy użytkownika. W przedsiębiorstwie zatrudnionych jest 30 pracowników zmianowych, pracujących w zespołach 10-osobowych przez 8 godzin. W okresie 24 godzin trzech różnych użytkowników będzie wykorzystywał tę samą stację roboczą systemu Windows XP Professional. Każdy pracownik zmianowy ma indywidualne konto logowania.

Jak nazwana została metoda, dzięki której nazwy użytkowników mogą być grupowane w zestawy trój-osobowe tak, aby tylko jedna licencja trybu Na urządzenie była rejestrowana w serwerze usługi License Logging (Rejestrowanie licencji), zamiast 30 licencji trybu Na urządzenie?

- A. License Groups (Grupy licencji)
- B. License Revocation (Unieważnienie licencji)
- C. License Clustering (Klaster licencji)
- D. License Aggregation (Sumowanie licencji)

Odpowiedzi do zadania 4.3

-L. Prawidłowe odpowiedzi: A oraz C

- A. **Prawidłowo** Licencja CAL urządzenia (Windows Device CAL) umożliwia urządzeniu, takiemu jak stacja robocza, połączenie z serwerem bez względu na to, ilu użytkowników wykorzystuje to urządzenie, tego typu licencje są przydatne dla przedsiębiorstw, które mają wielu użytkowników wykończających tę samą stację roboczą, jak w **przypadku** pracy zmianowej (na przykład „call center”).
- B. **Nieprawidłowo** Patrz uzasadnienie do odpowiedzi A.
- C. **Prawidłowo** Licencja CAL użytkownika (Windows User CAL) umożliwia pojedynczemu użytkownikowi dostęp do serwera z wielu urządzeń, takich jak stacja robocza. Tryb ten jest przydatny dla użytkowników, którzy w różnych porach korzystają z kilku stacji roboczych lub urządzeń.
- D. **Nieprawidłowo** Patrz uzasadnienie do odpowiedzi G.

2.. Prawidłowa odpowiedź: C

- A. **Nieprawidłowo** Patrz uzasadnienie do odpowiedzi C.
- B. **Nieprawidłowo** Patrz uzasadnienie do odpowiedzi C.
- C. **Prawidłowo** Całkowita liczba licencji CAL (w trybie Na serwer) dla systemu Server Alpha to 500, dla systemu Server Beta to 525, a dla systemu Server Gamma 540. W tym przypadku całkowita liczba wymaganych licencji wynosi 1565.
- D. **Nieprawidłowo** Całkowita liczba licencji CAL (w trybie Na serwer) dla systemu Server Alpha to 500, dla systemu Server Beta to 525, a dla systemu Server Gamma 540. W tym przypadku całkowita liczba wymaganych licencji wynosi 1565- Jeśli zarejestrowanych byłoby 1800 licencji CAL trybu Na serwer, tylko 1565 spośród nich byłoby wymaganych dla zapewnienia zgodności.

«j. Prawidłowa odpowiedź: D

- A. **Nieprawidłowo** Patrz uzasadnienie do odpowiedzi D.
- B. **Nieprawidłowo** Każdy projektant może być przypisany w trybie licencjonowania Per User (Na użytkownika), co pozwala projektantom uzyskiwać dostęp do większej liczby systemów. Dla tego dla 17 projektantów wymaganych będzie 17 licencji trybu Na użytkownika. Każdy komputer typu Tablet PC używany przez zespół handlowców może zostać przypisany za pomocą trybu Per Device (Na urządzenie), z czego wynika, że dla 11 komputerów typu Tablet PC wymaganych będzie 11 licencji trybu Per Device (Na urządzenie). Rozwiązanie opisane w punkcie B jest zgodne z wymogami licencjonowania, ale nie prezentuje minimalnej liczby wymaganych licencji.
- C. **Nieprawidłowo** Patrz uzasadnienie do odpowiedzi B.

D. Prawidłowo Każdy projektant może być przypisany w trybie licencjonowania Per User (Na użytkownika), co pozwala projektantom uzyskiwać dostęp do większej liczby systemów. Dlatego dla 17 projektantów wymaganych będzie 17 licencji trybu Na użytkownika. Każdy komputer typu Tablet PC używany przez zespół handlowców może zostać przypisany za pomocą trybu Per Device (Na urządzenie), z czego wynika, że dla 11 komputerów typu Tablet PC wymaganych będzie 11 licencji trybu Per Device (Na urządzenie).

Prawidłowa odpowiedź: D

4.

A. Nieprawidłowo Patrz uzasadnienie do odpowiedzi **D**.

B. Nieprawidłowo Patrz uzasadnienie do odpowiedzi **D**.

C. Nieprawidłowo Patrz uzasadnienie do odpowiedzi **D**.

D. Prawidłowo Stacje robocze Windows 2000 Professional dostarczane są wraz z wbudowanymi licencjami CAL Terminal Services, tak więc dodatkowe licencje nie są wymagane. 7 stacji roboczych systemu Windows XP Professional nie jest dostarczanych razem z licencjami CAL Terminal Services, czyli dla tych systemów dodatkowe licencje będą wymagane. 31 stacji roboczych systemu Windows NT 4 oraz 15 stacji systemu Macintosh (OSX) wymaga licencji CAL Terminal Services. Do tej pory zakupiono 20 licencji, tak więc trzeba dokonać zakupu 53 licencji, aby spełnić wymagania zgodności zasad licencjonowania.

ii. Nieprawidłowo Patrz uzasadnienie do odpowiedzi **D**.

Prawidłowa odpowiedź: A

5.

A. Prawidłowo Grupowanie licencji jest zbiorem użytkowników, którzy wspólnie wykorzystują jedną lub kilka licencji CAL. W momencie, kiedy użytkownik łączy się do produktu serwera, usługa License Logging (Rejestrowanie licencji) analizuje użytkownika według jego nazwy, ale przypisuje licencję CAL na podstawie przydziału odnoszącego się do grupy licencji.

B. Nieprawidłowo Poprawna nazwa metody to License Groups (Grupy licencji).

C. Nieprawidłowo Poprawna nazwa metody to License Groups (Grupy licencji).

D. Nieprawidłowo Poprawna nazwa metody to License Groups (Grupy licencji).

Zadanie 4.4 Zdalne zarządzanie serwerami

Ze względu na hałas i nienajlepsze warunki do pracy w pomieszczeniach przeznaczonych dla serwerów większość administratorów ze swoich biur zarządzają zdalnie systemami Windows Server 2003. Administratorzy zaglądają do serwerowni od czasu do czasu, w celu wykonania niektórych zadań, takich jak zmiana taśmy kopii zapasowej, ale bardzo rzadko administrator spędza tu większość swojego czasu pracy.

System Windows Server 2003 został wyposażony w kilka metod zarządzania zdalnego. Pierwszym narzędziem jest konsola Computer Management (Zarządzanie komputerem), którą można skonfigurować tak, aby przy jej użyciu podłączyć się do systemu zdalnego i wykonywać wiele tych samych zadań, które można przeprowadzać lokalnie. Do pojedynczej konsoli Computer Management (Zarządzanie komputerem) można dodać kilka serwerów, co oznacza, że administrator może wykorzystywać pojedyncze narzędzie do zarządzania wieloma systemami.

Inną metodą zdalnego zarządzania serwerem jest korzystanie z programu Terminal Services (Usługi terminalowe). Narzędzie to umożliwia administratorowi wykonywanie wszystkich zadań związanych z zarządzaniem tak, jakby wykonywał je siedząc przed prawdziwą konsolą serwera.

Kolejnym sposobem zarządzania zdalnego są narzędzia HTML dla administracji zdalnej. Pozwalają one administratorowi podłączyć się do usługi sieci Web uruchomionej w systemie Windows Server 2003 i wykonywać ograniczony zestaw zadań administracyjnych. Narzędzia te mają zastosowanie w sytuacji, kiedy do podłączenia do serwera wykorzystywać trzeba łącza sieci rozległej WAN o niskiej przepustowości, przykładowo korzystające z połączeń modemowych, których użycie jest nieprzydatne w przypadku stosowania programu Terminal Services (Usługi terminalowe).

Usługa Remote Assistance (Pomoc zdalna) różni się niewiele od metody kontroli serwera wykorzystującej program Terminal Services (Usługi terminalowe). Administrator pracujący przy serwerze może wygenerować zaproszenie umożliwiające innemu administratorowi zdalną obserwację serwera lub współpracę w realizacji wykonywanych zadań.

Pytania do zadania 4.4

1. Rooslan jest głównym administratorem w przedsiębiorstwie średniej wielkości. Jego biuro znajduje się w centrali firmy w Melbourne, w Australii. Rooslan odebrał właśnie telefon od Alexa, który opiekuje się serwerami w jednym z oddziałów firmy w Auckland, w Nowej Zelandii. Obie lokacje połączone są poprzez linię ISDN PRL. Alex chce zmodyfikować niektóre ustawienia rejestru jednego z serwerów w Auckland i chciałby, aby Rooslan kontrolował, czy procedura modyfikacji jest wykonywana prawidłowo. Która z wymienionych poniżej technologii umożliwi Rooslanowi obserwowanie wykonywanych przez Alexa modyfikacji rejestru serwera oraz pozwoli mu w każdym momencie na zwrócenie uwagi na nieprawidłowości?
 - A. Remote Assistance (Pomoc zdalna)
 - B. Terminal Services Remote Administration Mode (Tryb programu Usługi terminalowe dla administracji zdalnej)

- C. HTML Remote Administration Tools (Narzędzia HTML dla administracji zdalnej)
- D. Computer Management Console (Konsola Zarządzanie komputerem)
- E. REGEDT32

2.

Rooslan pracuje w domu i łączy się z serwerem RRAS przedsiębiorstwa wykorzystując linie telefoniczne. Serwer RRAS umożliwia dostęp do systemów Windows Server 2003 pracujących w sieci LAN firmy. Jest godzina 2:15 i w budynku biura nikt nie pracuje. Rooslan chce rozpocząć defragmentację dysków twardych kilku serwerów w firmie. Domowa stacja robocza Rooslana systemu Windows XP Professional nie należy do domeny przedsiębiorstwa działającej pod kontrolą systemu Windows Server 2003. Które z wymienionych poniżej narzędzi może wykorzystać Rooslan do rozpoczęcia defragmentacji dysków?

- A. Aby połączyć się z systemem zdalnym i zapoczątkować defragmentację dysków, Rooslan może użyć wężła Disk Defragmenter (Defragmentator dysku) konsoli Computer Management (Zarządzanie komputerem) jego systemu Windows XP Professional.
- B. Remote Assistance (Pomoc zdalna)
- C. Terminal Services Remote Administration (Tryb usług terminalowych dla administracji zdalnej)
- D. Rooslan może użyć program Defrag.exe wiersza poleceń na swoim systemie Windows XP Professional.

3.

Administrator chce zmienić nazwę autonomicznego systemu Windows Server 2003 znajdującego się w lokacji zdalnej sieci przedsiębiorstwa. System ten pracuje jako serwer FTP ORZ WWW, a jego lokalny administrator jest nieobecny. Serwer ten nie należy do domeny przedsiębiorstwa działającej pod kontrolą systemu Windows Server 2003, natomiast do tej domeny należy stacja robocza administratora (system Windows XP Professional). Które z wymienionych poniżej narzędzi może wykorzystać administrator do realizacji tego zadania? (wybierz wszystkie właściwe odpowiedzi)

- A. Lokalna konsola Computer Management (Zarządzanie komputerem)
- B. Narzędzia HTML dla administracji zdalnej
- C. Tryb administracji zdalnej programu Terminal Services (Usługi terminalowe)
- D. Active Directory Users And Computers Console (Użytkownicy i komputery usługi Active Directory)

4.

Administrator opiekuje się siecią niewielkiego przedsiębiorstwa, które niedawno wykupiło firmę konkurencyjną. Przedsiębiorstwo jest zorganizowane w postaci jednej domeny systemu Windows Server 2003, do której należą wszystkie komputery. Firma konkurencyjna ma sześć serwerów autonomicznych systemu Windows Server 2003. Dwie sieci zostały zintegrowane, a pomiędzy stacją roboczą administratora a serwerami zdalnymi nie została umieszczona żadna zapora ogniowa. Komputer systemu Windows XP Professional administratora należy do domeny, a administrator ma uprawnienia członka grupy Domain Administrator (Administratorzy domeny). Poza tym, administrator ma również administracyjne uprawnienia do serwerów autonomicznych oraz numery telefonów do administratorów serwerów w każdej lokacji, którzy są zalogowani w systemach w godzinach pracy firmy. Które z wymienionych poniżej narzędzi może być wykorzystywane do zdalnego konfigurowania autonomicznych systemów Windows Server 2003 tak, aby zostały przyłączone do domeny przedsiębiorstwa? (wybierz wszystkie właściwe odpowiedzi)

- A- Konsola Computer Management (Zarządzanie komputerem) systemu Windows XP Professional administratora

- B. Active Directory Users and Computers (Użytkownik i komputery usługi Active Directory)
 - C. Narzędzia HTML dla administracji zdalnej
 - D. Tryb administracji zdalnej programu Terminal Services (Usługi terminalowe)
 - E. Remote Assistance (Pomoc zdalna)
- O. Alex jest administratorem systemu znajdującego się w Outback, w Australii, w którym zainstalowane jest urządzenie zdalnego nadzoru satelitarnego. Urządzenie jest połączone z lokacją centralną w Sydney poprzez linię ISDN. Alex ma pewne problemy związane z konfiguracją na serwerze oprogramowania nadzoru i łączy się z administratorem w centrali, który próbował z nim rozmawiać przy użyciu tego oprogramowania. Administrator w centrali poprosił Alexa, aby wysłał zaproszenie pomocy zdalnej, dzięki czemu łatwiej mu będzie pomóc podczas wykonywania procedury konfiguracyjnej. Która z wymienionych poniżej metod umożliwi odebranie zaproszenia pomocy zdalnej wysłane przez Alexa?
- A. Alex może wysłać do administratora zaproszenie pomocy zdalnej przy użyciu programu Windows Messenger oraz Remote Assistance Wizard (Kreator pomocy zdalnej).
 - B. Alex może wysłać zaproszenie: pomocy zdalnej poprzez wiadomość poczty elektronicznej, za pomocą programu Remote Assistance Wizard (Kreator pomocy zdalnej).
 - C. Ali:x może utworzyć: zaproszenie w postaci pliku i umieścić plik na serwerze FTP, z którego administrator plik ten pobierze.
 - D. Alex może uruchomić klienta programu Remote Desktop Connection (Połączenie pulpitu /dalnego) i skonfigurować go tak, aby połączył się z administratorem systemu.
 - E. Alex może utworzyć zaproszenie w postaci pliku i umieścić plik w folderze udostępnionym, do którego administrator ma dostęp.

Odpowiedzi do zadania 4.4

- X. Prawidłowa odpowiedź: A
- A. Prawidłowo Program Remote Assistance (Pomoc zdalna) umożliwia Alexowi wysłanie zaproszenia do Roosłana, dzięki któremu Rooslan będzie mógł obserwować ekran serwera podczas wykonywanych przez/. Alexa modyfikacji.
 - B. Nieprawidłowo Metoda ta umożliwi Rooslanowi zdalne przeglądanie serwera, nie pozwoli jednak na obserwację zmian rejestru przeprowadzanych przez Alexa.
 - C. Nieprawidłowo Ta technologia pozwala Rooslanowi na zdalną administrację serwera, nie umożliwia jednak przeglądania rejestru serwera ani obserwacji zmian przeprowadzanych przez Alexa.
 - D. Nieprawidłowo Metoda ta umożliwi Rooslanowi zdalne przeglądanie serwera, nie pozwoli jednak na obserwację zmian rejestru przeprowadzanych przez Alex.
 - E. Nieprawidłowo Metoda ta nie umożliwi przeglądania rejestru serwera ani obserwacji zmian przeprowadzanych przez Alexa.
- 2.. Prawidłowa odpowiedź: C
- A. Nieprawidłowo Program defragmentacji dysku dostarczany razem z systemem Windows XP bądź Windows Server 2003 nie może być wykorzystywany do przeprowadzenia zdalnej defragmentacji dysku.

B. Nieprawidłowo Ponieważ budynek, w którym znajdują się serwery, jest pusty, nikt nie będzie mógł wysłać zaproszenia programu Remote Assistance (Pomoc zdalna).

C. Prawidłowo Narzędzie to umożliwi Rooslanowi połączenie zdalne do każdego serwera i pozwoli rozpocząć defragmentację dysków.

D. Nieprawidłowo Polecenie Defrag.exe nie może być wykorzystywane do przeprowadzania defragmentacji dysków systemów zdalnych.

3.

Prawidłowe odpowiedzi: B oraz C

A. Nieprawidłowo Ponieważ system nie należy do domeny, administrator nie będzie mógł się zalogować przy użyciu lokalnej konsoli Computer Management (Zarządzanie komputerem) i wykonywać na tym serwerze zadań administracyjnych.

B. Prawidłowo Narzędzia HTML dla administracji zdalnej mogą być używane do zmiany nazwy serwera i do przyłączenia go do domeny. Zmiana nazwy niektórych serwerów nie jest możliwa, na przykład serwerów certyfikacji.

C. Prawidłowo Tryb administracji zdalnej programu Terminal Services (Usługi terminalowe) może być wykorzystywany do zmiany nazwy autonomicznego serwera członkowskiego.

D. Nieprawidłowo Konsola ta nie może być wykorzystywana do zmiany nazwy serwera autonomicznego.

Prawidłowe odpowiedzi: C, D oraz I*

4.

A. Nieprawidłowo Nie istnieje sposób, aby dokonać uwierzytelnienia lokalnej konsoli Computer Management (Zarządzanie komputerem) wymaganego przez autonomiczne serwery zdalne i tym samym nie będzie możliwości dokonania zmiany członkostwa domeny.

B. Nieprawidłowo Konsola ta może być używana do wprowadzenia do domeny konta komputera serwera autonomicznego, ale nie można zdalnie za jej pomocą zmienić członkostwa domeny tych serwerów.

C. Prawidłowo Narzędzia HTML dla administracji zdalnej mogą być używane do zmiany członkostwa domeny autonomicznych systemów Windows Server 2003-

D. Prawidłowo W ten sposób można przyłączyć się do konsoli serwera i zmienić członkostwo domeny serwera autonomicznego.

I*~ Prawidłowo Administrator może zadzwonić do jednej z osób obsługi technicznej w każdej lokacji (w czasie ich pracy) i polecić przesłanie zaproszenia pomocy zdalnej.

Prawidłowe odpowiedzi: A, B, C oraz E

5.

A. Prawidłowo Opisana metoda dostarczania zaproszenia jest prawidłowa.

B. Prawidłowo Opisana metoda dostarczania zaproszenia jest prawidłowa.

C. Prawidłowo Opisana metoda dostarczania zaproszenia jest prawidłowa.

D. Nieprawidłowo Metoda ta nie zadziała, ponieważ nie przesyła zaproszenia, a oprócz tego, to Alex powinien połączyć się z systemem administratora, a nie administrator z serwerem, na którym pracuje Alex.

E. Prawidłowo Opisana metoda dostarczania zaproszenia jest prawidłowa. Po skopiowaniu zaproszenia do komputera lokalnego administratora, będzie on mógł rozpocząć sesję zdalną.

Zadanie 4.5

Rozwiązywanie problemów związanych z kolejkami druku

Podczas korzystania z serwerów druku może pojawić się kilka rodzajów problemów. Pierwszy typ problemu to sytuacja, kiedy na serwerze jest za mało przestrzeni dyskowej dla prawidłowej obsługi buforowania dużych zadań druku. Istnieją dwa sposoby naprawy takiej sytuacji: zwiększenie przestrzeni dyskowej dysku, który obsługuje bufor druku lub przeniesienie bufora druku na inny wolumin, na którym jest więcej miejsca.

Problemy występują również, jeśli dla niektórych użytkowników wydruki powinny być wykonywane szybciej niż dla innych użytkowników. Zagadnienia takie są rozwiązywane poprzez zmianę priorytetu zadań wydruku. Kilka drukarek udostępnionych może być powiązanych z jednym urządzeniem drukuającym, a każdej drukarce udostępnionej można przypisać inny priorytet drukowania, lin wyższa liczba określająca priorytet, tym szybciej realizowane są zadania druku.

Pytania do zadania 4.5

- X. Foley jest administratorem systemów w firmie prawniczej. W (innie pracuje 7-0 sekretarek, które zajmują się obsługą administracyjną prawników. Sekretarki wykorzystują wydajną drukarkę laserową udostępnioną w systemie Windows Server 2003. W sekretariatach regularnie drukowane są duże dokumenty. Pomimo, że: drukarka jest szybka, w zasadzie pracuje w sposób ciągły. W niektórych sekretariatach zauważono, że ze względu na ilość realizowanych zadań w kolejce, niejednokrotnie pomiędzy wysłaniem zadania druku a jego realizacją upływa około 20 minut. W żadnym sekretariacie nikt nie chce przeglądać list dostępnych drukarek i wyszukiwać te, które mają mniej zadań do wykonania. Które z wymienionych poniżej opcji powinien rozważyć Foley, aby skrócić czas potrzebny do wydrukowania dokumentów we wszystkich sekretariatach?
- A. Foley powinien zamówić drugą, taką samą (ten sam producent i model) wydajną drukarkę laserową i powinien utworzyć pulę drukarek.
 - B. Foley powinien określić różne priorytety drukarki dla każdej sekretarki, w oparciu o listę utworzoną przez kierowników poszczególnych grup. Priorytet dla najważniejszego sekretariatu powinna określać wartość 1, a dla najmniej ważnego wartość 99.
 - C. Foley powinien określić różne priorytety drukarki dla każdej sekretarki w oparciu o listę utworzoną przez kierowników poszczególnych grup. Priorytet dla najważniejszego sekretariatu powinna określać wartość 99, a dla najmniej ważnego wartość 1.
 - D. Foley powinien kupić dodatkowe trzy wydajne drukarki laserowe i zainstalować je na serwerze druku jako oddzielne drukarki udostępnione. Sekretarki będą mogły wybierać drukarki, których kolejki zawierają mniej zadań.

2. Administrator, który opiekuje się siecią przedsiębiorstwa średniej wielkości, odebrał kilka telefonów informujących, że na udostępnionej drukarce działu użytkownicy nie mogą wydrukować dużych zadań przekraczających 160 stron. To samo zadanie druku wysłane do drukarki udostępnionej na innym serwerze druku realizowane jest bez kłopotów. Użytkownicy poinformowali również, że mogą wydrukować co zadanie dzieląc cały dokument na 10-stronicowe fragmenty, co jednak jest bardzo niewygodne. Serwer, który obsługuje udostępnioną drukarkę działu, na tym samym woluminie obsługuje również folder udostępniony. Jakie czynności spośród wymienionych poniżej powinien przedsięwziąć administrator, aby rozwiązać ten problem?

- A. Administrator powinien zmienić właściwości drukarki udostępnionej, zwiększając maksymalny rozmiar drukowanych zadań do 200 stron.
- B. Administrator powinien usunąć ograniczenie przydziałów tak, aby umożliwić drukowanie dużych zadań.
- C. Administrator powinien na tym samym serwerze utworzyć nową drukarkę udostępnioną i określić dla niej to samo urządzenie drukujące.
- D. Administrator powinien „wyczyścić” dysk twardy usuwając niepotrzebne pliki foldera udostępnionego, dzięki czemu na dysku pozostanie więcej wolnej przestrzeni.

3. Administrator odebrał telefon od poirytowanego dyrektora (Gregory), który poinformował, że próbował bez rezultatu wydrukować dokument. Dyrektor powiedział, że inne zadanie druku rozpoczęte 20 minut temu również nie zostało zrealizowane. Dyrektor niecierpliwi się, ponieważ właśnie wyjeżdża na lotnisko. Administrator sprawdził kolejkę druku, która zawierała zadania pokazane w poniższej tabelce. Każdy użytkownik drukarki korzystał z domyślnej wartości priorytetu określonej liczbą 10.

2004Budget	Printing	Phillip	238/945
SalesDoc		Darren	24
Policies		James	45
Schematics		Lee	12
Takeoverbid		Gregory	5

Które z wymienionych poniżej czynności pozwolą wydrukować zadania dyrektora Gregory najszybciej, jak jest to możliwe oraz zezwolą na drukowanie dokumentu Phillipa jedynie wtedy, kiedy inne zadania kolejki zostaną zakończone?

- A. Należy zmienić priorytet dokumentu dyrektora Gregory i określić go liczbą 99 oraz zmienić priorytety dokumentów pozostałych użytkowników (Phillip, Darren, James oraz Lee) i określić je liczbą 1.
- B. Należy zmienić priorytet dokumentu dyrektora Gregory i określić go liczbą 1 oraz zmienić priorytety dokumentów pozostałych użytkowników (Phillip, Darren, James oraz Lee) i określić je liczbą 99.
- C. Należy zmienić priorytet dokumentu dyrektora Gregory i określić go liczbą 99. Następnie należy wstrzymać drukowanie dokumentu Phillipa i zmienić priorytet tego dokumentu przypisując mu wartość 1. Po wydrukowaniu pozostałych dokumentów kolejki, należy wznowić drukowanie dokumentu Phillipa.
- D. Należy zmienić priorytet dokumentu Gregora i określić go liczbą 1. Następnie należy wstrzymać drukowanie dokumentu Phillipa i zmienić priorytet tego dokumentu przypisując mu wartość 99. Po uruchomieniu drukowania dokumentu dyrektora Gregory, należy wznowić drukowanie dokumentu Phillipa.

4.

Foley jest administratorem systemów w firmie prawniczej. W firmie pracuje 20 sekretarek, które zajmują się obsługą administracyjną prawników. Sekretarki wykorzystują wydajną drukarkę laserową udostępnioną w systemie Windows Server 2003. W sekretariatach regularnie drukowane są duże dokumenty. Pomimo, że drukarka jest szybka, w zasadzie pracuje w sposób ciągły. W niektórych sekretariatach zauważono, że ze względu na ilość realizowanych zadań w kolejce, niejednokrotnie pomiędzy wysłaniem zadania druku a jego realizacją upływa około 20 minut. Pięć sekretarek pomaga starszym rangą pracownikom. Administrator chce skonfigurować system tak, aby zadania druku wysyłane przez te pięć sekretatek były drukowane szybciej niż zadania wysyłane przez pozostałe 15 sekretarek. Która z przedstawionych poniżej metod pozwoli zrealizować to zadanie?

- A. Należy utworzyć drugą drukarkę udostępnioną nazwaną Snrprtnr i określić dla niej to samo wydajne laserowe urządzenie drukujące. Dla tej drukarki należy przypisać priorytet równy 99. Utworzyć grupę zabezpieczeń i dodać do niej pięć sekretarek współpracujących ze starszymi rangą pracownikami. Tylko ta grupa będzie miała uprawnienia do drukowania przy użyciu drukarki udostępnionej Snrprtnr. Należy upewnić się, że pierwotna drukarka udostępniona ma priorytet określony liczbą 1. Na koniec należy skonfigurować stacje robocze dla tych pięciu sekretarek tak, aby drukowanie kierowane było do drukarki Snrprtnr, a nie do pierwotnie udostępnionej drukarki.
- B. Należy utworzyć drugą drukarkę udostępnioną nazwaną Snrprl ni i określić dla niej to samo wydajne laserowe urządzenie drukujące. Dla tej drukarki należy przypisać priorytet równy 1. Utworzyć grupę zabezpieczeń i dodać do niej pięć sekretarek współpracujących ze starszymi rangą pracownikami. Tylko ta grupa będzie miała uprawnienia do drukowania przy użyciu drukarki udostępnionej Snrprtnr. Należy upewnić się, że pierwotna drukarka udostępniona ma priorytet określony liczbą 99. Na koniec należy skonfigurować stacje robocze dla tych pięciu sekretarek tak, aby drukowanie kierowane było do drukarki Snrprtnr, a nie do pierwotnie udostępnionej drukarki.
- C. Należy utworzyć drugą drukarkę udostępnioną nazwaną Snrprtnr i określić dla niej to samo wydajne laserowe urządzenie drukujące. Dla tej drukarki należy przypisać priorytet równy 99. Utworzyć grupę zabezpieczeń i dodać do niej pięć sekretarek współpracujących ze starszymi rangą pracownikami. Tylko ta grupa będzie miała uprawnienia do drukowania przy użyciu drukarki udostępnionej Snrprtnr. Należy upewnić się, że pierwotna drukarka udostępniona ma priorytet określony liczbą 1. Na koniec należy skonfigurować stacje robocze dla 15 pozostałych sekretarek tak, aby drukowanie kierowane było do drukarki Snrprtnr, a nie do pierwotnie udostępnionej drukarki.
- D. Należy utworzyć drugą drukarkę udostępnioną nazwaną Snrprtnr i określić dla niej to samo wydajne laserowe urządzenie drukujące. Dla tej drukarki należy przypisać priorytet równy 99. Utworzyć grupę zabezpieczeń i dodać do niej konta 15 sekretarek, które nie współpracują ze starszymi rangą pracownikami. Tylko ta grupa będzie miała uprawnienia do drukowania przy użyciu drukarki udostępnionej Snrprtnr. Należy upewnić się, że pierwotna drukarka udostępniona ma priorytet określony liczbą 1. Na koniec należy skonfigurować stacje robocze dla pięciu sekretarek współpracujących ze starszymi rangą pracownikami tak, aby drukowanie kierowane było do drukarki Snrprtnr, a nie do pierwotnie udostępnionej drukarki.

Odpowiedzi do zadania 4.5

1. Prawidłowa odpowiedź: A

- A. **Prawidłowo** Pula drukarek będzie rozdzielać zadania wysłane do drukarki udostępnionej między dwa odrębne urządzenia drukujące.
- B. **Nieprawidłowo** Rozwiązanie takie nie zadziała z kilku powodów. Po pierwsze priorytety są przypisywane do drukarek udostępnionych, a nie do użytkowników. Dwie drukarki udostępnione drukują na tym samym urządzeniu drukującym, tak więc drukarka o wyższym priorytecie szybciej zrealizuje swoje zadania. Zadania wysłane do drukarki o priorytecie 99 będą wydrukowane szybciej niż zadania wysłane do drukarki o priorytecie 1.
- C. **Nieprawidłowo** Rozwiązanie takie nie zadziała, ponieważ priorytety są przypisywane do drukarek udostępnionych, a nie do użytkowników. Dwie drukarki udostępnione drukują na tym samym urządzeniu drukującym, tak więc drukarka o wyższym priorytecie szybciej zrealizuje swoje zadania.
- D. **Nieprawidłowo** W zadaniu zostało zaznaczone, że sekretarki nie mają być zmuszane do wyszukiwania, która drukarka ma krótszą kolejkę zadań.

2.. Prawidłowa odpowiedź: D

- A. **Nieprawidłowo** Drukarki udostępnione nie blokują drukowania zadań w oparciu o ilość stron wydruku.
- B. **Nieprawidłowo** W systemie Windows Server 2003 przydziały nie mogą być określone dla drukarek udostępnionych.
- C. **Nieprawidłowo** Działanie takie nie rozwiąże problemu, ponieważ wszystko wskazuje, że jego przyczyną jest brak wystarczającej wielkości przestrzeni dyskowej potrzebnej do obsługi buforowania dużych plików.
- D. **Prawidłowo** Duże zadania nie są drukowane, ponieważ dla bufora druku pozostało za mało przestrzeni dyskowej. Ze względu na ilość wolnej przestrzeni na dysku, system mógł utworzyć jedynie bufor o mniejszych rozmiarach, umożliwiającą realizację mniejszych zadań.

O. Prawidłowa odpowiedź: C

- A. **Nieprawidłowo** W takim przypadku dyrektor Gregory zanim otrzyma wydrukowany dokument, będzie w dalszym ciągu oczekiwał na zakończenie drukowania dokumentu Phillipa.
- B. **Nieprawidłowo** Działanie takie spowoduje, że dokument dyrektora Gregory otrzyma najniższy priorytet, co oznacza, że zostanie wydrukowany jako ostatni dokument kolejki druku. Oprócz tego, jeśli w międzyczasie do drukarki zostaną wysłane inne dokumenty, one również zostaną wydrukowane wcześniej niż dokument dyrektora Gregory.
- C. **Prawidłowo** Działanie takie spowoduje, że dokument dyrektora Gregory zostanie szybko wydrukowany. Dokumenty pozostałych użytkowników zostaną wydrukowane później. Po zakończeniu drukowania dokumentów pozostałych użytkowników zostanie wznowione drukowanie dokumentu Phillipa.
- D. **Nieprawidłowo** Działanie takie oznacza, że dyrektor Gregory otrzyma swój dokument po wydrukowaniu dokumentów użytkowników Darren, James oraz Lee, ponieważ dokumenty tych użytkowników mają wyższy priorytet niż jego dokument.

4. **Prawidłowa odpowiedź: A**

- A. **Prawidłowo** Działanie takie umożliwi pięciu sekretarkom współpracującym ze starszymi rangą pracownikami drukowanie dokumentów o wyższym priorytecie niż dla pozostałych sekretarek firmy.
- B. **Nieprawidłowo** Priorytet określony liczbą 1 oznacza, że grupa pięciu sekretarek, o których mowa w zadaniu, będzie oczekiwać na zakończenie pozostałych zadań druku, zanim wydrukowane zostaną ich zadania.
- C. **Nieprawidłowo** Działanie takie przydzieli dokumentom 15 sekretarek firmy, które nie współpracują ze starszymi rangą pracownikami, wyższy priorytet drukowania niż dla pozostałych pięciu sekretarek.
- D. **Nieprawidłowo** Grupa pięciu sekretarek współpracujących ze starszymi rangą pracownikami nie będzie mogła uzyskać dostępu do drukarki Snrprtnr, ponieważ wyłączny dostęp do tej drukarki otrzymała grupa pozostałych 15 sekretarek.

Zadanie 4.6

Monitorowanie zdarzeń

Monitorowanie zdarzeń umożliwia administratorowi przeglądanie aktywności, które miały miejsce na obserwowanych serwerach. Monitor zdarzeń w połączeniu z odpowiednio dobranymi zasadami inspekcji pozwala określić, którzy użytkownicy wykorzystują poszczególne prawa. Inspekcja konfigurowana jest poprzez zasady grupy i powinna być stosowana na poziomie domeny. W niektórych sytuacjach, takich jak dostęp do obiektu, należy przeprowadzać dodatkowe działania polegające na dodawaniu poszczególnych grup, których aktywność należy poddać inspekcji.

Pytania do zadania 4.6

1. Administrator opiekuje się siecią przedsiębiorstwa średniej wielkości. Iryleki j.i poleciła mu utworzenie dziennika inspekcji wszystkich użytkowników próbujących uzyskać dostęp do piwnego foldera, w którym przechowywane są tajne informacje linuy dotyczące jej finansów. Dyrekcja jest zainteresowana zarówno listą użytkowników, którzy uzyskali dostęp do tego foldera, jak i listą użytkowników, dla których dostęp /ostał odmówiony ze względu na niewystarczające uprawnienia NTFS. Jakiego rodzaju Inspekt je powinien skonfigurować administrator? (wybierz wszystkie właściwe odpowiedzi)
 - A. Successful Object Access (inspekcja dostępu do obiektu zakończonego powodzeniem)
 - B. Failed Object Access (inspekcja dostępu do obiektu zakończonego niepowodzeniem)
 - C. Successful Privilege Use (inspekcja użycia uprawnień zakończonego powodzeniem)
 - D. Failed Privilege Use (inspekcja użycia uprawnień zakończona niepowodzeniem)
 - E. Successful Directory Service Access (inspekcja dostępu do usługi Active Directory zakończonego powodzeniem)
 - F. Failed Directory Service Access (inspekcja dostępu do usługi Active Directory zakończonego niepowodzeniem)
2. Rooslan jest administratorem w niewielkiej firmie, która posiada mniej niż 100 użytkowników. Pewnej niedzieli podczas sprawdzania taśmy kopii zapasowej zauważył, że na jednej z kolorowych drukarek laserowych wydrukowane zostały nieodpowiednie zdjęcia, niezgodne z zasadą przedsiębiorstwa. W tym dniu nikogo nie było w biurze i administrator sprawdził dzienniki dostępu zdalnego. Okazało się, że 10 użytkowników było przyłączonych do sieci firmy zdalnie ze swoich domowych komputerów. Rooslan założył, że osoba, która wydrukowała zdjęcia przyjdzie później je zabrać, zanim w poniedziałek rano mogą zostać znalezione przez innych pracowników. Spośród 10 użytkowników, którzy zalogowali się zdalnie, tylko 5 osób miało wystarczające uprawnienia drukowania na tej konkretnej kolorowej drukarce laserowej. Rooslan skonfigurował zasadę inspekcji domeny dla szczególnego typu zdarzenia, a następnie korzystając z zaawansowanych właściwości zabezpieczeń drukarki udostępnionej poddał inspekcji grupę, która ma dostęp do drukarki. Jaki typ zdarzenia inspekcji powinien określić Rooslan w zasadzie grupy, aby zlokalizować kto wydrukował zdjęcia w niedzielę po południu?
 - A. Inspekcja zdarzenia użycia uprawnień zakończonego powodzeniem (Successful Privilege Use)
 - B. Inspekcja zdarzenia użycia uprawnień zakończonego niepowodzeniem (Failed Privilege Use)
 - C. Inspekcja systemowych zdarzeń zakończonych powodzeniem (Successful System Events)

- D. Inspekcja systemowych zdarzeń zakończonych niepowodzeniem (Failed System Events)
 - E. Inspekcja zdarzeń dostępu do obiektu zakończonych powodzeniem (Successful Object Access)
 - F. Inspekcja zdarzeń dostępu do obiektu zakończonych niepowodzeniem (Failed Object Access)
- o. Administrator opiekuje się systemem Windows Server 2003 IIS Web. Witryna sieci Web obsługuje grupę forum dyskusyjnych. Witryna jest zabezpieczona i dostęp do niej mają jedynie użytkownicy, którzy prawidłowo wprowadzili nazwę użytkownika i hasło. Pewnego dnia administrator zauważył, że nazwa jednego z kont, które korzystają z witryny, została złośliwie wysłana do forum. Administrator usunął tę wiadomość, ale postanowił sprawdzić, czy ktoś usiłuje odgadnąć hasło konta poprzez próby zalogowania się w zabezpieczonej witrynie. System Windows Server 2003 został uruchomiony jako serwer autonomiczny, który nie należy do domeny, jakiego rodzaju zdarzenia administrator powinien poddać inspekcji?
- A. Inspekcja zdarzeń logowania zakończonych powodzeniem (Successful Logon Events)
 - B. Inspekcja zdarzeń logowania zakończonych niepowodzeniem (failed Logon Events)
 - C. Inspekcja zdarzeń logowania na kontach zakończonych powodzeniem (Successful Account Logon)
 - D. Inspekcja zdarzeń logowania na kontach zakończonych niepowodzeniem (failed Account Logon)
 - E. Inspekcja zdarzeń dostępu do obiektów zakończonych powodzeniem (Successful Object Access)
 - F. Inspekcja zdarzeń dostępu do obiektów zakończonych niepowodzeniem (failed Object Access)
4. Zgodnie z zasadą obowiązującą w przedsiębiorstwie, wszystkie działania administratorów dotyczą kont i grup, takie jak tworzenie, usuwanie, zmiana nazwy oraz działania związane z wyłączeniem kont i zmianą ich haseł, muszą być poddane inspekcji. Zdarzenia te są przechowywane w dzienniku Security (Zabezpieczenia). Aby wypełnić wymagania zasady, administrator dokonuje edycji domyślnego obiektu CIPO domeny. Dla którego zdarzenia powinna zostać włączona inspekcja?
- A. Inspekcja zdarzeń użycia uprawnień zakończonych powodzeniem (Successful Privilege Use)
 - B. Inspekcja zdarzeń użycia uprawnień zakończonych niepowodzeniem (failed Privilege Use)
 - C. Inspekcja zdarzeń zarządzania kontami zakończonych powodzeniem (Successful Account Management)
 - D. Inspekcja zdarzeń logowania na kontach zakończonych niepowodzeniem (failed Account Logon)
 - E. Inspekcja zdarzeń logowania na kontach zakończonych powodzeniem (Successful Account Logon)
 - F. Inspekcja zdarzeń logowania na kontach zakończonych niepowodzeniem (failed Account Logon)

Odpowiedzi do zadania 4.6

X. Prawidłowe odpowiedzi: A oraz B

- A. **Prawidłowo** Inspekcja taka pozwoli utworzyć listę osób, które uzyskały dostęp do opisywanego w zadaniu foldera.
- B. **Prawidłowo** Inspekcja taka pozwoli utworzyć listę osób, które nie uzyskały dostępu do opisywanego w zadaniu foldera.
- C. **Nieprawidłowo** Administrator nie jest zainteresowany uzyskaniem informacji o użyciu uprawnień, lecz o dostępie do obiektu.
- D. **Nieprawidłowo** Patrz uzasadnienie do odpowiedzi C.
- E. **Nieprawidłowo** Patrz uzasadnienie do odpowiedzi C.
- F. **Nieprawidłowo** Patrz uzasadnienie do odpowiedzi C.

2.

Prawidłowa odpowiedź: E

- A. Nieprawidłowo Użycie drukarki rac/iej nie wiąże się z użyciem uprawnień, lecz z dostępem do obiektu.
- B. Nieprawidłowo Patrz uzasadnienie do odpowiedzi A.
- C. Nieprawidłowo Użycie drukarki raczej nie wiąże się ze zdarzeniami systemu, lecz z dostępem do obiektu.
- D. Nieprawidłowo Patrz uzasadnienie do odpowiedzi C.
- E. Prawidłowo Inspekcja taka w dzienniku Security (Zabezpieczenia) utworzy listę wszystkich użytkowników, którzy próbowali drukować na tej drukarce. Następnie Rooslan może sprawdzić w tym dzienniku, kto drukował w niedzielę.
- B Nieprawidłowo Ponieważ użytkownik mógł drukować za pomocą tej drukarki, nie ma powodu poddawać inspekcji zdarzenia nieudanego dostępu do obiektu. Działanie takie utworzy listę użytkowników, którzy próbowali bez powodzenia wydrukować zadania na tej drukarce.

3.

Prawidłowa odpowiedź: D

- A. Nieprawidłowo Ten typ zdarzeń występuje, jeśli zachodzi uwierzytelnienie konta przez kontroler domeny. (Opisywany serwet autonomiczny nie należy do domeny.
- B. Nieprawidłowo Ten typ zdarzeń występuje, jeśli zachodzi uwierzytelnienie konia przez kotmoler domeny. Opisywany serwet autonomiczny nie należy do domeny.
- (. Nieprawidłowo Inspekcja la utworzy lisię wszystkich zakończonych powodzeniem zdarzeń logowania w serwerze autonomicznym. Na liście tej nie zostaną umieszczone zdarzenia związane z nieudanymi próbami dostępu do serweta.
- I). Prawidłowo Inspekcja taka utworzy listę wszystkich nieudanych prób logowania w serwerze auto nomicznym. jest to typ zdarzenia, który powinien być poddany inspekcji pozwalającej sprawdzić, czy ktoś usiłuje odgadnąć hasło konta podanego w wiadomości prezentowanej na forum. Zgodnie Z zasadami zabezpieczeń, konto to powinno zostać wyłączone.
- E. Nieprawidłowo Ahy wykonać zadanie opisane w pytaniu, nie trzeba przeprowadzili' inspekcji obiektów. Inspekcji powinny być poddane zdarzenia logowania na kontach.
- E Nieprawidłowo Ahy wykonać zadanie opisane w pyłaniu, nie trzeba przeprowadzać inspekcji obiektów. Inspekcji powinny być poddane zdarzenia logowania na kontach.

Prawidłowa odpowiedź: C

4.

- A. Nieprawidłowo Utworzenie, usunięcie czy zmiana nazwy kont nie jest związana z użyciem uprawnień, natomiast czynności te są rejestrowane podczas inspekcji innego typu zdarzenia, podczas inspekcji zdarzeń związanych z zarządzaniem kontami.
- B. Nieprawidłowo Patrz uzasadnienie do odpowiedzi A.
- C. Prawidłowo Zdarzenia dotyczące zarządzania kontami zakończone powodzeniem zapisywane są w dzienniku systemu każdorazowo, jeśli następuje utworzenie, usunięcie bądź zmiana nazwy konta. Wpisy powstają również, jeśli tworzone i usuwane są grupy bądź zmieniana jest ich nazwa, a także jeśli konta zostają wyłączone lub zmienione zostaje hasło przypisane do konta.
- D. Nieprawidłowo Administrator nie jest zainteresowany zdarzeniami, dla których zarządzanie kontem zakończyło się niepowodzeniem, ponieważ administratorzy mają wystarczające uprawnienia, aby wykonywać zadania związane z zarządzaniem kontami.
- E. Nieprawidłowo Patrz uzasadnienie do odpowiedzi A.
- E Nieprawidłowo Patrz uzasadnienie do odpowiedzi A.

Zadanie 4.7

Monitorowanie bieżącej wydajności systemu

Utrzymanie sprawnie funkcjonującego serwera jest ważnym zadaniem administratora. Powolne działanie serwera denerwuje użytkowników, którzy najprawdopodobniej przeleją tę frustrację na osoby odpowiedzialne za pracę serwerów. Administrator systemu powinien utworzyć wzór odniesienia dotyczący wykorzystania procesora, sieci, dysku i pamięci zaraz po pierwszym skonfigurowaniu serwera. Następnie administrator powinien regularnie monitorować wydajność serwera w celu określenia, jakie zmiany wydajności nastąpiły w odniesieniu do wzorca. Statystyki wydajności są tworzone przez konsolę Performance (Wydajność). Za pomocą tej konsoli można również gromadzić statystyki dotyczące serwerów zdalnych, dzięki czemu administrator może w przybliżeniu ocenić wydajność serwerów, którymi się opiekuje.

Pytania do zadania 4.7

1. Administratorowi obawia się, że procesor serwera drukarki, który obsługuje 10 drukarek udostępnionych, nie jest w stanie odpowiednio szybko przetwarzać buforowania plików wydruku. Który z wymienionych poniżej sposobów pozwala sprawdzić, czy te obawy są słuszne?
 - A. We właściwościach drukarki udostępnionej należy sprawdzić statystykę wykorzystania procesora bufora druku.
 - li. Należy skonfigurować konsolę Performance (Wydajność) tak, aby dla serwera drukarki śledziła wykorzystanie procesora dla bufora druku (Process\%Processor Time\spoolsv) [Proccsor\Czas procesora %\spoolsv] w trakcie zwykłego dnia roboczego oraz należy skonfigurować wyświetlanie tak, aby pokazywana była wartość maksymalna.
 - C. Należy skonfigurować konsolę Performance (Wydajność) tak, aby dla serwera drukarki śledziła wykorzystanie procesora dla bufora druku (Process\%Processoi Time\spoolsv) [Proccsor\Czas procesora %\spoolsv] w trakcie zwykłego dnia roboczego oraz należy skonfigurować wyświetlanie tak, aby pokazywana była wartość średnia.
 - D. Należy skonfigurować konsolę Performance (Wydajność) tak, aby dla stacji roboczej administratora drukarki śledziła wykorzystanie procesora dla bufora druku (Process\%Processor Time\spoolsv) [Proccsor\Czas procesora %\spoolsv] w trakcie zwykłego dnia roboczego oraz należy skonfigurować wyświetlanie tak, aby pokazywana była wartość średnia.
- 2.. Rooslan ma zamiar wyjaśnić dlaczego wydajność jednego z systemów Windows Server 2003 jest niska. Rooslan nie ma pojęcia, co może być tego przyczyną - czy problem dotyczy dysku, procesora czy też wielkości dostępnej pamięci. Które z wymienionych sposobów mierzenia wydajności powinny dać lepsze wyobrażenie na temat różnych wydajności serwera mierzonych w trakcie dnia roboczego? (wybierz wszystkie właściwe odpowiedzi)
 - A. Rooslan powinien wykorzystać konsolę Performance (Wydajność) do prześledzenia wartości liczników % Processor Time (Czas procesora %), Current Disk Queue Length (Długość bieżącej kolejki

- dysku) oraz Available MBytes (Dostępna pamięć w MB). Widok powinien zostać skonfigurowany tak, aby pokazywane były wartości maksymalne w trakcie zwykłego dnia pracy.
- B. Rooslan powinien wykorzystać konsolę Performance (Wydajność) do prześledzenia wartości liczników % Processor Time (Czas procesora %), Current Disk Queue Length (Długość bieżącej kolejki dysku) oraz Available MBytes (Dostępna pamięć w MB). Widok powinien zostać skonfigurowany tak, aby pokazywane były wartości bieżące, a konsola powinna być uruchomiona w trakcie zwykłego dnia pracy.
- C. Rooslan powinien wykorzystać konsolę Performance (Wydajność) do prześledzenia wartości liczników % Processor Time (Czas procesora %), Current Disk Queue Length (Długość bieżącej kolejki dysku) oraz Available MBytes (Dostępna pamięć w MB). Widok powinien zostać skonfigurowany tak, aby pokazywane były wartości minimalne, a konsola powinna być uruchomiona w trakcie zwykłego dnia pracy.
- D. Rooslan powinien wykorzystać konsolę Performance (Wydajność) do prześledzenia wartości liczników % Processor Time (Czas procesora %), Current Disk Queue Length (Długość bieżącej kolejki dysku) oraz Available MBytes (Dostępna pamięć w MB). Widok powinien zostać skonfigurowany tak, aby pokazywane były wartości średnie, a konsola powinna być uruchomiona w trakcie zwykłego dnia pracy.
3. Rob obawia się, że przepustowość karty sieciowej serwera, który jest przez niego obsługiwany, powinna zostać zwiększona z 10 Mb do 100 Mb. Roli monitoruje dla karty sieciowej średnie wartości licznika Output Queue Length (Długość kolejki wyjściowej) w czasie zwykłego dnia pracy. jakie wartości powinny budzić zaniepokojenie i wskazywać, że kartę należy wymienić na szybszą? (wybierz, wszystkie właściwe odpowiedzi)
- A. 0
- B. 1
- C. 1
- D. 3
- E. 4

Odpowiedzi do zadania 4.7

1. Prawidłowa odpowiedź: C

- A. **Nieprawidłowo** Taka statystyka nie istnieje we właściwościach drukarki udostępnionej.
- B. **Nieprawidłowo** Parametr % Processor Time (Czas procesora %) w krótkich okresach czasu może osiągać wartość 100% i nie będzie odniesieniem do wartości średniej wykorzystania procesora przez bufor wydruku.
- C. **Prawidłowo** Statystyka ta jest dobrym wskaźnikiem określającym ilość czasu procesora serwera związanego % obsługą bufora druku w trakcie zwykłego dnia roboczego.
- D. **Nieprawidłowo** Działanie takie sprawdza stację roboczą, a nie serwer druku.

2.. Prawidłowa odpowiedź: D

- A. **Nieprawidłowo** Wartości maksymalne mogą pokazywać nietypowe szczytowe obciążenia i nie dają poglądu na temat wydajności średniej.

- B. Nieprawidłowo** Wartości bieżące nie powiedzą niczego na temat wydajności średniej w trakcie całego dnia.
- C. Nieprawidłowo** Wartości minimalne nie powiedzą niczego na temat wydajności średniej w trakcie całego dnia.
- D. Prawidłowo** Działanie takie daje dobre wyobrażenie na temat wydajności każdego podsystemu mierzonej w trakcie dnia pracy i na tej podstawie Rooslan będzie mógł określić dalszy sposób postępowania.

ó. Prawidłowe odpowiedzi: C, D oraz E

- A. Nieprawidłowo** Średnia wartość 0 nie jest powodem do obaw.
- B. Nieprawidłowo** Średnia wartość 1 nie jest powodem do obaw. Wartość taka oznacza, że podczas pracy karty sieciowej tylko czasami zdarzają się „zaległości”.
- C. Prawidłowo** Zgodnie z wyjaśnieniami dotyczącymi statystyk licznika konsoli Performance (Wydajność) wartość 2 lub wyższa jest powodem do obaw i może wskazywać, że potrzebna będzie wymiana karty.
- D. Prawidłowo** Patrz uzasadnienie do odpowiedzi C.
- E. Prawidłowo** Patrz uzasadnienie do odpowiedzi C.

Zadanie 4.8

Monitorowanie serwerów plików i druku

Ogromna większość serwerów sieci lokalnych wykonuje zadania związane z obsługą druku lub udostępnianiem plików. Dla administratorów sieci najważniejszą sprawą jest zapewnienie sprawnego i niezawodnego działania tych serwerów.

Administratorzy serwerów plików muszą zapewnić, aby woluminy przechowujące pliki nie zostały zapelnione. Sytuacja taka ma miejsce, jeśli stare dane przechowywane są przez długi czas po zakończeniu ich wykorzystywania, a cały czas zapisywane są nowe dane. Administratorzy powinni również zapewnić, aby poszczególni użytkownicy (w porównaniu do innych) nie przechowywali na serwerze nieproporcjonalnie wielkich ilości danych. Jednym ze sposobów zapewnienia, że wolumin nie zostanie przepełniony oraz że wszyscy użytkownicy będą mieli ograniczone możliwości przechowywania dowolnych ilości danych jest wdrożenie przydziałów na partycji systemu. Przydził uniemożliwia użytkownikowi zapis większej ilości danych niż zostało to dla niego określone. Zakładka Quota (Przydział) dostępna jest podczas edycji właściwości poszczególnych woluminów.

Kolejki druku mogą być monitorowane bezpośrednio na serwerze lub zdalnie. Oprócz tego mogą być monitorowane za pomocą konsoli Perloi mańce (Wydajność). Konsola ta może być wykorzystana do utworzenia raportu przybliżonego, informującego o bieżącej liczbie zadań druku przypisanych do dowolnego serwera druku. Dzięki temu administrator może zdecydować, czy obciążenie zadaniami druku powinno być rozdzielone pomiędzy inne serwery druku, jeśli działanie takie nie zabierze zbyt dużo czasu.

Pytania do zadania 4.8

L. Rooslan jest administratorem sieci średniej wielkości wydziału lokalnego uniwersytetu. Rooslan opiekuje się pięcioma Systemami Windows Server 2003. Jeden z tych systemów jest wykorzystywany do udostępniania plików wydziału dla Studentów, absolwentów, pracowników akademickich i administracji. W serwerze plików zainstalowane są dwa dyski. Pierwszy dysk jest podzielony na dwa woluminy. Na jednym woluminie o pojemności 10 GB zainstalowany jest system operacyjny, a drugi wolumin służy do przechowywania udostępnionych folderów dla studentów. Drugi dysk skonfigurowany w postaci pojedynczego woluminu o pojemności 20 GB służy do udostępniania plików dla absolwentów, pracowników akademickich oraz pracowników administracji. Rooslan obawia się, że woluminy, które przechowują dane niedługo zapelnia się i dlatego ma zamiar uruchomić mechanizmy przydziałów dysków. Wszyscy studenci wydziału są członkami grupy Undergrad, wszyscy absolwenci są członkami grupy Postgrad, wszyscy pracownicy akademicki są członkami grupy Academic, a wszyscy pracownicy administracji należą do grupy Secret. Każdy użytkownik należy tylko do jednej grupy. Uprawnienia udziału są zdefiniowane w ten sposób, że do danego udziału dostęp uzyskują jedynie członkowie odpowiedniej grupy. Po przeprowadzeniu konsultacji z przedstawicielami różnych grup Rooslan zdecydował wprowadzić następujące mechanizmy przydziałów dysków: Maksymalna wielkość danych przechowywanych na serwerze przez studentów to 100 MB. Maksymalna wielkość danych przechowywanych na serwerze przez absolwentów to 300 MB.

Maksymalna wielkość danych przechowywanych na serwerze przez pracowników administracji to 500 MB.

Maksymalna wielkość danych przechowywanych na serwerze przez pracowników akademickich to 800 MB. Która z wymienionych poniżej metod pozwoli Rooslanowi wprowadzić opisany schemat przydziałów dysku?

- A. Rooslan powinien przeprowadzić edycję właściwości udziału przeznaczonego dla studentów, ograniczyć wielkość przydziałów do wartości 100 MB i zaznaczyć pole wyboru Deny More Disk Space To Users Over Quota (Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału). Następnie Rooslan powinien przeprowadzić edycję właściwości udziału dla absolwentów oraz ograniczyć wielkość przydziałów do wartości 300 MB i zaznaczyć pole wyboru Deny More Disk Space To Users Over Quota (Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału). Kolejno powinien przeprowadzić edycję właściwości udziału dla pracowników administracji oraz ograniczyć wielkość przydziałów do wartości 500 MB i zaznaczyć pole wyboru Deny More Disk Space To Users Over Quota (Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału). Na koniec powinien przeprowadzić edycję właściwości udziału dla pracowników akademickich oraz ograniczyć wielkość przydziałów do wartości 800 MB i zaznaczyć pole wyboru Deny More Disk Space To Users Over Quota (Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału).
- B. Rooslan powinien przeprowadzić edycję właściwości foldera przeznaczonego dla studentów, ograniczyć wielkość **przydziałów** do wartości 100 MB i zaznaczyć pole wyboru Deny More Disk Space To Users Over Quota (Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału). Następnie Rooslan powinien przeprowadzić edycję właściwości foldera dla absolwentów oraz ograniczyć wielkość przydziałów do wartości 300 MB i zaznaczyć pole wyboru Deny More Disk Space To Users Over **Quota** (Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału). Kolejno powinien przeprowadzić edycję właściwości foldera dla **pracowników** administracji oraz ograniczyć wielkość **przydziałów** do wartości 500 MB i zaznaczyć pole wyboru Deny More Disk Space To Users Over Quota (Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału). Na koniec powinien przeprowadzić edycję właściwości foldera dla pracowników akademickich oraz ograniczyć wielkość przydziałów do wartości 800 MB i zaznaczyć pole wyboru Deny More Disk Space To Users Over Quota (Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału).
- O Rooslan powinien przeprowadzić edycję właściwości woluminu, na którym przechowywany jest udział przeznaczony dla studentów. Rooslan powinien przejść do zakładki Quotas (Przydział), zaznaczyć pole wyboru Enable Quota Management (Włącz zarządzanie przydziałami) oraz Deny Disk Space To Users Exceeding Quota Limit (Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału). Następnie na zakładce Quota Entries (Wpisy przydziału) Rooslan powinien dodać grupę Undergrad i ograniczyć przydział do wartości 100 MB. W kolejnych krokach Rooslan powinien przeprowadzić analogiczne modyfikacje dla właściwości woluminów, na których przechowywane są udziały dla absolwentów, pracowników administracyjnych i akademickich. Powinien przejść do zakładki Quotas (Przydział) i zaznaczyć pole wyboru Enable Quota Management (Włącz zarządzanie przydziałami) oraz Deny Disk Space To Users Exceeding Quota Limit (Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału). Na zakładce Quota Entries (Wpisy przydziału) Rooslan powinien dodać grupę Postgrad i ograniczyć dla niej przydział do wartości 300 MB. Następnie powinien dodać grupę Secrat i ograniczyć dla niej przydział do wartości 500 MB, a na koniec powinien dodać grupę Academ i ograniczyć dla niej przydział do wartości 800 MB.
- D. Rooslan powinien przeprowadzić edycję właściwości woluminu, na którym przechowywany jest udział przeznaczony dla studentów. Rooslan powinien przejść do zakładki Quotas (Przydział), zaznaczyć pole wyboru Enable Quota Management (Włącz zarządzanie przydziałami) oraz Deny Disk Space To Users Exceeding Quota Limit (Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału)

oraz ograniczyć przydział do wartości 100 MB. Powinien następnie wykonać na taśmie magnetycznej kopię zapasową woluminu, który przechowuje udziały przeznaczone dla absolwentów, pracowników administracji i pracowników akademickich. W kolejnym kroku Rooslan powinien usunąć wolumin i ponownie utworzyć partycje dysku twardego dzieląc go na trzy jednakowe woluminy. Na nowych woluminach Roosla powinien odtworzyć odpowiednio udział przeznaczony dla absolwentów na pierwszym woluminie, udział dla pracowników administracji na drugim woluminie, a na trzecim woluminie udział przeznaczony dla pracowników akademickich. W kolejnym kroku Rooslan powinien przeprowadzić edycję właściwości woluminu, na którym przechowywane są udziały dla studentów, przejść do zakładki Quotas (Przydział), zaznaczyć pola wyboru F.nable Quota Management (Włącz zarządzanie przydziałami) oraz Deny Disk SpaceTo Users Exceeding Quota Limit (Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału) i ograniczyć przydział do wartości 300 MB. Następnie Rooslan powinien przeprowadzić edycję właściwości woluminu, na którym przechowywane są udziały dla pracowników administracji, przejść do zakładki Quotas (Przydział), zaznaczyć pola wyboru Knable Quota Managemenr (Włącz zarządzanie przydziałami) oraz Deny Disk Space To Users Exceeding Quota Limit (Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału) i ograniczyć przydział do wartości 500 MB. Na koniec Rooslan powinien przeprowadzić edycję właściwości woluminu, na którym przechowywane są udziały dla pracowników akademickich, przejść do zakładki Quo-tas (Przydział), zaznaczyć pola wyboru Knable Quoia Management (Włącz zarządzanie przydziałami) oraz Deny Disk SpaceTo Users Exceeding QuOta Limit (Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału) i ograniczyć przydział do wartości 800 MB.

2.

Rob zdefiniował schemat przydziałów dysku dla 250 użytkowników partycji serwera plików systemu Windows Server 2003. Dla 30 użytkowników limit wynosi 10 MB, dla 45 limit wynosi 15 MB, dla 100 limit wynosi 30 MB, dla 25 limit wynosi 60 MB, a dla 50 użytkowników limit wynosi 100 MB. W sieci znajdują się jeszcze cztery systemy Windows Server 2003, dla których należy określić identyczny schemat przydziałów dysku. Którą z wymienionych poniżej metod może zastosować Rob do wprowadzenia opisanego schematu przydziałów dysku dla pozostałych czterech serwerów?

- A. Przydziały są stosowane poprzez zasadę grupy. Rob powinien dodać pozostałe cztery serwery do tej samej jednostki organizacyjnej.
- B. Rob powinien wykorzystać konsolę Active Directory Users And Computers (Użytkownicy i komputery usługi Active Directory) do dodania pozostałych czterech serwerów do grupy zabezpieczeń
 - przydziału, która została utworzona dla serwera pierwszego.
- C. /ul.nu.i tego nie można wykonać bez zasrosowania produktu zarządzania przydziałami opracowanego przez innego producenta.
- D. Ustawienia przydziału są przechowywane w rejestrze. Na pierwszym serwerze Rob powinien wyeksportować klucz rejestru odnoszący się do przydziału, a następnie zaimportować ten klucz, do rejestrów pozostałych czterech serwerów.
- E. Na stronie wpisów przydziału Rob powinien zaznaczyć wszystkie 250 wpisów i wyeksportować je do pliku. Następnie Rob powinien skopiować ten plik do pozostałych serwerów i zaimportować go na stronie wpisów przydziału każdej partycji, dla której ma być stosowany ten schemat przydziałów.

3.

Laherty jest konsultantem IT dla niewielkiej firmy zajmującej się projektami graficznymi. W firmie tej system Windows Server 2003 pracuje jako serwer plików, który obsługuje pojedynczy wolumin. Serwer ten jest również serwerem druku i jest podłączony do kolorowej drukarki laserowej, która jest używana do drukowania materiałów o rozmiarach plakatów, jak również jest podłączony do zwykłej drukarki czarno-białej przeznaczonej do drukowania dokumentów takich jak listy czy notatki. Laherty skonfigurował dla tego serwera schemat przydziałów dysku, który zezwala ośmiu użytkownikom firmy

przechowywać pliki zajmujące maksymalnie 8 GB przestrzeni dyskowej. Laherty jest jedyną osobą, która może zmieniać uprawnienia dostępu do serwera plików, a do tej firmy przyjeżdża raz w tygodniu. Podczas wizyty w firmie w piątek, jeden z użytkowników, Rob, poinformował, że od środy nie może wydrukować kilku plakatów. Rob poinformował administratora również o tym, że plakaty te może wydrukować na czarno-białej drukarce. Rob nie próbował na kolorowej drukarce wydrukować innych dużych plików. Laherty sprawdził, że inni użytkownicy mogą normalnie drukować na obu drukarkach i korzystając z ich sysremów można wydrukować plik plakatu Roba. Ponowna próba wydrukowania pliku plakatu przez Roba zakończyła się niepowodzeniem, natomiast okazało się, że Rob może wydrukować nieduże kolorowe zdjęcia. Które z opisanych poniżej powodów najlepiej wyjaśnia, dlaczego Rob nie mógł znowa wydrukować?

- A. Zostały zmienione uprawnienia dla drukarki udostępnionej.
 - B. Dla Roba przydzielony dla drukarki został za bardzo ograniczony.
 - C. Na stacji roboczej Roba (system Windows XP) został nieprawidłowo zainstalowany sterownik **drukarki**.
 - D. Przydzielona **przeźreni** dyskowej na serwerze dla Roba została prawie całkowicie wykorzystana.
 - E. Plik, który Rob próbował wydrukować, został uszkodzony.
 - F. Plik, który Rob próbował wydrukować, nie mieści się w pamięci drukarki.
4. Rooslan jest administratorem w firmie, w której zostały zainstalowane cztery serwery druku. Rooslan chce się dowiedzieć, który z tych serwerów w ciągu dnia realizuje najwięcej, a który najmniej zadań. Informacje takie są potrzebne, ponieważ Rooslan planuje utworzyć nowe drukarki udostępnione i w tym celu chciałby wybrać najmniej obciążony serwer druku. Opióć tego Rooslan chce dowiedzieć się ile stron zostało wydrukowanych licząc od ostatniego uruchomienia. Która z opisanych poniżej metod pozwala Rooslanowi zrealizować to zadanie?
- A. We właściwościach drukarki każdej udostępnionej drukarki na każdym serwerze druku należy sprawdzić statystyki Total Pages Printed Since Last Restart (Całkowita liczba wydrukowanych Stron od ostatniego uruchomienia) oraz Total Jobs Printed Since Last Restart (Całkowita liczba wykonanych zadań od ostatniego uruchomienia).
 - B. Na swojej stacji roboczej Windows XP Rooslan powinien uruchomić konsolę Performance (Wydajność) i dodać obiekt licznika Total Pages Printed (Całkowita liczba wydrukowanych stron) dla wszystkich czterech serwerów druku.
 - C. Na swojej stacji roboczej Windows XP Rooslan powinien uruchomić konsolę Performance (Wydajność) i dodać obiekt licznika Total Jobs Printed (Wszystkie wydrukowane zadania) dla wszystkich czterech serwerów druku.
 - D. Na swojej stacji roboczej Windows XP Rooslan powinien uruchomić konsolę Performance (Wydajność) i dodać obiekty liczników Total Pages Printed (Całkowita liczba wydrukowanych stron) oraz Total Jobs Printed (Wszystkie wydrukowane zadania) dla wszystkich czterech serwerów druku, które mają być monitorowane.

Odpowiedzi do zadania 4.8

1. Prawidłowa odpowiedź: D

- A. **Nieprawidłowo** Przydziały nie mogą być definiowane poprzez edycję właściwości udziału. Przydziały są określane jako właściwości woluminu.

- B. **Nieprawidłowo** Przydziały nie mogą być definiowane poprzez edycję właściwości foldera. Przydziały są określane jako właściwości woluminu.
- C. **Nieprawidłowo** Pomimo, że przydziały określane są we właściwościach woluminu, nie mogą być stosowane do grup, a jedynie do poszczególnych użytkowników lub do całego woluminu.
- D. **Prawidłowo** Przydziały mogą być określane w odniesieniu do woluminu dla poszczególnych użytkowników oraz mogą być stosowane do wszystkich użytkowników wybranego woluminu. Przydziały nie mogą być definiowane dla konkretnych grup zabezpieczeń. Dzięki utworzeniu kopii zapasowej i nowych partycji dysku, dla każdego udziału został zdefiniowany odpowiedni przydział dla użytkowników, którzy wykorzystują dany udział.

2.

Prawidłowa odpowiedź: E

- A. **Nieprawidłowo** Przydziały nie są stosowane poprzez zasadę grupy.
- B. **Nieprawidłowo** Przydziały nie są definiowane poprzez grupy zabezpieczeń.
- C. **Nieprawidłowo** Ustawienia przydziału mogą zostać wyeksportowane do pliku, a następnie zaimportowane na innej partycji.
- D. **Nieprawidłowo** Ustawienia przydziałów nie są określane poprzez eksport i import kluczy rejestru.
- ii. **Prawidłowo** Opisana metoda jest używana do umieszczania przydziałów na innej partycji lub na innym serwerze. W tym celu należy w konsoli Quota F.tries (Wpisy przydziałów) zaznaczyć wszystkie wpisy, które mają zostać wyeksportowane i w menu przydziału wybrać polecenie eksportowania. Następnie należy skopiować plik do miejsca, z którego można go pobrać pracując na innym serwerze i za pomocą jego konsoli Quota Knrries (Wpisy przydziału) z menu Quota (Przydział) wybrać polecenie Import.

Prawidłowa odpowiedź: 1)

3.

- A. **Nieprawidłowo** Nikt oprócz Laherry'ego nie może zmieniać tych uprawnień, a Laherry przyjeżdża do firmy w piątek. Rob nie mógł drukować dużych plików już od środy, CO wskazuje na inną przyczynę problemu.
- B. **Nieprawidłowo** W systemie Windows Server 2003 brak obsługi przydziałów dla **drukarek**.
- C. **Nieprawidłowo** Przyczyna taka jest mało prawdopodobna, ponieważ Rob może drukować nie duże kolorowe zdjęcia.
- D. **Prawidłowo** Przed wysłaniem do drukarki zadania, druku są buforowane. W opisywanej sytuacji serwer ma pojedynczy wolumin, dla którego zastosowane zostały przydziały dysku. Prawdopodobną przyczyną problemów buforowania pliku wydruku jest przekroczenie limitu przydziału dysku.
- E. **Nieprawidłowo** Przyczyna ta jest mało prawdopodobna, ponieważ inni użytkownicy mogą wydrukować ten plik.
- F. **Nieprawidłowo** Przyczyna ta jest mało prawdopodobna, ponieważ inni użytkownicy mogą wydrukować ten plik.

Prawidłowa odpowiedź: D

4.

- A. **Nieprawidłowo** Takie statystyki nie istnieją.
- B. **Nieprawidłowo** Działanie takie gromadzi informacje dotyczące liczby wydrukowanych stron.
- C. **Nieprawidłowo** Działanie takie gromadzi informacje dotyczące liczby wydrukowanych zadań.
- D. **Prawidłowo** Działanie takie gromadzi potrzebne informacje. Rooslan może pozostawić tę konsolę uruchomioną przez pewien czas, aby upewnić się, że pokazywane wyniki są dokładne. Może również w tym czasie zatrzymać i ponownie uruchomić serwery, ale istotnie długa przerwa w działaniu powoduje zafałszowanie wyników.

Zadanie 4.9 Zarządzanie serwerem sieci Web

Program Internet Information Services (Internetowe usługi informacyjne) w wersji 6 jest dostarczany razem z systemem Windows Server 2003, ale program ten nie jest instalowany w sposób domyślny. Dostępna jest również wersja systemu Windows Server 2003, która została opracowana specjalnie dla obsługi stron sieci Web. Wersja ta nosi nazwę Web Edition. Podstawowym zadaniem programu IIS jest obsługa Stron sieci Web, obojętnie czy dostęp do nich uzyskiwany jest poprzez sieć Internet czy lokalnie (w sieci LAN). Program IIS ma jednak o wiele szersze zastosowania. IIS może być wykorzystywany jako platforma obsługi usług .NET Web, Windows Media, certyfikatów oraz usług administracji zdalnej HTML systemu Windows Server 2003. Program IIS obsługuje także serwisy FTP używane do transferu plików pomiędzy hostami zdalnymi a serwerami. Program IIS jest również wykorzystywany do obsługi protokołu NNTP (Network News Transfer Protocol), umożliwiając na serwerach obsługę grup dyskusyjnych, które mogą być odczytywane przez klientów programów takich jak Outlook Express, czy klientów innych grup dyskusyjnych.

Konfiguracja dostępu do programu IIS może być zrealizowana w różny sposób. Dostęp może być ograniczony lub przydzielony w oparciu o adres IP, nazwę DNS lub adres sieci (Network Address). Dostęp może być również ograniczony tylko dla tych Stacji, które mają prawidłowy certyfikat lub dla tych stacji, które zostały uwierzytelnione w systemie Windows, CO ogranicza dostęp do użytkowników mających konta w systemie lub domenie. Te formy ograniczeń nie wykluczają się wzajemnie, to znaczy przykładowo klient może być proszony o podanie tożsamości, nawet jeśli wykorzystuje stację znajdującą się w dopuszczonym zakresie adresów sieci.

Liczba połączeń do witryn sieci Web może być również ograniczana. Podejście takie jest przydatne z kilku powodów. Po pierwsze uniemożliwia obciążenie serwera obsługującego zbyt wielu użytkowników. Po drugie redukuje wpływ serwera sieci Web na połączenia internetowe w przypadku ogromnego ruchu.

Pytania do zadania 4.9

1. Rooslan jest administratorem systemu Windows Server 2003, na którym uruchomiony jest program IIS (Internet Information Services). Na serwerze utrzymywana jest pojedyncza witryna sieci Web, która zawiera poufne informacje dotyczące firmy. Dostęp do tych informacji mogą uzyskiwać jedynie stacje umieszczone w konkretnych podsięciach korporacyjnej sieci rozległej WAN. Rooslan powinien umożliwić dostęp do serwera dla hostów wykorzystujących adresy IP znajdujące się w następujących zakresach:

Od 10.10.10.1 do 10.10.10.126

Od 10.10.10.129 do 10.10.10.190

Od 10.10.20.225 do 10.10.20.238

Od 10.10.30.193 do 10.10.30.254

Rooslan przeprowadza edycję domyślnych właściwości witryny sieci Web i na zakładce Directory Security (Zabezpieczenia katalogów) kliknął przycisk Edit (Edytuj) znajdujący się w ramce IP Address And Domain Name Restrictions (Ograniczenia adresów IP i nazw domen). Rooslan zaznaczył opcję Denied Access (Odmówiony dostęp), a następnie kliknął przycisk Add, aby utworzyć listę wyjątków. Które z wymienionych poniżej identyfikatorów sieci (Network ID) oraz masek podsieci (Subnet Mask) powinien wprowadzić Rooslan, aby umożliwić dostęp jedynie dla adresów IP objętych zakresami wyspecyfikowanymi w zadaniu? (wybierz wszystkie właściwe odpowiedzi)

- A. Identyfikator sieci: 10.10.10.0, maska podsieci: 255.255.255.128
- B. Identyfikator sieci: 10.10.10.0, maska podsieci: 255.255.255.0
- C. Identyfikator sieci: 10.10.10.128, maska podsieci: 255.255.255.64
- D. Identyfikator sieci: 10.10.10.128, maska podsieci: 255.255.255.192
- E. Identyfikator sieci: 10.10.20.224, maska podsieci: 255.255.255.224
- E Identyfikator sieci: 10.10.20.224, maska podsieci: 255-255-255.240
- G. Identyfikator sieci: 10.10.30.192, maska podsieci: 255.255.255.192

2.

Oksana obawia się, że nowa witryna sieci Web, którą ma uruchomić, szybko przeciąży używane w firmie łącze do sieci Internet. Witryna sieci Web będzie utrzymywana w oparciu o system Windows Server 2003, na którym uruchomiony został program MS 6.0 i będzie można z niej pobierać Strumieniowe dane oraz pliki. Oksana konsultowała się z administratorem sieci, który Sugerował, że witryna sieci Web będzie powodowała poważnych problemów może zajmować maksymalnie 2 MBps pasma dostępnego dla firmy. Oprócz tego, Oksana chce również ograniczyć maksymalną liczbę użytkowników łączących się do witryny sieci Web do 200 jednoczesnych połączeń. Która z opisanych poniżej metod pozwoli Oksanie wprowadzić przedstawione powyżej ograniczenia ruchu witryny sieci Web? (wybierz wszystkie właściwe odpowiedzi)

- A. Oksana powinna przeprowadzić edycję właściwości sieci systemu Windows Server 2003, IM którym utrzymywana jest witryna sieci Web i zmienić wartość maksymalnej prędkości wyjściowej na 2,048 kilobajta (kB) na sekundę.
- B. Oksana powinna przeprowadzić edycję właściwości witryny sieci Web. Na zakładce Performance (Wydajność) powinna w ramce Bandwidth throttling (Ograniczanie przepustowości) zaznaczyć pole wyboru limit "The Network Bandwidth Available To this Web Site (Ogranicz przepustowość sieci dostępną dla witryny sieci Web) i wpisać w polu Maximum Bandwidth (in KB per second) [Maksymalna przepustowość (przepustowość w kilobajtach na sekundę)] liczbę 2.
- C. Oksana powinna przeprowadzić edycję właściwości witryny sieci Web. Na zakładce Performance (Wydajność) powinna zaznaczyć pole wyboru Limit the Network Bandwidth Available to this Web Site (Ogranicz przepustowość sieci dostępną dla witryny sieci Web) i wpisać w polu Maximum Bandwidth (in KB per second) [Maksymalna przepustowość (przepustowość w kilobajtach na sekundę)] liczbę 2000,000.
- D. Oksana powinna przeprowadzić edycję właściwości witryny sieci Web. Na zakładce Performance (Wydajność) powinna zaznaczyć pole wyboru Limit The Network Bandwidth Available To This Web Site (Ogranicz przepustowość sieci dostępną dla witryny sieci Web) i wpisać w polu Maximum Bandwidth (in KB per second) [Maksymalna przepustowość (przepustowość w kilobajtach na sekundę)] liczbę 2048.
- E. Oksana powinna przeprowadzić edycję właściwości witryny sieci Web. Na zakładce Performance (Wydajność) powinna zaznaczyć opcję Połączenia witryny sieci Web i w polu Connections Limited To (Połączenia ograniczone do) wpisać wartość 100.

F. Oksana powinna przeprowadzić edycję właściwości witryny sieci Web. Na zakładce Performance (Wydajność) powinna zaznaczyć opcję Połączenia witryny sieci Web i w polu Connections Limited To (Połączenia ograniczone do) wpisać wartość 200.

«j. Określając właściwości domyślnej witryny sieci Web (Default Web Site) autonomicznego serwera systemu Windows Server 2003 (uruchomiony program IIS), w ramce Authentication Methods (Metody uwierzytelnienia) na zakładce Directory Security (Zabezpieczenia katalogu) administrator usunął zaznaczenie pola wyboru Enable Anonymous Access (Włącz dostęp anonimowy). Które z wymienionych poniżej metod uwierzytelnienia będą dostępne dla użytkowników? (wybierz wszystkie właściwe odpowiedzi)

- A. Integrated Windows Authentication (Zintegrowane uwierzytelnienie systemu Windows)
- B. Digest Authentication (Uwierzytelnienie szyfrowane)
- C. Basic Authentication (Uwierzytelnienie podstawowe)
- D. .NET Passport Authentication (Uwierzytelnienie usługi Passport w sieci -NET)

4. Administrator opiekuje się witryną sieci Web systemu Windows Server 2003 utrzymywaną przez dostawcę usług internetowych ISP. Administrator chce utrzymywać na tym serwerze kilka innych witryn, ale dostawca ISP nie jest w stanie przydzielić do serwera dodatkowych publicznych adresów IP. Publiczny adres IP przydzielony do serwera to 207.46.248.234. Administrator chce dodatkowo utrzymywać następujące witryny:

w wio. adatum. com

wurw.alpineskihouie.com

www.proseware. com www.

taihpinloys. com

Każda winyna zawiera różne dane, zupełnie niepowiązane z innymi witrynami. Które z wymienionych poniżej **procedur** należy wykonać, aby rozwiązać opisany problem? (wybierz dwie odpowiedzi - każdy wybór jest częścią prawidłowego rozwiązania)

- A. Należy skonfigurować serwer DNS, który będzie obsługiwał rekordy dla witryn wunu.adatum.com, uiuw.alpineskihoisc.com, www.proseware.com oraz unuw.taihpinloys.com tak, aby rekordy te określałyby adres IP: 207.46.248.234.
- B. Należy skonfigurować serwer DNS, który będzie obsługiwał rekordy dla witryn www.ariatum.com, www.alpinskihouse.com, www.proscwarc.com oraz, www.tailspintoys.com tak, aby rekordy te były określane przez adres IP: 207-46.234.248.
- C. Należy utworzyć cztery odrębne witryny sieci Web wivw.aJalurn.com, www.alpineskihouse.com, www.proseware.com oraz www.tailspintoys.com. W programie Web Site Creation Wizard (Kreator tworzenia witryny sieci Web) należy zdefiniować adres IP każdej witryny wpisując 207.46.248.234. Jako nagłówek hosta każdej witryny sieci Web należy wpisać odpowiednią nazwę witryny. W ścieżce katalogu macierzystego każdej witryny sieci Web należy wpisać c:\inetpub\wwwroot. Następnie należy wyłączyć domyślną witrynę sieci Web (Default Web Site).
- D. Należy utworzyć cztery odrębne witryny sieci Web www.adatum.com, www.alpineskihouse.com, www.proseware.com oraz www.tailspintoys.com. W programie Web Site Creation Wizard (Kreator tworzenia witryny sieci Web) należy zdefiniować adres IP każdej witryny wpisując 207.46.234.248. Jako nagłówek hosta każdej witryny sieci Web należy wpisać odpowiednią nazwę witryny. W ścieżce katalogu macierzystego każdej witryny sieci Web należy wpisać poszczególne katalogi, w których

umieszczone zostały odpowiednie dane każdej witryny sieci Web. Następnie należy wyłączyć domyślną witrynę sieci Web (Default Web Site).

- E. Należy utworzyć cztery odrębne witryny sieci Web uiww.adatum.com, www.alpineskihouse.com, www.proseivare.com oraz www.tailspintoys.com. W programie Web Site Creation Wizard (Kreator tworzenia witryny sieci Web) należy zdefiniować adres IP każdej witryny wpisując 207.46.248. 234. Jako nagłówek hosta każdej witryny sieci Web należy wpisać odpowiednią nazwę witryny. W ścieżce katalogu macierzystego każdej witryny sieci Web należy wpisać poszczególne katalogi, w których umieszczone zostały odpowiednie dane każdej witryny sieci Web. Następnie należy wyłączyć domyślną witrynę sieci Web (Default Web Site).

Odpowiedzi do zadania 4.9

1. Prawidłowe odpowiedzi: A, D, F oraz G

- A. Prawidłowo Wpis ten dopuszcza dostęp do witryny sieci Web dla pierwszego zestawu adresów - od 10.10.10.1 do 10.10.10.126. Adres 10.10.10.127 jest adresem rozgłoszeniowym (broadcast) dla tej podsieci i tym samym nie jest przypisany do żadnego hosta rozległej sieci kooperatoracyjnej WAN.
- B. Nieprawidłowo Wpis taki zezwala na dostęp dla I tostów o adresach / zakresu od 10.10.10.224 do 10.10.10.254, a dla takiego zakresu adresów dostęp witryny sieci Web nie powinien być przy
dzienny.
- C. Nieprawidłowo W tym przypadku nieprawidłowa jest maska podsieci. Dziesięć maski pod
sieci mogą przyjmować wartości 0, 128, 192, 224, 240, 248, 252, 254 oraz 255.
- D. Prawidłowo Wpis ten dopuszcza dostęp do witryny sieci Web dla drugiego zestawu adresów
- Od 10.10.10.129 do 10.10.10.190. W tym schemacie podzali, na podsieci adres 10.10.10.128
jest adresem siei i i tym samym nie jesi adresem hosta. AdICS 10.10.10.190 jest adresem rozgłosze
iiiowym (broadcast) i dlatego nie jesi przydzielany do hosta.
- E. Nieprawidłowo Wpis taki zezwala na dostęp do witryny sieci Web dla hostów o adresach
z zakresu od 10.10.20.225 do 10.10.20.255.
- F. Prawidłowo Wpis ten dopuszcza za dostęp do witryny siec i Web dla trzei iego zestawu adresów-od.
10.10.20.225 do 10.10.20.238. Adres 10.10.20.224 jesi adresem sieci, a adres 10.10.20.238 jest
adresem rozgłoszeniowym dla tego konkretnego schematu podziału na podsieci.
- G. Prawidłowo Wpis ten dopuszcza dostęp do witryny sieci Web dla czwartego zestawu adresów
- od, 10.10.30.193 do 10.10.30.254. Adres 10.10.30.192 jest adresem sieci, a adres 10.10.30.254
jest adresem rozgłoszeniowym dla tego konkretnego schematu podziału na podsieci.

- td. Prawidłowe odpowiedzi: D oraz F

- A. Nieprawidłowo Wykorzystanie pasma kart sieciowych nie może być kontrolowane przez właści
wości sieci.
- B. Nieprawidłowo Spowoduje to ograniczenie ruchu do 2 KB, a nie do 2 MB.
- C. Nieprawidłowo Pasma zostanie ograniczone do przybliżonej wartości 1,953 MB na sekundę.
- D. Prawidłowo 2048kB to to samo co 2 MB. Pasma zostanie ograniczone do wartości 2 MB
na sekundę.

D. Nieprawidłowo Działanie takie ograniczy liczbę jednoczesnych połączeń do 100, a nie do 200.

F. Prawidłowo Działanie takie, zgodnie z wymogami zadania, ogranicza liczbę jednoczesnych połączeń do 200.

O. Prawidłowe odpowiedzi: A, C oraz D

A. Prawidłowo Metoda ta jest dostępna i korzysta z koni utworzonych w autonomicznym serwerze systemu Windows Server 2003.

B. Nieprawidłowo Opcja ta jest dostępna, o ile system Windows Server 2003 znajduje się w środowisku usługi Active Directory. Ponieważ system jest autonomiczny i tym samym nie należy do domeny, opcja ta nie może być użyta.

C. Prawidłowo Ta opcja jest dostępna i działa z większością przeglądarek. Wadą tej metody jest przesyłanie informacji związanych z uwierzytelnieniem za pomocą zwykłego tekstu, a nie w postaci zaszyfrowanej.

D. Prawidłowo Ta metoda uwierzytelnienia jest dostępna, chociaż wymaga dalszej konfiguracji ze strony administratora.

4. Prawidłowe odpowiedzi: A oraz E

A. Prawidłowo Jest to pierwsza część prawidłowej odpowiedzi.

B. Nieprawidłowo Wybrany został nieprawidłowy adres IP* w którym zastąpione zostały miejscami ilw.i ostatnie oktety.

C Nieprawidłowo Działanie takie- będzie powodować, że wszystkie witryny sieci Web będą kierowane do tych samych danych, a nie do odrębnych zawartości.

D. Nieprawidłowo Wybrany został nieprawidłowy adres IP, w którym zostały zastąpione miejscami dwa ostatnie oktety.

E. Prawidłowo W opisanym rozwiązaniu wybrany został prawidłowy adres IP i zostały Wskazane odpowiednie katalogi kierujące do unikatowych danych poszczególnych witryn sieci Web.

18 Zarządzanie i wprowadzanie metod odzyskiwania danych po awarii (5.0)



Awarie będą się zdarzały. Dyski popsują się, pliki zostaną zagubione, a w zasilaczu przepali się bezpiecznik, oznajmiając to zdarzenie kilkoma iskrami i kłębkami gryzącego dymu. Administratorzy systemów nie powinni beczynie oczekiwać, aż zdarzy się awaria i dopiero wtedy określać sposób działania. Zanim nastąpi uszkodzenie administrator powinien zaplanować i wdrożyć procedury, które przywrócą działanie systemu tak szybko, jak jest to możliwe.

Pierwszym krokiem procedury ochrony danych przechowywanych w systemie Windows Server 2003 jest prawidłowo wykonana kopia zapasowa. System Windows Server 2003 został wyposażony w aplikację umożliwiającą administratorowi wykonywanie większości zadań związanych z tworzeniem kopii zapasowych. Kopie zapasowe najważniejszych systemów powinny być wykonywane co 24 godziny, a w niektórych przypadkach nawet częściej. Kopie zapasowe powinny być zapisywane na różnych typach nośników.

System Windows Server 2003 został wyposażony w nową dla tej linii produktów, funkcję automatycznego odzyskiwania systemu ASR (Automated System Recovery). Funkcja ASR może być wykorzystywana do odtworzenia całkowicie niesprawnego systemu. Funkcja ASR zapisuje niektóre informacje konfiguracyjne na specjalnej dyskiecie oraz pozostałe informacje w zestawie kopii zapasowej ASR. Funkcja automatycznego odzyskiwania systemu przywraca jedynie system. Dane przechowywane w systemie nie zostaną odtworzone i dla nich musi być wykonywana zwykła kopia zapasowa.

Jeśli awarii ulega dysk, równie ważnym zagadnieniem dla administratorów jest opanowanie umiejętności naprawy woluminu odpornego na uszkodzenia za pomocą konsoli Disk Management (Zarządzanie dyskami). Proces odtworzenia woluminu dublowanego różni się od procedury przywracania woluminu RAID-5. Administratorzy powinni testować konfiguracje odporne na uszkodzenia poprzez wyłączanie dysków i sprawdzanie, czy system operacyjny w dalszym ciągu sprawnie funkcjonuje.

Ostatnim istotnym zagadnieniem jest możliwość poprawnego odtworzenia plików i folderów na podstawie kopii zapasowych. Jeśli stosowana jest kopia przyrostowa lub różnicowa, ogólnie mówiąc, najpierw należy odtworzyć starsze zestawy kopii zapasowych, a następnie zastąpić dane nowszymi zestawami kopii zapasowych.

Sprawdzanie umiejętności i sugerowane ćwiczenia praktyczne

Poniżej przedstawiono umiejętności potrzebne do opanowania tematu „Zarządzanie i wprowadzanie metod odzyskiwania danych po awarii” objętego *egzaminem 70-290 -Zarządzanie i obsługa środowiska Windows Server 2003*:

- Przywracanie systemu serwera.
 - » Zadanie kontrolne 1: Wykonanie kopii zapasowej ASR serwera, a następnie wykorzystanie procesu ASR do przywrócenia systemu tego serwera.
 - » Zadanie kontrolne 2: Wykonanie kopii zapasowej danych o stanie systemu (System State) serwera, na którym został zainstalowany program IIS (Internet Information Services). Zmiana ustawień programu IIS. Odtworzenie danych o stanie systemu (System State) i zwrócenie uwagi, jakie zmiany nastąpiły w ustawieniach programu IIS.
- Zarządzanie procedurami wykonywania kopii zapasowych.
 - » Zadanie kontrolne 1: Wykorzystywanie różnego rodzaju nośników, takich jak napędy taśmowe, lokalne dyski twarde czy magazyny sieciowe do przechowywania zestawów kopii zapasowych.
 - » Zadanie kontrolne 2: Utworzenie kilku różnych kopii zapasowych i zapisywanie ich na lokalnym dysku twardym. Na zakładce Restore and Manage Media (Przywracanie i zarządzanie nośnikiem) należy usunąć każdy z katalogów skojarzonych z odpowiednim plikiem. Następnie należy kliknąć prawym przyciskiem myszy plik i wybrać polecenie Catalog Pile (Plik katalogu). Należy wyszukać inną kopię zapasową i zezwolić na ponowne utworzenie katalogu.
- Przywracanie po awarii urządzeń sprzętu serwera.
 - » Zadanie kontrolne 1: Utworzenie dublowanego woluminu rozruchowego bądź systemowego. Ponowne uruchomienie systemu Windows Server 2003 bez zestawu dublowanego.
 - » Zadanie kontrolne 2: Utworzenie zestawu RAID-5 za pomocą konsoli Disk Management (Zarządzanie dyskami). Zapisanie pewnych danych na woluminie, który jest obsługiwany przez zestaw RAID-5. Wyłączenie jednego z dysków zestawu RAID-5, a następnie ponowna aktywacja zestawu. Naprawa zestawu RAID-5.
- Przywracanie danych kopii zapasowej.
 - » Zadanie kontrolne 1: Ćwiczenia praktyczne dotyczące odtwarzania, na podstawie pełnej kopii zapasowej, konkretnych zestawów plików i folderów w oddzielnej lokalizacji na serwerze.
 - »> Zadanie kontrolne 2: Przygotowanie pełnej kopii zapasowej i trzech przyrostowych, wykonanych po pełnej kopii zapasowej. Odtworzenie kopii we właściwej kolejności w innej lokalizacji foldera tak, aby starsze pliki nie zastąpiły nowszych.
- Harmonogram zadań wykonywania kopii zapasowych.
 - » Zadanie kontrolne 1: Utworzenie zadania kopii zapasowej i zaplanowanie jego uruchamiania codziennie.
 - » Zadanie kontrolne 2: Utworzenie zadania kopii zapasowej, które wykonuje pełną kopię zestawu plików i folderów raz w tygodniu. Utworzenie drugiego zadania kopii zapasowej, które wykonuje kopię przyrostową tego samego zestawu plików i folderów we wszystkie pozostałe dni tygodnia.

Lektura uzupełniająca

Przed przystąpieniem do egzaminu należy przestudiować przedstawione poniżej dodatkowe źródła informacji.

Zadanie 5.1

Rozdział 13 „Odzyskiwanie systemu po awarii”.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Dane o stanie systemu”.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Automatyczne odzyskiwanie systemu. Przegląd”.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Kopiowanie w tle woluminu. Przegląd”.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Przywracanie autorytatywne, podstawowe i normalne”.

Zadanie 5.2

Rozdział 7 „Tworzenie kopii zapasowych danych”

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Obsługa nośników”.

Zadanie 5.3

Rozdział 11 lekcja 4: „Implementacja macierzy dyskowych RAID”.

Rozdział 13 „Odzyskiwanie systemu po awarii”.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Zastępowanie uszkodzonego zestawu dublowanego nowym”.

Zadanie 5.4

Rozdział 7 lekcja 2: „Odzyskiwanie danych” oraz lekcja 3: „Zaawansowane funkcje tworzenia kopii zapasowych i odzyskiwania danych”.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Odzyskiwanie danych”.

Zadanie 5.5

Rozdział 7 lekcja 3: „Zaawansowane funkcje tworzenia kopii zapasowych i odzyskiwania danych”.

Microsoft Corporation. Windows Server 2003 Help and Support Center (Centrum pomocy i obsługi technicznej). Temat: „Planowanie kopii zapasowych”.

Zadanie 5.1

Przywracanie systemu serwera

W sytuacji, kiedy po awarii systemu Windows Server 2003 nie pomaga proste ponowne jego uruchomienie, muszą być zastosowane inne sposoby przywrócenia funkcjonalności systemu. Nową opcją systemu Windows Server 2003 jest funkcja Attomarc System Recovery (Automatyczne odzyskiwanie systemu) używana w połączeniu z dyskiecią zawierającą ustawienia systemu Windows, specjalnym zestawem kopii zapasowej ASR oraz nośnikiem instalacji innego systemu Windows Server 2003, na podstawie którego odzyskiwany jest system. Metoda ASR powinna być stosowana w ostateczności, gdyż w trakcie jej przeprowadzania następuje ponowna instalacja plików systemu operacyjnego. Warto zapamiętać, że kopia zapasowa ASR nie obejmuje danych przechowywanych na serwerze, a jedynie w.r/ne pliki systemu Windows Server 2003.

Podczas przywracania systemu kontrolera domeny administrator musi zdecydować, jaki zostanie zastosowany rodzaj odzyskiwania usługi katalogowej. Przywracanie autorytatywne bazy danych usługi katalogowej Microsoft Active Directory zapisanej w postaci zestawu kopii zapasowej ma pierwszeństwo w odniesieniu do bazy danych usługi katalogowej replikowanej w domenie. Typ nieautorytatywnego odzyskiwania powoduje, że bieżąca baza danych usługi Active Directory zastąpi bazy danych odzyskaną na podstawie kopii zapasowej.

W niektórych przypadkach odzyskiwanie danych o stanie systemu (System State) pozwala na przywrócenie funkcjonalności i serwera. Zestaw danych o stanie systemu zawiera między innymi rejestry systemu i bazy danych (X)M i (lass) Registration. Pliki rozruchowe są chronione przez usługi Windows File Protection (Mirona plików systemu Windows). W zależności od zainstalowanych usług w systemie Windows Server 2003 dane o stanie systemu mogą zawierać również bazy danych usług, certyfikatów (Certificate Services), bazy danych usługi Active Directory oraz Folder Sysvol w przypadku kontrolera domeny, informacje o usługach klasą w przypadku serwera klastrów oraz metabazę programu IIS (Internet Information Services). Jeśli jeden z tych obszarów działania serwera został uszkodzony, przywrócenie danych o stanie systemu może przywrócić funkcjonowanie systemu serwera.

Pytania do zadania 5.1

1. Rooslan jest administratorem sieci przedsiębiorstwa średniej wielkości, które ma 400 pracowników zatrudnionych w dwóch lokalizacjach. Codziennie o godzinie 2:00 wykonywana jest pełna kopia zapasowa trzech kontrolerów domeny systemu Windows Server 2003, wliczając w to dane o stanie systemu. Pewnego dnia rano Foley, który jest pomocnikiem Rooslana, przypadkowo usunął trzy jednostki organizacyjne usługi Active Directory. Foley nie zauważył pomyłki przez kilka godzin, a w tym czasie pomyłkowe zmiany zostały replikowane do pozostałych kontrolerów domeny. W ciągu ostatnich 24 godzin w usłudze katalogowej nie zostały dokonane żadne inne modyfikacje i dlatego Rooslan zdecydował się przywrócić dane o stanie systemu na podstawie kopii zapasowej wykonanej o godzinie 2:00. Który typ odzyskiwania przywróci w bazie danych usługi Active Directory trzy usunięte jednostki organizacyjne?

A- Przywracanie autorytatywne

- B. Przywracanie nieautorytatywne
- C. Przywracanie podstawowe
- D. Przywracanie natychmiastowe

2.3. Rooslan odebrał telefon od swojego mocno wystraszonego pomocnika Foleya, z którym współpracuje opiekując się siecią w przedsiębiorstwie średniej wielkości. Foley przypadkowo usunął z bazy danych usługi Active Directory jednostkę organizacyjną kont użytkowników dyrekcji. Zanim Foley mógł naprawić błąd, kontrolery domeny przeprowadziły replikację i zmiana została rozesłana w całej sieci. Kopia zapasowa danych o stanie systemu dla wszystkich kontrolerów domeny wykonywana jest codziennie o godzinie 2:00. Ponieważ dzisiaj żadne inne zmiany nie zostały dokonane w bazie danych usługi katalogowej, Rooslan polecił, aby Foley na jednym z kontrolerów domeny przygotował proces przywracania autorytatywnego. Rooslan odszukał w serwerowni nośnik ostatniej kopii zapasowej, a następnie wyłączył jeden z kontrolerów domeny systemu Windows Server 2003. W jakim trybie Rooslan powinien uruchomić kontroler domeny systemu Windows Server 2003?

- A. Kontroler domeny systemu Windows Server 2003 powinien być uruchomiony przy użyciu opcji Last Known Good Configuration (Ostatnia znana dobra konfiguracja).
- B. Kontroler domeny Systemu Windows Server 2003 powinien być uruchomiony przy użyciu opcji Safe mode (Tryb awaryjny).
- C. Kontroler domeny systemu Windows Server 2003 powinien być uruchomiony przy użyciu opcji Recovery Console (Konsola odzyskiwania).
- D. Kontroler domeny systemu Windows Server 2003 powinien być uruchomiony w normalnym trybie.
- E. Kontroler domeny systemu Windows Server 2003 powinien być uruchomiony przy użyciu opcji Directory Services Restore (Odzyskiwanie usługi katalogowej).

Administrator opiekuje się pięcioma systemami Windows Server 2003, które są serwerami członkowskimi w domenie. Te pięć serwerów, w oparciu o program IIS (Internetowe usługi informacyjne) utrzymuje różne witryny sieci Web. W każdym serwerze zostały zainstalowane dwa dyski twarde. Na pierwszym dysku znajduje się wolumin przechowujący pliki systemu operacyjnego i programów. Na drugim dysku zainstalowany jest wolumin przechowujący wszystkie dane witryny sieci Web. Kopia zapasowa danych witryny sieci Web oraz danych o stanie systemu (System State) jest wykonywana co 24 godziny i zapisywana na serwerze plików w sieci. Wszystkie ustawienia witryny sieci Web, takie jak uprawnienia zabezpieczeń czy ograniczenia dostępu domeny, są inne dla każdej witryny.

Dzisiaj rano awarii uległ dysk twardy systemu operacyjnego jednego z serwerów IIS. Drugi dysk, przechowujący dane witryny sieci Web, jest w pełni sprawny. Administrator pobrał z magazynu dysk zapasowy, zainstalował na nim system Windows Server 2003 oraz programy, które były zainstalowane na serwerze. Którą z wymienionych poniżej metod może zastosować administrator do przywrócenia funkcjonalności serwera sprzed jego awarii? (wybierz wszystkie właściwe odpowiedzi)

- A. Wszystkie funkcje serwera zostały już przywrócone i nie są wymagane żadne dodatkowe czynności.
- B. Na podstawie kopii zapisanych w folderze udostępnionym w sieci, do odtworzenia plików zawierających witryny sieci Web należy użyć programu Backup Utility (Kopia zapasowa). Pliki te należy przywrócić na drugim dysku twardym serwera IIS.
- C. Dla serwera IIS należy zastosować tryb Directory Services Restore (Odzyskiwanie usługi katalogowej), aby przywrócić dane o stanie systemu (System State) na podstawie kopii zapasowych przechowywanych w folderze udostępnionym w sieci.

- ' D. Po zalogowaniu w serwerze IIS, który jest odtwarzany, z foldera udostępnionego w sieci należy wgrać najnowszą kopię zapasową na lokalny dysk twardy. Następnie, na podstawie tej kopii, należy przywrócić dane o stanie systemu (System State) i jeśli jest to wymagane, ponownie uruchomić serwer.
- E. Po zalogowaniu w serwerze IIS, który jest odtwarzany, należy za pomocą programu Backup Utility (Kopia zapasowa) odtworzyć dane o stanie systemu (System State) na podstawie kopii przechowywanej w lokalizacji sieciowej i jeśli jest to wymagane, ponownie uruchomić serwer.

4.

Które z wymienionych poniżej stwierdzeń są prawdziwe w odniesieniu do odtwarzania autonomicznego głównego urzędu certyfikatu (CA), spowodowanego uszkodzeniem dysku twardego zawierającego wolumin, na którym przechowywane był system operacyjny i baza danych certyfikatów?

- A. Baza danych certyfikatów może być odtwarzana jedynie za pomocą przystawki Certification Authority (Urząd certyfikacji).
- B. Jeśli została uszkodzona lub zgubiona baza danych programu CA, to podczas jej przywracania meta-baza programu IIS musi również zostać odtworzona.
- C. Podczas przywracania danych o stanie systemu na serwerze utrzymującym autonomiczny urząd certyfikacji CA, musi być wprowadzone hasło.
- D. I hasło musi zostać wprowadzone, jeśli odtwarzane są następujące elementy: Private Key (klucz prywatny), CA Certificate (urząd certyfikacji CA), Certificate Database (baza danych certyfikacji) oraz Certificate Database log (dziennik bazy danych certyfikacji), dla których kopia zapasowa została wykonana za pomocą przystawki Certification Authority (Urząd certyfikacji) konsoli MMC (Microsoft Management Console).
- E. Baza danych certyfikacji jest przywracana podczas wykonywania procedur ASR (Automatyczne odzyskiwanie systemu).

5.

Włamywać-/ uzyskał dostęp do serwera sieci Web i usunął lub uszkodził wiele istotnych plików systemu Windows Server 2003- Po przyjrzeniu się uszkodzeniom, administrator doszedł do wniosku, że są one bardzo poważne i musi wykorzystać konsolę odzyskiwania, aby przywrócić funkcjonalność serwera. Cztery dni temu administrator przygotował serwer pod kątem procedury automatycznego odzyskiwania systemu. Która z wymienionych poniżej metod przedstawia właściwy sposób uruchomienia funkcji automatycznego odzyskiwania systemu?

- A. Należy ponownie uruchomić serwer przy użyciu dyskietki ASR przygotowanej cztery dni temu w trybie Directory Services Restore (Odzyskiwanie usługi katalogowej).
- B. Należy ponownie uruchomić serwer przy użyciu instalacyjnego dysku CD-ROM systemu Windows Server 2003 i odpowiednim momencie umieścić w napędzie dyskietkę ASR, która została przygotowana cztery dni temu.
- C. Należy ponownie uruchomić serwer w trybie Safe (tryb awaryjny) i w odpowiednim momencie umieścić w napędzie dyskietkę ASR, która została przygotowana cztery dni temu.
- D. Należy uruchomić serwer w trybie Directory Services Restore (Odzyskiwanie usługi katalogowej) i w odpowiednim momencie umieścić w napędzie dyskietkę ASR, która została przygotowana cztery dni temu.
- E. Należy uruchomić konsolę Recovery (Konsola odzyskiwania) i w odpowiednim momencie umieścić w napędzie dyskietkę ASR, która została przygotowana cztery dni temu.

- 6.** Oksana jest pomocnikiem administratora w przedsiębiorstwie i opiekuje się dwoma systemami Windows Server 2003, na których zainstalowany jest program IIS (Internetowe usługi informacyjne). Każdy serwer obsługuje pojedynczą witrynę sieci Web, każda o innej konfiguracji. Te odrębne konfiguracje dotyczą list hostów, dla których dopuszczony i zabroniony został dostęp, jak również list dostępu dla kont. W obu systemach Windows Server 2003 program IIS został zainstalowany w lokalizacji domyślnej. Oksana zadzwoniła do przełożonego informując go, że na jednym z serwerów IIS wirus usunął 95% danych witryny sieci Web, jak również uszkodził metabazę IIS. System został wyczyszczony za pomocą uaktualnionego skanera antywirusowego, który usunął wszystkie ślady zainfekowanych plików. Jednakże kilka obszarów systemu zostało uszkodzonych wskutek działania wirusa, co powoduje bardzo niestabilną pracę systemu. Główne aktualizacje różnych obszarów witryny sieci Web przeprowadzane zostały w ciągu tygodnia. Dzisiaj jest piątek. W minionym tygodniu Oksana wykonała następujące zadania związane z odzyskiwaniem serwera po ewentualnej awarii.

Czwartek: Kopia zapasowa ASR (Automatyczne odzyskiwanie systemu).

Środa: Przyrostowa kopia zapasowa danych witryny sieci Web.

Wtorek: Przyrostowa kopia zapasowa danych witryny sieci Web.

Poniedziałek: Kopia zapasowa danych o stanie systemu (System State).

Niedziela: Pełna kopia zapasowa danych witryny sieci Web.

Wszystkie ważne nośniki kopii zapasowych są do dyspozycji. Którą z wymienionych poniżej metod powinna zastosować Oksana, aby odtworzyć metabazę programu IIS oraz dane witryny sieci Web?

- A. Oksana musi wykonać jedynie procedurę ASR (Automatyczne odzyskiwanie systemu).
- B. Oksana musi przeprowadzić procedurę ASR (Automatyczne odzyskiwanie systemu). Po jej zakończeniu powinna odtworzyć dane na podstawie kopii zapasowej wykonanej w środę.
- C. Oksana musi przeprowadzić procedurę ASR (Automatyczne odzyskiwanie systemu). Po jej zakończeniu powinna odtworzyć dane na podstawie kopii zapasowych wykonanych w niedzielę, wtorek i środę.
- D. Oksana musi odtworzyć dane na podstawie poniedziałkowej kopii zapasowej danych o stanie systemu, pełnej kopii zapasowej wykonanej w niedzielę oraz przyrostowej kopii zapasowej wykonanej w środę.
- E. Oksana musi odtworzyć poniedziałkową kopię zapasową danych o stanie systemu, pełną kopię zapasową wykonaną w niedzielę oraz przyrostowe kopie zapasowe wykonane we wtorek i środę.

- 7.** W serwerowni wybuchł pożar. Zniszczeniu uległy wszystkie dyskiety ASR, natomiast jednostka pamięciowa zawierająca taśmy kopii zapasowych pozostała nienaruszona. Trzy systemy Windows Server 2003 zostały zniszczone, na szczęście dwa inne serwery pozostały nietknięte. Każdy system Windows Server 2003 wyposażony był w napęd taśm DAT o pojemności 40 GB. Pełna kopia ASR każdego serwera została wykonana kilka dni temu. Każdy serwer ma inną konfigurację. Które z wymienionych poniżej twierdzeń jest prawdziwe w kontekście odtworzenia trzech uszkodzonych serwerów przy założeniu wykorzystywania procedury ASR (Automatyczne odzyskiwanie systemu)?

- A. Po naprawie sprzętu serwery te nie będą mogły być przywrócone. Specjalne pliki umieszczone na dyskietkach ASR są unikalne dla systemu serwera, który należy odtworzyć. Jeśli dyskietka zostaje zgubiona, odpowiednie zestawy ASR tego serwera stają się nieprzydatne.

- B. Po naprawie sprzętu serwery te będą mogły być przywrócone. W tym celu należy wykonać kopię zapasową ASR na jednym z działających serwerów i utworzyć nową dyskietkę. Dyskietka ta może być następnie wykorzystana dla uszkodzonych serwerów do przeprowadzenia procedury ASR.
- C. Po naprawie sprzętu serwery te będą mogły być przywrócone. W tym celu należy na jednym z działających serwerów uruchomić program Backup Utility (Kopia zapasowa) i użyć go do odtworzenia na dyskietce plików Asr.sif oraz Asrnp.sif na podstawie zestawów kopii zapasowych ASR funkcjonujących serwerów. Następnie tę dyskietkę ASR można wykorzystać do wykonania procedur ASR uszkodzonych serwerów.
- D. Po naprawie sprzętu serwery te będą mogły być przywrócone. W tym celu należy na jednym z działających serwerów uruchomić program Backup Utility (Kopia zapasowa) i użyć go do odtworzenia na dyskietce plików Asr.sif oraz Asrnp.sif na podstawie zestawów kopii zapasowych ASR każdego z uszkodzonych serwerów. Następnie odpowiednie dyskietki ASR można wykorzystać do wykonania procedur ASR na odpowiadających im uszkodzonych serwerach.

8.

Rooslan chce upewnić się, że jedynie członkowie grupy Administratorzy mogą odtwarzać dane o stanie systemu (System State) zawierające bazę danych urzędu certyfikacji dla poszczególnych systemów Windows Server 2003. Która z wymienionych poniżej metod opisuje prawidłowo sposób realizacji tego zadania, przy założeniu, że dla grupy Backup Operators (Operatorzy kopii zapasowych) nie zostaną zabrane uprawnienia wykonywania innych zestawów kopii zapasowych?

- A. Należy upewnić się, że podczas uruchamiania procedury wykonywania kopii zapasowych, w oknie dialogowym Backup Job Information (Informacje zadania kopii zapasowej) zaznaczona została opcja Allow Only The Owner And The Administrator Access To This Backup Data (Zezwalaj tylko właścicielowi lub administratorowi na dostęp do danych w kopii zapasowej).
- B. Na zakładce Restore And Manage Media (Przywracanie i zarządzanie nośnikiem) należy wybrać właściwości nośnika, na którym zostaną zapisane dane o stanie systemu. Następnie należy zmienić uprawnienia tak, aby jedynie grupa Administratorzy miała dostęp do tego nośnika.
- C. Uprawnienia związane z przywracaniem zestawu kopii zapasowych zawsze są przypisane do grupy Administratorzy, jak również do grupy Backup Operators (Operatorzy kopii zapasowych). Uprawnienia te nie mogą być ograniczane tylko do jednej grupy.
- D. Należy przeprowadzić edycję lokalnego obiektu zasady grupy i zmienić zasadę Backup Files And Directories (Tworzenie kopii zapasowych plików i katalogów), która znajduje się w kontenerze Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment (Konfiguracja komputera/Ustawienia systemu Windows/Ustawienia zabezpieczeń/Zasady lokalne/Przypisywanie praw użytkownika). Dla tej zasady należy usunąć grupę Backup Operators (Operatorzy kopii zapasowych).
- E. Należy przeprowadzić edycję lokalnego obiektu zasady grupy i zmienić zasadę Restore Files And Directories (Odtwarzanie plików i katalogów), która znajduje się w kontenerze Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment (Konfiguracja komputera/Ustawienia systemu Windows/Ustawienia zabezpieczeń/Zasady lokalne/Przypisywanie praw użytkownika). Dla tej zasady należy usunąć grupę Backup Operators (Operatorzy kopii zapasowych).

Odpowiedzi do zadania 5.1

Prawidłowa odpowiedź: A

- A. **Prawidłowo** Przywracanie autorytatywne oznacza, że obiekty usługi Active Directory, które zostały pierwotnie usunięte z bazy danych usługi, nie będą zastępowane podczas następnego procesu replikacji z innymi kontrolerami domeny. Jeśli nie zostałyby zastosowane przywracanie autorytatywne, następny proces replikacji przeprowadzany pomiędzy kontrolerami domeny po prostu usunąłby te obiekty.
- B. **Nieprawidłowo** Każdy obiekt usługi Active Directory odzyskany za pomocą przywracania nieautorytatywnego i usunięty po wykonaniu kopii zapasowej, zostanie usunięty z bazy danych usługi podczas kolejnego procesu replikacji wykonywanego pomiędzy kontrolerami domeny.
- C. **Nieprawidłowo** Każdy obiekt usługi Active Directory odzyskiwany za pomocą przywracania podstawowego i usunięty po wykonaniu kopii zapasowej, zostanie usunięty z bazy danych usługi podczas kolejnego procesu replikacji wykonywanego pomiędzy kontrolerami domeny.
- D. **Nieprawidłowo** Nie istnieje taki rodzaj przywracania.

2.

Prawidłowa odpowiedź: 1"

- A. **Nieprawidłowo** Uruchomienie kontrolera domeny w trybie List Known Good Configuration (>statni.t znana dobra konfiguracja) nie umożliwi odtworzenia bazy danych usługi Active Directory w ten sposób, że zostanie odzyskana jednostka organizacyjna zawierająca konta zespołu dytekcji.
- B. **Nieprawidłowo** Uruchomienie kontrolera domeny w trybie Safe (tryb awaryjny) nie umożliwi odtworzenia bazy danych usługi Active Directory w ten sposób, że zostanie odzyskana jednostka organizacyjna zawierająca konta zespołu dytekcji.
- C. **Nieprawidłowo** Baza danych usługi Active Directory nie może być odzyskiwana za pomocą programu Recovery Console (Konsola odzyskiwania).
- D. **Nieprawidłowo** Uruchomienie kontrolera domeny w normalnym trybie nie umożliwi odtworzenia bazy danych usługi Active Directory w ten sposób, że zostanie odzyskana jednostka organizacyjna zawierająca konta zespołu dytekcji.
- U. **Prawidłowo** Tryb Directory Services Restore (odzyskiwanie usługi katalogowej) został opracowany specjalnie do przywracania bazy danych usługi Active Directory. W tym celu administrator może **wybrać** typ odzyskiwania bazy danych usługi katalogowej: autorytatywny lub nieautorytatywny.

3.

Prawidłowe odpowiedzi: D oraz E

- A. **Nieprawidłowo** Pomimo, że dane istnieją, brak wszystkich ustawień dotyczących witryny sieci Web. Ustawienia te przechowują dane o stanie systemu (System State) i muszą zostać odtworzone.
- B. **Nieprawidłowo** Ponieważ pliki witryny sieci Web nie zostały uszkodzone, ich odtwarzanie niczego nie zmieni. Działanie takie po prostu zastąpi pliki, przechowywane na drugim dysku twarde, ich duplikatami.
- C. **Nieprawidłowo** Ponieważ serwery te nie są kontrolerami domeny, nie przechowują bazy danych usługi Active Directory. W przypadku serwerów członkowskich, ta opcja rozruchowa jest niedostępna.
- D. **Prawidłowo** Metabaza programu IIS zawierająca jego ustawienia jest kopiowana zawsze podczas wykonywania kopii zapasowej danych o stanie systemu. Pomimo, że dane te mogą być odtwarzane z lokalizacji sieciowej, można je również wcześniej skopiować na lokalny dysk twardy.

EJ Prawidłowo Metabaza programu IIS zawierająca jego ustawienia jest kopiowana zawsze podczas wykonywania kopii zapasowej danych o stanie systemu. Jeśli administrator jest zalogowany na serwerze, może odtwarzać dane kopii zapasowych przechowywanych na serwerach zdalnych.

4.

Prawidłowe odpowiedzi: B, D oraz E

- A. **Nieprawidłowo** Baza danych certyfikatów może być odtwarzana przy użyciu programu Backup Utility (Kopia zapasowa), ponieważ baza ta jest częścią danych o stanie systemu (System State).
- B. **Prawidłowo** Bez prawidłowo funkcjonującego programu IIS, skonfigurowanego dla obsługi urzędu CA, usługi certyfikacji stron sieci Web nie zostaną uruchomione. Po zainstalowaniu CA wykonywane są odpowiednie modyfikacje metabazy programu IIS.
- C. **Nieprawidłowo** Aby odtworzyć dane o stanie systemu, nie jest wymagane żadne hasło. Uprawnienia związane z wykonywaniem kopii zapasowych i ich przywracaniem mogą być jednak ograniczone jedynie do grupy administratorów.
- D. **Prawidłowo** Zabezpieczenie to stanowi dodatkowy poziom bezpieczeństwa tak, aby osoba, która uzyskała dostęp do taśm kopii zapasowych, nie potrafiła na ich podstawie utworzyć swojej własnej wersji takiego samego urzędu certyfikacji. Jeśli kopia zapasowa bazy danych powstaje podczas kopiowania danych o stanie systemu, dostęp do danych nie jest chroniony hasłem.
- E. **Prawidłowo** Funkcja Autoniaied System Recovery (Automatyczne odzyskiwanie systemu) przechowuje dane o stanie systemu, a baza danych certyfikacji jest ich częścią.

5.

Prawidłowa odpowiedź: B

- A. **Nieprawidłowo** Dyskietka ASR nie może być używana do uruchomienia komputera. Na dyskietce znajdują się **informacje** dotyczące systemu, ale na ich podstawie nie można uruchomić systemu Windows Server 2003-
- B. **Prawidłowo** Jest to poprawna metoda przeprowadzenia procedury automatycznego odzyskiwania systemu Windows Servct 7.003. Dyskietka przygotowana za pomocą funkcji Automated System Recovery (Automatyczne odzyskiwanie systemu) nie jest dyskietką rozruchową i zawiera jedynie ważne pliki konfiguracji systemu, takie jak opis rozmieszczenia plików na dysku potrzebny na początku procesu przywracania systemu. Pozostałe pliki są kopiowane na podstawie nośnika instalacyjnego lub zestawu kopii zapasowej ASR.
- C. **Nieprawidłowo** Uruchomienie w trybie awaryjnym nie rozpoczyna procesu ASR (Automatyczne odzyskiwanie systemu).
- D. **Nieprawidłowo** W trybie Direcrory Services Restore (Odzyskiwanie usługi katalogowej) nie można rozpocząć procesu ASR.
- E. **Nieprawidłowo** Konsola odzyskiwania nie może być używana do zainicjowania procesu ASR.

6.

Prawidłowa odpowiedź: C

- A. **Nieprawidłowo** Procedura ASR (Automatyczne odzyskiwanie systemu) nie przywraca danych, chociaż dzięki niej przywrócona zostanie metabaza programu IIS oraz naprawione zostaną pliki powodujące niestabilność systemu.
- B. **Nieprawidłowo** Patrz uzasadnienie do odpowiedzi A.
- C. **Prawidłowo** Dzięki procedurze ASR (Automatyczne odzyskiwanie systemu) przywrócona zostanie metabaza programu IIS oraz naprawione zostaną pliki powodujące niestabilność systemu.

Ponieważ wykonywane są przyrostowe kopie zapasowe, aby przywrócić wszystkie brakujące pliki, należy je odtworzyć na podstawie wszystkich kopii przyrostowych oraz pełnej kopii zapasowej.

- D. **Nieprawidłowo** Działanie takie nie usunie niestabilności systemu spowodowanej uszkodzeniem plików innych niż te, które znajdują się w kopii zapasowej danych o stanie systemu (System State). Poza tym nie zostaną odtworzone pliki, które zostały zarchiwizowane we wtorek.
- E. **Nieprawidłowo** Pomimo, że działanie to odtworzy metabazę i wszystkie dane witryny sieci Web, nie zostaną przywrócone inne pliki, które powodują niestabilność systemu.

7.

Prawidłowa odpowiedź: D

- A- **Nieprawidłowo** To twierdzenie jest nieprawdziwe. Nowa dyskietka ASR może zostać wygenerowana na podstawie odpowiedniego zestawu kopii zapasowych ASR zapisanych na taśmach dla danego serwera.
- B. **Nieprawidłowo** Każdy serwer ma inną konfigurację, co oznacza, że informacje na poszczególnych dyskietkach ASR każdego serwera się różnią.
- C. **Nieprawidłowo** Opisana procedura jest bliska **prawidłowej**. Aby uszkodzone serwery zostały właściwie odtworzone, należy odzyskać pliki Aas.sif oraz Asrnp.sif na podstawie zestawów kopii zapasowych uszkodzonych serwerów, a nie serwerów sprawnych, w przeciwnym razie dyskietki te będą zawierać nieprawidłowe informacje.
- D. **Prawidłowo** Podczas tworzenia plików zestawu kopii zapasowej ASR, pliki zapisywane na dyskietce ASR są zapisywane również na nośnikach kopii zapasowej. Oznacza to, że jeśli nawet dyskietka ASR zostanie zgubiona, istnieje możliwość **odtworzenia informacji** o przechowywanych plikach zestawu kopii zapasowej ASR.

Prawidłowa odpowiedź: A

- A. **Prawidłowo** jest to jedyna metoda ograniczania, którzy użytkownicy lub grupy mogą wykonywać odtwarzanie poszczególnych zestawów kopii zapasowej.
- B. **Nieprawidłowo** Taka **funkcja** nie została umieszczona na zakładce Restore And Manage Media (Przywracanie i zarządzanie nośnikiem).
- C. **Nieprawidłowo** Dostęp może być ograniczony tylko do grupy Administratorzy zgodnie z procedurą opisaną w punkcie A.
- D. **Nieprawidłowo** Działanie takie nie zmieni ptaw grupy Backup Operators (Operatorzy kopii zapasowych) związanych z odtwarzaniem zestawów kopii, uniemożliwi natomiast członkom tej grupy wykonywanie kopii zapasowych folderów i plików.
- E. **Nieprawidłowo** Działanie takie uniemożliwi członkom grupy Backup Operators (Operatorzy kopii zapasowych) przywracanie wszystkich danych, nie tylko danych o stanie systemu.

Zadanie 5.2

Zarządzanie procedurami tworzenia kopii zapasowych

Podczas tworzenia kopii zapasowej danych o stanie systemu (System State) w zestawie kopii zapisane zostaną następujące elementy: rejestr systemu, baza danych COM+ Class Registration, plik rozruchowe oraz. pliki systemowe, które są chronione przez usługę Windows File Protection (Ochrona plików systemu Windows). W zależności, które usługi zostały zainstalowane w systemie Windows Server 2003, dane o stanie systemu mogą zawierać dodatkowo bazę danych usługi certyfikacji, usługi Active Directory oraz folder Sysvol w przypadku kontrolera domeny, informacje o usłudze klastra w przypadku serwera klastra oraz metabazę programu IIS.

Jeśli administrator chce sprawdzić, czy kopia zapasowa została wykonana prawidłowo, weryfikacja musi zostać skonfigurowana przed uruchomieniem zadania tworzenia kopii zapasowej. Weryfikacja zadania tworzenia kopii zapasowej nie może być deklarowana po ukończeniu zadania. Weryfikacja sprawdza, czy pliki i foldery kopii są zgodne z plikami i folderami, które były kopiowane. Pomimo, że sprawdzanie dzienników kopii zapasowych może informować administratora o tym, że wystąpił błąd, to nie mogą tam znaleźć się informacje o tym, czy plik kopii jest zgodny z plikiem oryginalnym.

Zesławy kopii zapasowych mogą być przechowywane na różnych typach nośników, takich jak taśmy, dyski twarde i/y niektóre postacie pamięci wymiennych. Oprócz tego, kopie zapasowe mogą być zapisywane w folderach udostępnionych w sieci. Niektóre urządzenia zapisujące, jak na przykład nagrywarki CD-ROM nie są obsługiwane przez program Backup (Kopia zapasowa) systemu Windows Server 2003.

Pytania do zadania 5.2

Rooslan jest administratorem systemu Windows Server 2003, na którym został uruchomiony program IIS (Internet Information Services). Serwer ten jest wykorzystywany do wystawiania osobom trzecim certyfikatów cyfrowych w Internecie. Certyfikaty te umożliwiają abonentom dostęp do specjalnie chronionej części witryny sieci Web, która nie jest dostępna dla pozostałych użytkowników odwiedzających tę witrynę. Rooslan ma zamiar raz na tydzień tworzyć kopię zapasową konfiguracji programu IIS i bazy danych certyfikatów. Oprócz tego, Rooslan chce co tydzień tworzyć kopię zapasową wszystkich plików i folderów w katalogu C:\Inetpub, a codziennie kopię zapasową zmienionych plików i folderów tego katalogu przy użyciu takiej metody, która zajmie najmniejszą przestrzeń na nośniku kopii. Którą z wymienionych metod powinien zastosować Rooslan? (wybierz wszystkie właściwe odpowiedzi)

- A. Pełna kopia zapasowa wykonywana codziennie
- B. Pełna kopia zapasowa wykonywana raz w tygodniu
- C. Pełna kopia zapasowa zawierająca dane o stanie systemu (System State), wykonywana raz w tygodniu
- D. Różnicowa kopia zapasowa wykonywana codziennie
- E. Przyrostowa kopia zapasowa wykonywana codziennie

- 2.** Która z wymienionych poniżej metod będzie automatycznie weryfikować poprawność wykonania kopii zapasowej?
- A. Podczas uruchamiania zadania kopii zapasowej należy kliknąć przycisk Advanced (Zaawansowane) i zaznaczyć opcję Verify Data After Backup (Weryfikuj dane po wykonaniu kopii zapasowej).
 - B. Należy wykorzystać program Backup Wizard (Kreator kopii zapasowej), aby uruchomić weryfikację zadania.
 - C. Na zakładce Restore And Manage Media (Przywracanie i zarządzanie nośnikiem) programu Backup Utility (Kopia zapasowa) należy wybrać właściwości wykonywanej kopii zapasowej i zaznaczyć opcję Verify (Weryfikuj).
 - D. W programie Backup Utility (Kopia zapasowa) systemu Windows Server 2003 nie istnieje możliwość sprawdzenia poprawności wykonania kopii zapasowej.

- 3.** Które z wymienionych poniżej urządzeń mogą być wykorzystywane do zapisywania kopii zapasowej w programie Backup Utility (Kopia zapasowa)? (wybierz wszystkie właściwe odpowiedzi)
- A. Nagrywarka dysku CD-ROM
 - B. Folder udostępniony w sieci
 - C. Napęd taśmy magnetycznej DAT
 - D. Nagrywarka dysków DVD-ROM

- 4.** Administrator opiekuje się kilkoma serwerami plików systemu Windows Server 2003. Niedawno firma zakupiła serwer plików, który w porównaniu do pozostałych serwerów sieci LAN, wyposażony jest w urządzenia pamięci masowej o znacznie większej pojemności. Administrator jest w trakcie przenoszenia na nowy serwer kilku folderów udostępnionych przechowywanych na pozostałych serwetach. Ponieważ dla każdego serwera plików określone zostały unikatowe uprawnienia NTFS, administrator wykorzystuje program narzędziowy Backup And Restore (Kopia zapasowa), aby zapewnić, że podczas kopiowania na nowy serwer uprawnienia oryginalnych plików i folderów zostaną prawidłowo przeniesione. Zesrwy kopii zapasowych zostały umieszczone na jednym woluminie nowego serwera w następujących lokalizacjach:

E:\Filcshbak1.bkf

E:\Filesbak2.bkf

E:\Filesbak3.bkf Administrator uruchomił program Backup Utility (Kopia zapasowa) systemu Windows Server 2003 i chce zaimportować w programie Backup Utility (kopia zapasowa) każdy z tych zestawów kopii zapasowych do zakładki Restore And Manage Media (Przywracanie i zarządzanie nośnikiem) tak, aby na nowym serwerze można było przywrócić wszystkie pliki i foldery w nowych katalogach. Która z opisanych poniżej metod pozwoli zrealizować to zadanie?

- A. Należy dwukrotnie kliknąć każdy plik. Dzięki temu pliki zostaną zaimportowane do zakładki Restore And Manage Media (Przywracanie i zarządzanie nośnikiem).
- B. W programie Windows Explorer (Eksplorator Windows) należy przeciągnąć każdy plik kopii zapasowej do zakładki Restore And Manage Media (Przywracanie i zarządzanie nośnikiem) programu Backup Utility (Kopia zapasowa).

- C. W programie Backup Wizard (Kreator kopii zapasowej), w menu Tools (Narzędzia) należy wybrać polecenie Catalog A Backup File (Sprządź wykaz plików kopii zapasowej). Następnie należy oddzielnie wyszukać każdy plik i sporządzić dla niego wykaz.
- D. Nośniki, które nie zostały utworzone za pomocą programu Backup Utility (Kopia zapasowa), nie mogą być importowane w celu ich odtworzenia.

Odpowiedzi do zadania 5.2

1. Prawidłowe odpowiedzi: C oraz E

- A. **Nieprawidłowo** Przy użyciu takiej metody nie zostaną zapisane informacje o konfiguracji programu IIS lub bazy danych certyfikacji. Poza tym stosowanie tej metody nie minimalizuje miejsca zajmowanego na nośniku kopii zapasowej.
- B. **Nieprawidłowo** Przy użyciu takiej metody nie zostaną zapisane informacje o konfiguracji programu IIS lub bazy danych certyfikacji.
- C. **Prawidłowo** Dzięki tej metodzie zostanie utworzona kopia zapasowa konfiguracji programu IIS i bazy danych certyfikatów, a także wymagana **pełna** kopia plików i folderów.
- D. **Nieprawidłowo** Różnicowa kopia zapasowa wykorzystuje więcej miejsca na nośniku kopii niż kopia przyrostowa. Różnicowa kopia zapisuje wszystkie informacje utworzone lub zmodyfikowane od momentu wykonania ostatniej pełnej kopii zapasowej.
- E. **Prawidłowo** Przyrostowa kopia zapasowa wykorzystuje najmniej miejsca na nośniku kopii. Kopia ta zapisuje jedynie dane, które zostały utworzone lub zmodyfikowane od momentu wykonania ostatniej przyrostowej kopii zapasowej.

2.. Prawidłowa odpowiedź: A

- A. **Prawidłowo** Opisana metoda zapewnia, że kopia zapasowa wybranych danych zostanie poprawnie zapisana.
- B. **Nieprawidłowo** W programie Backup Utility (Kopia zapasowa) systemu Windows Server 2003 nie umieszczono opcji dotyczącej weryfikacji zadania kopii zapasowej.
- C. **Nieprawidłowo** Opcja ta nie istnieje.
- D. **Nieprawidłowo** To nie jest prawidłowa odpowiedź. Zadanie może być **sprawdzone** bezpośrednio po jego wykonaniu poprzez zaznaczenie opcji Verify Data After Backup (Weryfikuj dane po wykonaniu kopii zapasowej).

O. Prawidłowe odpowiedzi: B oraz C

- A. **Nieprawidłowo** Nagrywarki dysków CD-ROM w programie Backup Utility (Kopia zapasowa) systemu Windows Server 2003 nie mogą być wykorzystywane jako urządzenia, na których zapisywane są kopie zapasowe.
- B. **Prawidłowo** W programie Backup Utility (Kopia zapasowa) systemu Windows Server 2003 kopie zapasowe mogą być zapisywane w folderze udostępnionym w sieci.
- C. **Prawidłowo** Napędy taśmowe są tradycyjną metodą zapisu kopii zapasowej i jako takie są rozpoznawane przez program Backup Utility (Kopia zapasowa) systemu Windows Server 2003.

D. Nieprawidłowo Nagrywarki dysków CD-ROM i DVD-ROM nie są rozpoznawane przez program Backup Utility (Kopia zapasowa) systemu Windows Server 2003 jako urządzenia zapisu kopii zapasowych.

Prawidłowa odpowiedź: C

4.

- A. Nieprawidłowo** Pomimo, że działanie takie uruchomi program Backup Utility (Kopia zapasowa), nie spowoduje to automatycznego wybrania plików dla funkcji importu lub przywracania.
- B. Nieprawidłowo** Metoda taka nie zadziała.
- C. Prawidłowo** Jest to jedyna metoda, dzięki której dane tych plików mogą zostać dodane do zakładki Restore And Manage Media (Przywracanie i zarządzanie nośnikiem).
- D. Nieprawidłowo** To jest nieprawdziwe twierdzenie. Polecenie Catalog A Backup File (Sporządź wykaz plików kopii zapasowej) umieszczone w menu Tools (Narzędzia) umożliwia zaimportowanie plików do programu kopii zapasowej.

Zadanie 5.3

Przywracanie systemu po awarii sprzętu

Jeśli konfiguracja serwera przewidywała odporność na uszkodzenia, awaria dysku serwera w odniesieniu do zagadnień przywracania funkcjonalności systemu nie jest aż tak bardzo „katastroficznym” zdarzeniem, jak mogłoby się to wydawać początkowo. System Windows Server 2003 może zostać skonfigurowany za pomocą konsoli Disk Management (Zarządzanie dyskami) tak, aby wykorzystywał zestawy dublowane lub RAID-5. Obie te konfiguracje umożliwiają funkcjonowanie serwera w przypadku awarii dysku twardego.

W systemie Windows Server 2003 woluminy dublowane (RAID-1) są przede wszystkim wykorzystywane dla woluminów rozruchowych bądź systemowych. Spowodowane jest to po części tym, że wolumin rozruchowy c/y systemowy nie może być skonfigurowany przez narzędzia zarządzania dyskami systemu Windows Server 2003 (nie ma ich w programowej RAID-1). Serwer może być uruchamiany w oparciu o dysk zestawu dublowanego, a po utworzeniu zestawu dublowanego nowa opłata rozruchowa dodawana jest do menu stanowego systemu operacyjnego (plik serwera boot.ini).

Woluminy RAID-5 są wykorzystywane głównie do przechowywania plików danych i programów. Zestaw taki wymaga stosowania co najmniej trzech dysków, a maksymalna liczba dysków zestawu to 32. Pomimo awarii jednego z dysków zestawu, wolumin RAID-5 nie przerywa funkcjonowania, a jedynie zmniejszona zostaje jego wydajność. W późniejszym terminie administrator może wyłączyć serwer, zainstalować dysk zapasowy i zregenerować wolumin.

Pytania do zadania 5.3

1. Rooslan jest administratorem systemu Windows Server 2003. W serwerze tym zainstalowane zostały cztery dyski twarde S (Small Computer System Interface). Serwer obsługuje dwa woluminy, a każdy z nich obejmuje w całości jeden dysk SCSI. Pierwszy dysk obsługuje pierwszy wolumin, na którym umieszczone są pliki systemu operacyjnego i programów. Drugi dysk twardy obsługuje drugi wolumin, na którym przechowywane są dane programów oraz kilka folderów udostępnionych. Za pomocą konsoli Disk Management (Zarządzanie dyskami) zostały skonfigurowane zestawy dublowane. Pierwszy wolumin jest dublowany na dysku trzecim, a drugi wolumin na dysku czwartym.

Awarii uległ dysk czwarty. Jakie działania musi przeprowadzić Rooslan, aby przywrócić odporność na uszkodzenia opisywanego serwera? (wybierz wszystkie właściwe odpowiedzi)

- A. Zanim zostanie zainstalowany dysk zapasowy, Rooslan musi usunąć dublowanie dysków pomiędzy pierwszym i trzecim dyskiem.
- B. Zanim zostanie zainstalowany dysk zapasowy, Rooslan musi usunąć dublowanie dysków pomiędzy drugim i czwartym dyskiem.
- C. Po zainstalowaniu dysku zapasowego, Rooslan musi utworzyć nowy zestaw dublowany pomiędzy drugim i czwartym dyskiem.

- D. Rooslan musi usunąć uszkodzony dysk, zainstalować nowy, a następnie przerwać dublowanie pomiędzy dyskiem pierwszym i trzecim.

2.

Oksana jest administratorem systemu Windows Server 2003- Na tym serwerze, za pomocą konsoli Disk Management (Zarządzanie dyskami), w oparciu o drugi dysk twardy został utworzony zestaw dublowany woluminu systemowego. Uszkodzeniu uległ pierwszy dysk twardy zawierający wolumin systemowy, a system zawiesił się. Administrator dysponuje dyskiem zapasowym. Którą z opisanych metod powinna zastosować Oksana, aby przywrócić odporność na uszkodzenia systemu Windows Server 2003?

- A. Należy użyć nośnika instalacyjnego systemu Windows Server 2003 do uruchomienia programu Reawery Console (Konsola odzyskiwania) i usunąć dublowanie dysków. Następnie należy wyłączyć serwer i zainstalować dysk zastępczy. W oparciu o nośnik instalacyjny systemu Windows Server 2003 należy ponownie uruchomić program Reawery Console (Konsola odzyskiwania) i utworzyć nowy zestaw dublowany.
- B. Należy usunąć uszkodzony dysk i uruchomić komputer bez zestawu dublowanego. Następnie należy uruchomić: konsolę Disk Management (Zarządzanie dyskami) i usunąć dublowanie odnoszące się do uszkodzonego dysku. W kolejnym kroku należy wyłączyć system i zainstalować dysk Zastępczy oraz uruchomić serwer w oparciu wolumin dublowany. Po uruchomieniu, w konsoli Disk Management (Zarządzanie dyskami) należy zainicjować nowo zainstalowany dysk i przekształcić go na dynamiczny, a następnie utworzyć dublowany z.i-siaw pomiędzy pierwotnie dublowanym i nowym dyskiem.
- C. Należy usunąć uszkodzony dysk i zainstalować dysk zastępczy. Następnie należy uruchomić serwer w oparciu o nośnik instalacyjny systemu Windows Server 2003 i wybrać opcję dotyczącą naprawy instalacji.
- D. Należy usunąć uszkodzony dysk i zainstalować dysk zastępczy. Następnie należy uruchomić serwer wybierając tryb Last Known Good Configuration (Ostatnia znana dobra konfiguracja) i uruchomić program System Repair Wizard (Kreator naprawy systemu).

3.

Rooslan jest administratorem systemu Windows Server 2003. Serwer na którym uruchomiony jest program SQL Server 2000, wyposażony jest w sześć dysków twardych SCSI. Dwa pierwsze dyski tworzą zestaw dublowany i obsługują wolumin zawierający pliki systemu operacyjnego i programów. Pozostałe cztery dyski SCSI skonfigurowane zostały jako macierz RAID-5 i tworzą pojedynczy wolumin zawierający całą bazę danych. Obecnie zajętych jest 40% woluminu. Jeden z czterech dysków woluminu RAID-5 uległ awarii. Które z wymienionych poniżej twierdzeń opisujących powyższą sytuację są prawdziwe?

- A. Serwer będzie kontynuował działanie, a żadne informacje nie zostaną utracone.
- B. Serwer zawiesi się. Funkcjonowanie serwera zostanie przywrócone po wymianie uszkodzonego dysku.
- C. Po ponownym aktywowaniu woluminu serwer będzie kontynuował swoje operacje. Nowe dane nie będą mogły być zapisywane na woluminie RAID-5, natomiast bieżące dane mogą być odczytywane i na ich podstawie może być utworzona kopia zapasowa.
- D. Wszystkie dane zostaną utracone. Zestaw rozłożony, a nie RAID-5, jest odporny na uszkodzenia.

4. W systemie Windows Server 2003 zainstalowanych zostało 9 dysków twardych SCSI. Na dysku 1 przechowywany jest system operacyjny. Dyski 2, 5 i 8 tworzą pojedynczy wolumin RAID-5. Dyski 3, 4 oraz 6 tworzą pojedynczy wolumin RAID-5. Dysk 1 jest dublowany na dysku 7. W oparciu o dysk 9 utworzony jest pojedynczy wolumin.

Które z dysków mogą jednocześnie ulec awarii, przy założeniu, że serwer będzie w pełni funkcjonował po ponownym uruchomieniu?

- A. Jednoczesna awaria dysków 1, 2 oraz 5.
- B. Jednoczesna awaria dysków 6, 7 oraz 8.
- C. Jednoczesna awaria dysków 1, 7 i 8.
- D. Jednoczesna awaria dysków 1, 6 i 9.
- E. Jednoczesna awaria dysków 1, 2 i 3.

Odpowiedzi do zadania 5.3

1. Prawidłowe odpowiedzi: li oraz C

- A. **Nieprawidłowo** Pierwszy i trzeci dysk są sprawne, a nie przerwanie dublowania tych dysków nie ma związku z przywróceniem odporności na uszkodzenia, a jedynie zmniejszy bieżący jej poziom.
- B. **Prawidłowo** Dopóki dublowanie nie zostanie usunięte, nie można utworzyć nowego zestawu dublowanego).
- C. **Prawidłowo** Dziabnie takie pr/ywioći odporność u.i uszkodzenia poprze/ ponowne utworzenie zestawu dublowanej'/) zawierającego nowy dysk.
- D. **Nieprawidłowo** Przerwanie dublowania pierwszego i trzeciego dysku nie poprawi odporności na uszkodzenia. Problem dotyczy dysku drugiego i czwartego.

2.. Prawidłowa odpowiedź: B

- A. **Nieprawidłowo** Program Recovery Console (Konsola odzyskiwania) nie może być wykorzystywany do usuwania bądź tworzenia zestawów dublowanych.
- B. **Prawidłowo** Jest to jedyna metoda przywrócenia odporności na uszkodzenia tego serwera. Po utworzeniu woluminu dublowanego serwer może wykorzystywać ten wolumin tak, jak poprzednio.
- C. **Nieprawidłowo** Procedura ta nie przywróci odporności na uszkodzenia pierwotnej konfiguracji serwera.
- D. **Nieprawidłowo** Procedura ta nie przywróci odporności na uszkodzenia pierwotnej konfiguracji serwera.

O. Prawidłowa odpowiedź: A

- A. **Prawidłowo** Serwer będzie kontynuował działanie, a żadne dane nie zostaną utracone. Pogorszy się wydajność operacji odczytu i zapisu ze względu na konieczność wykorzystywania informacji sumy kontrolnej (parzystości) do umożliwienia odczytu danych. Dysk musi zostać wymieniony w późniejszym terminie.

- B. Nieprawidłowo** Wolumin może być ponownie aktywowany za pomocą konsoli Disk Management (Zarządzanie dyskami) i tym samym odpowiedź jest nieprawidłowa.
- C. Nieprawidłowo** Ponieważ tylko 40% woluminu jest używane, na dysku dane mogą być zapisywane i odczytywane. Operacje tej będą jednak realizowane przy zmniejszonej wydajności.
- D. Nieprawidłowo** Zestawy rozłożone nie są odporne na uszkodzenia i tym samym odpowiedź jest nieprawidłowa. Uszkodzenie jednego dysku zestawu RAID-5 nie powoduje utraty danych tego woluminu.

Prawidłowe odpowiedzi: B oraz E

- A. Nieprawidłowo** Dysk 1 jest dublowany na dysku 7 i dlatego jest odporny na uszkodzenia. Jednakże dysk 2 tworzy ten sam wolumin RAID-5 co dysk 5. Wolumin RAID-5 nie jest odporny na jednoczesne uszkodzenie dwóch dysków.
- B. Prawidłowo** Dysk 6 i dyski 7 lub 8 nie tworzą razem woluminu RAID-5. Dysk 7 tworzy zestaw dublowany razem z dyskiem 1, a dysk 8 i dyski 6 lub 7 nie tworzą razem woluminu RAID-5.
- C. Nieprawidłowo** Dyski 1 i 7 tworzą zestaw dublowany woluminu systemowego.
- D. Nieprawidłowo** Dysk 9 nie jest odporny na uszkodzenie.
- E. Prawidłowo** Dysk 1 jest dublowany na dysku 7, tak więc może ulec awarii. Dysk 2 nie tworzy woluminu RAID 5 razem z dyskiem 1, a więc może ulec awarii. Podobnie dysk 3 nie tworzy woluminu RAID 5 razem z dyskiem 2 i również jego awaria nie przeszkodzi funkcjonowaniu serwera.

Zadanie 5.4 Odtwarzanie danych kopii zapasowych

Celem każdej procedury odtwarzania jest zapewnienie, aby wszystkie dane zestawu kopii zapasowej zostały prawidłowo przywrócone. Za wyjątkiem sytuacji, kiedy codziennie wykonywana jest pełna kopia zapasowa zapisywana na oddzielnych nośnikach, bardziej złożonym zadaniem jest wybór odpowiednich taśm kopii zapasowej oraz odpowiednia kolejność ich przywracania.

Zrozumienie procedur odtwarzania plików jest bezpośrednio związane ze zrozumieniem sposobów działania różnych metod wykonywania kopii zapasowych. Administrator systemu powinien rozumieć, dlaczego w przypadku przyrostowych kopii muszą być odtworzone wszystkie taśmy zapisane po wykonaniu ostatniej pełnej kopii zapasowej. Podobnie w przypadku wykonywania różnicowej kopii zapasowej trzeba zdawać sobie sprawę, dlaczego do przywrócenia danych potrzebna będzie tylko pełna kopia opasowa i ostatnia kopia różnicowa.

Pomimo, że administratorzy systemów wykonują kopie zapasowe z obawy przed skutkami awarii sprzętu, to najczęściej przywracanie danych ma miejsce, jeśli użytkownik zagubił lub usunął plik. Administrator oszczędza swój czas, jeśli potrafi szybko odnaleźć właściwy zestaw kopii zapasowej zawierający brakujący plik, a nie musi przywracać całonocnego zestawu kopii zapasowych w poszukiwaniu pojedynczego pliku.

Pytania do zadania 5.4

1. Administrator w średniej wielkości fabryce opiekuje się kilkoma systemami Windows Server 2003. Jeden z tych serwerów pełni rolę serwera plików i druku. W serwerze zainstalowane są trzy dyski, a na jednym z nich zainstalowany jest system operacyjny. Pozostałe dwa dyski tworzą zestaw rozłożony, który obsługuje kilka folderów udostępnionych. Kopie zapasowe są zapisywane na taśmach DAT za pomocą napędu zainstalowanego w serwerze, natomiast same nośniki przechowywane są poza lokacją. Zestaw kopii zapasowej zawiera wszystkie pliki i foldery wolumenu rozłożonego, na którym umieszczone są foldery udostępnione oraz dane o stanie systemu (System State). Dla pozostałej części systemu operacyjnego kopia zapasowa nie jest tworzona, nie licząc comiesięcznej kopii zapasowej ASR (Automatyczne odzyskiwanie systemu). Procedura wykonywania kopii zapasowych przedstawia się następująco:

2:00 Niedziela. Pełna kopia zapasowa wraz z danymi o stanie systemu.

2:00 Od poniedziałku do soboty'. Przyrostowa kopia zapasowa wraz z danymi o stanie systemu.

W czwartek o godzinie 14:00 awarii uległ drugi dysk zestawu rozłożonego. Administrator dysponuje w lokacji identycznym dyskiem zapasowym i może pobrać znajdujące się poza lokacją taśmy kopii zapasowych z ostatnich siedmiu dni, wliczając w to zestaw kopii i dyskietkę ASR. Które czynności Spośród wymienionych poniżej są wymagane do odtworzenia woluminu rozłożonego?

- A. Należy usunąć uszkodzony dysk i zastąpić go zapasowym. Za pomocą konsoli Disk Management (Zarządzanie dyskami) należy zregenerować wolumin rozłożony.

- B. Należy usunąć uszkodzony dysk i zastąpić go zapasowym, a następnie ponownie uruchomić serwer w oparciu o dysk instalacyjny CD-ROM i w odpowiednim momencie umieścić dyskietkę ASR, aby wykonać procedurę ASR.
- C. Należy usunąć uszkodzony dysk i zastąpić go zapasowym. Następnie należy odtworzyć dane o stanie systemu i za pomocą konsoli Disk Management (Zarządzanie dyskami) zregenerować wolumin rozłożony.
- D. Należy usunąć uszkodzony dysk i zastąpić go zapasowym. Za pomocą konsoli Disk Management (Zarządzanie dyskami) należy ponownie utworzyć wolumin rozłożony obejmujący dysk pierwotny i nowy dysk. Przy użyciu programu Backup Utility (Kopia zapasowa) należy odtworzyć dane woluminu rozłożonego na podstawie zestawu kopii zapasowych utworzonych w niedzielę i czwartek.
- E. Należy usunąć uszkodzony dysk i zastąpić go zapasowym. Za pomocą konsoli Disk Management (Zarządzanie dyskami) należy ponownie utworzyć wolumin rozłożony obejmujący dysk pierwotny i nowy dysk. Przy użyciu programu Backup Utility (Kopia zapasowa) należy odtworzyć dane woluminu rozłożonego na podstawie zestawu kopii zapasowych utworzonych w niedzielę, poniedziałek, wtorek, środę i czwartek.

2. 3. Administrator opiekuje się czterema serwerami plików systemu Windows Server 2003 wydziału uniwersyteckiego. Sekretarka wydziału zadzwoniła informując, że przypadkowo usunęła z serwera ważny plik. Był to dokument, który miał być jutro prezentowany pr./cz. dziekana wydziału podczas Sympozjum i dlatego ważne jest, aby plik ten odtworzyć możliwie szybko. Różnicowa kopia zapasowa wykonywana jest każdego wieczoru o godzinie 22:00 za wyjątkiem piątku, kiedy to wykonywana jest pełna kopia zapasowa. (Zauważ, że kopia zapasowa jest zapisywana na oddzielnej taśmie oznaczanej Zgodnie z bieżącym dniem tygodnia. Dzisiaj jest czwartek. Sekretarka sądzi, że usunęła plik wczoraj rano. (Krami 1.1/ plik był modyfikowany w poniedziałek i nie był otwierany w ciągu weekendu, /..ikła dając. Ż.c sekretarka nie myliła się, które / wymieniony) li poniżej i. i M u kopii zapasowy! li będą zawierały kopię usuniętego pliku? (wybierz wszystkie właściwe odpowiedzi)

- A. Taśma zapisana w piątek
- B. Taśma zapisana w sobotę
- C. Taśma zapisana w niedzielę
- D. Taśma zapisana w poniedziałek
- E. Taśma zapisana we Wtorek
- E Taśma zapisana w środę

Administrator opiekuje się serwerem plików systemu Windows Server 2003 biura rachunkowego. Jedna z księgowych poinformowała, że przypadkowo usunęła z serwera kilka ważnych arkuszy kalkulacyjnych. Różnicowa kopia zapasowa jest wykonywana codziennie rano za wyjątkiem poniedziałku, kiedy to o godzinie 2:00 wykonywana jest pełna kopia zapasowa. Każdego dnia kopia zapasowa zapisywana jest na oddzielnej taśmie oznaczanej zgodnie z bieżącym dniem tygodnia. Dzisiaj jest piątek. Księgowa uważa, że usunęła arkusze wczoraj wieczorem. Brakuje pięciu arkuszy kalkulacyjnych. Tylko dwa z nich opracowane zostały w ostatnim tygodniu. Pierwszy został zmodyfikowany w poniedziałek po południu, a drugi nie był edytowany za wyjątkiem niewielkich zmian wykonanych w środę. Które z przedstawionych twierdzeń dotyczących taśm kopii zapasowych są prawdziwe? (wybierz wszystkie właściwe odpowiedzi)

- A. Trzy pliki, które nie były modyfikowane w ostatnim tygodniu, będą znajdowały się jedynie na taśmie kopii zapasowej wykonanej w poniedziałek.
 - B. Wszystkie pięć plików znajduje się na taśmie kopii zapasowej wykonanej w czwartek.
 - C. Dwa spośród pięciu usuniętych plików będą znajdować się na taśmie kopii zapasowej wykonanej w czwartek.
 - D. Dwa spośród usuniętych plików arkuszy kalkulacyjnych będą znajdować się na taśmie kopii zapasowej wykonanej w środę.
 - E. Żaden z usuniętych plików nie będzie znajdował się na taśmie kopii zapasowej wykonanej we wtorek.
4. Rooslan jest odpowiedzialny za wykonywanie kopii zapasowych systemu Windows Server 2003, który obsługuje kilka witryn sieci Web. Witryny te zawierają dane, które są codziennie zmieniane przez poszczególnych administratorów tych witryn. Wszystkie pliki witryn sieci Web znajdują się na innym dysku i woluminie niż ten, na którym przechowywane są pliki systemu operacyjnego i programów. Pełna kopia zapasowa zawierająca również dane o stanie systemu zapisywana jest w lokalizacji sieciowej. Wykonywana jest w każdy wtorek o godzinie 3:00, a jej wykonanie zajmuje średnio około dwóch godzin. Różnicowa kopia zapasowa danych witryny sieci Web zapisywana jest w lokalizacji sieciowej i wykonywana jest codziennie o godzinie 3:30 za wyjątkiem wtorku. Wykonanie różnicowej kopii zajmuje około półtorej godziny. W sobotę o godzinie 4:30 awarii uległ dysk przechowujący wolumin witryn sieci Web. Administrator po odebraniu powiadomienia dotarł do serwerowni o godzinie 5:30. Administrator dysponował zapasowym dyskiem twardym identycznym, jak ten, który się popsuł. Po wymianie uszkodzonego dysku administrator rozpoczął procedurę odtworzenia danych. Który z wymienionych poniżej zestawów kopii zapasowych będzie wykorzystywał administrator, aby przywrócić najpełniejszą wersję danych witryn sieci Web? (wybierz wszystkie właściwe odpowiedzi)
- A. Zestaw kopii zapasowej wykonanej we wtorek
 - B. Zestaw kopii zapasowej wykonanej w środę
 - C. Zestaw kopii zapasowej wykonanej w czwartek
 - D. Zestaw kopii zapasowej wykonanej w piątek
 - E. Zestaw kopii zapasowej wykonanej w sobotę
- O. Rooslan jest odpowiedzialny za wykonywanie kopii zapasowych serwera intranetu oddziału przedsiębiorstwa. Serwer ten działa pod kontrolą systemu Windows Server 2003 i uruchomiony na nim został program IIS. W serwerze zainstalowany jest pojedynczy dysk fizyczny zawierający wolumin sformatowany w systemie NTFS, na którym został udostępniony folder Wwwwroot. Do tego udziału mają dostęp wyłącznie administratorzy i pracownik odpowiedzialny za utrzymanie serwera intranetu. Pracownik odpowiedzialny za utrzymanie serwera intranetu ma ten udział przypisany poprzez skrypt logowania do oddzielnej litery dysku. Rooslan wykonuje kopię zapasową ASR serwera każdego pierwszego dnia miesiąca. W każdy poniedziałek o godzinie 7:00 Rooslan wykonuje pełną kopię zapasową foldera Wwwwroot wraz z jego podfolderami, jak również kopiowane są dane o stanie systemu. We wtorek, w środę, czwartek i piątek o godzinie 8:00 Rooslan wykonuje przyrostową kopię zapasową foldera Wwwwroot i jego podfolderów. W trakcie weekendu nie jest wykonywana żadna kopia zapasowa. Wszystkie kopie zapasowe są zapisywane na taśmie DAT i oznaczane są zgodnie z dniem tygodnia, w którym zostały wykonane. W czwartek po lunchu pracownik odpowiedzialny za utrzymanie serwera Intranetu powiadomił Rooslana, że rano serwer został zaatakowany przez wirus. Wirus usunął wszystkie dokumenty jego dysku twardego oraz wszystkie pliki i foldery w katalogu Wwwwroot, który był zamapowany. W serwerowni Rooslan odnalazł taśmy kopii zapasowych wykonanych w ciągu ostatnich

siedmiu dni. Które taśmy kopii zapasowych będą potrzebne do przywrócenia najpełniejszej wersji plików witryny Web? (wybierz wszystkie właściwe odpowiedzi)

- A. Taśma zapisana w poniedziałek
- B. Taśma zapisana we wtorek
- C. Taśma zapisana w środę
- D. Taśma zapisana w czwartek
- E. Taśma zapisana w piątek

6.7. Oksana jest odpowiedzialna za administrację kilku serwerów plików wydziału lokalnego szkoły wyższej. W każdym serwerze plików zainstalowane zostały trzy dyski twarde. Pierwszy dysk zawiera pojedynczy wolumin, na którym przechowywane są pliki systemu operacyjnego i programów. Pozostałe dwa dyski tworzą pojedynczy wolumin łączony. Wszystkie foldery udostępnione umieszczone zostały na woluminie łączonym. Kopie zapasowe zapisywane są co M godziny na taśmie L > AT. Pełna kopia zapasowa wszystkich plików i folderów woluminu łączonego, wliczając w to dane o stanie systemu (System State), wykonywana jest w każdą niedzielę o godzinie 5:00. Przyrostowe kopie zapasowe wykonywane są w poniedziałki, środy i piątki o godzinie 6:00. Każda taśma oznaczana jest zgodnie z dniem tygodnia, w którym została zapisana. W piątek wczesnym popołudniem awarii uległ dysk woluminu łączonego. Oksana wymieniła uszkodzony dysk i ponownie utworzyła wolumin łączony. Która z wymienionych poniżej procedur prawidłowo opisuje kolejność odtwarzania taśm na woluminie łączonym?

- A. Taśma zapisana w niedzielę, po której odtworzona zostanie taśma piątkowa
- B. Taśma zapisana w piątek, po której odtworzona zostanie taśma zapisana w niedzielę
- C. Taśma zapisana w niedzielę, po której odtworzona zostanie taśma poniedziałkowa, środowa i piątkowa.
- D. Taśma zapisana w piątek, po której odtwarzane są taśmy zapisane w środę, poniedziałek, a na koniec odtworzona zostanie taśma zapisana w niedzielę.
- E. Taśma zapisana w niedzielę, po której odtwarzane są taśmy zapisane w poniedziałek i piątek

Rooslan opiekuje się systemem Windows Set ver 200.3. Serwer używany jest do przeprowadzania analiz naukowych doświadczeń. W serwerze zainstalowane są cztery dyski twarde SCSI. Na jednym dysku zainstalowany jest pojedynczy wolumin, na którym przechowywany jest system operacyjny i program analizy danych. Pozostałe trzy dyski SCSI tworzą pojedynczy wolumin rozłożony. Na woluminie rozłożonym przechowywane są zarówno przetworzone, jak i nieprzetworzone dane. Pełna kopia zapasowa woluminu rozłożonego wykonywana jest codziennie o 6:00. Różnicowa kopia zapasowa woluminu rozłożonego wykonywana jest co cztery godziny - o godzinie 10:00, o 14:00, o 18:00 i o 22:00. Dla zapisu kopii zapasowych codziennie używanych jest pięć taśm DAT, jedna taśma dla każdej kopii zapasowej. Taśmy oznaczane są nazwą dnia tygodnia oraz godziną, o której dana kopia została wykonana. O godzinie 19:08 we wtorek jeden z dysków twardych SCSI zestawu rozłożonego uległ awarii. Rooslan wymienił uszkodzony dysk i utworzył nowy wolumin rozłożony do godziny 19:30. Rooslan dysponuje 10 ostatnimi taśmami DAT kopii zapasowych tego serwera. Które z wymienionych taśm powinien zastosować Rooslan, aby w jak najkrótszym czasie odtworzyć dane zestawu rozłożonego?

- A. Taśma pełnej kopii zapasowej zapisanej we wtorek o godzinie 6:00, po której odtwarzana jest taśma różnicowej kopii zapasowej zapisanej we wtorek o godzinie 18:00.
- B. Taśma kopii zapasowej zapisanej we wtorek o godzinie 18:00, po której odtwarzana jest taśma zapisana we wtorek o godzinie 6:00.

- C. Taśma zapisana we wtorek o godzinie 18:00, po której odtwarzana jest taśma zapisana we wtorek o godzinie 14:00, a na koniec odtwarzana jest wtorkowa z godziny 6:00.
- D. Taśma zapisana we wtorek o godzinie 6:00, po której odtwarzana jest taśma zapisana we wtorek o godzinie 10:00, następnie wtorkowa taśma z godziny 14:00, a na koniec odtwarzana jest wtorkowa z godziny 18:00.
- E. Odtworzyć należy jedynie taśmę zapisaną we wtorek o godzinie 18:00.

8.

Mick jest administratorem systemu Windows Server 2003. Serwer jest używany do obsługi folderów udostępnionych oddziału lokalnego lotniska. Na serwerze zainstalowane są dwa dyski twarde SCSI. Każdy z nich obsługuje pojedynczy wolumin. Pierwszy wolumin przechowuje pliki systemu operacyjnego i pliki programów. Na drugim woluminie obsługiwane są foldery udostępnione. Kopie zapasowe serwera wykonywane są codziennie i są zapisywane na oddzielnych taśmach DAT oznaczanych dniem tygodnia, w którym dana kopia została wykonana. Procedura wykonywania kopii zapasowych przedstawia się następująco:

Sobota godzina 4:00 - pełna kopia zapasowa
Niedziela godzina 4:00 - różnicowa kopia zapasowa
Poniedziałek godzina 5:30 - przyrostowa kopia zapasowa
Wtorek godzina 4:00 - różnicowa kopia zapasowa
Środa godzina 5:30 - przyrostowa kopia zapasowa
Czwartek godzina 4:00 - różnicowa kopia zapasowa
Piątek godzina 5:40 - przyrostowa kopia zapasowa

W czwartek o godzinie 13:34 awarii uległ dysk obsługujący wolumin, na którym przechowywane były foldery udostępnione. Mick dysponował dyskiem zapasowym i w ciągu pół godziny ponownie utworzył wolumin. Mick ma dostęp do taśm kopii zapasowych z ostatnich 10 dni. Która z poniższych metod odtwarzania taśm opisuje kolejność przywracania, jaką powinien zastosować Mick, aby odtworzone pliki folderów udostępnionych były najbardziej zbliżone do ich wersji pierwotnej?

- A. Taśma zapisana w sobotę
- B. Taśma zapisana w czwartek, po której kolejno odtwarzane są taśmy środowa, poniedziałkowa, a na końcu taśma zapisana w sobotę.
- C. Taśma zapisana w czwartek, po której kolejno odtworzone zostaną taśmy zapisane we wtorek, w niedzielę, a na końcu odtworzona zostanie taśma sobotnia.
- D. Taśma zapisana w sobotę, po której odtworzone zostaną taśmy zapisane w niedzielę, we wtorek, a na koniec odtworzona zostanie taśma zapisana w czwartek.
- E. Taśma zapisana w sobotę, po której odtwarzana jest taśma poniedziałkowa, a na końcu odtworzona zostanie taśma zapisana w środę.
- F. Taśma zapisana w sobotę, po której odtwarzane są kolejno taśmy poniedziałkowa, środowa, a na końcu odtwarzana jest taśma zapisana w czwartek.

9.

Laherty jest administratorem systemu Windows Server 2003. Na serwerze tym uruchomiony jest program IIS, który służy do obsługi kilku witryn sieci Web. W serwerze zainstalowane zostały cztery dyski twarde SCSI. Na pierwszym dysku SCSI utworzony jest pojedynczy wolumin zawierający pliki systemu operacyjnego i pliki programów. Pozostałe trzy dyski twarde są skonfigurowane jako macierz RAID-5 i tworzą wolumin, na którym przechowywane są wszystkie dane witryn sieci Web. Kopia

zapasowa woluminu RAID-5 wykonywana jest co 24 godziny i zapisywana na odrębnych taśmach DAT. Harmonogram wykonywania kopii zapasowych jest następujący:

Piątek godzina 6:00 - pełna kopia zapasowa wliczając w to dane o stanie systemu

Sobota godzina 6:00 - różnicowa kopia zapasowa

Niedziela godzina 6:00 - przyrostowa kopia zapasowa

Poniedziałek godzina 6:00 - różnicowa kopia zapasowa

Wtorek godzina 6:00 - przyrostowa kopia zapasowa

Środa godzina 6:00 - różnicowa kopia zapasowa

Czwartek godzina 6:00 - przyrostowa kopia zapasowa Poniższe pliki są zapisywane lub modyfikowane w dniu i o godzinie wyspecyfikowanej obok każdego pliku:

rileA.hun	Utworzony w piątek o 13:00
FilcB.htm	Zmodyfikowany w sobotę o 14:00
FileC.htm	Zmodyfikowany w niedzielę o 10:00
FileI).htni	Utworzony w poniedziałek o 9:00
lilcF.lilm	Zmodyfikowany we wtorek o 11:00
lilcl.htm	Zmodyfikowany w środę o 16:00

W czwartek o 17:12 wirus zaatakował system Windows Server 2003 i usunął wszystkie dane przechowywane na woluminie RAID 5. Iaherty usunął wirus z serwera i rozpoczął przywracanie danych. Na początku odtworzył wszystkie pliki kopii zapasowej wykonanej w piątek, a następnie kolejno odtworzył wszystkie pliki kopii sobotniej, poniedziałkowej, środowej, a na koniec odtworzył kopię Czwartkową. Przy użyciu opisanej procedury, które pliki nie zostaną odtworzone lub dla których nie zostanie odtworzona ich najnowsza wersja?

- A. FilcA.htm
- B. Filcli.htm
- C. PilcC.htm
- D. FileD.htm
- 1. lilcE.lum
- F. FilcF.htm

Odpowiedzi do zadania 5.4

1. Prawidłowa odpowiedź: E

- A. **Nieprawidłowo** Na woluminach rozłożonych nie są zapisywane sumy kontrolne i tym samym, jeśli jeden dysk zestawu ulega awarii, wszystkie dane woluminu zostają utracone. Wolumin taki musi być odtworzony w oparciu o taśmy kopii zapasowych.
- B. **Nieprawidłowo** Funkcja ASR przywraca pliki systemowe, a nie dane. Dla danych musi być wykonywana kopia zapasowa niezależna od procedur ASR.

- C. **Nieprawidłowo** Na woluminach rozłożonych nie są zapisywane sumy kontrolne i tym samym, jeśli jeden dysk zestawu ulega awarii, wszystkie dane woluminu zostają utracone. Wolumin taki musi być odtworzony w oparciu o taśmy kopii zapasowych. W tym przypadku nie będą przydatne dane o stanie systemu, gdyż wszystkie utracone dane znajdowały się w folderach udostępnionych.
- D. **Nieprawidłowo** Opisana procedura byłaby prawidłowa, gdyby kopie zapasowe wykonywane od poniedziałku do soboty były kopiami różnicowymi, a nie przyrostowymi. Zastosowanie opisanej metody spowoduje, że nie zostałyby przywrócone żadne pliki zmienione po godzinie 2:00 w niedzielę do zakończenia procesu tworzenia kopii zapasowej rozpoczętej o godzinie 2:00 w środę.
- E. **Prawidłowo** Jest to prawidłowa procedura. Ponowne utworzenie woluminu rozłożonego oznacza, że wolumin taki nie zawiera danych. Podczas odtwarzania danych należy upewnić się, że wykorzystane zostaną zestawy pełnej kopii zapasowej oraz wszystkie przyrostowe kopie zapasowe, co oznacza, że przywróconych zostanie możliwie jak najwięcej danych.

2. Prawidłowe odpowiedzi: A, D oraz E

- A. **Prawidłowo** Taśma piątkowa zawiera pełną kopię zapasową i będzie zawierać kopię pliku, jako że plik ten istniał już w piątek o godzinie 22:00.
 - B. **Nieprawidłowo** Ponieważ nikt nie otwierał pliku przez weekend, plik nie mógł być zmieniony, co oznacza, że nie został dołączony do listy plików różnicowej kopii zapasowej.
 - C. **Nieprawidłowo** Ponieważ nikt nie otwierał pliku przez weekend, plik nie mógł być zmieniony, co oznacza, że nie został dołączony do listy plików różnicowej kopii zapasowej.
 - D. **Prawidłowo** Plik został zmieniony w poniedziałek i tym samym został tego dnia zapisany na taśmie kopii zapasowej. Ponieważ wykonywana jest różnicowa kopia, bit archiwalny nie został ustawiony.
 - E. **Prawidłowo** Pomimo, że plik został zmieniony w poniedziałek, bit archiwalny nie został ustawiony (różnicowa kopia zapasowa). Oznacza to, że wtorkowa taśma będzie również zawierać kopię pliku.
- E **Nieprawidłowo** Plik został usunięty w środę, tak więc taśma środowa nie będzie zawierać tego pliku.

Prawidłowe odpowiedzi: A oraz C

3.

- A. **Prawidłowo** Wszystkie pięć plików znajduje się na taśmie poniedziałkowej, chociaż dwa z nich zostały zmodyfikowane w następnych dniach tygodnia.
- B. **Nieprawidłowo** Jedynie dwa pliki, które zostały zmodyfikowane w tym tygodniu będą znajdowały się na czwartkowej taśmie.
- C. **Prawidłowo** Ponieważ kopia zapasowa w czwartek wykonywana jest o godzinie 2:00, pliki będą się na niej znajdować. Pliki zostały usunięte w czwartek wieczorem. Zmiany drugiego pliku poczynione zostały w środę po południu, co oznacza, że kopia zapasowa tego pliku została pierwszy raz wykonana w czwartek rano.
- D. **Nieprawidłowo** Arkusz kalkulacyjny, który został zmodyfikowany w środę po południu nie będzie znajdował się na środowej taśmie kopii zapasowej, ponieważ ta różnicowa kopia zapasowa wykonywana jest w środę o godzinie 2:00.
- E. **Nieprawidłowo** Na taśmie wtorkowej kopii zapasowej będzie się znajdować arkusz kalkulacyjny zmodyfikowany w poniedziałek po południu.

4.

Prawidłowe odpowiedzi: A oraz D

- A. Prawidłowo Ten zestaw kopii zapasowej zawiera dane o stanie systemu, których częścią składową jest metabaza programu IIS, jak również wszystkie pliki witryn sieci Web aktualne we wtorek rano.
- B. Nieprawidłowo Środowa kopia zapasowa nie jest potrzebna, ponieważ wszystkie pliki, które zawiera, znajdować się będą w zestawie kopii zapasowej wykonanej w piątek. Ten zestaw kopii byłby jednak potrzebny, jeśli wykonywana byłaby kopia przyrostowa, a nie różnicowa.
- C. Nieprawidłowo Czwartkowa kopia zapasowa nie jest potrzebna, ponieważ wszystkie pliki, które zawiera, znajdować się będą w zestawie kopii zapasowej wykonanej w piątek. Ten zestaw kopii byłby jednak potrzebny, jeśli wykonywana byłaby kopia przyrostowa, a nie różnicowa.
- D. Prawidłowo Ten zestaw kopii zapasowej będzie zawierał wszystkie pliki zmodyfikowane pomiędzy pełną kopią zapasową wykonaną we wtorek rano a początkiem wykonywania kopii piątkowej. Utracone zostaną wszystkie pliki zmodyfikowane w piątek w ciągu dnia, ponieważ sobotnia kopia zapasowa nie zakończyła się przed awarią dysku.
- E. Nieprawidłowo Ta kopia zapasowa nie zakończyła się i nie nadaje się do odtwarzania, ponieważ przed jej zakończeniem nastąpiła awaria dysku.

5. 6.

Prawidłowe odpowiedzi: A, B, C oraz I)

- A. Prawidłowo Poniedziałkowa taśma zawiera wszystkie pliki w pierwotnej postaci. Każdy plik, który został zmodyfikowany może zostać zastąpiony poprzez odtworzenie taśm zapisanych w następnych dniach tygodnia.
- B. Prawidłowo Na tej taśmie znajdują się wszystkie pliki, które zostały zmodyfikowane pomiędzy poniedziałkiem a wtorkiem.
- C. Prawidłowo Na tej taśmie znajdują się wszystkie pliki, które zostały zmodyfikowane pomiędzy wtorkiem a środą.
- D. Prawidłowo Na tej taśmie znajdują się wszystkie pliki, które zostały zmodyfikowane pomiędzy środą a piątkiem.
- E. Nieprawidłowo Taśma piątkowa nie została jeszcze zapisana.

Prawidłowa odpowiedź: C

- A. Nieprawidłowo Opuszczone zostały przyrostowe kopie zapasowe wykonane w poniedziałek i środę.
- B. Nieprawidłowo Opuszczone zostały przyrostowe kopie zapasowe wykonane w poniedziałek i środę, jak również nowsze pliki piątkowej kopii zapasowej zostaną zastąpione starszymi plikami taśmy poniedziałkowej.
- C. Prawidłowo Jest to prawidłowy sposób odtworzenia woluminu. Najpełniejszy zestaw zostanie zapisany jako pierwszy, po czym wraz z odtwarzaniem kolejnych kopii przyrostowych, coraz nowsze wersje plików zastępują ich wersje starsze. Najnowsza kopia przyrostowa zapisana jest na taśmie piątkowej.
- D. Nieprawidłowo Opisana została odwrotna kolejność odtwarzania kopii zapasowych. Taki sam rezultat można uzyskać odtwarzając jedynie taśmę zapisaną w niedzielę.
- E. Nieprawidłowo Opuszczone zostały pliki, które były modyfikowane pomiędzy poniedziałkiem a środą.

7.

Prawidłowa odpowiedź: A

- A. Prawidłowo** Najpierw należy odtworzyć wszystkie dane, które istniały na woluminie we wtorek o godzinie 6:00. Taśma zapisana we wtorek o 18:00 zastąpi te pliki, które zostały zmienione oraz doda nowo utworzone pliki powstałe od utworzenia pełnej kopii zapasowej zapisanej we wtorek o 6:00.
- B. Nieprawidłowo** Odtwarzanie w takiej kolejności przywróci wszystkie pliki utworzone lub zmodyfikowane, powstałe po wykonaniu kopii zapasowej we wtorek o godzinie 6:00. Wszystkie zmodyfikowane pliki zostaną zastąpione przez pliki, które istniały we wtorek o godzinie 6:00. W ten sposób wszystkie pliki zmodyfikowane po porannej pełnej kopii zapasowej zostaną utracone poprzez ich zastąpienie starszymi plikami.
- C. Nieprawidłowo** Odtwarzanie w takiej kolejności przywróci wszystkie pliki utworzone lub zmodyfikowane powstałe po wykonaniu kopii zapasowej we wtorek o godzinie 6:00. Wszystkie zmodyfikowane pliki zostaną zastąpione przez pliki, które istniały we wtorek o godzinie 6:00. W ten sposób wszystkie pliki zmodyfikowane po porannej pełnej kopii zapasowej zostaną utracone poprzez ich zastąpienie starszymi plikami.
- D. Nieprawidłowo** Pomimo, że dane zostaną prawidłowo odtworzone, metoda ta nie minimalizuje czasu potrzebnego do przywrócenia plików. Taki sam rezultat można uzyskać odtwarzając po prostu taśmę zapisaną we wtorek o godzinie 6:00, po której odtworzona zostanie taśma z godziny 18:00. Tak więc stosując opisaną w odpowiedzi metodę, dwie taśmy będą odtwarzane niepotrzebnie.
- Ii. Nieprawidłowo** W ten sposób odtworzone zostaną jedynie pliki zmienione lub utworzone od momentu wykonania wtorkowej kopii zapasowej z godziny 6:00. Wszystkie pliki istniejące na serwerze, które nie zostały zmienione lub utworzone w ciągu ostatnich 13 godzin, nie zostaną przywrócone.

Prawidłowa odpowiedź: F

8.

- A. Nieprawidłowo** Działanie takie przywróci pliki folderów udostępnionych, które były aktualne sześć dni przed awarią.
- B. Nieprawidłowo** Jest to odpowiedni zestaw taśm, ale przyjęta została odwrotna kolejność ich odtwarzania, tak więc wszystkie pliki -zmodyfikowane w ciągu ostatnich sześciu dni zostaną zastąpione, ich wersjami, które istniały poprzedniej soboty rano.
- & Nieprawidłowo** Działanie takie oznacza, że nie wszystkie pliki zostaną odtworzone, a także że nowsze wersje plików zostaną zastąpione ich starszymi wersjami.
- D. Nieprawidłowo** Zrozumienie, dlaczego ta odpowiedź jest nieprawidłowa, jest trochę bardziej złożone. Przy zastosowaniu opisanej procedury, ze względu na naturę kopii zapasowych, każdy plik zapisany pomiędzy godziną 4:00 w niedzielę a godziną 5:30 w poniedziałek nie zostanie odtworzony. Dzieje się tak, ponieważ kopia zapasowa wykonana w poniedziałek o 4:00 zeruje bit archiwalny i tym samym wtorkowa różnicowa kopia zapasowa zapisuje jedynie pliki zmienione po wykonaniu poniedziałkowej kopii zapasowej. Ta sama uwaga dotyczy plików zapisanych pomiędzy wtorkiem i środą rano.
- E. Nieprawidłowo** Opisana sekwencja pomija pliki zapisane pomiędzy godziną 5:30 w środę a godziną 4:00 w czwartek.
- F. Prawidłowo** Opisana sekwencja pozwoli odtworzyć najbardziej pełną wersję plików folderów udostępnionych, czyli wszystkie pliki, które istniały w folderze do godziny 4:00 w czwartek.

Prawidłowe odpowiedzi: B oraz D

- A. **Nieprawidłowo** Plik FileA.htm będzie przywrócony po odtworzeniu kopii zapasowej wykonanej w sobotę.
- B. **Prawidłowo** Najnowsza wersja pliku FileB.htm nie zostanie odtworzona. Bit archiwalny został ustawiony podczas wykonywania niedzielnej kopii zapasowej, co oznacza, że różnicowa kopia poniedziałkowa pominie ten plik.
- C. **Nieprawidłowo** Plik FileC.htm będzie przywrócony po odtworzeniu kopii zapasowej wykonanej w poniedziałek.
- D. **Prawidłowo** Plik FileD.htm nie zostanie odtworzony. Bit archiwalny został ustawiony podczas wykonywania wtorkowej kopii zapasowej, co oznacza, że różnicowa kopia środowa pominie ten plik.
- E. **Nieprawidłowo** Plik FileE.htm będzie przywrócony po odtworzeniu różnicowej kopii zapasowej wykonanej w środę.
- F. **Nieprawidłowo** Plik FileF.htm będzie przywrócony po odtworzeniu przyrostowej kopii zapasowej wykonanej w czwartek.

Zadanie 5.5

Planowanie zadań kopii zapasowych

Zadania związane z wykonywaniem kopii zapasowych powinny być uruchamiane w okresach minimalnego wykorzystywania serwera. Oznacza to najczęściej godziny nocne, a nie normalne godziny pracy administratora w biurze. Dla uniknięcia konieczności przychodzenia do pracy o godzinie drugiej w nocy lub nawiązywania o tej porze połączenia programu Terminal Services (Usługi terminalowe), program Backup Utility (Kopia zapasowa) systemu Windows Server 2003 umożliwia zaplanowanie zadań kopii zapasowych.

Dostępne są różne opcje tworzenia harmonogramu. Zadania mogą być skonfigurowane tak, aby rozpoczynały się podczas uruchamiania systemu, wtedy, kiedy system jest bezczynny, kiedy użytkownik się zalogował, codziennie, co tydzień lub co miesiąc. Zadania mogą zostać skonfigurowane, aby rozpoczynały się co tydzień, co drugi tydzień lub co każdy setny tydzień, podobnie mogą być uruchamiane codziennie, co drugi dzień bądź CO każdy setny dzień.

Administratorzy najczęściej tworzą na serwerze kilka zaplanowanych zadań. Jedno wykonuje pełną kopię zapasową w określonym dniu tygodnia, a inne wykonują przyrostową lub różnicową kopię zapasową w pozostałe dni tygodnia. Typ harmonogramu zależy od typu nośnika używanego do zapisywania zestawów kopii zapasowych. Przyrostowe kopie zapasowe wykonywane przez sześć dni po pełnej kopii zapasowej zabierają mniej czasu i miejsca niż różnicowe kopie zapasowe.

Pytania do zadania 5.5

1. Administrator opracowuje strategię tworzenia kopii zapasowych dla systemu Windows Server 2003, na którym uruchomiony został program IIS. Serwer wyposażony jest w pojedynczy dysk twardy, który, obsługuje pojedynczy wolumin. Należy osiągnąć następujące cele:

Cel główny: Wykonanie pełnej kopii zapasowej raz w tygodniu.

Cele pomocnicze: Skopiowanie metabazy programu IIS w poniedziałek, środę i piątek. Zapewnienie, żeby wszystkie pliki zmodyfikowane lub utworzone od momentu wykonania ostatniej pełnej kopii zapasowej zapisywane były we wtorek i w czwartek.

Które z wymienionych poniżej zestawów kopii zapasowych spełniają wszystkie postawione wymagania? (wybierz wszystkie właściwe odpowiedzi)

- A. Pełna kopia zapasowa wykonywana każdej niedzieli o godzinie 2:00. Codzienna kopia zapasowa wraz z danymi o stanie systemu wykonywana w poniedziałki, środy i piątki o godzinie 3:00.
- B. Pełna kopia zapasowa wykonywana w poniedziałek o godzinie 2:00. Codzienna kopia zapasowa wraz z danymi o stanie systemu wykonywana w środę, piątek i niedzielę o godzinie 3:00. Różnicowa kopia zapasowa wykonywana we wtorek i w czwartek o godzinie 3:30.

- C. Pełna kopia zapasowa wraz z danymi o stanie systemu wykonywana w piątek o 23:00. Przyrostowa kopia zapasowa wraz z danymi o stanie systemu wykonywana w środę i poniedziałek o godzinie 23:30. Różnicowa kopia zapasowa wykonywana we wtorek i w czwartek o godzinie 23:30.
- D. Pełna kopia zapasowa wraz z danymi o stanie systemu wykonywana w środę o 23:00. Codzienna kopia zapasowa wraz z danymi o stanie systemu wykonywana w poniedziałek i piątek o godzinie 23:00. Różnicowa kopia zapasowa wraz z danymi o stanie systemu wykonywana we wtorek i w czwartek o godzinie 23:00.
- E. Przyrostowa kopia zapasowa wraz z danymi o stanie systemu wykonywana w poniedziałek, środę i piątek o godzinie 2:00. Różnicowa kopia zapasowa wraz z danymi o stanie systemu wykonywana we wtorek i w czwartek o godzinie 2:00. Kopia zapasowa typu Kopia wykonywana w niedzielę o godzinie 2:00.

2.

Rooslan opracowuje strategię wykonywania kopii zapasowych dla czterech systemów Windows Server 2003, które są używane do udostępniania plików wydziału uniwersyteckiego. Urządzenia sprzętu każdego systemu Windows Server 2003 są odporne na uszkodzenia i tym samym cel podstawowy strategii wykonywania kopii zapasowych dotyczy przywracania usuniętych bądź zgubionych plików, jak również ich rozmieszczania, a nie odtwarzania plików po awarii. Obowiązuje również zasada wydziału narzucająca wymóg wykonywania raz w tygodniu obrazu danych o stanie systemu serwerów pliku w lokalizacji archiwalnej w okresie 20 lat. Strategia wykonywania kopii zapasowych opracowywana przez Rooslana powinna uwzględniać następujące założenia:

Warunek 1: Co najmniej raz w tygodniu musi być wykonana jedna kopia zapasowa wszystkich plików i folderów każdego systemu Windows Server 2003.

Warunek 2: Maksymalnie dwa zestawy kopii zapasowych mogą być używane podczas dowolnych operacji związanych z odtwarzaniem pojedynczego pliku, wliczając w to pełne przywrócenie wszystkich plików i folderów serwera.

Warunek 3: Powinna istnieć możliwość odzyskiwania plików w oparciu o ich dzienne kopie. Jeśli plik został zmieniony we wtorek, środę i czwartek, na podstawie zestawów kopii zapasowych musi istnieć możliwość odzyskania trzech różnych wersji tego pliku. Kilka kopii tego samego pliku nie jest potrzebnych do spełnienia warunku 3.

Która z opisanych poniżej strategii wykonywania kopii zapasowych spełni postawione wymagania? (wybierz wszystkie właściwe odpowiedzi)

- A. Pełna kopia zapasowa każdego serwera wykonywana w poniedziałki o godzinie 1:30. Kopia zapasowa typu Kopia wykonywana dla każdego serwera codziennie o godzinie 2:00 za wyjątkiem poniedziałku.
- B. Pełna kopia zapasowa każdego serwera wykonywana w czwartki o godzinie 22:00. Przyrostowa kopia zapasowa wykonywana dla każdego serwera codziennie o godzinie 23:00 za wyjątkiem poniedziałków.
- C. Pełna kopia zapasowa wszystkich plików i folderów każdego serwera wykonywana codziennie o godzinie 21:00.
- D. Pełna kopia zapasowa wszystkich plików i folderów każdego serwera wykonywana o 23:00 w poniedziałki, środy, piątki i soboty. Przyrostowa kopia zapasowa wszystkich serwerów wykonywana we wtorki, czwartki i niedziele o godzinie 23:00.

- o. Oksana opracowuje strategię wykonywania kopii zapasowych dla systemu Windows Server 2003, na którym uruchomiony został program IIS. Na serwerze utrzymywane są witryny sieci Web charakteryzujące się dużym ruchem oraz częstymi aktualizacjami danych (praktycznie co godzinę). Niektóre aspekty konfiguracji programu IIS zmieniane są w ciągu tygodnia. Kopie zapasowe muszą być wykonywane regularnie. Strategia opracowywana przez Oksanę powinna uwzględniać następujące warunki:

Warunek 1: Pełna kopia wszystkich danych witryny sieci Web musi być wykonywana co najmniej raz na dwa tygodnie.

Warunek 2: Dane o stanie systemu muszą być zapisywane co najmniej dwa razy na tydzień.

Warunek 3: Żadna kopia zapasowa za wyjątkiem pełnej kopii zapasowej nie powinna zawierać plików i folderów, które nie zostały zmienione lub utworzone w ciągu ostatnich 24 godzin. Wyjątkiem od tej zasady są dane o stanie systemu.

Który Z wymienionych poniżej harmonogramów wykonywania kopii zapasowych spełni wszystkie trzy warunki!"

- A. Pełna kopia zapasowa wybranych plików i folderów wykonywana w poniedziałki o godzinie 23:50. Przyrostowa kopia zapasowa wybranych plików i folderów wykonywana codziennie o godzinie 23:55 z wyjątkiem poniedziałków.
- B. Pełna kopia zapasowa wybranych plików i folderów wykonywana co drugi poniedziałek o godzinie 23:50. Różnicowa kopia zapasowa wybranych plików i folderów wykonywana codziennie o godzinie 23:55 z wyjątkiem poniedziałków. Kopia zapasowa danych o stanie systemu wykonywana w poniedziałki, środy i piątki o godzinie 14:00.
- C. Pełna kopia zapasowa wybranych plików i folderów wykonywana co drugi poniedziałek o godzinie 12:05. Przyrostowa kopia zapasowa wybranych plików i folderów, wliczając w to dane o stanie systemu, wykonywana codziennie o godzinie 23:55.
- D. Pełna kopia zapasowa wybranych plików i folderów wykonywana co drugi poniedziałek o godzinie 12:05. Codzienna kopia zapasowa wybranych plików i folderów, wliczając w to dane o stanie systemu, wykonywana codziennie o godzinie 23:59.
- E. Pełna kopia zapasowa wybranych plików i folderów wykonywana co drugi poniedziałek o godzinie 12:05. Kopia zapasowa rypu Kopii wybranych plików i folderów, wliczając, w to dane o stanie systemu, wykonywana codziennie o godzinie 23:59.
4. Wymienieni poniżej użytkownicy mają konta, które należą do odpowiednich grup autonomicznego systemu Windows Server 2003.

Orin - Administrators (Administratorzy)

Oksana - Backup Operators (Operatorzy kopii zapasowych)

Rooslan - Power Users (Użytkownicy zaawansowani)

Mick - Replicator (Replikator)

Laherty - Network Configuration Operators (Operatorzy konfiguracji sieci)

Lokalna zasada grupy nie zmienia kont żadnego z tych użytkowników lub grup. Pełna kopia zapasowa wszystkich plików i folderów serwera, wliczając w to dane o stanie systemu, wykonywana jest codziennie o godzinie 2:00. W konfiguracji tego harmonogramu, w programie Backup Utility (Kopia zapasowa) zaznaczone zostało, żeby to zadanie kopii zapasowej uruchamiane było za pomocą konta

o odpowiednich uprawnieniach. Które z wymienionych kont użytkownika ma wystarczające uprawnienia do uruchamiania tego zadania kopii zapasowej?

- A. Orin
- B. Oksana
- C. Rooslan
- D. Mick
- E. Laherty

Odpowiedzi do zadania 5.5

1. Prawidłowe odpowiedzi: B oraz D

- A. **Nieprawidłowo** Działanie takie umożliwi zrealizowanie celu głównego oraz pierwszego celu pomocniczego. Nie zostanie osiągnięty drugi cel pomocniczy.
- B. **Prawidłowo** Działanie takie umożliwi zrealizowanie celu głównego oraz obu wymagań pomocniczych. Metabaza kopiowana jest pod /.as wykonywania kopii zapasowej danych o stanie systemu. Oznacza to, że metabaza będzie kopiowana w poniedziałek, środę, piątek oraz w niedzielę. Kopia zapisywana w niedzielę nie jest potrzebna, ale nie dyskwalifikuje rozwiązania. Różnicowa kopia zapasowa wykonywana we wtorek i czwartek realizuje drugą część celu pomocniczego.
- C. **Nieprawidłowo** Działanie takie umożliwi zrealizowanie celu podstawowego oraz pierwszego celu pomocniczego. Drugi cel pomocniczy nie zostanie zrealizowany, ponieważ przyrostowa kopia zapasowa spowoduje, że podczas wykonywania wtorkowej i czwartkowej różnicowej kopii zapasowej zapisane zostaną jedynie pliki zmienione od momentu wykonania ostatniej kopii **przyrostowej**, a nie ostatniej pełnej kopii zapasowej.
- D. **Prawidłowo** Dzięki takiej procedurze cele główny i pomocnicze zostaną osiągnięte. Istotną sprawą jest zapamiętanie, że różnicowa i codzienna kopia zapasowa nie zeruje bitu archiwalnego. Następną kopią zapasową wykonywaną po kopii różnicowej lub codziennej zakłada się, że kopia pliku nie została jeszcze wykonana, jeśli plik został zmieniony lub że plik jest nowy licząc od momentu ostatniej kopii zapasowej.
- E. **Nieprawidłowo** Pomimo, że przyrostowa kopia zapasowa zeruje bit archiwalny, nie może być traktowana jako pełna kopia zapasowa serwera wykonywana raz w tygodniu. Kopia zapasowa typu Kopia nie zeruje bitu archiwalnego i dlatego działa podobnie jak kopia różnicowa.

2. Prawidłowe odpowiedzi: A, C oraz D

- A. **Prawidłowo** Pełna kopia zapasowa każdego serwera wykonywana w poniedziałki o godzinie 1:30 spełnia warunek 1. Wykorzystywanie kopii zapasowych typu Kopia spełnia warunek 2, natomiast codzienne wykonywanie tych kopii zapasowych (typu Kopia) spełnia warunek nr 3.
- B. **Nieprawidłowo** Pomimo, że pierwszy i trzeci warunek są spełnione, nie będzie spełniony warunek drugi, ponieważ w sytuacji, kiedy wykonywana jest przyrostowa kopia zapasowa, podczas odtwarzania może zachodzić konieczność użycia kilku zestawów kopii zapasowych.
- C. **Prawidłowo** Procedura spełnia wszystkie trzy warunki. W porównaniu do innych opcji, jej realizacja wymaga więcej miejsca na nośnikach kopii, ale postawione warunki są spełnione.

D. Prawidłowo Procedura spełnia wszystkie trzy warunki. Podczas odtwarzania plików wymagana będzie najwyżej jedna kopia przyrostowa i tym samym spełniony będzie warunek 2.

ó. Prawidłowe odpowiedzi: C oraz D

- A. Nieprawidłowo Ten harmonogram kopii zapasowej nie spełnia warunku drugiego.
- B. Nieprawidłowo Warunek trzeci nie będzie spełniony, jeśli stosowana będzie różnicowa kopia zapasowa.
- C. Prawidłowo Procedura ta spełnia wszystkie trzy wymagania.
- D. Prawidłowo Procedura ta spełnia wszystkie trzy wymagania. Pomimo, że codzienna kopia zapasowa nie zeruje bitu archiwalnego, za jej pomocą kopiowane będą wybrane pliki lub foldery, które zostały zmodyfikowane w danym dniu i tym samym warunek trzeci zostanie spełniony.
- E. Nieprawidłowo Kopia zapasowa typu Kopia działa podobnie do różnicowej kopii zapasowej w odniesieniu do bitu archiwalnego - bit len nie jest zerowany, jednak kopia zapasowa typu Kopia zapisuje wszystkie pliki, w tym również pliki, które nie zostały zmodyfikowane.

4. Prawidłowe odpowiedzi: A oraz B

- A. Prawidłowo Członkowie grup Administratorzy i Backup Operators (Operatorzy kopii zapasowych) posiadają odpowiednie uprawnienia umożliwiające uruchomienie zaplanowanych zadań kopii zapasowych.
- B. Prawidłowo Członkowie grup Administratorzy i Backup Operators (Operatorzy kopii zapasowych) posiadają odpowiednie uprawnienia umożliwiające uruchomienie zaplanowanych zadań kopii zapasowych.
- O Nieprawidłowo Członkowie grupy Power Users (Użytkownicy zaawansowani) nie posiadają wystarczających uprawnień do uruchomienia zaplanowanych zadań kopii zapasowych.
- I). Nieprawidłowo Członkowie grupy Replicaor (Replikator) nie posiadają wystarczających uprawnień do uruchomienia zaplanowanych zadań kopii zapasowych.
- E. Nieprawidłowo Członkowie grupy Network Configuration Operators (Operatorzy konfiguracji sieci) nie posiadają wystarczających uprawnień do uruchomienia zaplanowanych zadań kopii zapasowych.

Część III

Dodatki





Zadania egzaminacyjne omawiane w tym rozdziale:

- Rozwiązywanie problemów dotyczących programu Terminal Services (Usługi terminalowe)
- Diagnostyka i rozwiązywanie zagadnień dotyczących zabezpieczeń programu Terminal Services (Usługi terminalowe)
- Diagnostyka i rozwiązywanie zagadnień dotyczących dostępu klienta do programu Terminal Services (Usługi terminalowe)

W rozdziale 2 zostały omówione sposoby wykorzystywania programu *Terminal Services* (Usługi terminalowe), w szczególności usługi *Remote Desktop for Administration* (Pulpit zdalny dla administracji) umożliwiające podłączenie zdalne do sesji serwera z programu klienta. Usługa *Remote Desktop for Administration* (Pulpit zdalny dla administracji) jest instalowana w sposób domyślny w każdym systemie Microsoft Windows Server 2003, a po jej włączeniu w module System znajdującym się w grupie programów *Control Panel* (Panel sterowania), serwer będzie obsługiwał dwa jednocześnie połączenia dla użytkowników, którzy należą do grupy *Remote Desktop Users* (Użytkownicy pulpitu zdalnego).

Program *Terminal Services* (Usługi terminalowe) systemu Windows Serwer 2003 obsługuje również aplikacje dla wielu użytkowników, którzy jednocześnie mają uruchomione sesje. Funkcja ta, podobna do trybu *Terminal Services Application Server* systemu Windows 2000, jest obecnie nazywana *terminal Services* (Serwer terminali). W niniejszym dodatku omówiony został program *Terminal Server* oraz niektóre zagadnienia dotyczące obsługi i rozwiązywania problemów związanych ze środowiskiem programu.

Instalowanie i konfigurowanie środowiska programu Terminal Server (Serwer terminali)

Poniżej wymienione zostały główne czynniki dotyczące instalowania środowiska programu *Terminal Server* (Serwer terminali).

Komponenty programu Terminal Server

Program *Terminal Server* (Serwer terminali) może być instalowany za pomocą modułu *Add/Remove Windows Components Wizard* (Kreator składników systemu Windows). Moduł można znaleźć w aplikacji *Add/Remove Programs* (Dodaj lub usuń programy) lub wybierając program *Configure Your Server Wizard* (Kreator konfigurowania serwera) na stronie *Manage Your Server* (Zarządzanie tym serwerem). Zaleca się, aby jako serwer terminali konfigurować autonomiczne serwery członkowskie, a nie kontrolery domeny. Zalecenia dotyczące urządzeń sprzętu zostały zamieszczone w programie *Help and Support Center* (Centrum pomocy i obsługi technicznej).

Aplikacje

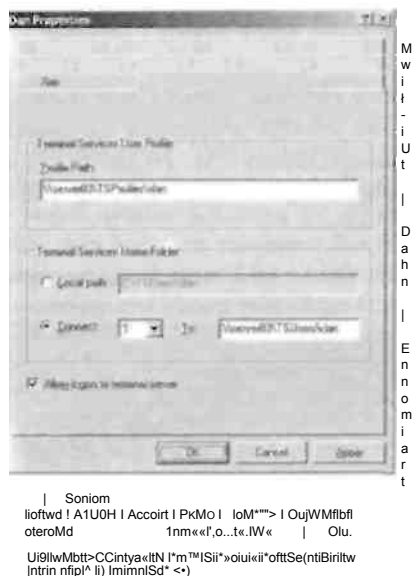
Ponieważ aplikacje serwera terminali dostarczane są jednocześnie dla wielu użytkowników, niektóre klucze rejestrów, pliki i foldery muszą być inaczej instalowane niż w przypadku serwera, który nie świadczy usług terminalowych. Aby zainstalować aplikacje na serwerze terminali, zawsze należy używać narzędzia *Add/Remove Programs* (Dodaj lub usuń programy), które znajduje się w grupie programów *Control Panel* (Panel sterowania). Narzędzie *Add/Remove Programs* (Dodaj lub usuń programy) będzie automatycznie przełączać serwer terminali w tryb instalacji zanim zostanie uruchomiona procedura instalacji aplikacji. W trybie instalacji, serwer terminali obsługuje odpowiednio konfigurację aplikacji tak, aby mogła być uruchamiana w trybie wieloużytkownikowym.

Czasami narzędzie *Add/Remove Programs* (Dodaj lub usuń programy) nie może być wykorzystywane przez aplikacje, poprawki lub inne procesy związane z instalacjami. Na przykład, producent może udostępniać aktualizacje aplikacji poprzez Internet, a uruchomienie tych aktualizacji nie może odbywać się za pośrednictwem narzędzia *Add/Remove Programs* (Dodaj lub usuń programy). W takim przypadku należy otworzyć okno wiersza poleceń i przed rozpoczęciem instalacji, użyć polecenia *Change User/Install*. Po zakończeniu procesu należy użyć polecenia *Change User/Execute*. Oprócz tego warto odnotować, że niektóre aplikacje wymagają skryptów dostosowujących proces instalacji tak, aby zmodyfikowane zostało działanie aplikacji na serwerze terminali.

Zaleca się, aby program *Terminal Server* został zainstalowany przed instalacją jakiegokolwiek aplikacji, która będzie uruchamiana w trybie wieloużytkownikowym. Podobnie, przed usunięciem programu *Terminal Server* (Serwer terminali), powinny zostać odinstalowane wszystkie aplikacje, które zostały zainstalowane do pracy w trybie wieloużytkownikowym. Jeśli zachodzi potrzeba zainstalowania dodatkowej aplikacji na istniejącym serwerze terminali, należy upewnić się przy użyciu programu *Terminal Server Connections* (Połączenia serwera terminali), czy zostały odłączone wszystkie bieżące sesje oraz czy zablokowane zostało nawiązywanie nowych połączeń (poprzez wpisanie w wierszu poleceń komendy **change logon /disable**). Po zainstalowaniu aplikacji należy wpisać w wierszu poleceń komendę **change logon /enable**, która ponownie umożliwi nawiązywanie połączeń. Włączanie lub wyłączanie połączeń usług terminalowych można również przeprowadzać na zakładce *Remote* (Zdalny) we właściwościach modułu System.

Podczas instalacji programu Terminal Server (Serwer terminali) użytkownik może wybrać dwie opcje: *Full Security* (Zabezpieczenie pełne) oraz *Relaxed Security* (Zabezpieczenie obniżone). Tryb *Full Security* (Zabezpieczenie pełne) jest trybem domyślnym, w którym chronione są niektóre pliki systemu operacyjnego i udostępnione pliki programów. Starsze aplikacje mogą nie działać przy tej bardziej chronionej konfiguracji i w takim przypadku można wybrać tryb *Relaxed Security* (Zabezpieczenia obniżone). Ustawienia te mogą być zmieniane w dowolnym momencie w konsoli *Terminal Server Configuration* (Konfiguracja serwera terminali) za pomocą zakładki *Server Settings* (Ustawienia serwera).

Wielu administratorów nie rozumie przeznaczenia foldera macierzystego usług terminalowych (*Terminal Services Home Folder*). Ustawienie to może być określane jako część właściwości konta użytkownika lub poprzez zasadę grupy. Określa ono położenie foldera, który jest wykorzystywany przez program *Terminal Services* (Usługi terminalowe) do przechowywania plików dotyczących użytkownika dla aplikacji wieloużytkownikowych. Omawiane ustawienie przedstawia rysunek A-1. Ustawienie to nie wpływa na lokalizację magazynu plików danych użytkownika. Ustawienia domyślne określają, że folder macierzysty usług terminalowych jest tworzony jako folder o nazwie Windows umieszczony w profilu użytkownika. Aby określić miejsce przechowywania danych użytkownika, należy skonfigurować standardowe ustawienie *Home Folder* (Folder macierzysty) na zakładce *Profile* (Profil) we właściwościach konta użytkownika lub stosować zalecaną metodę pizekicrowywania foldera *My Doaimcnts* (Moje dokumenty).



Rysunek A-1 *Ustawienie Terminal Services Home Folder (Folder macierzysty usług terminalowych) konta użytkownika*

Instalacja klienta programu Pulpit zdalny

Program klienta (*Mstsc.exe*) usługi *Remote Desktop* (Pulpit zdalny) jest domyślnie instalowany we wszystkich systemach Windows Server 2003 i Microsoft Windows XP. Program kliencki obsługuje wszystkie 32-bitowe platformy systemu Windows i może być instalowany za pośrednictwem zasady grupy na systemach Windows 2000, a na wcześniejszych platformach za pomocą innych metod instalowania aplikacji. Po zainstalowaniu, program klienta jest dość trudno odszukać w menu Start. Wygodniej będzie utworzyć w znanym miejscu skrót programu, który można odnaleźć w grupie programów *Accessories* (Akcesoria) w folderze Komunikacja.

Licencjonowanie

Po zakończeniu 120-dniowego okresu testowego, nie będą ustanawiane połączenia z komputerem, na którym uruchomiony jest program *Terminal Server* (Serwer terminali), chyba że serwer terminali będzie mógł uzyskać licencje klienta z serwera licencji (*Terminal Server License Server*). Dlatego, jako jeden z elementów instalowania programu *Terminal Server* należy zainstalować usługę *Terminal Server License Server* (Serwer licencji serwera terminali), przy czym zaleca się jej instalowanie na serwerze, który nie jest serwerem terminali.

Aby zainstalować program *TerminalServer Licensing* (Licencjonowanie serwera terminali), należy użyć apletu *Add/Remove Programs* (Dodaj lub usuń programy). Użytkownik będzie musiał określić, czy serwer ma być serwerem licencji przedsiębiorstwa (*Enterprise License Server*) czy domeny (*Domain License Server*). Najczęściej spotykaną konfiguracją jest Enterprise License Server, a serwer taki udostępnia licencje serwerom terminali w każdej domenie lasu systemów Windows 2000 lub Windows Server 2003. Serwer licencji domeny (*Domain License Server*) jest używany, jeśli dla każdej domeny obsługiwana jest odrębna baza danych licencji lub jeśli serwery terminali pracują w grupach roboczych bądź domenach systemu Windows NT 4.

Po zainstalowaniu programu *Terminal Server Licensing* (Licencjonowanie serwera terminali) zarządzany jest za pomocą konsoli o tej samej nazwie, która jest umieszczona w grupie programów *Administrative Tools* (Narzędzia administracyjne). Pierwszą czynnością wykonywaną przez administratora jest aktywacja serwera licencji kliknięciem prawym przyciskiem myszy ikony serwera (*Terminal Server License Server*) i wybranie polecenia *Activate Server* (Uaktywnij serwer). Po aktywowaniu serwera, muszą zostać zainstalowane pakiety licencji klienta. W programie *Help and Support Center* (Centrum obsługi i pomocy technicznej) zamieszczone zostały szczegółowe informacje opisujące ten proces. Program *Terminal Server Licensing* obsługuje dwa typy licencji dostępu klienta CAL: *Per Device* (Na urządzenie) oraz *Per Session* (Na sesję). Oba typy licencji CAL mogą być zarządzane za pomocą tego samego serwera licencji serwera terminali.

Licencjonowanie serwera terminali jest obsługiwane niezależnie od licencji dostępu serwera i klienta (CAL) dla systemu Windows Server 2003. W rozdziale 9 omówione zostały szczegółowo zagadnienia zarządzania licencjami pozostałych rodzajów serwerów i klientów.



Wskazówka egzaminacyjna Licencje CAL programu Terminal Server (Serwer terminali) są licencjami dla połączeń sesji użytkownika na serwerze terminali. W dalszym ciągu należy brać pod uwagę wyznaczenia licencjonowania dla aplikacji, do których dostęp uzyskują użytkownicy podczas swoich sesji. Należy sprawdzać wymogi umowy licencyjnej EULA (End User License Agreements) w celu określenia odpowiedniego sposobu licencjonowania aplikacji obsługiwanych na serwerze terminali.

Zarządzanie i rozwiązywanie problemów dotyczących programu Terminal Server (Serwer terminali)

Do konfigurowania serwerów terminali oraz ustawień użytkownika, połączeń i sesji programu *Terminal Services* (Usługi terminalowe) można używać kilku narzędzi. Narzędzia te to programy *Group Policy Editor* (Edytor zasady grupy), *Terminal Services Configuration* (Konfiguracja usług terminalowych), przystawka *Active Directory Users and Computers* (Użytkownicy i komputery usługi Active Directory) oraz klient programu *Remote Desktop* (Pulpit zdalny). Niniejsza sekcja omawia sposoby wykorzystywania poszczególnych narzędzi oraz opisuje najważniejsze ustawienia konfiguracji poprzez analizę tworzenia, wykorzystania i usuwania sesji użytkownika.

Punkty administracji

Nawiązywanie połączenia użytkownika z serwerem terminali powoduje powstanie kilku procesów, a na każdym z tych etapów można przeprowadzać konfigurację zmieniając działanie połączenia.

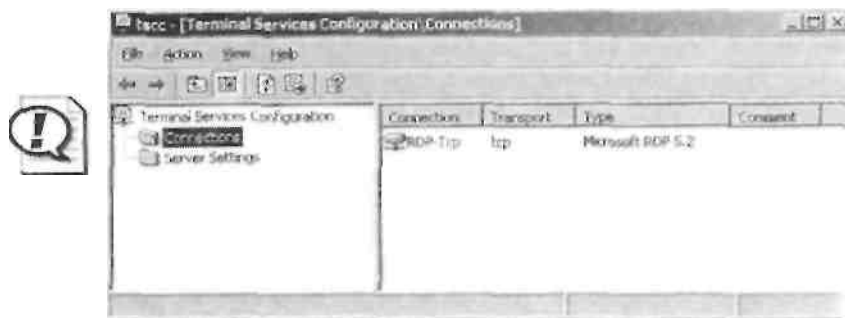
Klient programu *Remote Desktop* (Pulpit zdalny) umożliwia 32-bitowym platformom systemu Windows nawiązywanie połączenia z serwerem terminali w oparciu o protokół RDP (*Remote Desktop Protocol*). W porównaniu do poprzednich wersji usług terminalowych, obecna wersja klienta jest znacznie poprawiona i obejmuje szerszy zakres danych, które są przekierowywane (wliczając w to system plików, porty szeregowo, drukarki, dźwięk oraz strefy czasowe) oraz obsługuje połączenia przy rozdzielczości 7A bitów dla koloru. Program klienta został wyposażony w szereg ustawień, za pomocą których konfigurowane są połączenia i wrażenia użytkownika. Niektóre z tych ustawień zostały zaprezentowane, na rysunku A-2. Ustawienia zapisywane są w plikach *Remote Desktop Connection* (Połączenie pulpitu zdalnego). Pliki te mają rozszerzenie .rdp i mogą być łatwo otwierane podczas nawiązywania połączenia w innym terminie lub mogą być używane do dystrybucji dla innych jako profil połączenia. Ustawienia pliku .rdp lub klient programu *Remote Desktop* (Pulpit zdalny) określają bieżące połączenia użytkownika z serwerem terminali.



Rysunek A-2- Klient programu Remote Desktop (Pulpit zdalny)

W momencie, kiedy użytkownik nawiązuje połączenie z serwerem terminali, serwer sprawdza właściwości programu *Terminal Services* (Usługi terminalowe) konta użytkownika i określa niektóre ustawienia. Jeśli usługi terminalowe konta użytkownika przechowywane są na serwerze terminali, ustawienia programu *Terminal Services* prezentowane są we właściwościach kont użytkowników w przystawce *Local (Users and Groups)* (Użytkownicy i grupy lokalne). Konta użytkowników umieszczane są częściej w usłudze Active Directory. W takim przypadku ustawienia programu *Terminal Services* (Usługi terminalowe) prezentowane są w przystawce *Active Directory Users and Computers* (Użytkownicy i komputery usługi Active Directory) na zakładkach *Environment* (Środowisko), *Remote Control* (Sterowanie zdalne) oraz *Terminal Services Profile* (Profil usług terminalowych) w oknie dialogowym właściwości użytkownika (ustawienia zostały przedstawione poprzednio na rysunku A-1). Ustawienia konta użytkownika zastępują ustawienia klienta programu *Remote Desktop* (Pulpit zdalny).

Klient łączy się z serwerem terminali specyfikując nazwę serwera lub jego adres IP (Internet Protocol). *Terminal Server* (Serwer terminali) odbiera żądanie połączenia poprzez określoną kartę sieciową. Połączenie jest przedstawiane w postaci obiektu połączenia, który jest widoczny w konsoli *Terminal Services Configuration* (Konfiguracja usług terminalowych), jak ilustruje to rysunek A-3. Właściwości obiektu połączenia konfiguruje ustawienia, które określają wszystkie połączenia użytkownika realizowane przez kartę sieciową. Ustawienia połączenia będą zastępować ustawienia żądania klienta i ustawienia konta użytkownika.



Rysunek A-3. *Terminal Services Configuration* (Konfiguracja usług terminalowych)

Wskazówka egzaminacyjna Właściwości połączenia RDP-Tcp serwera terminali dostępne są za pośrednictwem programu *Terminal Services Configuration* (Konfiguracja usług terminalowych) i będą zastępować ustawienia konta użytkownika i klienta dla wszystkich sesji tego połączenia z tym konkretnym serwerem terminali.

Zasada grupy systemu Windows Server 2003 wyposażona została w szereg zasad dotyczących komputera i użytkownika, dzięki którym można kontrolować program *Terminal Services* (Usługi terminalowe). Konfiguracje określone przez obiekty GPO (*Group Policy Object*) będą zastępować ustawienia klienta programu *Remote Desktop* (Pulpit zdalny), ustawienia konta użytkownika lub ustawienia połączeń RDP-Tcp serwerów terminali. Oczywiście ustawienia te stosowane będą wyłącznie do użytkowników lub komputerów będących w zakresie jednostki organizacyjnej, z którą obiekt GPO został powiązany. Jeśli w środowisku występują wyłącznie serwery terminali uruchomione w oparciu o systemy operacyjne rodziny Windows Server 2003, zasada grupy będzie włączać program *Terminal Services Configuration* (Konfiguracja usług terminalowych) przy najmniejszym nakładzie zadań

administracyjnych. Zasady grupy usług terminalowych nie stosują się do serwerów terminali uruchomionych w oparciu o poprzednie wersje systemu Windows.

Narzędzie administracyjne *Terminal Services Manager* (Menedżer usług terminalowych) po ustanowieniu sesji może być wykorzystywane do monitorowania użytkowników, sesji i aplikacji na każdym serwerze terminali. Program *Terminal Services Manager* może być również używany do zarządzania serwerem oraz do podłączania, odłączania bądź zerowania sesji użytkownika.

Przed dalszą analizą opcji i narzędzi programu *Terminal Server Configuration* (Konfiguracja serwera terminali) warto zapamiętać, które ustawienia konfiguracji mają pierwszeństwo:

1. Zasady grupy na poziomie komputera. Większość ustawień programu *Terminal Services Configuration* może być określana przez obiekty GPO powiązane z jednostką organizacyjną, w której zostały utworzone obiekty komputera serwera terminali. Zasady te zastępują ustawienia określone przez pozostałe narzędzia.
2. Zasady grupy na poziomie użytkownika.
3. Konfiguracja serwera terminali lub połączenia RDP-Tcp, określane za pomocą narzędzia *Terminal Services Configuration* (Konfiguracja usług terminalowych). Pomimo, że narzędzie to jest ściśle związane z serwerem i z połączeniem i z tego też powodu nie może definiować pojedynczej konfiguracji, tak jak jest to realizowane za pomocą zasad **grupy**, narzędzie to może być wykorzystywane do konfigurowania serwerów terminali systemu Windows 2000. Poza tym, zdarza się, że konfiguracja dotycząca serwera terminali i konfiguracja dotycząca połączenia powinny być odmienne. Program *Terminal Services Configuration* (Konfiguracja usług **terminalowych**) pozwala obsługiwać takie sytuacje.
4. Właściwości konta użytkownika skonfigurowane za pomocą przystawki *Active Directory Users And Computers* (Użytkownicy i komputery usługi Active Directory).
5. Konfiguracja klienta programu *Remote Desktop* (Pulpit zdalny).

Konfiguracja połączenia

Możliwość nawiązania połączenia i zalogowania się w serwerze terminali determinowana jest przez szereg czynników, a nieprawidłowe działanie każdego z nich generuje inny komunikat o błędzie:

- **Połączenie z serwerem terminali musi być możliwe do zrealizowania**, jeśli klient nie może nawiązać połączenia za pomocą protokołu TCP/IP lub jeśli wyłączone jest połączenie RDP-Tcp serwera terminali, wyświetlany jest niewiele wyjaśniający komunikat, który informuje, że klient nie mógł połączyć się z serwerem.
- **Włączony musi być program Remote Desktop (Pulpit zdalny)**. Możliwość akceptowania przez serwer terminali nowych połączeń może być kontrolowana na zakładce *Remote* (Zdalny) w oknie dialogowym właściwości apletu System lub poprzez użycie poleceń **change logon /disable** oraz **change logon /enable**. Jeśli logowanie jest zablokowane, wyświetlony zostanie komunikat o błędzie wskazujący, że sesje serwera terminali zostały zablokowane lub że logowanie zdalne jest wyłączone.
- **Serwer musi dysponować wolnymi połączeniami**. Właściwości połączenia, czyli domyślnie właściwości połączenia RDP-Tcp, na zakładce *Network Adapter* (Karta sieciowa) określają liczbę dostępnych połączeń (zobacz rysunek A-4). Jeśli wyczerpane zostały wszystkie dostępne połączenia, wyświetlany jest komunikat o błędzie, który wskazuje, że wystąpił błąd sieci.



Rysunek A-4. Zakładka *Network Adapter* (Karta sieciowa) okna dialogowego *RDP-Tcp Properties* (Właściwości RDP-Tcp)

- Szyfrowanie musi być zgodne. Ustawienia domyślne określają, że do serwera terminali przyłączyć się może dowolny klient, bez Względu na jego możliwości związane z szyfrowaniem. Jeśli wymagania dotyczące szyfrowania zostały **zmienione, klient, który** nie obsługuje tego typu szyfrowania nie będzie mógł nawiązać połączenia. Typ szyfrowania określany jest we właściwościach połączenia na zakładce *General* (Ogólne) na podstawie listy *Encryption* (Szyfrowanie), tak jak przedstawia to rysunek A-5.



Rysunek A-5. Zakładka *General* (Ogólne) okna dialogowego *RDP-Tcp Properties* (Właściwości RDP-Tcp).

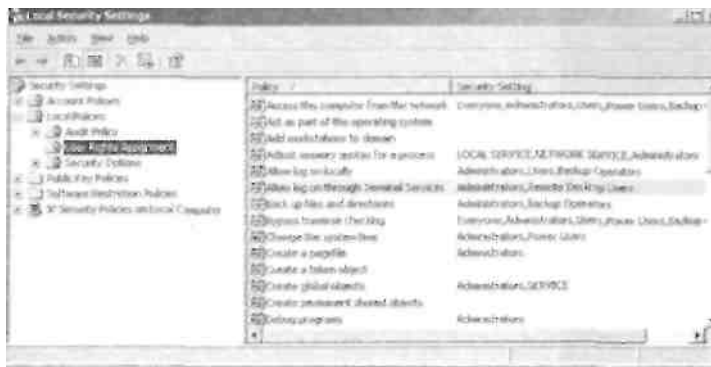
- Użytkownik musi mieć wystarczające uprawnienia do nawiązania połączenia. Zgodnie z rysunkiem A-6, grupa *Remote Desktop Users* (Użytkownicy pulpitu zdalnego) mają uprawnienie *User Access* (Dostęp użytkownika), dzięki czemu mogą logować się w serwerze. Lista ACL połączenia może być modyfikowana tak, aby w konfiguracjach dostęp był określony inaczej niż przez ustawienia domyślne. Szczegółowe informacje na ten temat można znaleźć w programie *Help and Support Center* (Centrum pomocy i obsługi technicznej). Jeśli użytkownik nie posiada wystarczających

uprawnień do połączenia, wyświetlony jest komunikat wskazujący, że użytkownik nie uzyskał dostępu do sesji.

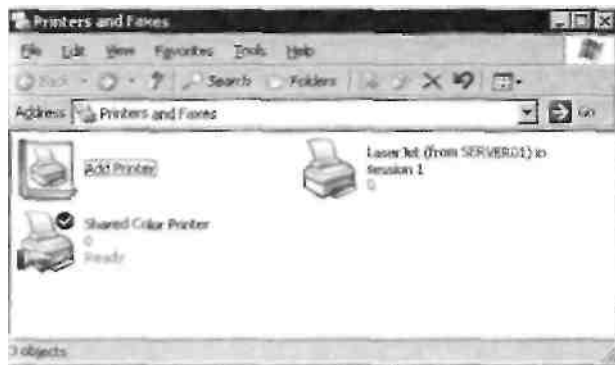


Rysunek A-6. Zakładka Permissions (Uprawnienia) okna dialogowego RDP-Tcp Properties (Właściwości RDP-Tcp)

- Użytkownik musi mieć **prawa logowania użytkownika w serwerze terminali**. System Windows .Server 2003 odróżnia prawo logowania lokalnego w serwerze od prawa wymaganego do zalogowania się w serwerze przy użyciu połączenia pulpitu zdalnego. Na rysunku A 7 pokazane zostały ustawienia *Allow Log On Through Terminal Services* (Zezwalaj na logowanie za pomocą usług terminalowych) oraz *Deny Log On Through Terminal Services* (Odmawiaj logowania za pomocą usług terminalowych), które mogą być używane do zarządzania tymi prawami przy użyciu zasady grupy lub zasady lokalnej. Na serwerach członkowskie li grupy *Administrators* (Administratorzy) oraz *Remote Desktop Users* (Użytkownicy pulpitu zdalnego) posiadają prawa do logowania za pomocą usług terminalowych. W przypadku kontrolerów domen, ustawienia domyślne określają, że jedynie **administratorzy** mają takie uprawnienia. Jeśli **użytkownik** nie ma wystarczających uprawnień, zostanie wyświetlony komunikat wskazujący, że zasada serwera terminali nie pozwala na logowanie.



Rysunek A-7. Prawo użytkownika Allow Log On Through Terminal Services (Zezwalaj na logowanie za pomocą usług terminalowych)



Rysunek A-10. Folder *Printm And Faxes* (Drukarki i faksy) prezentujący przekierowane drukarki klienta

Podobnie jak dla pr/ekicrowania dysku, pr/ckierowanic drukarki jcsł określone na zakładce *Local Settings* (Ustawienia lokalne) klienta pogramu *Retnote Desktop* (Pulpit zdalny). Pr/ckierowanic drukarki może być wyłączone przy użyciu właściwości połączenia RDP Tcp. Funkcja ta może być również zablokowana, jeśli we właściwościach konta użytkownika nie zostało włączone ustawienie *Connect Client Printers At Logon* (Podłącz /i drukarki klienta po zalogowaniu), zgodnie z rysunkiem Ali. Zaznaczenie tej opcji dla konta użytkownika nie spowoduje pr/ekicrowania drukarki, Klient musi określić pr/ckierowanic na zakładce *Local Resources* (Zasoby lokalne). Jeśli jednak ustawienie jest wyłączone, ustawienie konta użytkownika zastąpi ustawienie klienta. Właściwości konta użytkownika udostępniają również ustawienie *Default To Main Client Printer* (Domyślnie użyj głównej drukarki klienta), które, jeśli pr/ckierowanic <liuk.ii ki jest włączone, będzie definiować taką domyślną drukarkę; dla sesji serwera teiminali, jaka została określona dla stacji roboczej użytkownika. Jeśli natomiast ustawienie *Default To Main Client Printer* (Domyślnie użyj głównej drukarki klienta) jest wyłączone, sesja pogramu *Terminal/Sewer* (Serwer terminali) będzie używać domyślnej drukarki komputera progianui *Terminal Serner*. Ustawienie pr/ekicrowania drukarki może być określane za pomocą obiektu CPO.



Rysunek A-II. Zakładka *Enyironment* (Środowisko) okna dialogowego właściwości użytkownika

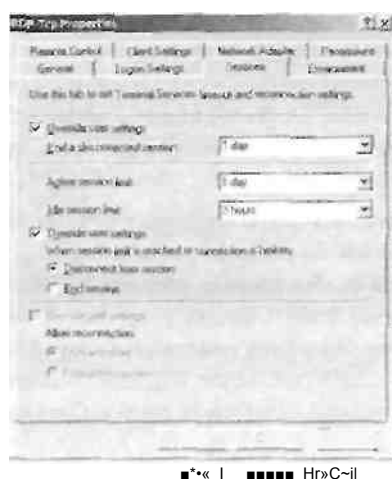
- **Przekierowanie portu** szeregowego. Opcja ta umożliwia użytkownikowi uruchamianie w trakcie sesji serwera terminali aplikacji, która wykorzystuje urządzenie przyłączone do portu szeregowego stacji roboczej użytkownika, takie jak czytnik kodów paskowych. Funkcja ta jest również umieszczona na zakładce *Local Resources* (Zasoby lokalne) programu klienta i może być wyłączana we właściwościach połączenia RDP-Tcp. Przekierowanie portu szeregowego może być również określane przy użyciu Obiektu GPO.
- **Mapowanie portów LPT i COM.** Opcja ta umożliwia użytkownikowi wewnątrz sesji serwera terminali zainstalowanie drukarki, która jest przypisana do drukarki podłączonej do portów LPT lub COM stacji roboczej użytkownika. Ta metoda przekierowania drukarki nie jest potrzebna w przypadku korzystania z systemu Windows Server 2003 i klienta programu *Remote Desktop* (Pulpit zdalny), które obsługują znacznie prostszy sposób opisany powyżej, jednak w dalszym ciągu domyślne ustawienia określają, że mapowanie portów LPT i COM jest włączone. Właściwości połączenia RDP-Tcp mogą być wykorzystywane do wyłączania mapowania portów. Czynność ta może być również zrealizowana za pomocą obiektu GPO.
- **Mapowanie schowka.** Opcja ta umożliwia użytkownikowi kopiowanie i wklejanie informacji pomiędzy sesją programu *Terminal Server* (Serwer terminali) a pulpitem. Dla klienta programu *Remote Desktop* (Pulpit zdalny) **domyślnie** funkcja ta jest włączona i nie może być zmieniona przy użyciu interfejsu użytkownika (UI). Właściwości połączenia RDP-Tcp mogą być wykorzystywane do wyłączania mapowania schowka. Czynność ta może być również zrealizowana za pomocą obiektu GPO.

Zarządzanie sesjami i procesami

Konsola *Terminal Services Manager* (Menedżer usług terminalowych) umożliwia monitorowanie oraz **kontrolę** sesji i procesów serwera terminali. Konsola umożliwia odłączenie, wylogowanie lub zerwanie sesji bądź użytkownika, umożliwia wysyłanie wiadomości do użytkownika lub Zakończenie procesu uruchomionego przez dowolnego użytkownika. Program *Task Manager* (**Menedżer** zadań) może być również wykorzystywany do monitorowania i kończenia procesów. W tym celu wystarczy po prostu zaznaczyć pole wyboru *Show Processes From All Users* (Pokaż procesy wszystkich użytkowników), jeśli wydajność serwera terminali jest bardzo niska, należy użyć konsoli *Terminal Services Manager* (Menedżer serwera terminali) lub programu *Task Manager* (Menedżer zadań) w celu przejrzania procesów uruchomionych przez wszystkich. Dzięki temu, możliwe będzie określenie, czy jeden z nich nie zajmuje nadmiernie czasu procesora.

Zarządzanie sesjami użytkownika

Istnieją różne ustawienia definiujące działanie sesji użytkownika, która przez pewien czas jest aktywna, bezczynna lub odłączona. Ustawienia te mogą być określane na zakładce *Sessions* (Sesje) okna dialogowego właściwości programu *Terminal Server Connection* (Połączenia serwera terminali). Okno programu zostało przedstawione na rysunku A-12. Ustawienia te mogą być również określane za pomocą zasad grupy.



Rysunek A-12. Zakładka *Session* (Sesja) okna dialogowego *RDP-Tcp Properties* (Właściwości RDP-Tcp)

Równoważenie obciążenia serwerów terminali

Realizacja równoważenia obciążenia serwerów terminali była trudnym zadaniem podczas korzystania z poprzednich wersji usług terminalowych. Systemy Windows Server 2003 Enterprise oraz Datacenter Editions zostały wyposażone w mechanizmy tworzenia klastrów serwerów, który jest grupą logiczną serwerów terminali. Jeśli użytkownik łączy się do klastra, zostaje skierowany do jednego z serwerów. Jeśli sesja użytkownika została rozłączona, a użytkownik próbuje ponownie połączyć się z serwerem, serwer terminali odbierający połączenie sprawdza w katalogu sesji (Session Directory), który serwer terminali obsługiwał rozłączoną sesję, a następnie przekierowuje klienta do odpowiedniego serwera.

Celem skonfigurowania klastra serwerów terminali potrzebne będą następujące komponenty:

- **Technologia równoważenia obciążenia**, taka jak NLB (Network Load Balancing) czy metoda cykliczna systemu DNS. Rozwiązanie równoważenia obciążenia będzie rozdzielać połączenia klientów do każdego serwera terminali.
- **Terminal Services Session Directory** (Katalog sesji usług terminalowych). Należy włączyć usługę *Terminal Services Session Directory*, która jest domyślnie instalowana w systemach Windows Server 2003 w wersjach Enterprise oraz Datacenter. Usługa włączana jest za pomocą konsoli *Services* (Usługi) w grupie programów *Administrative Tools* (Narzędzia administracyjne). Zaleca się, aby usługa katalogu sesji była włączana na serwerze, na którym nie jest uruchomiony program *Terminal Services*. Usługa *Terminal Services Session Directory* (Katalog sesji usług terminalowych) obsługuje bazę danych, która śledzi każdą sesję użytkownika serwerów klastra. Komputer, na którym uruchomiona została usługa katalogu sesji tworzy grupę lokalną *Session Directory Computers* (Komputery katalogu sesji), do której należy dodać wszystkie konta komputerów serwerów klastra.
- **Konfiguracja połączenia serwera terminali**. Ostatnim krokiem jest skierowanie serwerów klastra do katalogu sesji. Proces ten definiuje, że serwer jest częścią katalogu, określa nazwę serwera katalogu sesji oraz nazwę klastra, która może być dowolną nazwą pod warunkiem, że taka sama nazwa została określona dla każdego serwera klastra. Ustawienia te mogą być określane w węzle *Server Settings* (Ustawienia serwera) konsoli *Terminal Services Configuration* (Konfiguracja serwera).

terminali) lub mogą być określone za pomocą obiektu GPO stosowanego do jednostki organizacyjnej, w której umieszczone są obiekty komputerów serwerów terminali klastra.

Podczas łączenia się użytkownika z klastrem ma miejsce następujący proces:

1. Kiedy użytkownik loguje się w klastrze serwerów terminali, który odbiera początkowe żądanie rejestracji Identa, wysyła zapytanie do serwera katalogu sesji.
2. Serwer katalogu sesji sprawdza nazwę użytkownika w swojej bazie danych i odpowiada w następujący sposób serwerowi, który przysłał zgłoszenie: » Jeśli użytkownik nie ma rozłączonych sesji, logowanie jest kontynuowane na serwerze, który obsługuje początkowe połączenie,
» Jeśli użytkownik ma rozłączoną sesję na innym serwerze, sesja klienta zostaje skierowana do tego właśnie serwera i tam będzie kontynuowany proces logowania.
3. Jeśli użytkownik loguje się w nowej lub rozłączonej sesji, aktualizowany zostaje katalog sesji.



Wskazówka egzaminacyjna Należy zapoznać się z wszystkimi elementami wymaganymi do zainstalowania klastra serwerów terminali. Przed decyzją o wdrożeniu klastra serwerów terminali w przedsiębiorstwie warto zapoznać się ze szczegółowymi instrukcjami zamieszczonymi w programie Help And Support Center (Centrum pomocy i obsługi technicznej).

Sterowanie zdalne

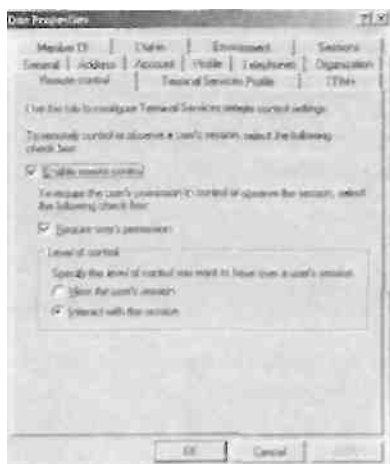
Program *TerminalServer* (Serwer terminali) umożliwia administratorowi przeglądanie oraz przejęcie kontroli sesji użytkownika. Cecha ta umożliwia monitorowanie działań użytkownika na serwerze terminali nie tylko administratorom, ale również pozwala na działania podobne do programu *Remote Assistance* (Pomoc: zdalna), które pozwalają pracownikom działu pomocy technicznej kontrolować sesje użytkowników oraz wykonywać czynności takie, aby również użytkownicy mogli obserwować ich realizację.

W celu ustanowienia zdalnego sterowania zarówno użytkownik, jak i administrator muszą mieć nawiązane sesje serwera terminali. Administrator musi otworzyć konsolę *Terminal Server Manager* (Menedżer serwera terminali) znajdującą się w grupie programów *Administrative tools* (Narzędzia administracyjne), następnie musi kliknąć prawym przyciskiem myszy sesję użytkownika i wybrać polecenie *Control* (Kontrola). Ustawienia domyślne określają, że użytkownik będzie powiadamiany o tym, że administrator chce podłączyć się do sesji i musi takie żądanie zaakceptować lub odrzucić.



Ważne Usługa Remote Control (Sterowanie zdalne) jest dostępna wyłącznie, jeśli konsola Terminal Server Manager (Menedżer serwera terminali) używana jest *wewnątrz* sesji serwera terminali. Nie można włączyć funkcji sterowania zdalnego otwierając konsolę Terminal Server Manager (Menedżer serwera terminali) na swoim komputerze PC.

Ustawienia sterowania zdalnego dotyczą możliwości przeglądania i sterowania zdalnego sesji, jak również tego, czy użytkownik ma udzielać zgody na dostęp administratora. Ustawienia te mogą być konfigurowane we właściwościach konta użytkownika na zakładce *Remote Control* (Zdalne sterowanie), tak jak ilustruje to rysunek A-13 oraz mogą być określone poprzez właściwości połączenia RDP-Tcp. Te ostatnie zastępują ustawienia konta użytkownika. Do określania konfiguracji sterowania zdalnego można również wykorzystywać zasadę grupy.



Rysunek A-13. Zakładka *Remote Control*! okna dialogowego właściwości użytkownika

Oprócz włączania ustawień umożliwiających sterowanie zdalne administrator musi posiadać uprawnienia pozwalające na ustanowienie kontroli zdalnej poprzez połączenie z serwerem terminali. Wykorzystując zakładkę *Permissions* (Uprawnienia) okna dialogowego *RDP-Tcp Properties* (Właściwości RDP) administrator może przypisać szablon uprawnień *Full Control* (Pełna kontrola) lub poprzez kliknięcie przycisku *Advanced* (Zaawansowane) może przypisać uprawnienia *Remote Control* (Sterowanie zdalne) do grupy, co ilustruje rysunek A-14.



Rysunek A-14. *Uprawnienie Remote Control/ (Sterowanie zdalne)*

Podsumowanie

Niniejszy dodatek dokonuje przeglądu programu *TerminalServer* oraz narzędzi, technologii i procesów wykorzystywanych do konfigurowania i ewentualnego rozwiązywania problemów z nim związanych. Podobnie jak w przypadku pozostałych fragmentów zestawu szkoleniowego, podstawowym celem tego dodatku jest przygotowanie czytelnika do egzaminu certyfikującego 70-290. Planując zainstalowanie i obsługę programu *Terminal Server* w sieci przedsiębiorstwa warto zapoznać się z dodatkowymi informacjami zamieszczonymi w programach Centrum pomocy i obsługi technicznej oraz Microsoft Knowledge Base.



802.11 Dotyczy rodziny specyfikacji sieci bezprzewodowych IEEE (Institute of Electrical and Electronics Engineers).

802.11a Rozszerzenie specyfikacji 802.11, które stosuje się do bezprzewodowych sieci lokalnych (WLAN) i udostępnia transmisję dla przepustowości 54 Mbps w paśmie 5 GHz.

802.11b Rozszerzenie specyfikacji 802.11, dotyczące bezprzewodowych sieci lokalnych (WLAN) i udostępniające transmisję dla przepustowości 11 Mbps (przy czym możliwe są trzy mniejsze prędkości - 5.5, 2 oraz 1 Mbps) w paśmie 2.4 GHz. Specyfikacja 802.11b została zatwierdzona w 1999 r., rozszerzając pierwotny standard 802.11 i umożliwiając działanie sieci bezprzewodowych porównywalnych do sieci Ethernet. Standard ten nazywany jest także **Wi-Fi**.

802.11g Rozszerzenie specyfikacji 802.11 dotyczące bezprzewodowych sieci LAN i umożliwiające transmisję o przepustowości 54 Mbps w paśmie 2.4 GHz. Standard 802.11g jest kompatybilny z wcześniejszym standardem 802.11b, dzięki czemu urządzenia obu standardów mogą ze sobą współpracować.

A

ACPI (Advanced Configuration Power Interface) Specyfikacja definiująca zarządzanie zasilaniem urządzeń komputerowych. Zgodność ze standardem ACPI jest wymagana dla urządzeń wykorzystujących technologię Plug and Play oraz funkcje zarządzania energią.

Active Directory (usługa **Active Directory**) Usługa katalogowa wprowadzona w systemie **Microsoft Windows 2000 Server** i obsługiwana w dalszym ciągu w systemie **Windows Server 2003**. Usługa ta zastąpiła zestaw funkcji katalogowych systemu **Windows NT** i wprowadziła funkcjonalność zintegrowaną z systemami **DNS (Domain Name System)**, **LDAP (Lightweight Directory Access Protocol)** oraz **Kerberos** (protokół zabezpieczeń).

ActiveX Zestaw luźno zdefiniowanych technologii, umożliwiających tworzenie komponentów oprogramowania sieciowego i ich współdziałanie w środowisku sieci.

Adres IP (IP address) 32-bitowa liczba, przedstawiana najczęściej w postaci czterech dziesiętnych liczb rozdzielanych kropką (na przykład 192.168.1.10). Jest to unikatowy identyfikator komputera w sieci Internet. Każde urządzenie w sieci Internet ma unikatowy adres IP.

Adres MAC (media access control) Unikatowy 48-bitowy numer przypisany przez producenta karcie sieciowej. Adresy MAC są używane do mapowania podczas komunikacji w sieciach TCP/IP.

Adres Precyzyjna lokalizacja pamięci lub dysku, w której przechowywany jest fragment informacji. Również unikatowy identyfikator w sieci. W Internecie kod, poprzez który identyfikowany jest użytkownik o formacie *username@hostname*, gdzie **username** jest nazwą użytkownika, nazwą logowania lub konta, a **hostname** jest nazwą wykorzystywanego komputera lub dostawcy usług internetowych. Nazwa hosta może powstawać z połączenia kilku wyrazów oddzielanych kropką.

ADSI (Active Directory Service Interface) Interfejs programowy umożliwiający dostęp do usługi Active Directory.

Anonimowa usługa FTP Sposób wykorzystania programu FTP polegający na zalogowaniu się w innym komputerze i skopiowaniu pliku nie posiadając konta na tym komputerze. Podczas logowania jako nazwa użytkownika wpisywane jest słowo „anonymous”, a jako hasło adres poczty elektronicznej. W ten sposób użytkownik uzyskuje dostęp do publicznie dostępnych plików. Zobacz *FTP (File Transfer Protocol)*.

AppleTalk Architektura sieci lokalnej komputerów firmy Macintosh dla połączeń z drukarkami. W sieci systemu Windows Server 2003 i klientów systemu Macintosh może funkcjonować jako sieć AppleTalk integrująca wykorzystanie tej usługi (wcześniej nazywana *Service* for Macintosh).

ARP (Address Resolution Protocol) Protokół w zestawach protokołów TCP/IP (Transmission Control Protocol/Internet Protocol) i AppleTalk, który umożliwia dla pakietów IP zamianę adresu IP na adres MAC (media access control).

ATM (Asynchronous Transfer Mode) Technologia sieciowa bazująca na przesyłaniu danych w komórkach lub pakietach o ustalonych rozmiarach. Ponieważ przesyłanie komórek zawierających informacje nie musi być konieczne okresowe, transmisja nazywana jest asynchroniczną.

Atrybut archiwalny (Archive lub A) Atrybut każdego pliku używany przez programy tworzenia kopii zapasowych do określania, czy dany plik powinien zostać skopiowany. Atrybut archiwalny jest ustawiany (wartość TRUE) każdorazowo, kiedy plik zostaje utworzony lub zmodyfikowany. Zadania różnicowych lub przyrostowych kopii zapasowych będą tworzyć kopie pliku tylko wtedy, kiedy atrybut archiwalny ma wartość: TRUE.

Atrybut Charakterystyka. W odniesieniu do zarządzania plikami w systemie Windows jest to **informacja** określająca, czy plik może być wyłącznie odczytywany, czy jest ukryty, skompresowany, zaszyfrowany, nadający się do archiwizowania bądź indeksowania.

Automatyczne odzyskiwanie systemu ASR (Automated System Recovery) Cecha systemu Windows Server 2003 pozwalająca administratorowi przywrócić prawidłowe funkcjonowanie uszkodzonego serwera. Przy użyciu kreatora ASR w programie Backup Utility (Kopia zapasowa) użytkownik tworzy zestaw ASR, który zawiera dyskiecie z wykazem plików systemowych oraz kopie zapasową odpowiednich plików. Jeśli serwer ulega awarii, należy go uruchomić z instalacyjnego dysku CD-ROM systemu Windows Server 2003, a następnie nacisnąć F2, aby uruchomić program automatycznego odzyskiwania systemu.

B

BDC (backup domain controller) W domenie systemu Windows NT jest to komputer, który przechowuje bazę danych zawierającą wszystkie informacje o kontach i zabezpieczeniach dotyczących podstawowego kontrolera domeny PDC (primary domain controller). Baza danych jest regularnie i automatycznie synchronizowana z kopią danych kontrolera PDC. Kontroler BDC przeprowadza również uwierzytelnienia rejestracji w systemie i w razie potrzeby może być przejąć rolę kontrolera PDC. W domenach systemów Windows Server 2003 lub Windows 2000 kontrolery BDC są niepotrzebne — wszystkie kontrolery domeny są partnerami i mogą zarządzać katalogiem.

Biblioteka DLL (dynamic-link library) Moduł programowy zawierający kody wykonywalne i dane używane używane przez różne aplikacje. Program wykorzystuje bibliotekę DLL tylko gdy jest aktywny, a biblioteka jest usuwana z pamięci po zamknięciu programu.

BIOS (Basic Input/Output System) Program używany przez mikroprocesor komputera osobistego do uruchomienia systemu oraz do zarządzania przepływem danych pomiędzy systemem operacyjnym i urządzeniami komputera, takimi jak dyski twarde, dyski CD-ROM, karty sieciowe, klawiatury i myszy.

BITS (Background Intelligent Transfer Service) Usługa używana do przesyłania plików pomiędzy klientem a serwerem HTTP (Hypertext Transfer Protocol). Usługa BITS wykorzystuje momenty bezczynności sieci, dzięki czemu nie zostaje zwiększone zapotrzebowanie na pasmo.

Blok SMB (Server Message Block) Protokół warstwy aplikacji umożliwiający klientowi dostęp do plików i drukarek serwerów zdalnych. Klienci i serwery, dla których została włączona obsługa SMB, mogą komunikować się poprzez warstwę transportu i sieci, wliczając w to protokół TCP/IP.

Blokada konta (account lockout) Funkcja ochrony, która powoduje zablokowanie konta użytkownika, jeśli liczba nieudanych prób logowania przekroczyła określoną wartość w zdefiniowanym okresie. Za pomocą zablokowanego konta nie można zarejestrować się w systemie, a konta takie może odblokować administrator.

BOOTP Protokół używany w sieciach TCP/IP (Transmission Control Protocol/Internet Protocol) do rozpoznawania przez kartę sieciową swojego adresu IP, do zlokalizowania w sieci serwera BOOTP oraz do zlokalizowania pliku pobieranego do pamięci w celu uruchomienia komputera. Protokół umożliwia uruchomienie komputera, który nie ma zainstalowanego dysku twardego lub stacji dyskiety. Nazywany jest też protokołem ładowania początkowego BOOTP.

Brama (gateway) Urządzenia używane do połączenia sieci wykorzystujących różne protokoły.

Buforowanie (Caching) Proces używany do poprawy wydajności poprzez pozostawianie poprzednio wykorzystywanych informacji w lokalizacji, do której jest szybszy dostęp w porównaniu do lokalizacji pierwotnej. Buforowanie dysku twardego jest używane przez usługę File and Print Sharing (Udostępnianie plików i drukarek) w sieciach Microsoft Networks, która przechowuje niedawno odczytywane informacje z dysku w pamięci, dzięki czemu dostęp do nich jest szybszy. Program Remote Desktop Connection (Połączenie pulpitu zdalnego) może buforować na lokalnym dysku twardym poprzednio **przeglądane** ekrany serwera terminali, dzięki czemu zostaje poprawiona wydajność połączenia protokołu RDP (Remote Desktop Protocol).

C

Certyfikat (certificate) Dokument cyfrowy używany do sprawdzania autentyczności i powiązania klucza publicznego z jednostką dysponującą odpowiednim **kluczem** prywatnym.

D

Dane o stanie systemu (System State) Zestaw ważnych plików systemu, dzięki którym można przywrócić funkcjonalność systemu, takich jak rejestr, baza danych rejestracji COM+ oraz pliki rozruchowe, dla których trzeba regularnie tworzyć kopie zapasowe.

DDE (Dynamic Data Exchange) Sposób komunikacji pomiędzy procesami zaimplementowanymi w rodzinie systemów Windows. Jeśli programy obsługujące standard DDE działają w tym samym czasie, mogą pomiędzy sobą wymieniać dane na zasadzie „konwersacji”. Konwersacje są dwukierunkowymi połączeniami między dwoma aplikacjami, które transmitują dane naprzemiennie.

Delegowanie (delegate) Przypisanie innemu użytkownikowi lub grupie praw administracyjnych do fragmentu przestrzeni nazw.

Deskryptor zabezpieczeń (security descriptor) Atrybut obiektu przechowujący informacje kontrolne o własności i dostępie.

DHCP (Dynamic Host Configuration Protocol) Protokół zestawu protokołów TCP/IP (Transmission Control Protocol/Internet Protocol) używany do automatycznego przypisywania adresów IP i konfigurowania klientów sieci.

Długość kolejki (Queue Length) Licznik wydajności mierzący liczbę instrukcji oczekujących na przetworzenie przez obiekt, taki jak procesor czy dysk fizyczny. Jeśli wartość licznika Queue Length (Długość kolejki) w dłuższym okresie czasu jest większa niż 2 lub 3, oznacza to, że zasoby systemu nie są wystarczające dla obsługi żądań kierowanych do systemu.

DNS (Domain Name System) Usługa sieci TCP/IP (Transmission Control Protocol/Internet Protocol), wliczając w to Internet, która przekształca nazwy domen na adres IP. Dzięki temu użytkownicy mogą wykorzystywać łatwiejsze do zapamiętania nazwy, takie jak FinanceServer lub Adatum.com, zamiast używać adresów IP, jak na przykład 192.168.1.10.

Domena Grupa komputerów współużytkująca zasadę zabezpieczeń oraz bazę danych kont użytkowników. Domena systemu Windows Server 2003 nie jest tym samym, co domena sieci Internet. Zobacz *nazwa domeny*.

Domena podrzędna (child domain) Domena umieszczona bezpośrednio poniżej innej nazwy domeny (która nazywana jest domeną nadrzędną). Przykładowo Engineering.scribes.com jest domeną podrzędną domeny nadrzędnej scribes.com. Nazywana również poddomeną.

Drukarka logiczna (logical printer) Przedstawienie drukarki fizycznej. Drukarka logiczna jest tworzona na komputerze systemu Windows i składa się ze sterownika drukarki, jej ustawień oraz innych danych dotyczących konfiguracji. Kontroluje, kiedy i w jaki sposób zadanie druku zostanie wysłane do **drukarki**.

Drzewo (tree) Drzewo w usłudze Active Directory jest loszsetzeniem idei drzewa katalogu. Jest hierarchią obiektów i kontenerów, która pokazuje, w jaki sposób obiekty są połączone lub u prezentuje ścieżkę pomiędzy obiektami. Punktem końcowym drzewa jest zazwyczaj obiekt.

Drzewo konsoli (console tree) Domyślnie jest to okno po lewej stronie konsoli MMC (Microsoft Management Console), w którym wyświetlane są elementy konsoli.

Dublowanie (mirroring) 1. Dwie partycje na dwóch dyskach twardych (nazywanych również macierzą RAID-1) skonfigurowanych w taki sposób, że każda z nich zawiera takie same informacje. Jeśli jeden dysk ulega awarii, dane pozostają na drugim dysku, dzięki czemu ich przetwarzanie można kontynuować. 2. Serwer protokołu FTP (File Transfer Protocol), udostępniający kopię tych samych plików, które udostępnia inny serwer. Niektóre serwery FTP są tak popularne, że trzeba je dublować, dzięki czemu obciążenie zostaje rozłożone między różne witryny.

DWORD Typ danych składający się z czterech bajtów wyrażonych szesnastkowo.

Dysk dynamiczny (dynamic disk) Dysk skonfigurowany przy użyciu woluminów. Konfiguracja dysku przechowywana jest w bazie danych LDM (Logical Disk Manager) i jest replikowana do innych dysków dynamicznych tego samego komputera. Dyski dynamiczne obsługiwane są jedynie w systemach Windows Server 2003, Windows XP oraz Windows 2000.

Dysk podstawowy (basic disk) Dysk fizyczny, skonfigurowany przy użyciu partycji. Struktura dysku jest kompatybilna z poprzednimi wersjami systemu Windows oraz kilkoma innymi systemami operacyjnymi.

Dziedziczenie (inheritance) Proces, dzięki któremu uprawnienia są przekazywane z obiektu nadrzędnego do obiektu podrzędnego. Funkcja dziedziczenia została wprowadzona w usłudze Active Directory oraz na woluminach dyskowych w formacie NTFS.

E

EAP (Extensible Authentication Protocol) Rozszerzenie protokołu PPP (Point-to-Point) umożliwiające narzucenie metody uwierzytelnienia dla sprawdzania połączeń PPP.

Emisja wielokrotna (multicasting) Jednoczesne wysyłanie wiadomości do kilku miejsc docelowych w sieci. W odróżnieniu od rozgłoszenia (broadcasting), podczas emisji wielokrotnej dane przesyłane są tylko do wybranych odbiorców.

Ethernet Protokół sieci lokalnej (LAN). Standard Ethernet obsługuje prędkość transmisji 10 Mbps, wykorzystuje topologię szyny oraz kable koncentryczne, światłowodowe bądź przewody dwużyłowych skrętek. Nowsza wersja protokołu Ethernet, nazywana Fast Ethernet, obsługuje prędkość transmisji 100 Mbps, a najnowsza wersja 1000 Mbps (Gigabit Ethernet).

F

Failover (poprawna praca pomimo usterki) Tryb pracy automatycznego przejęcia zadań przez systemy zastępcze - rezerwowa baza danych, serwer lub sieć w przypadku awarii systemu podstawowego lub jego wyłączenia w celach konserwacji. W klastrze serwerów jest to proces wyłączenia zasobów jednego węzła w przewidzianej kolejności i odtworzenia ich na innym węźle.

FRS (File Replication Service) Usługa odpowiedzialna za zapewnienie spójności loldera SYSVOL kontrolera domeny. Usługa FRS przeprowadza replikację lub kopiowanie wszystkich zmian w folderze SYSVOL do innych kontrolerów domeny. Usługa FRS może być również używana do replikowania folderów rozproszonego systemu plików DFS (Distributed File System).

FTP (File Transfer Protocol) Metoda przesyłania plików pomiędzy komputerami w sieci bądź poprzez linii telefoniczne. Ponieważ protokół FTP został zaimplementowany w różnych systemach, jest to prosta metoda transferu informacji pomiędzy zazwyczaj bardzo różnymi systemami, jak komputery PC czy minikomputery.

G

Globalny identyfikator unikatowy GUID (globally unique identifier) Fragment mechanizmu identyfikacji generowany przez usługę Active Directory dla każdego obiektu katalogu. Jeśli nazwa obiektu komputera lub użytkownika zostaje zmieniona lub obiekt zostaje przeniesiony (wraz ze zmianą nazwy), zmieniona zostanie również nazwa wyróżniająca DN, identyfikator zabezpieczeń SID oraz względna nazwa wyróżniająca RDN, natomiast identyfikator GUID pozostanie taki sam.

Głos poprzez sieć IP VoIP (Voice over Internet Protocol) Metoda wykorzystywania sieci Internet jako medium do przekazywania rozmów telefonicznych.

Główna nazwa użytkownika UPN (User Principal Name) Atrybut każdego obiektu użytkownika usługi Active Directory, który jednoznacznie identyfikuje użytkownika w całości. Nazwa UPN zawiera nazwę logowania użytkownika oraz przyrostek, na przykład smithbates@contoso.com.

Główna tablica pliku MFT (master file table) Specjalny plik systemowy na woluminie NTFS (system plików NT) zawierający bazę danych opisującą każdy plik i podkatalog woluminu.

Główny rekord rozruchowy MBR (master boot record) Pierwszy sektor dysku twardego, z którego komputer odczytuje informacje potrzebne podczas uruchamiania. Rekord MBR zawiera tablicę partycji komputera oraz niewielki program - główny kod rozruchowy.

Gniazdo (socket) Punkt końcowy połączenia. Dwa gniazda tworzą pełną ścieżkę dwukierunkowego kanału przesyłowego danych pomiędzy komputerami w sieci. Interfejs Windows Sockets API jest sieciowym interfejsem programowym aplikacji (API) przeznaczonym dla programistów piszących programy w środowisku systemu Windows.

Grupa dyskusyjna (newsgroup) W sieci Internet — rozproszony system ogłoszeń elektronicznych dotyczący poszczególnych tematów. Biuletyny Usenet News (nazywany również Netnews) jest systemem obsługującym tysiące grup dyskusyjnych, dostępnym dla wszystkich uczestników sieci Internet.

Grupa globalna (global group) Grupa, która może być używana w swojej domenie lub w domenach objętych relacjami zaufania. Może jednak zawierać tylko konta użytkowników oraz inne grupy globalne swojej domeny.

Grupa licencji (license group) Grupa użytkowników lub urządzeń współdzielących jedną lub kilka licencji **dostępu** klienta (CAL). Grupy licencji są zarządzane za pomocą programu narzędziowego *Licensing* (Licencje), który jest umieszczony w folderze *Adminhtnuive Tbolt* (Narzędzia administracyjne).

Grupa uniwersalna (universal group) Grupa, która może być używana w dowolnym miejscu drzewa lub lasu domen. Członkami takiej grupy mogą być podmioty dowolnej domeny, jak również uprawnienia mogą być przydzielane w dowolnej domenie. Grupy uniwersalne są dostępne, jeśli domena działa w trybie macierzystym.

H

Hipertekst (hypertext) System zapisywania i wyświetlania tekstu, który w różny sposób umożliwia powiązanie tekstu dostępnego na kilku poziomach szczegółowości. Dokumenty hipertekstu mogą również zawierać odnośniki do powiązanych dokumentów, podobnie jak dokumenty wymieniane w stopkach.

Host Każde urządzenie w sieci wykorzystujące protokół TCP/IP. Nazwą tą określa się również komputer w sieci, w którym można się zalogować. W celu pobrania plików z komputera — hosta, można używać protokołu FTP. Można też używać innych **protokołów** (takich jak Telnet), aby wykoizysty-wać komputer - host.

HTML (Hypertext Markup Language) Język używany do zapisywania stron wykorzystywanych w sieci Internet lub intranet. Język HTML umożliwia dołączanie kodów definiujących czcionki, układ, wbudowaną grafikę i odnośniki hipertekstu.

HTTP (Hypertcirt Transfer Protocol) Metoda, dzięki której strony sieci Web są przesyłane w sieci.

I

IAS (Internet Authentication Service) Implementacja usługi RADILIS (Remote Authentication Dial-In User Service) zrealizowana przez firmę Microsoft. Jest to system uwierzytelnienia i rozliczania używany przez wielu dostawców usług internetowych (ISP). Jeśli użytkownik łączy się z dostawcą usług internetowych korzystając z nazwy użytkownika i hasła, informacje te są przesyłane do serwera usługi RADIUS, który sprawdza ich poprawność, a następnie uwierzytelnia dostęp do systemu dostawcy ISP.

ICMP (Internet Control Message Protocol) Protokół używany do zgłaszania problemów odnotowywanych podczas dostarczania danych, przykładowo nieosiągalny host bądź niedostępny port. Protokół ICMP jest używany również do wysyłania pakietu sprawdzającego dostępność hosta. Host odbierający, jeśli jest dostępny i działa prawidłowo, odsyła pakiet. Zobacz/wg.

Identyfikator obiektu OID (object identifier) Unikatowy identyfikator globalny (GUID) przypisywany przez agenta DSA (Directory System Agent) podczas tworzenia obiektu. Identyfikator GUID jest przechowywany w atrybucie obiektu GUID, który jest częścią każdego obiektu. Atrybut GUID obiektu nie może być modyfikowany bądź usuwany. Podczas przechowywania odniesień do obiektów usługi Active Directory w zewnętrznym magazynie (przykładowo w bazie danych) należy używać identyfikatora GUID obiektu, ponieważ w przeciwieństwie do nazwy, identyfikator **ten** nie będzie zmieniany.

Identyfikator zabezpieczeń SID (Security Identifier) Unikatowa liczba przypisywana do każdego komputera, grupy i konta użytkownika w sieciach systemów Windows Server 2003, Windows 2000 lub Windows NT. Procesy wewnętrzne systemu operacyjnego odnoszą się do identyfikatora SID konta, a nie do nazwy. Usunięty identyfikator SID nie jest nigdy ponownie wykorzystywany.

Instancja (instance) Niepodzielny poziom licznika wydajności. Obiekt wydajności, taki jak LogicalDisk (Dysk logiczny) ma liczniki, jak na przykład % Free Space (Wolne miejsce %). Licznik **ten** może mieć instancje, które reprezentują określone wystąpienia tego licznika, na przykład wolne miejsce na woluminie C:\ oraz na woluminie D:\.

IntelliMirror Zbiór technologii umożliwiających wykorzystywanie przez użytkownika swojego środowiska pomimo, że przenosi się on z jednego komputera na inny. Przenoszone składniki to profile użytkownika, dane i aplikacje.

IP (Internet Protocol) Protokół warstwy sieciowej wykorzystywany jako podstawa sieci Internet. Protokół IP umożliwia routing informacji pomiędzy sieciami w postaci pakietów, a następnie, po **dotarciu** pakietów do miejsca przeznaczenia, umożliwia ponowne połączenie **informacji** w całość.

IPP (Internet Printing Protocol) Protokół umożliwiający klientowi wysłanie zadania do drukarki poprzez sieć Internet lub Intranet. Komunikacja pomiędzy klientem a drukarką pozostaje poddana kapsułkowaniu za pomocą protokołu HTTP.

IPSec (Internet Protocol Security) Standard opracowany przez IETF (Internet Engineering Task Force), **udostępniający** mechanizmy uwierzytelnienia i szyfrowania w sieci Internet. Protokół IPSec jest szeroko wykorzystywany w wirtualnych sieciach prywatnych (VPN).

IPv6 (Internet Protocol wersja 6) Nowa wersja protokołu IP (Internet Protocol) obsługiwana przez system Windows Server 2003. Bieżąca wersja IP to wersja 4, nazywana również IPv4. Protokół IPv6, poprzednio nazywany IPng (IP—The Next Generation), jest rozwojową aktualizacją i będzie przez pewien czas współistniał z wersją 4.

IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange) Protokoły transportowe używane w sieciach Novell NetWare.

Jakość usługi QoS (Quality of Service) Zestaw standardów zapewniających odpowiednią jakość transmisji w sieci.

Jądro (kernel) Część programu wykonywalnego (lub systemu operacyjnego), która zarządza procesorem. Jądro planuje i rozdziela wątki, obsługuje przerwania i wyjątki oraz w przypadku wieloprocesorowości odpowiada za synchronizację.

Jednocześnie (concurrent) W tym samym czasie.

Jednostka alokacji (allocation unit) Najmniejsza ilość miejsca (zarządzalna) na dysku twardym lub woluminie. Nazywana jest również klastrem.

Jednostka organizacyjna OU (organizational unit) Obiekt kontenera usługi Active Directory używany do grupowania komputerów, użytkowników i innych zasobów w logiczne jednostki. Jednostka organizacyjna jest najmniejszą jednostką, do której można stosować zasadę grupy. Jest również najmniejszym zakresem, w odniesieniu do którego mogą być przekazywane uprawnienia administracyjne.

K

Karta inteligentna (smart card) Urządzenie wielkości karty kredytowej, które bezpiecznie przechowuje informacje o tożsamości użytkownika, takie jak hasła, certyfikaty, klucze prywatne i publiczne oraz informacje osobiste.

Kerberos System zabezpieczeń dotyczący identyfikacji, opracowany w instytucie MIT (Massachusetts Institute of Technology), który przeprowadza uwierzytelnienie użytkowników podczas logowania. Działanie systemu polega na przypisywaniu każdemu użytkownikowi logującemu się w sieci unikatowego klucza nazywanego biletem. Bilet jest wbudowaną wiadomością potrzebną do zidentyfikowania nadawcy. Protokół zabezpieczeń Kerberos jest podstawowym mechanizmem uwierzytelniania w systemach Windows Server 2003 i Windows 2000 Server.

Klaster (cluster) 1. Zbiór komputerów połączonych w ten sposób, że tworzą pojedynczy system. Architektura klastra używana jest do równoważenia obciążenia oraz do uzyskania odporności na uszkodzenia systemu. 2. W odniesieniu do urządzeń pamięciowych, klaster jest najmniejszą ilością przestrzeni dyskowej, która może być przydzielona dla pliku.

Kodek (codec) Technologia **kompresji** i dekompresji danych, w szczególności dla głosu i obrazu. Kodeki mogą być programowe, sprzętowe lub mogą być połączeniem obu tych rozwiązań.

Konsola MM(; (Microsoft Management Console) Struktura obsługi narzędzi administracyjnych nazywanych przystawkami. Konsola może zawierać narzędzia, foldery bądź inne kontenery, strony sieci Web oraz różne elementy administracyjne. Komponenty te są wyświetlane w lewym oknie konsoli, nazywanym drzewem konsoli. Konsola ma jedno lub kilka okien, które umożliwiają przeglądanie drzewa konsoli. Zobacz *przystawka*.

Konsola odzyskiwania (Recovery Console) Interfejs wiersza poleceń pozwalający na ograniczony dostęp do systemu w celu jego naprawy. Konsola odzyskiwania jest uruchamiana poprzez rozruch komputera w oparciu o dysk CD-ROM systemu Windows Server 2003. Następnie w odpowiednim momencie należy nacisnąć R (Repair).

Kontener (container) Obiekt usługi Active Directory posiadający atrybuty i będący częścią przestrzeni nazw usługi Active Directory. Inaczej niż w przypadku innych obiektów, najczęściej nie reprezentuje niczego konkretnego, jest tylko zbiorem grupy obiektów lub innych kontenerów.

Konto użytkownika (user account) Dostęp użytkownika do sieci. Każde konto użytkownika ma unikatową nazwę i identyfikator zabezpieczeń SID.

Kontroler domeny (domain controller) Serwer domeny, który akceptuje logowanie kont i rozpoczyna proces ich uwierzytelnienia. W domenie usługi Active Directory kontroler domeny zarządza dostępem do zasobów sieci i bierze udział w replikacji.

L

L2TP (Layer Two Tunneling Protocol) Rozszerzenie protokołu PPP (Point-to-Point Protocol) używanego w połączeniu z protokołem IPSec umożliwiające tworzenie bezpiecznych połączeń VPN.

Las (forest) Grupa kilku drzew usługi Active Directory, pomiędzy którymi istnieją dwukierunkowe przechodnie relacje zaufania. Wszystkie drzewa lasu współużytkują wspólny schemat, konfigurację oraz wykaz globalny GC (Global Catalog). Jeśli las zawiera kilka drzew, drzewa nie tworzą ciągłej przestrzeni nazw. Inaczej niż w przypadku drzew, las nie wymaga nazwy wyróżniającej.

LDAP (Lightweight Directory Access Protocol) Protokół używany do uzyskiwania dostępu do usługi katalogowej. Protokół LDAP jest uproszczoną wersją protokołu DAP (Directory Access Protocol), który używany jest do uzyskiwania dostępu do katalogów standardu X.500. Protokół LDAP jest podstawowym protokołem dostępu dla usługi Active Directory.

LDIF (Lightweight Data Interchange Format) Format plików ASCII używany do **przesyłania** danych pomiędzy usługami katalogowymi protokołu LDAP (Lightweight Directory Access Protocol).

Licencja dostępu klienta CAL (Client Access License) Zgodne z prawem wykorzystywanie usługi lub aplikacji. Licencje CAL mogą być konfigurowane w trybie Na serwer oraz w trybie Na urządzenie lub na użytkownika.

Lista kontroli dostępu ACL (access control list) Zestaw danych przypisanych do pliku, katalogu lub innych zasobów, definiujący uprawnienia użytkowników lub grup dostępu do tego zasobu. W usłudze Active Directory, ACL jest listą wpisów kontroli dostępu (ACE) przechowywanych w obiekcie chronionym przez tę listę. W systemie Microsoft Windows NT lista ACL jest przechowywana w postaci wartości binarnych nazywanych deskryptorem zabezpieczeń.

Lista odwołaniu certyfikatów CRL (certificate revocation list) Podpisana cyfrowo lista certyfikatów (publikowana przez urząd certyfikacji), które zostały odwołane.

LISTSERV Rodzina programów obsługujących listy pocztowe w sieci Internet poprzez rozprowadzanie wiadomości adresowanych do list oraz poprzez automatyczne dodawanie bądź usuwanie członków tych list.

Lmhosts Tekstowy plik ASCII podobny do pliku Hosts, ale używany do skojarzenia adresów IP z nazwami hostów w sieci. Aby łatwiej rozróżniać oba pliki, plik Lmhosts warto zapamiętać jako LAN Manager Hosts.

Lokacja (site) W usłudze Active Directory jest to obszar kilku podsieci połączonych za pośrednictwem szybkich i niezawodnych łączy. Kiedy użytkownicy logują się w lokacji, programy klientów używają serwery usługi Active Directory tej samej lokacji. Zobacz *szybkie i niezawodne połączenie (well-connected)*.

Lokalna grupa domen (domain local group) Lokalna grupa używana na listach ACL jedynie w jej własnej domenie. Lokalna grupa domen może zawierać użytkowników, grupy globalne dowolnej domeny lasu, grupy uniwersalne oraz inne grupy lokalne swojej własnej domeny.

M

Macierz dyskowa RAID (redundant array of independent disks) Zestaw technik zarządzania i rozmieszczania informacji na dysku, dzięki któremu system uzyskuje odporność na uszkodzenia.

Magazyn identyfikatorów (identity store) Baza danych identyfikatorów zabezpieczeń lub podmiotów zabezpieczeń. Usługa Active Directory jest magazynem identyfikatorów domeny systemu Windows Server 2003.

Menedżer dysku lokalnego LDM (Logical Disk Manager) Usługa odpowiedzialna za informacje o konfiguracji dysków, które zostały skonfigurowane jako dyski dynamiczne.

Menedżer kont zabezpieczeń SAM (Security Accounts Manager) Usługa używana podczas logowania, która zarządza informacjami o koncie użytkownika, w tym o członkostwie w grupach.

Menedżer urządzeń (Device Manager) Narzędzie administracji używane do zarządzania urządzeniami komputera. Program umożliwia przeglądanie i zmianę właściwości urządzenia, aktualizacji sterowników, konfigurowanie ustawień urządzeń oraz ich odinstalowywanie.

Mobilny profil użytkownika (roaming user profile) Profil przechowywany w dostępnej lokalizacji sieciowej, dzięki czemu użytkownik gdziekolwiek się loguje, pobiera swój profil (pulpit, dane aplikacji i ustawienia). Zobacz *projd*.

N

NAS (Network Access Serwet) Serwer akceptujący połączenia protokołu PPP (Point-to-Point Protocol) w sieci, którą obsługuje. **NAT (Network Address Translation)** Technologia umożliwiająca używanie w lokalnej sieci LAN

jednego zestawu adresów IP dla komunikacji wewnętrznej oraz drugiego zestawu adresów IP dla

ruchu zewnętrznego. Nazwa domeny (domain name) W usłudze Active Directory jest to nazwa przypisana zbiorowi

komputerów sieci, które współużytkują ten sam katalog. W sieci Internet jest to unikatowa nazwa tekstowa identyfikująca określonego hosta. Komputer może mieć kilka nazw domeny, ale dana nazwa domeny wskazuje tylko na jeden komputer. Serwer nazw DNS rozwiązuje nazwy domen wyszukując ich adresy IP

Nazwa wyróżniająca DN (distinguished name) Unikatowa nazwa w kontekście usługi Active Directory. Nazwa DN identyfikuje domenę, która przechowuje obiekt, jak również pełną ścieżkę w hierarchii kontenerów doprowadzającą do obiektu.

Nazwa zwykła CN (common name) Nazwa główna obiektu w katalogu protokołu LDAP (Lightweight Directory Access Protocol), takim jak usługa Active Directory. Nazwa CN musi być unikatowa w kontenerze lub jednostce organizacyjnej (OU), wewnątrz której istnieje dany obiekt.

NetBEUI (NetBIOS Enhanced User Interface) Prosty i szybki protokół wymagający niewiele pamięci, ale funkcje ramowania są możliwe tylko w sieciach *token ring*. Lokalizacje zdalne podłączane poprzez routery do komunikacji nie mogą wykorzystywać protokołu NetBEUI.

NNTP (Network News Transfer Protocol) Protokół opracowany dla dystrybucji, zapytań, pobierania i umieszczania artykułów w sieci Internet.

O

Obiekt (object) Zestaw atrybutów, które reprezentują konkretny element taki jak użytkownik, drukarka bądź aplikacja. Atrybuty przechowują dane opisujące rzeczy identyfikowane przez obiekt. Atrybutami użytkownika mogą być jego nazwisko, imię i adres e-mail. Klasyfikacja obiektów definiuje, który typ atrybutów jest używany. Na przykład obiekty sklasyfikowane jako użytkownik umożliwiają użycie atrybutów typu nazwisko, numer telefonu, adres e-mail, podczas gdy klasa obiektu organizacja zezwala na stosowanie atrybutów takich jak nazwa organizacji czy kategoria biznesu. W zależności od typu atrybutu może on mieć jedną lub kilka wartości.

Obiekt podrzędny (child object) Obiekt znajdujący się wewnątrz innego obiektu. Przykładowo plik jest obiektem podrzędnym folderu, który jest dla niego obiektem nadrzędnym.

Obiekt zasady grupy GPO (Group Policy Object) Zbiór zasad przechowywany w dwóch lokalizacjach: w kontenerze zasady grupy (GPC) oraz w szablonie zasady grupy (GPT). Kontener GPC jest obiektem usługi Active Directory przechowującym informacje o wersji, statusie i innych zasadach (przykładowo o obiektach aplikacji). Szablon GPT jest używany dla zasad związanych z danymi dotyczącymi plików i magazynów oprogramowania, skryptami oraz rozmieszczaniem informacji. Szablon GPT jest umieszczany w folderze woluminu systemowego kontrolera domeny.

Odporność na uszkodzenia (fault tolerance) Cecha systemu zapewniająca integralność danych w przypadku awarii jednego z elementów sprzętu lub oprogramowania. Wiele odpornych na uszkodzenia systemów komputerowych dubluje wszystkie operacje — tzn. wszystkie operacje wykonywane są na co najmniej dwóch powielonych systemach, dzięki czemu w przypadku awarii jednego z systemów, drugi przejmuje jego zadania.

P

Pakiet (packet) Podstawowa jednostka informacji przesyłana w sieci. Każdy pakiet zawiera adres miejsca docelowego, adres nadawcy, informacje dotyczące sum kontrolnych oraz dane. Rozmiar i format pakietu zależy od wykorzystywanego protokołu.

Partycja podstawowa (primary partition) Część dysku twardego oznaczona przez system operacyjny jako dysk logiczny, na podstawie którego można przeprowadzić **rozruch** komputera. System MS-DOS obsługuje wyłącznie partycje podstawowe. Dyski oparte o strukturę głównego rekordu rozruchowego (MBR) mogą zawierać do czterech partycji podstawowych. Komputery zbudowane w oparciu o procesory Intel Itanium używają tablicy partycji GUID, która może obsługiwać do 128 partycji podstawowych.

Partycja rozszerzona (extended partition) Fragment dysku twardego, z którego nie można przeprowadzać rozruchu komputera i który może zostać podzielony na dyski logiczne. Na dysku twardym może być tylko jedna partycja rozszerzona.

Ping Program narzędziowy protokołu IP (Internet Protocol), za pomocą którego można sprawdzić, czy inny komputer jest dostępny i czy funkcjonuje. Program wysyła krótką wiadomość, na którą inny komputer automatycznie odpowiada. Jeśli natomiast **komputer** nie odpowiada na wiadomość wysianą przez program Ping, oznacza to najczęściej, że pomiędzy tymi komputerami nie może zostać nawiązana komunikacja na poziomie protokołu IP.

Plik HOSTS Lokalny plik tekstowy ASCII, który przypisuje nazwy hostów do adresów IP. Każda linia reprezentuje jeden host i rozpoczyna się od adresu IP, po którym umieszczana jest jedna lub kilka spacji, a po nich nazwa hosta.

Podmiot zabezpieczeń (security principal) Jednostka, do której może być przydzielane uprawnienie do zasobu. Podmiot zabezpieczeń jest obiektem, który zawiera atrybut identyfikatora zabezpieczeń SID. System Windows Server 2003 obsługuje cztery podmioty zabezpieczeń: użytkownicy, komputery, grupy i obiekt InetOrgPerson.

Podpis cyfrowy (digital signature) Atrybut sterownika, aplikacji lub dokumentu, który identyfikuje twórcę pliku. Podpis cyfrowy firmy Microsoft jest dołączany do wszystkich sterowników dostarczanych przez firmę Microsoft, dzięki czemu użytkownik ma pewność co do stabilności i kompatybilności sterowników używanych w systemie Windows Server 2003 oraz Windows 2000 Server.

Podsicć (subnet) Część sieci protokołu TCP/IP (Transmission Control Protocol/Internet Protocol), w której wszystkie urządzenia korzystają ze wspólnego prefiksu. Na przykład wszystkie urządzenia,

MCSE Training Kit: Egzamin 70-290

dla których adres IP rozpoczyna się liczbą 198, znajdują się w tej samej podsieci. Sieci IP są dzielone przy użyciu maski podsieci. **Podstawowy kontroler domeny PDC (primary domain controller)** Serwer w domenie systemu Windows NT, który uwierzytelnia logowanie oraz obsługuje zasady zabezpieczeń i bazę danych domeny. W domenach systemów Windows 2000 lub Windows Server 2003, które uruchomione zostały w trybie mieszanym, jest to jeden z kontrolerów domeny w każdej domenie, określony jako wzorzec emulatora PDC zapewniający kompatybilność z klientami i serwerami wersji wcześniejszych.

Pomoc zdalna (Remote Assistance) Usługa umożliwia początkującym użytkownikom wykorzystywanie programu Windows Messenger do wysłania prośby do eksperta o osobistą pomoc interaktywną. Po zaakceptowaniu prośby i nawiązaniu sesji zdalnej, ekspert może przeglądać pulpit użytkownika; jeśli użytkownik początkujący na to zezwolił, może również kontrolować pulpit.

POP (Post Office Protocol) Protokół umożliwiający serwerom pocztowym sieci Internet udostępnianie poczty i pobieranie jej do poszczególnych komputerów. Protokół ten oznaczany jest zwykle wraz z wersją (POP2, POP3 itd), aby uniknąć pomyłek z punktami obecności (POP).

Port Z punktu widzenia systemu komputerowego jest to punkt fizycznego podłączenia urządzeń, za pomocą których **przekazywane** są informacje do komputera i z komputera. Przykładowo drukarka jest najczęściej podłączona do portu równoległego (nazywanego również portem LPT), a modem jest najczęściej podłączany do portu szeregowego (nazywanego inaczej portem COM). W odniesieniu do sieci port jest numerowanym kanałem komunikacji, poprzez który przekazywane są informacje pomiędzy komputerami. Przykładowo program **Terminal Services** (Usługi terminalowe) komunikuje się poprzez port 3389.

Powiązanie (biulding) Połączenie programowe pomiędzy kartą sieciową a sieciowym protokołem transportu, takim jak TCP/IP (Transmission Control Protocol/Internet Protocol).

Poziom funkcjonalności domeny (domain functional level) Poziom funkcjonowania domeny usługi Active Directory. Wraz ze zwiększeniem poziomu funkcjonalności, staje się dostępna cóża?, większa liczba funkcji usługi Active Directory. Istnieją cztery poziomy: mieszany systemu Windows 2000, macierzysty systemu Windows 2000, tymczasowy systemu Windows Server 2003 oraz macierzysty systemu Windows Server 2003-

PPTP (Point-to-Point Tunneling Protocol) Protokół umożliwiający połączenia pomiędzy routami oraz pomiędzy hostami a siecią poprzez linie telefoniczne (lub połączenia sieci, które funkcjonują tak, jak linie telefoniczne). Zobacz *SLIP (Serial Line Internet Protocol)*.

Prawo użytkownika (user right) Uprawnienie dotyczące logowania, które pozwala na wykonywanie zadań systemowych, takich jak logowanie lokalne lub przywracanie plików bądź folderów. Ponieważ prawa użytkownika odnoszą się do systemu, a nie do zasobu, będą zastępować uprawnienia do poszczególnych zasobów. Przykładowo użytkownicy posiadający prawo Backup Files And Folders (Tworzenie kopii zapasowych plików i folderów), będą mogli kopiować pliki na taśmę, nawet jeśli nie mają uprawnień odczytu do tego pliku.

Profil (profile) Profil pobierany jest podczas logowania użytkownika i definiuje środowisko, wliczając w to ustawienia sieci, połączenia drukarek, ustawienia pulpitu i używane programy.

Profil użytkownika (user profile) Informacje o kontach użytkownika. Zobacz *profil*.

Prywatne sieci wirtualne VPN (Virtual Private Network) Sieć wykorzystująca publiczne połączenia do komunikacji pomiędzy węzłami. Sieci VPN używają szyfrowania (na przykład protokołu IPSec), a także innych mechanizmów zabezpieczeń zapewniając w ten sposób, że tylko uwierzytelnieni użytkownicy uzyskują dostęp do sieci, a dane nie zostaną przechwycone.

- Przedsiębiorstwo (enterprise)** Termin obejmujący całą organizację, włączając w to biura zdalne i oddziały.
- Przekierowanie foldera (folder redirection)** Opcja zasady grupy umożliwiająca umieszczenie na serwerach sieci specjalnych folderów użytkownika, takich jak folder My Documents (Moje dokumenty).
- Przestrzeń nazw (namespace)** Nazwa lub grupa nazw zdefiniowana zgodnie z konwencją nazewnictwa; każdy wspólny obszar, w którym dana nazwa może zostać rozwiązana. Usługa Active Directory jest przede wszystkim przestrzenią nazw, tak jak każda usługa katalogowa. W sieci Internet używana jest hierarchiczna przestrzeń, która dzieli nazwy na kategorie znane jako domeny najwyższego poziomu, takie jak .com, .edu, and .gov.
- Przydział dysku (disk <pool>)** Ograniczenie nakładane przez administratora, dotyczące wielkości przestrzeni dysku dostępnej dla użytkownika.
- Przystawka (snap-in)** Narzędzie, które może być dodane do konsoli MMC (Microsoft Management Console). Aby rozszerzyć funkcje przystawki, można do niej dodawać rozszerzenia.
- Przywracanie autorytatywne (authoritative restore)** Określa rodzaj odzyskiwania usługi Active Directory. Podczas przeprowadzania odzyskiwania autorytatywnego przy użyciu programów Backup Utility (Kopia zapasowa) i Ntdsutil w trybie Directory Services Restore (Odzyskiwanie usługi katalogowej), pr/wyiwacany autorytatywnie katalog lub określone obiekty katalogu zostają replikowane do pozostałych kontrolerów domeny w lesie. Zobacz *przywracanie nieautorytatywne*.
- Przywracanie nieautorytatywne (non-authoritative restore)** Podczas przywracania danych o stanie systemu kontrolera domeny odtwarzana jest usługa Active Directory. Po ponownym uruchomieniu kontrolera domeny informacje o katalogu od nos/ą się; do okresu, w którym tworzona była kopia zapasowa. Zostają one uaktualnione w trakcie zwykłego procesu replikacji danych pomiędzy kontrolerami domeny.
- Pula nośników (media pool)** Zbiór logiczny nośników wymiennych, do których stosują się te same zasady zarządzania.
- Pula nośników kopii zapasowych (backup media pool)** Digiczny zbiór nośników kopii zapasowych używanych w systemach Windows Server 2003 i Windows 2000 Server.
- Pulpit zdalny dla administracji (Remote Desktop for Administration)** Technologia bazująca na programie Terminal Services (Usługi terminalowe), która udostępnia dwa połączenia zdalne wykorzystywane w celach administracji. W systemie Windows 2000 usługa znana jest jako program Terminal Server (Serwet terminali) w trybie administracji zdalnej.
- Punkt obecności POP (point of presence)** Lokacja fizyczna w geograficznym obszarze, w którym dostawca usługi sieci (pizykładowo firma telekomunikacyjna) posiada urządzenia, do których użytkownik może się podłączyć. Biuro centralne lokalnej firmy telekomunikacyjnej jest czasami również określane jako POP dla danego obszaru.

R

- RADIUS (Remote Authentication Dial-In User Service)** Bezpieczny system uwierzytelniania stosowany przez wielu dostawców usług internetowych (ISP). Użytkownik podłącza się do dostawcy ISP i wprowadza swoją nazwę użytkownika i hasło. Informacje te są sprawdzane przez serwer RADIUS, a następnie serwer umożliwia dostęp do systemu dostawcy ISP.
- Relacje zaufania (trust relationship)** Pojęcie, które dotyczy zabezpieczeń oznaczające, że stacja robocza lub serwer ufają kontrolerowi domeny, który w ich imieniu dokonuje uwierzytelnienia

użytkowników podczas logowania. Oznacza ono również, że w zakresie uwierzytelnienia logowania kontroler domeny ufa kontrolerowi domeny w innej domenie.

Replikacja (replication) Usługa umożliwia w sieci komputerów kopiowanie zawartości katalogu (katalog eksportu) do innego katalogu (katalog importu). W usłudze Active Directory zmiany są replikowane do wszystkich kontrolerów domeny zgodnie z regularnym harmonogramem.

Replikacja typu multimaster (multimaster replication _____) Cecha usługi Active Directory. Replikacja typu multimaster przeprowadza automatyczne przekazywanie informacji o każdym obiekcie (takim jak grupy, użytkownicy, komputery, domeny, jednostki organizacyjne itd) utworzonym na kontrolerze domeny do pozostałych kontrolerów tej domeny. Wszystkie kontrolery domeny zawierają te same dane o katalogu, dzięki czemu domena nie jest zależna od pojedynczego źródła informacji o katalogu.

Router Urządzenie sieci (lub komputer z odpowiednim oprogramowaniem), które obsługuje połączenia pomiędzy co najmniej dwiema sieciami. Routery przesyłają pakiety zgodnie z ich adresami docelowymi oraz decydują, którą trasą pakiety będą przesyłane.

Rozgłoszenie (broadcasting) Jednoczesne wysłanie wiadomości do wszystkich komputerów w sieci. Zobacz *multitemhja*.

Rozproszony system plików DFS (Distributed file system) System zarządzania plikami, który może być rozmieszczony na oddzielnych komputerach, ale dla użytkownika przedstawiany jest jako pojedyncze drzewo katalogu.

Rozwiązywanie nazwy (name resolution) Proces przypisywania nazwy odpowiadającemu jej adresowi IP.

Równoważenie obciążenia sieci NLB (Network Load Balancing) Technologia umożliwiająca sprawne wykorzystanie kilku kart sieciowych.

S

Schema (schemat) Zestaw definicji klas i atrybutów obiektu, które mogą być przechowywane w usłudze Active Directory. Podobnie jak inne obiekty usługi Active Directory, obiekty schematu mają listę kontroli dostępu ACL, dzięki której zmiany obiektu mogą być przeprowadzane jedynie przez autoryzowanych użytkowników.

Serwer (server) Komputer udostępniający usługi innym komputerom sieci. Przykładowo serwer plików udostępnia pliki dla klientów innych komputerów.

Serwer członkowski (member server) Serwer, który jest częścią domeny, ale nie jest kontrolerem domeny. Serwery członkowskie mogą być dedykowane do obsługi plików, usług drukowania lub innych funkcji. Serwer członkowski nie sprawdza logowania i nie obsługuje bazy danych zabezpieczeń.

Serwer proxy (proxy server) Serwer, który odbiera żądania klientów przeszukujących wirryny sieci Web oraz przekazujący odpowiedzi z powrotem do klienta. Serwery proxy w sposób istotny poprawiają wydajność dla grup użytkowników dzięki buforowaniu wyszukanych stron. Oprócz tego, serwery proxy zapewniają ochronę poprzez ekranowanie adresów IP klientów wewnętrznych od sieci Internet.

Serwer typu "headless" Zarządzany zdalnie serwer bez monitora, klawiatury, myszy lub karty video.

Serwery nazw DNS Serwery zawierające informacje o fragmencie bazy danych DNS (Domain Name System). Serwery te udostępniają nazwy komputerów dla zapytań dotyczących rozpoznawania nazw w sieci Internet. Nazywane są również *Serwerami nazw domen*.

Sieci rozległe WAN (wide area network) Dowolna sieć złożona obsługująca obszar większy niż pojedynczy budynek czy miasteczko uniwersyteckie. **Sieć (network)** Co najmniej dwa komputery połączone ze sobą w celu współużytkowania zasobów.

Sieć lokalna LAN (local area network) Grupa połączonych komputerów najczęściej umieszczonych blisko siebie (w tym samym budynku bądź na tym samym piętrze), pomiędzy którymi przesyłane są dane.

Składnik ActiveX (ActiveX component) Składnik oprogramowania wielokrotnego użytku, funkcjonujący zgodnie ze specyfikacją i w środowisku technologii ActiveX.

Skojarzenie (Associate) Przypisanie pliku o danym rozszerzeniu do określonego programu. Dwukrotne kliknięcie pliku % danym rozszerzeniem powoduje, że uruchamiany zostaje skojarzony program, a plik zostaje otwarty. W systemie Windows skojarzone rozszerzenia plików są najczęściej nazywane zarejestrowanymi typami plików.

Skrypt logowania (logon script) Najczęściej jest to plik wsadowy uruchamiany podczas logowania lub wylogowywania użytkownika z systemu. Skrypt logowania jest używany do konfigurowania indywidualnego środowiska użytkownika. Skrypt wykonywany podczas wylogowania powoduje przywrócenie pewnych predefiniowanych ustawień systemu. Skrypty te mogą być przypisywane do wielu pojedynczych użytkowników lub stosowane poprzez zasadę grupy.

SLIP (Serial Line Internet Protocol) Protokół używany do uruchomienia protokołu IP (Internet Protocol) za pomocą modemów poprzez linie szeregowo lub telefoniczne. Szybko został zastąpiony przez protokół PPTP (Point-to-Point Tunneling Protocol). Protokół SLIP jest częścią mechanizmów dostępu zdalnego w systemie Windows zaimplementowanym w celu zapewnienia kompatybilności z innymi rodzajami oprogramowania dostępu zdalnego.

SOAP (Simple Object Access Protocol) Protokół oparty na XML/HTTP, który stanowi sposób komunikacji pomiędzy aplikacjami poprzez sieć Internet, niezależnie od platformy

Specyfikacja RFC (Requests for Comments) Zbiór uzupełnianych informacji szczegółowo omawiających działanie rodziny protokołów TCP/IP. Niektóre specyfikacje RFC są oficjalnymi dokumentami grupy IETF (Internet Engineering Task Force) definiującymi standardy TCP/IP i sieci Internet, podczas gdy inne są jedynie propozycjami, które mogą dopiero stać się standardami. Niektóre specyfikacje mają charakter podręcznika, a inne są dokumentacją techniczną.

Stacja robocza (workstation) W systemie Windows NT jest to komputer działający pod kontrolą systemu operacyjnego Windows NT Workstation. W szerszym kontekście, jest to wydajny komputer zoptymalizowany do zastosowań graficznych, do komputerowego wspomagania projektów (CAD) lub do innych zastosowań wymagających wysokiej wydajności.

Sterownik urządzenia (Device Driver) Program, który umożliwia określonemu urządzeniu, takiemu jak modem, karta sieciowa lub drukarka, komunikację z systemem operacyjnym. Pomimo, że urządzenie może zostać zainstalowane w komputerze, system operacyjny nie może wykorzystywać tego urządzenia dopóki nie zostanie zainstalowany i skonfigurowany odpowiedni sterownik. Podczas rozruchu komputera sterowniki urządzeń są automatycznie pobierane do pamięci (dla wszystkich włączonych urządzeń) i od tego momentu działają niewidocznie dla użytkownika.

Strefa (zone) Część przestrzeni nazw systemu DNS (Domain Name System), która zawiera pojedynczą domenę lub domenę i poddomeny zarządzane jako pojedyncza, odrębna jednostka.

Strona (page) Dokument lub zbiór informacji dostępnych w sieci Web. Strona może zawierać pliki tekstowe, graficzne, obrazu oraz pliki dźwiękowe. Termin strona odnosi się również do części pamięci, która jest przenoszona przez menedżera pamięci wirtualnej pomiędzy dyskiem twardym a pamięcią operacyjną.

Stronicowanie (paging) Operacja pamięci wirtualnej, w trakcie której strony są przenoszone z pamięci do dysku twardego w sytuacji, kiedy pamięć zostaje zapełniona. Jeśli wątek uzyskuje dostęp do strony, która nie znajduje się w pamięci, występuje błąd strony, a menedżer pamięci, na podstawie tablic stron, wyszukuje odpowiednie strony, a następnie pobiera je i umieszcza w pamięci.

Superszakres (superscope) Zbiór zakresów pogrupowanych pod względem administracyjnym w jedną całość. Grupowanie zakresów umożliwia posiadanie kilku podsieci logicznych w jednej podsieci fizycznej.

System plików NTFS Macierzysty system plików dla systemów Windows Server 2003, Windows 2000 oraz Windows NT. Obsługuje długie nazwy plików, szereg uprawnień dotyczących udostępnionych plików **potrzebnych do zarządzania dostępem** do plików i folderów **oraz** transakcje, które umożliwiają zakończenie dowolnego zadania przerwanego wskutek zatrzymania operacji systemu.

System RSM (Removable Storage Management) Cecha systemu Windows Server 2003, która stanowi interfejs dla bibliotek nośników i mechanicznych zmieniaaczy, umożliwiając w ramach pojedynczego systemu wielu aplikacjom współużytkowanie bibliotek lokalnych, nośników taśmowych lub napędów dyskowych oraz kontrolowanie nośników wymienialnych.

SystemRoot Ścieżka i folder, w którym przechowywane są pliki systemu Windows. W ścieżce można używać wartości **%SystemRoot%**, która zastępuje rzeczywistą lokalizację. Aby zidentyfikować folder SystemRoot w komputerze, należy w wierszu poleceń wpisać **%SystemRoot%**.

SYSVOL Folder na kontrolerze domeny zawierający zasady grupy i skrypty logowania, folder SYSVOL, jest replikowany pomiędzy kontrolerami domeny za pomocą usługi replikacji plików (FRS).

Szerokość pasma (bandwidth) W sieciach jest to określenie zdolności do transmisji kanału komunikacyjnego, wyrażanej w megabitach na sekundę (Mbps). Przykładowo pasmo sieci Kthcmct wynosi Mbps, a sieci Fast Ethernet 100 Mbps.

Szybkie i niezawodne połączenia (wcll-connected) Szybkie i **niezawodne** połączenia wykorzystywane do komunikacji w lokacji usługi Active **Directory**. Definicja „wystarczająco” szybkiej i niezawodnej sieci zależy od liczby zadań, które muszą być wykonywane w danej sieci.

Szyfrowanie za pomocą klucza publicznego (public-key cryptography) Metoda zabezpieczania transmisji, podczas **której** używane są dwa klucze - klucz publiczny służący do szyfrowania danych oraz klucz prywatny służący do deszyfrowania danych.

T

Tablica partycji GUID (GPT) Miejsce przechowywania informacji o konfiguracji dysku używane w 64-bitowych wersjach systemu Windows. **TCP/IP (Transmission Control Protocol/Internet Protocol)** Zestaw protokołów używanych przez sieci do komunikacji w Internecie.

Telnet Protokół i program używany do zalogowania się z jednej lokacji sieci Internet do innej lokacji. Program i protokół Telnet udostępnia okno logowania innego hosta.

Terminal Urządzenie umożliwiające przysyłanie poleceń do innego komputera. Zestaw minimalny takiego urządzenia to klawiatura, ekran wyświetlacza oraz niektóre proste obwody. Najczęściej

na komputerze osobistym używane jest oprogramowanie, które emuluje terminal fizyczny, umożliwiając wprowadzanie poleceń na innym komputerze.

Token Ring Typ sieci komputerowej, w której połączenia komputerów tworzą pierścień. Żeton (*token*), który jest specjalnym wzorem bitów, krąży w tym pierścieniu. Aby skomunikować się z innym komputerem, dany komputer przechwytuje żeton, dołącza do niego wiadomość, a żeton kontynuuje poruszanie się w pierścieniu „upuszczając” wiadomość w lokalizacji docelowej.

Tryb macierzysty (native modę) W domenach systemu Windows 2000 sytuacja, kiedy wszystkie kontrolery domeny zostały zaktualizowane do systemu Windows 2000, a administrator włączył działanie trybu macierzystego. W serwerach domen systemu Windows Server 2003, w których nie występują kontrolery domen systemów Windows 2000 lub Windows NT 4, tryb macierzysty jest po prostu nazywany trybem lub poziomem funkcjonalnym systemu Windows Server 2003- Zobacz *poziom funkcjonalny domeny*.

U

Ul (hive) Jedna z pięciu sekcji rejestru. Każdy ul jest odrębnym zbiorem kluczy, podkluczy oraz waitości, które przechowują informacje o konfiguracji komputera. Każdy ul jest plikiem, który może być przenoszony z jednego systemu do innego, ale jego edycja przeprowadzana jest wyłącznie za pomocą programu Registry F-ditor (F.dylor rejestru).

UNC (Univrsal Naming Convcnliion) Format komputerów osobistych do wskazania lokalizacji zasobu sieci. UNC] korzysta z następującego formatu: `\\Serwer\Scieżlut udostępnionego zasobu`. Do identyfikacji pliku `\\xaniple.txt` znajdującego się w folderze Sample na .serwerze Ample należy użyć następującego formatu nazwy UNC! `\\Ample\\Simple\\hjaimple.txt`.

UNIX System operacyjny opracowany do jednoczesnego wykorzystywania przez wielu użytkowników. W systemie wbudowany jest protokół TCP/IP (Transmission Control Pioioiol/Inictnet Protocol). a serwery tego systemu s.j bardzo popularne w sieci Internet.

UPnP (Univrsal Plug and Play) Stand.itii umożliwiający urządzeniom przyłączonym do sieci (Pi], peryferia, urządzenia bezprzewodowe) uzyskiwanie adresu IP (Internet Protocol). Następnie w oparciu o len adres, korzystając z protokołów sieci Internet i Web, takich jak HTTP (I lypcrtxt Transfer Protocol), urządzenia te mogą w sieci ogłosić swoją obecność i dostępność.

Uprawnienia czynne (cfcfciiivc permissions) Uprawnienia użytkownika lub grupy zasobu uwzględniające wszystkie uprawnienia bezpośrednio zdefiniowane oraz dotyczące zezwoleń, odmowy i dziedziczenia. Uprawnienia czynne określają rzeczywisty poziom dostępu dla podmiotu zabezpieczeń.

URL (Uniform Resource Locator) Typowy sposób przedstawiania adresu zasobu w sieci Internet, na przykład <http://www.iiidatum.com>. Najczęściej URL jest używany przy wprowadzaniu adresu w przeglądarkach sieci Web.

Urząd certyfikacji CA (certificatc authority) Usługa, która akceptuje oraz wypełnia żądania certyfikacji i jej unieważnienia. Może również zarządzać procesami rejestracji kierowanymi przez zasady, dzięki którym użytkownik uzyskuje certyfikację.

USB (universal serial bus) Interfejs pomiędzy komputerem a dodatkowymi urządzeniami, który umożliwia proste podłączenie i automatyczne wykrywanie urządzenia. Porty USB obsługują wiele urządzeń na jednym porcie i najczęściej umożliwiają przyłączanie urządzeń bez konieczności wyłączania zasilania komputera.

Usługa Aktualizacje automatyczne (Automatic Updates) Składnik usługi po stronie klienta, dzięki której system jest stale aktualizowany poprzez instalowanie poprawek i sterowników. Usługa

Automatic Updates (Aktualizacje automatyczne) jest również klientem w infrastrukturze usługi SUS (Software Update Services), dzięki której można w przedsiębiorstwie centralnie zarządzać aktualizacjami.

Usługa dostępu zdalnego RAS (Remote Access Service) Usługa ta umożliwia użytkownikom połączenie z lokalizacji zdalnej oraz uzyskanie dostępu do sieci celem współużytkowania plików, drukarek oraz poczty elektronicznej. Komputery rozpoczynające połączenie RAS jest klientem, a komputer, który udziela odpowiedzi jest serwerem RAS.

Usługa katalogowa (directory service) Przechowywanie danych katalogu i ich udostępnianie użytkownikom sieci. Przykładowo usługa Active Directory przechowuje informacje o kontach użytkowników takich jak nazwy, hasła, numery telefonów itd. oraz udostępnia te informacje innym użytkownikom tej samej sieci.

Usługa klastra (Cluster service) Zestaw oprogramowania zarządzającego wszystkimi aspektami działań klastri, który musi być uruchomiony na każdym węźle **klastra**.

Usługa lokalizacji rekordu zasobu SRV (service locator resource record) Rekord strefy DNS określający komputer (według nazwy), który świadczy określoną usługę. Rekordy SRV umożliwiają klientom kierowanie zapytań do systemu DNS.

Usługa Net Logon (Net Logon service) Usługa, która akceptuje żądania logowania dowolnego klienta oraz umożliwia uwierzytelnienie na podstawie bazy danych kont SAM (Security Accounts Manager).

Usługa przeglądania (Browser service) Usługa, która obsługuje bieżącą listę komputerów i przesyła tę listę do /- (dających jej programów). Jeśli użytkownik próbuje podłączyć się do zasobu domeny, usługa przeglądania udostępnia listę dostępnych zasobów. Między innymi lista wyświetlana w oknie programu My Network Places (Moje miejsca sieciowe) i w przystawce Active Directory Users and Computers (Użytkownicy i komputery usługi Active Directory) jest udostępniana przez usługę przeglądarki komputerów. Usługa nazywana jest również Przeglądarką komputera.

Usługa SUS (Software Update Services) Technologia bazująca na funkcjonalności serwera, która umożliwia scentralizowane pobieranie i zatwierdzanie aktualizacji i poprawek dostarczanych do klientów sieci korzystających z usługi Automatic Updates (Aktualizacje automatyczne).

Usługa VSS (Volumetric Shadow Copy Service) Usługa, która podczas wykonywania kopii zapasowej tworzy obraz pliku, dzięki czemu kopia zapasowa zostaje utworzona bez względu na to, czy pierwotny plik był zablokowany czy otwarty.

Usługa WINS (Windows Internet Naming Service) Usługa rozpoznawania nazw, dzięki której w środowisku wymagającym stosowania routingu, nazwy NetBIOS komputerów przekształcane są w adresy IP (Internet Protocol).

Usługi instalacji zdalnej RIS (Remote Installation Services) Usługi te umożliwiają klientom rozruch komputera z serwera sieci oraz korzystanie ze specjalnych narzędzi diagnostycznych zainstalowanych wcześniej na serwerze, dzięki którym instalowany jest system operacyjny klienta.

Usługi terminalowe (Terminal Services) Podstawowa technologia używana w programach Remote Desktop for Administration (Pulpit zdalny dla administracji), Remote Assistance (Pomoc zdalna) oraz Terminal Server (Serwer terminali).

Uwierzytelnienie (authentication) Weryfikacja tożsamości użytkownika komputera lub proces komputerowy. W systemach Windows Server 2003, Windows 2000 i Windows NT uwierzytelnienie powoduje porównanie identyfikatorów zabezpieczeń użytkownika SID i hasła z listą użytkowników uwierzytelnionych w kontrolerze domeny.

W

W pełni kwalifikowana nazwa domeny FQDN (fully qualified domain name) Nazwa domeny, która zawiera wszystkie domeny prowadzące do domeny głównej, określająca precyzyjnie lokalizację w drzewie przestrzeni nazw domeny. Przykładem nazwy FQDN jest *Accts.finance.adatum.com* lub *Sales.europe.microsoft.com*.

Wąskie gardło (bottleneck) Odnosi się do sytuacji, w której w systemie komputerowym jest zainstalowana niewystarczająca ilość pewnego zasobu, a żądanie zasobów bądź usług powoduje znaczący spadek wydajności.

Wątek (thread) Jednostka programu wykonywalnego, która jest związana z jednym (i tylko z jednym) procesem. W środowisku wielozadaniowym pojedynczy program może zawierać wiele wątków, które działają jednocześnie.

WBEM (Web-Based Enterprise Management) Zestaw standardowych technologii zarządzania i sieci Internet opracowany do zunifikowania zarządzania środowiskami sieci komputerowych przedsiębiorstw. Implementacja WBEM firmy Microsoft nazwana została Windows Management Instrumentation.

Węzeł (node) Lokalizacja w strukturze drzewa, która łączy jeden lub kilka elementów. W sieci lokalnej (LAN) jest to urządzenie, które może komunikować się z innymi urządzeniami w sieci. W klastrze jest to komputer, który jest członkiem klasra.

Wielokrotne łącze telefoniczne (multilink dialing) Połączenie dwóch lub więcej komunikacyjnych łącz telefonicznych w jedno łącze logiczne, dzięki czemu zwiększone zostaje dostępne pasmo.

Wielowątkowość (multithreading) Jednoczesne przetwarzanie kilku wątków wewnątrz tego samego programu. Ponieważ kilka wątków może być przetwarzanych równolegle, jeden wątek nie musi zostać zakończony przed rozpoczęciem przetwarzania innego wątku.

Wielozadaniowość (multitasking) 'technika komputerowa, dzięki której zadania są dołączane i odłączane od procesora tak szybko, że zadania sprawiają wrażenie wykonywanych jednocześnie. Sprawne działanie systemu wielozadaniowego zależy od tego, w jakim stopniu różne zadania są izolowane pomiędzy sobą.

Windows Sockets (Winsock) Winsock jest standardową metodą dla programów systemu Windows, umożliwiającą wykorzystywanie protokołu TCP/IP (Transmission Control Protocol/Internet Protocol). Jeśli używany jest protokół SLIP, interfejs Winsock może być używany do połączeń z siecią Internet.

WMI (Windows Management Instrumentation) Interfejs programowy umożliwiający dostęp do urządzeń, oprogramowania i innych komponentów komputera. Interfejs WMI jest implementacją firmy Microsoft specyfikacji WBEM (Web-Based Enterprise Management) mającej na celu ustanowienie standardów dotyczących zarządzania przedsiębiorstwem.

Wpis kontroli dostępu ACE (access control entry) Wpis na liście kontroli dostępu (ACL) definiujący poziom dostępu dla użytkownika lub grupy.

Wykaz (catalog) Spis plików zestawu kopii zapasowej.

Wykaz globalny GC (Global Catalog) Wykaz ten zawiera pełną replikę obiektów usługi Active Directory swojej domeny oraz częściową replikę wszystkich obiektów katalogu każdej domeny lasu. Wykaz globalny zawiera informacje o wszystkich obiektach lasu, dzięki czemu wyszukiwanie informacji nie generuje niepotrzebnych zapytań pomiędzy domenami. Pojedyncze zapytanie skierowane do wykazu globalnego pozwala uzyskać informacje, gdzie można wyszukać obiekt.

Względna nazwa wyróżniająca RDN (relative distinguished name) Stosowane w usłudze Active Directory pojęcie stanowiące część nazwy wyróżniającej, które jest atrybutem samego obiektu.

Względny identyfikator RID (relative identifier) Część identyfikatora zabezpieczeń SID, która jest unikatowa dla każdego obiektu.

Wzorzec emulatora PDC (PDC Emulator master) Kontroler domeny obsługujący klientów sieci, którzy nie mają zainstalowanego oprogramowania usługi Active Directory oraz replikuje zmiany w katalogach wszystkich zapasowych kontrolerów domen systemu Windows NT. Wzorzec emulatora PDC obsługuje również żądania uwierzytelnienia kont, dla których niedawno zmienione hasło nie zostało jeszcze zreplikowane w całej domenie.

Wzorzec nazw domen (domain naming master) Kontroler domeny wyznaczony do obsługi operacji dodawania lub usuwania domen w lesie. Zobacz *Wzorzec operacji*.

Wzorzec operacji (Operations Master) Kontroler domeny przypisany do specjalnych operacji usługi Active Directory, operacje punktowe, które nie mogą być wykonywane jednocześnie w różnych miejscach w sieci. Do operacji tych należą na przykład alokacja identyfikatorów zasobów (RID), modyfikacja schematu bądź dodawanie domen.

Wzorzec schematu (schema master) Pojedynczy kontroler domeny, któremu zostało przypisane zadanie śledzenia wszystkich aktualizacji schematu w lesie.

X

X.500 Standard usługi katalogowej ustanowiony przez ITU (International Telecommunications Union). Ten sam standard został również opublikowany przez organizację ISO/IEC (International Standards Organization/International Electrotechnical Commission). Standard X.500 definiuje model informacji używanych w usłudze katalogowej. Wszystkie informacje katalogu przechowywane są we wpisach, z których każdy należy do co najmniej jednej klasy obiektu. Rzeczywista informacja wpisu jest określona przez atrybuty znajdujące się w tym wpisie.

XML (Extensible Markup Language) Skrócona wersja języka SGML (Standard Generalized Markup Language), która umożliwia elastyczne projektowanie typów dokumentu definiowanych przez użytkownika oraz udostępnia stały, otwarty i łatwy do sprawdzenia format pliku do przechowywania i transmisji danych bądź tekstów w sieciach Web.

Z

Zakres (scope) W protokole DHCP (Dynamic Host Configuration Protocol) jest to zakres dostępnych adresów IP wydzielanych klientom usługi DHCP. W grupach zakres opisuje, gdzie w sieci uprawnienia mogą być przypisywane do grup.

Zalogować (log on) Zarejestrowanie się w komputerze. Na przykład: zaloguj się w sieci i odczytaj swoją pocztę elektroniczną.

Zapora ogniowa (firewall) Filtr ochronny wiadomości i informacji związanych z logowaniem. Organizacja połączona bezpośrednio do sieci Internet wykorzystuje zaporę ogniową do ochrony swojej sieci przed nieuwierzytelnionym dostępem. Zobacz *Serwerproxy*.

Zasada grupy (Group Policy) Ustawienia reguł stosowanych do komputerów i użytkowników w systemach Windows Server 2003 i Windows 2000 Server. Zasada grupy przechowuje zasady dotyczące instalowania plików i aplikacji, dotyczące skryptów logowania i wylogowania, skryptów startowych i kończących pracę systemu, zabezpieczeń domeny, zabezpieczeń protokołu IP (IPSec) itp.

Zasada inspekcji (audit policy) Definiuje rodzaj zdarzeń zabezpieczeń, które mają być rejestrowane. Zasada ta może być definiowana na serwerze lub komputerze osobistym.

Zaufanie lasu (forest trust) Przechodnie zaufanie jedno- lub dwukierunkowe, używane do współużytkowania zasobów pomiędzy lasami.

Zaufanie obszaru (realni trust) Używane podczas połączeń pomiędzy domenami systemu Windows Server 2003 a obszarami protokołu Kerberos spoza systemu Windows. Relacje zaufania obszaru mogą być przechodnie, nieprzechodnie, jednokierunkowe lub dwukierunkowe.

Zaufanie przechodnie (transitive trust) Zaufanie standardowe pomiędzy domenami systemu Windows Server 2003 w drzewie lub lesie domen. Zaufanie przechodnie jest zawsze dwukierunkowe. Jeśli domena dołączana jest do drzewa lub lasu, relacje zaufania przechodniego są automatycznie ustanawiane.

Zaufanie skrótowe (shortcut trust) Używane do skrócenia czasu logowania pomiędzy dwoma domenami lasu systemów Windows Server 2003 lub Windows 2000. Zaufania skrótowe są **przechodnie** i mogą być relacjami jednokierunkowymi lub **dwukierunkowymi**.

Zaufanie zewnętrzne (external trust) jednokierunkowe lub dwukierunkowe zaufanie umożliwiające dostęp do domeny systemu Windows NT 4 lub do domeny zlokalizowanej w innym lesie.

Zintegrowane strefy usługi Active Directory Strefa systemu DNS (Domain Name System) przechowywana w usłudze Active Directory, dzięki czemu uzyskuje cechy zabezpieczeń usługi Active Directory oraz może być używana w procesach replikacji typu multi-master.

Zmienna środowiskowa (environment variable) Ciąg informacji środowiskowych, takich jak dysk, ścieżka lub nazwa pliku skojarzona z nazwą symboliczną. Opcje modułu System w grupie programów Control Panel (Panel sterowania) oraz komenda wiersza poleceń Set mogą być używane do definiowania zmiennych środowiskowych.

Ż

Żądanie przerwania IRQ (interrupt request) Jeden z zestawów możliwych przerwania urządzeń sprzętu, identyfikowanych według numerów. Numer przerwania IRQ określa, który program obsługi przerwania będzie używany.

Żeton dostępu lub żeton zabezpieczeń dostępu (security access token) Zbiór identyfikatorów zabezpieczeń (SID), które reprezentują użytkownika i członkostwo użytkownika w grupie. Podsystem zabezpieczeń porównuje identyfikatory SID żetonu z identyfikatorami SID na liście kontroli dostępu (ACL) i na tej podstawie określa dostęp do zasobu.

Indeks

64-bitowa wersja systemu Windows Server 2003 19

A

ACL, *zobacz* listy kontroli dostępu
administratorzy
 delegowanie 25, 26
 hasła 30
 instalacja urządzenia 371
 przydział dysku 419
 własność zasobu 199
zarządzanie zdalne 584 adresy protokołu
IP (Internet Protocol)
 dostęp do witryny sieci Web 638, 641
 drukaiki 311
 Ograniczenia rozpoznawania 640, 642
 połączenia serwera terminali (<72
ALKSI (Active Directory Service Interfaces) 106
aktualizacja
 sterowniki 375, 376
 systemy operacyjne 326, 344, 584
 Usługi terminalowe 47 Aktualizacja automatyczna w
systemie Windows 335, 337 aktualizacja dysków 431
aktualizacja oprogramowania systemu Windows XP 601
aktywacja produktu 21, 30, 31, 35
Aleny i dzienniki wydajności 456, 457 konfiguracja
 licznika 456, 457 monitorowanie drukarki 307,
 308, 317, 318
aliasy, usługa WMIO (Windows Management Interface
 Command-line) 472
analizowanie zdarzeń 589
aplikacje
 raport zdarzeń 448
 Serwer terminali 668, 669 atrybut archiwalny 239, 274,
669 atrybuty folderu 582 Automatyczne odzyskiwanie systemu
(ASR) 489, 491, 630,
 633
 ćwiczenia praktyczne 495, 496
 dane o stanie systemu 640
 rozpoczynanie 636, 641
 tworzenie zestawu ASR 489, 491, 495
 używanie funkcji odzyskiwania systemu 491, 496, 630,
 640, 641
zdefiniowany 499 awarie
sieci 48

baza danych certyfikatów 640
baza danych SAM (Security Accounts Manager) 148
bezpośredni dostęp do pamięci (DMA) 368
BIOS (basic input/output system) 397
bufor druku 619, 627, 629, 636

C

CA (urząd certyfikacji) 635, 636, 640
certyfikat cyfrowy 534
CIM (Common Information Model) 470 codzienna
kopia zapasowa 240, 2/4, 669, 670 CRC (cyclical
redundancy check) 336 ćwiczenia praktyczne
 drukarki 286, 290, 302, 303, 312, 313, 585
 folderów udostępnionych 184, 186
 inspekcja dostępu do systemu plików 210, 211, 586
Internetowe usługi informacyjne (IIS) 220, 221 konsola
MMC (Microsoft Management Console) 40,
 41, 43, 44 konsola Wydajność 461, 462 koma grupy
128, 132, 138, 139, 535 konta komputera 154, 156, 160,
161, 167, 168, 535 konta użytkownika 75, 77, 89, 91. 98,
101. 110, III,
 535
licencjonowanie 584
Menedżer zadań 468
monitorowanie wydajności 451, 452, 461, 462, 586
narzędzia administracyjne 40, 41, 49. 50, 57 odzyskiwanie
danych 249, 250, 631 pamięć dyskowa 410, 412, 420,
422, 431. 432, 505,
 506 Podgląd zdarzeń 451, 452 Pomoc zdalna 57
profile użytkownika 98, 101, 534 przywracanie systemu
494, 496, 631 Pulpit zdalny 49, 50, 585 serwery sieci Web
586 sterowniki 372, 373, 379 SUS (Software Update
Services) 585 tworzenie kopii zapasowej 241, 243, 249,
250, 266,
 268, 631 uprawnienia systemu plików
200, 204 urządzenia sprzętu 372, 373, 379

D

dane

- przywracanie 247, 252
- separacja 396
- tworzenie kopii zapasowej 234, 278 dane
- o stanie systemu 486, 489
 - dołączanie danych 486
 - kontrolery domeny 488, 489
 - przywracanie 488, 489, 633, 638, 642, 662
 - tworzenie kopii zapasowej 487, 488, 494, 643, 669
 - zdefiniowany 499

dane o wydajności

- importowanie do programu Excel 461, 462
- monitorowanie 457
- zapisywanie 461 Dcfragmentator dysku 416, 417, 504, 524 delegacja 25, 26

DMA (direct memory access) 368 1)>daj

lub usuń programy 668, 669 Domain Name

Service (DNS) 152,214

zobacz także serwer DNS (Domain Name Service)

domeny

- dołączanie komputerów 151,152,155, 156
- usługa Active Directory 25

domenowe konta komputerów 152

domyślni witryna FTP 217 domyślna

witryna sieci Web 215, 217 Domyślna

zasada domeny 103 dostęp do systemu

plików

- inspekcja 206,212
- rozwiązywanie problemów 583
- uprawnienia 188,205. 562

drukarki 278, 325,615

- ćwiczenia praktyczne 286, 290, 302, 303,312, 313, 585
- dodawanie do puli 297, 298, 302, 303
- informacje dla zdających egzamin 320, 325
- inspekcja 309
- instalowanie 281, 283. 286, 288, 315, 316
- integracja usługi Active Directory 298, 301, 303
- Internet 301, 302
- konfigurowanie 283, 284, 298
- konserwacja 306, 307
- logiczne 280, 281, 285, 298, 303
- lokalne 281. 282
- model systemu Windows Server 2003 280, 281
- monitorowanie 307, 309, 315, 317, 318
- najważniejsze pojęcia 320
- opcje zabezpieczeń 293, 294
- planowanie 296, 297

pobieranie informacji 630, 634, 636

podłączanie klientów 285, 286, 289

podsumowanie 292, 305, 314, 319, 320

przegląd 278

przekierowanie 307, 312, 313, 678, 679

przydział podajnika papieru 295

przydziały dysków 636

publikowanie 299, 300

pytania i odpowiedzi 290, 291, 304, 305, 313, 314, 321,325,616,620 rozwiązywanie problemów 310, 312, 318, 319, 615 sieć 282

sterowniki 282, 306, 307, 318. 319 śledzenie

lokalizacji 300, 301 tryb offline 289, 290

udostępnianie 283, 284, 288. 615, 619

uprawnienia 293, 294,316,317 ustawienia

domyślne 295, 296 właściwości 283, 284.

293, 297

zadanie praktyczne 315, 118

drukarki logiczne 280, 281, 320

zobacz także drukarki

klienci podłączeni do 285, 286

konfigurowanie wielu obiektów 298, 303 drukarki

podłączone lokalnie 280 282 drukarki sieciowe 280,

282, 320 drukarki udostępnione 283, 284, 288, 615,

619 drukarki w trybie online 289, 290 drukowanie

Internet 301, 302

planowanie 296, 297

przekierowanie 307, 312, 313

rozwiązywanie problemów 310, 312, 318, 319

sprawdzanie dokumentów 289, 290

drukowanie w Internecie 301. 302

ustawianie 301

zarządzanie 302

drzewa i lasy 25

dublowanie 426

dublowanie dysków; *zobacz także* woluminy dublowane

Dynamie Host Configuration Protocol (DHCP) 22, 23 dysk

łączony 530 dyski

aktualizacja 431

detragmentacja 416, 417

dynamiczny 397, 400

fizyczny 394

inicjowanie 404

instalowanie 404

optymalizacja wydajności 524

podstawowy 397, 399, 400

przenoszenie pomiędzy serwerami 407, 408
 sprawdzanie 415, 416
 zarządzanie 402, 403, 408, 410
 dyski dynamiczne 396
 konfigurowanie 404, 405
 konwersja dysków podstawowych 408, 411, 508
 porównanie dysków podstawowych 399, 400
 wyjaśnienia 397, 399
 zarządzanie 508 dyski
 fizyczne 394, 504 dyski
 instalowane 257 dyski
 podstawowe 396
 konwersja na dyski dynamiczne 408, 411, 508
 porównanie dysków dynamicznych 399, 400
 wyjaśnienia 397
 zarządzanie 508 dyski rozłożone; *zobacz także*
 woluminy rozłożone dyskietka zerowania hasła 571
 dyskietki, ASR (Automatyczne odzyskiwanie sytemu) 490
 dziedziczenie 192, 195
 ponowna instalacja 194, 195
 wyjaśnienia 192, 193, 229
 zastępowanie 193, 194 dziedziczenie
 przywracania 194, 195 dziennik Aplikacja 448,
 584, 593 dziennik Synchronization 339
 dziennik System 308, 339, 448, 584, 593
 dziennik Usługa katalogowa 448 dziennik
 Zabezpieczenia 448, 584
 eksportowanie 209, 210
 filtrowanie 209, 44°
 inspekcja zdarzeń 108, 108, 210
 konfigurowanie 449, 450, 451
 odczytywanie 452
 ostrzeżenie 450
 pytania i odpowiedzi 591, 592, 594
 sprawdzanie 208, 210, 211
 ustawienia ogólne 449, 450
 dziennik Zatwierdzanie 339
 dzienniki inspekcji 207 dzienniki
 Wutrack.bin 339 dzienniki
 zdarzeń 584, 589

edycja obiektów GPO 540
 edytor listy kontroli dostępu (ACL) 188, 190
 EFI (Extensible Firmware Interface) 404
 eksportowanie
 dziennik Zabezpieczenia 209, 210

wpisy przydziałów 420 emulator PDC (Primate
 Domain Controller) 107 Enterprise Edition of Windows
 Server 2003 19, 34 Extensible Firmware Interface (EFI)
 404 Extensible Markup Language (XML) 53, 217

folder bufora druku 311 folder
 Drukarki i faksy 281, 678 folder
 Moje dokumenty 93 folder Repom
 582 foldery 176, 177
 zobacz także pliki
 atrybuty 582
 bufor druku 31 I
 uprawnienia 195
 współużytkowany 178, 187, 513
 wykonywanie kopii zapasowej 238
 foldery udostępnione 178, 187
 ćwiczenia praktyczne 184, 186
 informacje dla zdających egzamin 228, 233
 konfigurowanie dostępu ilo 562, Si, >. 5(>5
 kopie w tle 262, 265, 267
 najważniejsze pojęcia 229
 podłączenie 185
 podsumowanie 187, 227, 228
 przegląd 178, 179
 pytania i odpowiedzi 186, 187, 230, 509, 510, 513, 566.
 570
 rozwiązywanie problemów 225, 227, 563, 583
 serwery w trybie offline 184, 185, 186
 sesje użytkownika 184
 udziały ukryte 178, 229
 uprawnienia 181, 184, 565
 ustawianie 184, 185
 zadanie praktyczne 223
 zarządzanie 17), 181
 formatowanie woluminu 405
 FQDN (w pełni kwalifikowana nazwa domeny) 331
 funkcja Kopia w tle 262, 265, 274
 konfigurowanie 263, 264
 włączanie 262, 263, 267
 wykorzystywanie 264, 265

G

globalny identyfikator unikatowy GUID (globally unique
 identifier) 559 główna
 tablica pliku (MFT) 416

Główny koncentrator USB 521
 graficzny interfejs użytkownika (GUI) 21, 146
 grupa Administratorzy 670
 grupa Dialup 128
 grupa globalna Employees 587
 grupa Interakcyjni 127, 570
 grupa Logowanie anonimowe 128
 grupa Operatorzy konfiguracji sieci 670
 grupa Operatorzy kopii zapasowych 508, 513, 670
 grupa Replikator 670
 grupa Sieć 127
 grupa Użytkownicy pulpitu zdalnego 571, 575
 grupa Użytkownicy uwierzytelnieni 128, 569
 grupa Użytkownicy zaawansowani 670
 grupa Ws/.yscy 127, 569
 grupy 124
 drukarka 316
 dystrybucji 124, 142
 globalne 126, 142, 552, 553
 licencji 355, 362, 609
 •lokalna 125
 lokalne w domenie 125
 specjalna 127, 128
 tworzenie 130, 131
 uniwersalne 126, 142, 552, 553
 zabezpieczeń 124, 130, 131, 142
 zagnieżdżone 132, 552

H

harmonogram
 synchronizacja usługi SUS (Software Update Services)
 333, 334
 zadania drukowania 296, 297
 zadania kopii zapasowej 261, 262, 266, 271, 631, 665, 670
 hasła
 administrator 30
 opcje szyfrowania odwracalnego 74
 przypisywanie 70, 71
 rozwiązywanie problemów 568
 synchronizowane 559
 zagadnienia dotyczące różnych platform 106, 107
 zasady 104, 105, 572
 zerowanie 26, 109, 547, 571
 złożone 70 HTTP (Hypertext Transfer Protocol) 301

identyfikatory (ID) zdarzenia 594
 identyfikatory względne (RID) 559
 rola wzorca identyfikatora RID 563
 identyfikatory zabezpieczeń SID 188
 konta komputera 148, 163, 559
 konta użytkownika 68
 importowanie
 obiekty użytkowników 81, 82, 90, 91
 rejestrwanie danych o wydajności 461, 462
 informacje dla zdających egzamin
 zobacz także pytania i odpowiedzi
 diukarki 320, 325
 foldery udostępnione 228, 233
 konta grupy 142, 144
 konta komputera 172, 176
 konta użytkownika 118, 122
 monitorowanie wydajności 4/8, 481
 narzędzia administracyjne 60, 63
 pamięć dyskowa 439, 445
 przywracanie systemu 498, 501
 sterowniki 386, 389
 tworzenie kopii **zapasowej danych** 274, 278
 urządzenia sprzętu 386, 389 informacje o wykorzystaniu
 procesora. Czas procesora 629 inicjowanie dysków 404
 Inspekcja 206, 621
 analizowanie dziennika Zabezpieczenia 2(18, 10, 211
 ćwiczenia praktyczne 210, 211, 586
 dostęp do systemu plików 206, 212
 drukarki 309
 generowanie zdarzeń inspekcji 210
 konfigurowanie 206, 207, 210, 451, 452, 622, 625
 podsumowanie 212, 228
 pytania i odpowiedzi 211, 212, 231, 232, 622, 625
 uwierzytelnienie 107, 108
 włączanie 208, 210
 zasady 107, 108, 208, 210, 229 inspekcja zdarzeń
 zakończonych powodzeniem 207 instalowanie
 Aktualizacje automatyczne 336, 337
 drukarki 281, 283, 286, 288, 315, 316
 dysków 404
 Internetowe usługi informacyjne 213, 220
 Konsola odzyskiwania 492
 Serwer terminali 668, 670
 sterowników 368, 374, 377, 378
 urządzeń sprzętowych 368, 374, 376, 387, 534

usługi SUS (Software Update Services) 327, 329, 358, 359
 Windows Server 2003 21, 22, 27, 31 instalowanie
 pakietów serwisowych 346, 358 interfejs użytkownika
 (UI) 459 Interfejsy usługi Active Directory (ADS1) 106
 Internet Printing Protocol (IPP) 301 Internet Server
 Application Programming Interface
 (ISAPI) 329 Internetowe usługi informacyjne
 (IIS) 213, 222, 637
 administracja środowiska sieci Web 213, 214
 ćwiczenia praktyczne 220, 221
 drukowanie w Internecie 301
 instalowanie 213, 220
 konfiguracja usługi FTP (File Transfer Protocol) 217
 konfiguracja witryny sieci Web 215, 217, 220
 konfigurowanie dostępu do 637, 638, 641
 konsola Menedżer 213, 214
 Kreator blokowania 329
 metabaza 217, 341, 640, 662
 opcja Konfigurowanie kopii zapasowych i przywracania
 217, 644, 646
 opcje uwierzytelnienia 218
 podsumowanie 222, 228
 ponowne uruchamianie 340
 pytania i odpowiedzi 221, 222, 232, 233, 638, 642
 rozwiązywanie problemów ograniczeń adresacji
 protokołu IP 640, 642
 uprawnienia 219, 220
 usługa SUS (Software Update Services) 327
 zabezpieczanie plików 218, 220, 221 IPP (Internet
 Printing Protocol) 301 IRQ (żądanie przerwania) 368,
 541, 542 ISAPI (Internet Server Application
 Programming Interface) 329

J

jednostki organizacyjne (OU) 25, 153, 154, 540, 587, 673

K

karta sieciowa (NIC) 459
 karty inteligentne 74
 karty sieciowe 372, 628, 629
 katalog macierzysty 558, 567
 katalog macierzysty, Usługi terminalowe 669, 670
 Katalog sesji usług terminalowych 681
 katalog wirtualny sieci Web 217

katalogi wirtualne 217, 221, 229
 klastry 416
 Serwer terminali 680, 681
 klastry serwerów 680, 681
 klienci
 Aktualizacje automatyczne 335, 337
 podłączanie drukarek 285, 286, 289
 Pulpit zdalny 47, 48, 670
 Serwer terminali 671, 676
 klienci druku 285, 286
 klienci ICA (Integrated Computing Architecture) 677 klient
 usługi Active Directory 106, 107 klient usługi Aktualizacje
 automatyczne 327, 335, 337
 działanie podczas pobierania 336
 konfigurowanie za pomocą obiektów GPO 337, 338,
 360, 361
 opcje instalacyjne 336, 337
 zadanie praktyczne 360, 361 kod KIM
 (ielcasc-to-maiufacture) 357 kody statusów.
 Menedżer urządzeń 382, 383 kolejki druku 281,
 615, 620, 630 komputery
 dołączanie do domeny 151, 152, 155, 156
 powrót do konfiguracji domyślnej 373
 przypisywanie nazw 29, 30
 wyszukiwanie i podłączanie 159, 160
 komputery Itanium 19. 404 komputery
 systemu Windows 98 567 komunikaty o
 błędach
zobacz takie rozwiązywanie problemów
 konta komputera 165, 166
 Menedżci urządzeń 382, 383
 Serwer terminali 676 konfiguracja
 niestandardowa 22 konfiguracja zasobu 3/8
 konfiguracje macierzy RAID 424, 434, 648
 aktualizacja dysków 431
 ćwiczenia praktyczne 431, 432, 505
 oprogramowanie 395, 396, 415
 optymalizacja wydajności 524
 planowanie 431, 432
 porównanie 429, 430
 przywracanie serwera 648
 pytania i odpowiedzi 512, 514, 649, 652
 rozwiązywanie problemów 436, 438
 sprzęt 396, 424, 425, 430, 435, 436, 508
 woluminy dublowane 426, 428
 woluminy RAID-0 425, 426
 woluminy RAID-1 426, 428
 woluminy RAID-5 428, 430
 woluminy rozłożone 425, 426

- woluminy rozłożone z parzystością 428, 430
- konfigurowanie
 - Aktualizacje automatyczne 337, 338, 360, 361
 - dtukarki 283, 284, 298
 - dzienniki programu Podgląd zdarzeń 449, 450, 451, 452
 - Inspekcja 206, 207, 210, 451, 452, 622, 625
 - Kopia w tle 263, 264
 - obiekty użytkownika 72, 75, 76
 - pamięć dyskowa 403, 406, 410, 412
 - przydziały 418, 420
 - Pulpit zdalny 45, 46
 - Serwer terminali 668, 670, 673, 674, 676
 - sterowniki 375, 380
 - uprawnienia 188, 192, 200, 202, 563
 - uprawnienia systemu plików 188, 192, 200, 202, 563, 577
 - uprawnienia udziału 181, 182, 565
 - urządzenia sprzętu 375, 380, 534
 - usługa SUS (Software Update Service) 330, 331, 601
 - Windows Server 2003 22, 24, 31, 33
 - witryna usługi FTP (File Transfer Protocol) 217
 - witryny sieci Web 215, 217
- konserwacja
 - di ukarki 306, 307
 - systemy operacyjne 324, 365
 - woluminy pamięci dyskowej 415, 423 konsola MMC;
- zobacz także* Microsoft Management Console (MMC) Konsola
- odzyskiwania 382, 492, 494
 - ćwiczenie praktyczne 495, 496
 - instalowanie 492, 495
 - polecenia 493
 - ponowne przenoszenie 492
 - wykorzystanie 493, 494, 495, 496
 - zagadnienia zabezpieczeń 494
 - zdefiniowany 499 konsola Wpisy
- przydziału 635 konsola Wydajność 454, 463, 626
 - Alerty i dzienniki wydajności 456, 457
 - ćwiczenia praktyczne 461, 462
 - informacje o drukarce 630, 634, 636
 - liczniki dysku 460
 - liczniki pamięci 459
 - liczniki procesu 460
 - liczniki sieci 459
 - Monitor systemu 454, 456
 - monitorowanie danych wydajności 457
 - monitorowanie roli serwera 458
 - podsumowanie 463
 - pytania i odpowiedzi 462, 480, 627, 629
- Konsola zarządzania (MMC); *zobacz także* Microsoft Management Console
- konsola Zarządzanie komputerem 42, 43, 584
 - przystawka Zarządzanie dyskiem 402, 403
 - wykorzystywanie zarządzania zdalnego 610, 614
- konsola Zarządzanie serwerem plików 185
- konta grupy 122, 144
 - ćwiczenia praktyczne 128, 132, 138, 139, 535
 - Grupy zabezpieczeń 130, 131 informacje dla zdających egzamin 142, 144 konwersja 126, 127, 553
 - lektura uzupełniająca 537
 - modyfikowanie 131, 137
 - najważniejsze pojęcia 142
 - podsumowanie 129, 133, 140, 141, 142
 - polecenia LDIFDE (LDAP Data Interchange Format Directory Export) 134, 135, 138, 139
 - polecenie DSADD 136, 137 przegląd 122
 - przetwarzanie wsadowe 134, 135 pytania i odpowiedzi 129, 133, 139, 140, 143, 144, 550, 553
 - rodzaje 124, 142
- rozwiązywanie problemów 141, 225, 227
- Tożsamości specjalne 127, 128 tworzenie 136, 137, 139, 549 uprawnienia 586 zadanie praktyczne 140
- zagnieżdżanie 132, 552 zakres 125, 127, 142
- zarządzanie 130, 140, 549 konta komputerów 146, 176, 544
 - ćwiczenia praktyczne 154, 156, 160, 161, 167, 168, 535
 - dołączanie do domeny 151, 152, 155, 156 identyfikatory zabezpieczeń 148, 163, 559
 - informacje dla zdających egzamin 172, 176
 - lektura uzupełniająca 536, 537 podsumowanie 157, 162, 169, 172, 173 polecenie DSADD 149, 150 polecenie DSMOD 159, 165, 548 polecenie NETDOM 150, 152, 165, 547 problemy 165, 167 przegląd 146
 - przenoszenie 153, 154, 155 pytania i odpowiedzi 156, 157, 161, 162, 168, 169, 174, 176, 545, 563 rozwiązywanie problemów 163, 169, 170, 172, 535, 559
 - tworzenie 148, 152, 154, 544
 - tworzenie za pomocą skryptów 170

- uprawnienia 158 usuwanie 163. 164
- właściwości 159, 161 włączanie 164, 165
- wyłączanie 164, 165 wyszukiwanie i
- podłączanie 159, 160 zadanie praktyczne
- 169, 170 zarządzanie 158, 162, 544
- zdefiniowany 173
- zerowanie 165, 171, 172, 547, 586, 587
- konta użytkowników 66, 122
 - ćwiczenia praktyczne 75, 77, 89, 91, 98, 101, 1 10, 111, 535
 - hasła 70, 71, 74, 109
 - importowanie 81, 82
 - informacje dla zdających egzamin 118, 122
 - lektura uzupełniająca 536, 537
 - modyfikacja wielu **obiektów 74, 75, 77**
 - najważniejsze pojęcia 118
 - odblokowanie 109
 - podsumowanie 79, 92, 102, 112, 117, 1 18
 - profile użytkownika 93, 102
 - przegląd 66
 - przenoszenie użytkowników 75
 - pytania i odpowiedzi 78, 79, 91, 92, 101, 102, 1 12, 117, 119. 567
 - rozwiązywanie** problemów 115, 116, 536, 564
 - szablony 80. 81, 89, 90, 118
 - tworzenie 68, 71, 75, 76, 554
 - uprawnienia ↗86
 - ustawienia własności 69, 71, 72, 75, 76
 - usuwanie 109
 - uwierzytelnienie 103, 1 12, 536
 - właściwości konra 73, 74
 - włączanie 109
 - wyłączanie 71, 109
 - zadanie praktyczne 113, 115
 - zarządzanie 72, 75, 554
 - zmiana nazwy 109 konta zablokowane 1 18 kontener
- Komputery 153 konto Twórca/właściciel 128, 198, 199, 229, 569 konto wyłączone 118, 164 kontroler macierzy
- RAJD 537, 541 kontrolery domeny 23
 - dzienniki programu Podgląd zdarzeń 453
 - odtworzenie danych o stanie systemu 488, 489 kontrolery
- SCSI (Small Computer Systems Interface) 435 konwersja
- konta grupy 126, 127
- pamięci dyskowej 408, 411
- konwersja grupy 126, 127 Kopia zapasowa 236, 238 dane o
- stanie systemu 487 odtwarzanie plików 247, 248, 645, 647
- opcje dziennika Kopia zapasowa 257 opcje Ogólne 256, 257
- opcje wykluczania plików 258 pula nośników 254, 255
- tworzenie kopii -zapasowej plików 238 tworzenie zestawu
- ASR (Automatyczne odzyskiwanie
- systemu) 489, 491 uruchamianie i używanie 236, 237
- wyświetlanie wykazu 255, 256 kopia zapasowa danych 234, 278, 643 *zobacz także* odtwarzanie danych ćwiczenia
- praktyczne 241, 243. 249, 250, 266, 268, 631 dane o stanie .systemu 486, 488, 494, 643
- harmonogram zadań kopii zapasowych 261, 262, 266, 271, 631, 665, 670
- informacje dla zdających egzamin 2/4, 278
- konfiguracja IIS 217
- kopia w tle 262, 265, 267
- miejsce docelowe 238
- najważniejsze pojęcia 274
- odtworzenie danych na podstawie kopii zapasowej 247, 252, 631, 645, 647. 653. 664 opcje 256, 258 podstawy 236, 246
- podsumowanie 245, 246, 252, 269, 273, 274 polecenie
- Mcbakup 258, 261 procedura VSS 251 procedury
- zaawansowane 253, 269 programy narzędziowe systemu
- Windows 236, 238 przegląd 234 pytania i odpowiedzi 244, 245, 251, 268, 269, 275, 278, 644, 647, 670 rejestrowanie danych kopii
- zapasowej 257 rodzaje kopii zapasowych 239, 241, 274
- rozwiązywanie problemów 272, 273 serwer usługi SUS
- (Software Update Services) 341, 342 tworzenie zestawów
- ASR (Automatyczne odzyskiwanie
- systemu) 489. 491 urządzenia sprzętu 644, 646 weryfikacja 643, 644, 646 wybór plików i
- folderów 238 wykluczanie plików 258 zadanie
- praktyczne 270, 271 zagadnienia zabezpieczeń 253, 254, 261 zarządzanie nośnikami 254, 256, 643 kopie zapasowe 240, 274, 670

kopie zapasowe otwartych plików 253
 Kreator dodawania drukarki 281, 283, 285
 Kreator dodawania lub usuwania składników systemu
 Windows 668 Kreator inicjowania i konwersji dysków
 508, 515 Kreator instalacji usługi Active Directory 31
 Kreator konfigurowania serwera 22, 24, 31, 32, 668 Kreator
 kopii zapasowej 237 Kreator nowego woluminu 404, 405
 Kreator przygotowania automatycznego odzyskiwania
 systemu 489, 490
 Kreator przywracania 237

L

lasy i drzewa 25
 LDAP (Lightweight Directory Access Protocol) 24
 licencje 348, 356, 584, 604
 administrowanie 353, 354
 ćwiczenia praktyczne 585
 na serwer 349, 350, 607
 na urządzenie lub na użytkownika 349, 350, 607, 608
 najważniejsze pojęcia 362
 n.iizcdzieTryb licencjonowania 351
 podsumowanie 356, 361, 362
 poegląd 348, 604
 pytania i odpowiedzi 355, 356, 364, 365, 605, 609
 serwer licencji lokacji 352
 Serwer terminali 670, 671
 symbole statusu 354
 tworzenie grup licencji 355
 usługa Rejestrowanie licencji 351 licencje CAL (Client
 Access License) 348, 349, 362, 604, 607, 609
 rodzaje 349, 605, 607
 Serwer terminali 604, 609, 671
 urządzeń 349, 607
 użytkownika 349, 607
 uzyskiwanie 348
 licencje lokacji
 zobacz także licencje
 administrowanie 353, 354
 identyfikacja 352
 licencjonowanie
 w trybie Na serwer 349, 350, 362, 604, 607
 w trybie Na urządzenie 349, 350, 352, 604
 w trybie Na użytkownika 349, 350, 352, 604, 608 liczniki
 wydajności
 Błędy zadania 308
 dysku 460

Monitor systemu 455, 456
 monitorowanie drukarki 307, 308, 317, 318
 monitorowanie roli serwera 458
 pamięci 459
 procesu 460
 sieci 459
 Wszystkie wydrukowane strony 308, 317
 Wszystkie wydrukowane zadania 308
 Wydrukowane bajty/s 308
 Zadania 308 Lightweight Directory Access Protocol
 (LDAP) 24 linie ISDN BRI 597, 598, 599, 601, 602 lista
 kontroli dostępu (ACL) 26, 188, 577
 dla drukarek 294
 dla grup 124
 dla użytkowników 68 lista
 witryn zaufanych 329
 litery dysku, przypisywanie do woluminów 405, 406, 412
 logowanie za pomocą konta Gość 543 lokalne grupy domeny
 125, 142, 552, 553 lokalne obiekty zasady grupy GPO (Group
 Policy Objęci)
 540 lokalne profile użytkowników 94, 538,
 543 luźna topologia nadrzędny/podrzędny 332

M

magazyn
 zobacz także pamięć dyskowa
 dostępne opcje 394, 401
 system wymienny 236, 254 mapowanie
 portu COM 679 mapowanie portu LPT 67"
 mapowanie schowka 679 Menedżer urządzeń
 369, 371, 375, 380
 zobacz także urządzenia sprzętu
 aktualizowanie sterowników 375, 376
 ćwiczenie praktyczne 379
 ikona ostrzeżenia 368, 369
 kody statusów 382, 383
 konfigurowanie zasobu 378
 odinstalowywanie sterowników 377, 378
 podsumowanie 380
 przywracanie poprzedniej wersji sterownika 376, 377
 pytania i odpowiedzi 379, 380, 388, 389
 uzyskiwanie dostępu 369
 zadania 369, 370
 zarządzanie urządzeniami sprzętu 504, 516
 Menedżer usług terminalowych 576, 673, 680
 Menedżer zadań 464, 469

podsumowanie 469
 przegląd 464
 pytania i odpowiedzi 468, 480, 481
 zadanie praktyczne 468
 zakładka Aplikacje 464
 zakładka Procesy 465, 466
 zakładka Sieć 466, 467
 zakładka Użytkownicy 467
 zakładka Wydajność 466
 zdefiniowany 478 menu, konsola
 MMC 37, 38 metabaza 217, 341, 640,
 662, 669 MFT (master file table) 416
 Microsoft Active Directory, *zobacz* usługa Active Directory
 Microsoft Excel
 imponowanie danych o wydajności 461, 462
 odczyt dziennika zabezpieczeń 210 Microsoft
 Index Server 324 Microsoft Management Console
 (MMC) 36, 44
 dostosowywanie 38, 39
 menu i polecenia 37, 38
 nawigacja 36, 37 opcje
 konsoli 39, 40
 podsumowanie 41, 44
 przegląd 34, 36
 przystawki 38, 39
 pytania i odpowiedzi 41, 44, 62
 tryb autorski 39
 tryby użytkownika 39, 40
 zadania praktyczne 40, 41, 43, 44
 zarządzanie zdalne 42, 43
 zdefiniowany 61 Microsoft SQL Server Database
 Engine (MSI) 18 mobilne profile użytkownika (RUP)
 94, 95, 538
 grupa 97
 pytania i odpowiedzi 539, 542, 543
 synchronizacja 95
 wstępnie skonfigurowane 97
 model domeny 24 model grupy
 roboczej 24 Monitor systemu 454,
 456, 478
 konfigurowanie 454, 456
 monitorowanie drukarki 307, 308
 przeglądanie danych 455, 456 monitorowanie
 roli serwera 458 monitorowanie wydajności 446,
 481, 626
 ćwiczenia praktyczne 451, 452, 461, 462, 586
 drukarki 307, 309, 315, 317, 318, 630
 informacje dla zdających egzamin 478, 481
 kategorie obiektów 459, 460
 konsola Wydajność 454, 463

lektura uzupełniająca 506
 liczniki 455, 456, 458, 460
 Menedżer zadań 464, 469
 najważniejsze pojęcia 478
 Podgląd zdarzeń 448, 453
 podsumowanie 453, 463, 477, 478
 program narzędziowy Windows Management
 Instrumentation (WMI) 470, 475 przegląd 446, 626
 przydziały dysków 420, 630 pytania i odpowiedzi 452,
 453, 462, 479, 481, 627,
 629 role serwerów 458 rozwiązywanie
 problemów 476, 477 serwery plików 630
 Software Update Services (SUS) 339
 urządzenia sprzętu 516 wzorzec odniesienia
 457 zadania praktyczne 475, 476
 monitorowanie zdarzeń 621

N

narzędzia administracyjne 34, 63
 ćwiczenia praktyczne 40, 41, 49, 50, 57
 informacje dla zdających egzamin 60, 63
 konsola MMC (Microsoft Management Console) 36, 44
 Licencjonowanie serwera terminali 670
 najważniejsze pojęcia 61
 podsumowanie 41, 51, 58, 60, 61
 Pomoc zdalna 52, 58
 przegląd 34
 Pulpit zdalny dla administracji 45, 51
 pytania i odpowiedzi 41, 51, 57, 58, 62, 63
 rozwiązywanie problemów 59
 zadanie praktyczne 58, 59 Narzędzia HTML
 administracji zdalnej 584, 585, 610,
 613, 614 narzędzia
 odzyskiwania
 przywracanie sterownika 381, 382
 przywracanie systemu 492, 494
 narzędzia usługi katalogowej 554
 narzędzia wiersza poleceń
 zobacz także polecenia specyficzne
 LDIFDE (LDAP Data Interchange Format Directory
 Exponent) 134, 135, 138, 139
 usługa Active Directory 82, 88, 91
 zarządzanie dyskiem 408, 410 narzędzie administracji —
 Licencjonowanie 353, 354

narzędzie REDIRCOMP 153
 narzędzie Uprawnienia czynne 197
 NAT (Network Address Translation) 56
 nazwa domeny NetBIOS 152
 nazwa drukarki 282, 283
 nazwa główna użytkownika (UPN) 69, 107
 nazwa logowania użytkownika 70
 nazwy
 komputer 29, 30
 udział 282, 283
 wyróżniająca 82, 83 Network Address Translation (NAT) 56 NIC (karta sieciowa) 459 nierozpoznany nośnik 254 nieudany dostęp do plików, inspekcja 207 NLB (Network Load Balancing) 18, 681 NT LAN Manager (NTLM) 106

O

obiekty GPO (Group Policy Object) 26
 edycja 540
 lokalny 540
 stosowanie 542, 603
 zasada inspekcji 208
 zewnętrzny 540 obiekty GPO; *zobacz, także*
 obiekty zasady grupy obiekty komputerów
 dołączanie do domeny 151, 152, 155, 156
 przenoszenie 153, 154, 155
 tworzenie 149, 150, 153
 uprawnienia 158
 usuwanie 163, 164
 właściwości 159, 161
 wyszukiwanie i podłączanie 159, 160
 zmiana nazwy 154
 obiekty użytkownika
 importowanie 81, 82, 90, 91
 konfigurowanie 72, 75, 76
 modyfikowanie wielu obiektów 74, 75, 77
 przenoszenie 75
 szablony 80, 81, 89, 90
 tworzenie 68, 71, 75, 76, 80
 usuwanie 109
 właściwości 69, 71, 72, 75, 76
 właściwości użytkownika 69, 70
 włączanie/wyłączanie 109
 zarządzanie 72, 75, 82, 88
 zmiana nazwy 109 obiekty,
 usługa Active Directory 25

zobacz także specyficzne typy obiektów
 odblokowanie kont użytkowników 109 odporność na uszkodzenia 395, 396, 424, 648
 opcje sprawdzania 434, 436
 programowa macierz RAID 425
 przywracanie systemu serwera 649, 650, 651
 pytania i odpowiedzi 649, 652
 sprzętowa macierz RAID 424, 425
 wolumin systemowy 430 odtwarzanie danych; *zobacz*
 przywracanie danych,
 przywracanie systemu okno dialogowe Harmonogram zadania 261, 262 okno dialogowe Logowanie zakończone niepowodzeniem
 571 okno dialogowe Nowy obiekt -
 Komputer 149 okno dialogowe Nowy obiekt -
 Użytkownik
 przedstawiony 69, 70
 właściwości użytkownika 69, 70, 71
 okno dialogowe Właściwości
 drukarki 283, 284
 konta grupy 131
 obiekty użytkownika 72, 75 okno dialogowe Właściwości dokumentów 188, 189 okno dialogowe Właściwości domyślnej witryny sieci Web
 zakładka Dokumenty 216
 Zakładka Katalog macierzysty 215, 216
 zakładka Witryna sieci Web 215 okno dialogowe Właściwości RDP-Tcp 674, 675, 677.
 680, 683 okno dialogowe Właściwości serwera druku
 309 okno dialogowe Właściwości systemu 335 okno dialogowe Właściwości **urządzenia** 541 okno dialogowe Wpis inspekcji 206, 207 okno dialogowe Wpisy uprawnień dla dokumentów 190,
 191 okno dialogowe Wyszukiwanie drukarek 285, 286 okno dialogowe Wyszukiwanie komputerów 159, 160 okno dialogowe Zaawansowane ustawienia zabezpieczeń 193, 194, 195
 zakładka Inspekcja 206
 zakładka Uprawnienia 201
 zakładka Uprawnienia czynne 196, 197
 zakładka Właściciel 199 okno dialogowe Zaawansowane ustawienia zabezpieczeń
 dla dokumentów 189, 190 okno dialogowe Zmiana nazwy komputera 151, 152 opcja Blokuj 534 opcja Ignoruj 534
 opcja Ostatnia znana dobra konfiguracja 381, 385, 386,
 387 opcja
 Ostrzegaj 534

opcja Pełna ochrona 669
 opcja Pokaż urządzenia ukryte 521
 opcja Zabezpieczenia uproszczone 669
 opcje modemu 542
 opcje modułu Pomoc; Konsola odzyskiwania 493
 opcje przekierowania
 urządzenia sprzętu 677, 679
 zadania druku 307, 312, 313, 678, 679 Opcje
 telefonu i modemu 542 operacje „przeciągnij-i-
 upuść” 75 oprogramowanie
 aktualizacja 326, 344, 584
 drukarka 282
 licencje 348, 356
 Pakiety serwisowe 345, 347
 podatność 324
optymalizacja logowania 346
optymalizacja wydajności dysku 524, 533
 ćwiczenia praktyczne 505
 przegląd 524
 pytania i odpowiedzi 525, 533

P

Pakiety serwisowe 345, 347, 595
 instalowanie zasady grupy 346, 358
 pobieranie i uzyskiwanie 345, 346, 357
 podsumowanie 347, 361
 pytania i odpowiedzi 347, 364
 zadania praktyczne 357, 358
 pamięć dyskowa 392, 445
 aktualizacja dysków 431
 ćwiczenia praktyczne 410, 412, 420, 422, 431, 432, " 505, 506
 dynamiczny 397, 400
 dyski fizyczne 394
 informacje dla zdających egzamin 439, 445
 konfiguracje macierzy RAID 424, 434
 konfigurowanie 403, 406, 410, **412**
 konserwacja woluminów 41 5, 423
 konwersja 408, 41 1
 lektura uzupełniająca 506, 507
 monitorowanie 420
 najważniejsze pojęcia 440
 narzędzia wiersza poleceń 408, 410
 odporność na uszkodzenia 395, 396, 424, 425
 opcje 394, 401
 podstawowy 397, 399, 400
 podsumowanie 401, 414, 423, 434, 439, 440
 przegląd 392

przenoszenie dysków fizycznych 407, 408
 przydziały 418, 422
 pytania i odpowiedzi 400, 401, 413, 422, 423, 432, 434, 441, 445, 515 rozwiązywanie
 problemów 436, 439 separacja danych 396
 usługa RSM (Removable Storage Manager) 236, 254
 woluminy instalowane 395 woluminy logiczne 394, 395
 woluminy rozszerzone 406, 407, 412 zadania praktyczne 434, 436 zarządzanie 402, 403, 408, 410 pamięć podręczna 340
 pamięć, monitorowanie 459 Panel sterowania
 konfiguracja urządzenia 379 narzędzie Wybór trybu
 licencjonowania 351 partycja **podstawowa** 397, 404
 partycja rozruchowa 397 partycja rozszerzona 397, 407
 partycja systemowa 397 partycje
 podstawowa 397, 404
 rozszerzona 397, 407 tworzenie
 404, 410 parzystość 428
 generowanie informacji 530 woluminy
 rozłożone 428, 430, 524 pasmo 638, 639, 641
 pełna kopia zapasowa 669 plikBOOT.INI
 4.',<>
 plik o wartościach rozdzielanych przecinkami (CSV) 370 pliki
 Update.log w systemie Windows 339 pliki 174 177
 zob. także foldery
 fragmentacja 4 i 6
 nieprzenośne 532 sieci
 267
 stronicowania 532
 zaszyfrowane 74, 514, 675
 zestaw ASR (Automatyczne odzyskiwanie systemu) 491
 wykonywanie kopii zapasowej 238, 258 pobieranie
 Aktualizacje automatyczne 336
 Pakiety serwisowe 345, 357 podajnik
 papieru 295 Podgląd zdarzeń 39, 448,
 453 ćwiczenia praktyczne 451, 452
 dziennik Aplikacja 448 dziennik
 Serwer DNS 449 dziennik System 308,
 448

- dziennik Usługa katalogowa 448
- dziennik Usługi replikacji plików 449
- dziennik Zabezpieczenia 108, 208, 210, 448
- konfigurowanie dzienników 449, 450
- opis dzienników 448, 449
- pobieranie danych przez usługę Windows Management Instrumentation (WMI) 474
- podsumowanie 453
- pytania i odpowiedzi 452, 453, 479, 590, 594
- podpisy cyfrowe 371, 372 podstawowe
- uwierzytelnienie FTP 218 41, 51, 58, 60, 61
- podsumowanie
 - drukarki 292, 305, 314, 319, 320
 - foldery udostępnione 187, 227, 228
 - inspekcja dostępu do systemu plików 212, 228
 - Internetowe usługi informacyjne 222, 228
 - konsola MMC (Microsoft Management Console) 41, 44
 - konsola wydajność 463
 - konta grupy 129, 133, 140, 141, 142
 - konta komputera 157, 162, 169, 172, 173
 - konta użytkownika 79, 92, 102, 112, 117, 118
 - Ikencje oprogramowania 356, 361, 362
 - Menedżer zadań -169
 - monitorowanie 453, 463, 477, 478
 - odzyskiwanie danych 252, 269, 273, 274
 - Pakiety serwisowe 347, 361
 - pamięć dyskowa 401, 414, 423, 434, 439, 44()
 - Podgląd zdarzeń 453
 - Pomoc zdalna 58
 - program narzędziowy Windows Management Instrumentation (WMI) 475
 - przywracanie systemu 498, 499
 - Pulpit zdalny 51
 - sterowniki 374, 380, 384, 386, 387
 - tworzenie kopii zapasowej danych 245, 246, 252, 269 273, 274
 - uprawnienia systemu plików 205, 227, 228
 - urządzenia sprzętu 374, 380, 384, 386, 387
 - usługa SUS (Software Update Services) 344, 361, 362
 - wersje systemu Windows Server 2003 20
- pofragmentowane pliki 416, 417, 504, 524
- polecenie Bootcfg 493 polecenie Catalog A
- Backup File 647 polecenie Change User/Execute 669 polecenie Change User/Install 669 polecenie Chkdsk 408, 533 polecenie Convert 408
- polecenie CSVDE 81, 82, 90, 91, 557 polecenie DERM
 - konta komputera 163, 164, 548
 - konta użytkownika 82, 88
- polecenie DIABLE 493
- polecenie DISKPART 407, 409, 410, 411, 493
- polecenie DRIVERQUERY 370, 371 polecenie DSADD 82, 548, 557
 - konta grupy 136, 137
 - konta komputera 149, 150, 154
 - konta użytkownika 85, 87
- polecenie DSGET 82, 548
 - konta grupy 141
 - konta użytkownika 87, 88
- polecenie DSMOD 82, 548, 557
 - konta grupy 137
 - konta komputera 159, 165
 - konta użytkownika 87
- polecenie DSMOVE 82
 - konta komputera 154
 - konta użytkownika 88 polecenie
- DSQUERY 82, 83, 85, 548, 557
 - parametry 84, 85 polecenie Enable
- 493 polecenie Fsutil 409 polecenie JON, NE IDOM 152 polec c-nie- I r.iw. i¹) 1 polecenie Mounlvol 409
- polecenie Moverrec 547 polecenie Ner Start Spooler 311 polecenie NETDOM
 - konta komputerów 150, 152, 165, 547
 - polecenie JON 152 polecenie
- Ntbackup 236, 258, 261
 - zobacz także* Kopia zapasowa
 - ćwiczenie praktyczne 266
 - dane o stanie systemu 48/
 - przegląd 258, 259
 - składnia 258
 - używane przełączniki 259, 261, 487
- polecenie Ntdsutil 489, 557 polecenie Relresh 155
- połączenia bloku SMB (srvcr message block) 18
- połączenia jednoczesne 29 Połączenie pulpitu
- zdalnego 46, 47
 - aktualizacja 47
 - instalacja 670
 - konfiguracja 47, 48, 671
 - ustawienia klienta 47, 48, 671
 - ustawienia serwera 48 Pomoc i obsługa
- techniczna 52, 55, 681 Pomoc zdalna 52, 58, 584, 610
- ćwiczenia praktyczne 57

- inicjowanie 55
- oferowanie użytkownikom 54, 612, 614
- ograniczenia zapory ogniowej 56
- podsumowanie 58 przegląd 34, 52
- pytania i odpowiedzi 57, 58, 63, 613
- rozwiązywanie problemów 573, 575, 576
- zadanie praktyczne 58, 59 zagadnienia
- zabezpieczeń 53, 54, 55 zdefiniowany 61
- żądanie pomocy 52, 54 ponowne przenoszenie
- zobacz także* usuwanie Konsola odzyskiwania
- 492 uprawnienia 191
- port drukarki 282
- poziomy **funkcjonalności** domeny 124
- prawa logowania 676
- prawa użytkownika 571
- prawo Przywracanie plików i katalogów 199
- problemy i rozwiązania, *zobacz także* rozwiązywanie
 - problemów proces aktywacji 21, 30, 31
- proces defragmentacji 416, 417, 504, 524
 - poziomy progów 533
 - uruchamianie zdalne 613
- proces uwierzytelnienia 188
- profile
 - sprzęt 384, 385
 - użytkownik 93, 102
- profile grupy 97, 100, 101
- profile obowiązkowe 97, 98, 100, 101, 118, 538, 542
- profile sprzętowe 384, 385 profile użytkownika 93, 102, 538
 - ćwiczenia praktyczne 98, 101, 534
 - grupa 97, 100, 101
 - lokalna 94
 - mobilny 94, 95
 - obowiązkowy 97, 98, 100, 101, 118
 - podsumowanie 102
 - pytania i odpowiedzi 101, 102, 121, 122, 539, 543
 - synchronizacja 95
 - szablony 99
 - uprawnienia udziału 98, 99
 - wstępnie skonfigurowany 96, 97, 99, 101
 - wyjaśnienia 93, 94
 - zarządzanie 98, 101, 538 program CHKDSK 415, 416 program Choosc Licensing Modę 351
 - program Client for Microsoft Networks 178
 - program Excel
 - importowanie danych o wydajności 461, 462
 - odczytywanie dziennika zabezpieczeń 210 Program IIS; *zobacz* Internetowe usługi informacyjne program narzędziowy Check Disk 415, 416 program narzędziowy LDIFDE (LDAP Data Interchange Format Directory Export) 134, 135, 138, 139, 557 program narzędziowy Opcje zasilania 521 program narzędziowy WINMSD 516, 522 program wiersza poleceń DEFRAG 524 programowa macierz RAID 395, 396, 425
 - protokołowanie
 - aplikacja 448
 - kopia zapasowa 257
 - licencja 351, 353
 - system 448
 - zabezpieczenia 448 protokół Post Office Protocol
 - wersja 3 (POP3) 18 prywatne sieci wirtualne (VPN) 23
 - pi/<l>ierowanie dysku 677 przekierowanie dźwięku 677
 - pi/(kierowanie portu szeregowego 679 pizekierowanie urządzenia 677, 679 przełącznik /A 259 przełącznik /D 260 przełącznik /F 259 przełącznik /Ci 260 przełącznik /HC 261
 - przełącznik /J 259
 - przełącznik /I.261
 - przełącznik /IM 260
 - przełącznik /N 259
 - przełącznik /P 260
 - przełącznik /R 261
 - przełącznik /RS 261
 - przełącznik /SNAP 261
 - przełącznik /T 260
 - przełącznik/V 261
 - przełącznik -x 346
 - przełączniki
 - polecenie Ntbackup 259, 261
 - wiersz poleceń 82, 83 przełączniki polecenia
 - kopii zapasowej 258 przenoszenie
 - dysków pomiędzy serwerami 407, 408
 - obiektów komputera 153, 154, 155
 - obiektów użytkownika 75 przydział
 - żetonu 587 przydziały dysków 418, 420, 630
 - bufor wydruku 636
 - ćwiczenia praktyczne 420, 422
 - eksportowanie wpisów przydziałów 420

- konfigurowanie 418, 420, 421, 635
- monitorowanie 420
- testowanie 422
- wdrażanie 420, 422, 631, 632, 635
- przygotowanie do egzaminu 70-290
 - lektura uzupełniająca 506, 507, 536, 537, 564, 587, 588, 632
 - sprawdzone umiejętności i sugerowane zadania
- praktyczne 505, 506, 534, 536, 562, 563, 585, 586, 631
- przyłączanie komputerów do domeny 151, 152, 155, 156
- przyrostowa kopie zapasowe 239, 240, 274, 646
 - przestrzeń wymagana 646
 - przywracanie systemu 641
 - zadanie praktyczne 243, 244
 - zerowanie bitu archiwalnego 669
 - zwykle kopie zapasowe 241 przystawka
- Foldery udostępnione 178, 179
 - dostęp do edytora listy ACL (Access Control List) 190
 - węzeł Pliki otwarte 184
 - wz. ol Sesje 184
 - węzeł Udziały 179, 184 przystawka
- /arządzanie dyskami 102, 103
 - konfigurowanie przydziałów 418
 - rozwiązywanie problemów dysków 436, 437
 - tworzenie p.u. tycji za pomocą 410
- przystawki 36, 38, 39 przystawki
- autonomiczne 38 przy wraca nie
- autorytatywne 633, 639 przywracanie
- danych 247, 252, 630, 653
 - zobacz także* tworzenie kopii zapasowej, przywracanie systemu
 - ćwiczenia praktyczne 249, 250, 631
 - dane o stanie systemu 488, 489, 633, 638, 642, 662
 - informacje dla zdających egzamin 274, 278
 - Kopia zapasowa 247, 248, 645, 647
 - najważniejsze pojęcia 274
 - określanie lokalizacji przywracania 248
 - opcje 248, 249
 - podsumowanie 252, 269, 273, 274
 - przegląd 247
 - pytania i odpowiedzi 244, 245, 251, 268, 269, 277, 278, 654, 664
 - rozwiązywanie problemów 272, 273
 - serwer usługi SUS (Software Update Services) 342
- zestaw ASR (Automatyczne odzyskiwanie systemu) 491, 496 przywracanie nieautorytatywne 633, 639
- przywracanie partycji 639 przywracanie po awarii 381, 382, 630
 - ćwiczenia praktyczne 631
 - lektura uzupełniająca 632
 - pytania i odpowiedzi 634, 642 przywracanie poprzedniej wersji sterownika 376, 377, 381, 387 przywracanie systemu 484, 501, 630, 633
 - zobacz także* przywracanie danych
 - automatyczne 489, 491, 495, 496, 640
 - ćwiczenia praktyczne 494, 496, 631
 - dane o stanie systemu 486, 489, 494, 633, 638, 642
 - informacje dla zdających egzamin 498, 501
 - Konsola przywracania 492, 494, 495, 496
 - lektura uzupełniająca 632
 - najważniejsze pojęcia 499
 - opcje 485, 486
 - podsumowanie 498, 499
 - przegląd 484, 633
 - pytania i odpowiedzi 497, 498, 500, 501, 634, 642
- publikowanie
 - drukarki 299, 300
 - foldery udostępnione 180
- pule drukarek 297, 298, 302, 303, 619 pule
- nośników 254, 274
 - rodzaje 254, 255
 - zarządzanie 255 Pulpit zdalny dla
- administracji 45, 51
 - ćwiczenia praktyczne 49, 50, 585
 - licencje CAL 350
 - podsumowanie 51
 - Połączenie pulpitu zdalnego 46, 48
 - przegląd 34, 45
- pytania i odpowiedzi 51, 62, 63 rozwiązywanie problemów 48, 49, 59, 573, 575, 576 składniki domyślne 46 włączanie i
- konfigurowanie 45, 46 zdefiniowany 61 pytania i odpowiedzi
 - drukarki 290, 291, 304, 305, 313, 314, 321, 325, 616, 620 dziennik Zabezpieczenia 591, 592, 594 foldery udostępnione 186, 187, 230, 509, 510, 513, 566, 570 inspekcja dostępu do systemu plików 211, 212, 231, 232, 622, 625
 - Internetowe usługi informacyjne (MS) 221, 222, 232, 233, 638, 642
 - konsola MMC (Microsoft Management Console) 41, 44 konsola Wydajność 462, 480, 627, 629 konta grupy 129, 133, 139, 140, 143, 144, 552, 553 konta komputerów 156, 157, 161, 162, 168, 169, 174, 176, 545, 563

konta użytkowników 78, 79, 91, 92, 101, 102, 112,
117, 119, 567 licencje oprogramowania 355, 356, 364,
365, 605. 609 Menedżer zadań 468, 480, 481
monitorowanie wydajności systemu 452, 453, 462,
479, 481, 627, 629 narzędzia administracyjne 41, 51, 57,
58, 62, 63 odporność na uszkodzenia 649, 652
odzyskiwanie danych 244, 245, 251, 268, 269, 277,
278, 654, 664 optymalizacja wydajności dysku 525, 533
Pakiety serwisowe 347, 364 pamięć dyskowa 400, 401,
413, 422, 423, 432, 434,
441, 445, 515 Podgląd zdarzeń 452, 453, 479, 590, 594
Pomoc zdalna 57, 58, 63, 613 profile użytkownika 101,
102, 121, 122, 539, 543 program narzędziowy WMI
(Windows Management
Instrumentation) 474, 475, 481 przywracanie po awarii
634, 642 przywracanie systemu 497, 498, 500, 501, 634, 642
Pulpit zdalny 51
serwet sieci Web 638, 642
sterowniki 373, 374, 379, 380, 383, 384, 388, 389
tworzenie kopii zapasowej 244, 245, 251, 268, 269,
275, 278, 644, 647, 670 uprawnienia systemu plików
204, 205, 230, 231, 577,
582 urządzenia sprzętu 373, 374, 379, 380, 383, 384,
388,
389, 517, 542 usługa SUS (Software Update Strvices)
343, 363, 596,
603 Usługi terminalowe 572, 576
uwierzytelnienie 112, 122, 569, 572
wersje systemu Windows Scivei '!' 20, 34
zarządzanie zdalne 611, 614
Zasada grupy 535, 536, 539, 540, 542

R

RDP (Remote Desktop Protocol) 671
połączenia RDP-Tcp 673, 674, 675 rejestrowanie informacji
o kopiach zapasowych 257, 258 rekord MBR (Master Boot
Record) 397 Remote Desktop Protocol (RDP) 671
połączenia RDP-Tcp 673, 674, 675
RID (identyfikator względny) 559
rola wzorca identyfikatora RID 563
RJS (Remote Installation Services) 149
rozproszony system plików (Dfs) 106

rozruch w oparciu o kilka systemów 400
rozruchowy dysk CD-ROM 21 rozszerzenia
przystawek 38, 39 rozwiązywanie problemów
drukarki 310, 312, 318, 319, 615
foldery udostępnione 225, 227
konta grupy 141
konta komputerów 163, 169, 170, 172, 535, 559
konta użytkowników 115, 116, 536, 564
kopie zapasowe 272, 273
monitorowanie wydajności 476, 477
narzędzia administracyjne 59
pamięć dyskowa 436, 439
Pulpit zdalny 48, 49, 59, 573, 575, 576
sterowniki 381, 384, 385, 386
uprawnienia systemu plików 225, 227, 583
urządzenia sprzętu 381, 384, 385, 386
usługa SUS (Software Update Seryices) 340, 341
Usługi teiminalowe 48, 49, 563, 571, 576
uwierzytelnienie 116, 568 równoważenie obciążenia
680, 681 równoważenie obciążenia sieci NBI. (Nerwork
Load
Balancing) 18, 681 różnicowa kopia
zapasowa 240, 274, 646
wykonywanie ćwiczeń praktycznych 243
wymagane miejsce 646
zwykła kopia zapasowa 240, 241 RUT;
zobacz mobilne profile użytkownika

S

SAN (storage atea networks) 392
serwer aplikacji 23
serwer I)HCP (Dynamie Host Configuration Protoco
serwer DNS (Domain Namc Scrvice) 23, 449
dziennik serwera DNS 449
konfiguracja 152 serwer druku 22, 281, 584,
586, 630 serwer indeksowania 324 serwer
licencji domeny 670 serwer licencji lokacji 352
serwer licencji przedsiębiorstwa 670 serwer
licencji serwera terminali 670. 671 serwet
nośników sttumeniowych 23 serwer plików 22,
586, 630 serwer poczty 23 serwer proxy 331
Serwer terminali 23, 45, 46, 668, 683
administrowanie 671, 673, 680, 683
aplikacje 668, 669

- instalowanie 668, 669
- klastry 680, 681
- konfigurowanie 668, 670, 673, 674, 676
- licencjonowanie 670, 671
- opcje zabezpieczeń 669
- połączenia klienta 671, 676
- prawa logowania 676
- przegląd 668
- przekierowanie urządzenia 677, 679
- równoważenie obciążenia 680, 681
- sesje użytkownika 680
- składniki domyślne 46
- sterowanie zdalne 682, 683
- serwer VI»N 23
- serwer WINS (Windows Internet Name Service) 23 MIWI
- równie 610 serwery
 - konfigurowanie 22, 24, 31, 33
 - monitorowanie 458, 516
 - optymalizacja wydajności 505, 524
 - przenoszenie pomiędzy dyskami 407, 408
 - przywracanie systemu 631
 - zarządzanie zdalne 584, 585, 610
- serwery sieci Web 18, 637
 - zobacz, także* Internetowe usługi informacyjne (IIS)
 - ćwiczenia praktyczne 586
 - Funkcjonalność odzyskiwania 635, 640
 - pytania i odpowiedzi 638, 642
- rozwiązywanie problemów Ograniczeń adiesacji
- protokołu II> 640, 642 serwery w trybie offline 184, 185, 186 sesje użytkownika 184, 680 SID; *zobacz* identyfikatory zabezpieczeń SIL) sieci
 - modele usługi katalogowej 24
 - monitorowanie 459 sieci intranet 224 sieci lokalne (LAN) 23 sieci rozległe WAN 23, 595, 610 Simple Mail Transfer Protocol (SMTP) 18 słowo kluczowe „komputer” 547 SMP (symetryczna wieloprocessorowość) 18, 19 SMS (Systems Management Server) 346 sprzętowa macierz. RAID 396, 424, 425, 430, 435, 436, 508 sterowanie zdalne 682, 683 sterowniki 366, 389
 - zobacz także* urządzenia sprzętu
 - aktualizacja 375, 376
 - ćwiczenia praktyczne 372, 373, 379
 - drukarka 282, 306, 307, 318, 319
 - informacje dla zdających egzamin 386, 389
 - instalowanie 368, 374
 - kody statusów 382, 383
 - konfiguracja zasobu 378
 - konfigurowanie 375, 380
 - najważniejsze pojęcia 387
 - narzędzia odzyskiwania 381, 382
 - niepodpisane 534
 - odinstalowanie 377, 378
 - podpisane 371, 372, 373, 534
 - podsumowanie 374, 380, 384, 386, 387
 - przegląd 366, 367
 - przywracanie poprzedniej wersji 376, 377, 381, 387
 - pytania i odpowiedzi 373, 374, 379, 380, 383, 384, 388, 389
 - rozwiązywanie problemów 381, 384, 385, 386
 - zadanie praktyczne 384, 385 sterowniki drukarek PostScript 318 sterowniki IDE (Integrated Drive Electronics) 435 strona Poprzednie wersje 264, 265, 267, 268 strona Synchronizacja Servcr 333 strona Zarządzanie tym serwerem 22 strona Zatwierdzanie aktualizacji 334 suma Kontrolna CRC 336 SupponTools 150
 - SUS; *zobacz* usługa SUS (Software Update Services)
 - symbol „at” (@) 258
 - symbole statusów, licencjonowanie 354
 - symbole wieloznaczne 494
 - symetryczna wieloprocessorowość (SMP) 18, 19
 - synchronizacja
 - hasło 559
 - mobilny profil użytkownika 95
 - usługa SUS (Software Update Semces) 333.335,340, 359, 360 system operacyjny
 - aktualizacja 326, 344
 - aktywacja 30, 31
 - konservacja 324, 365 system
 - plików NTFS 415, 577
 - system RSM (Removable Storage Management) 236, 254
 - Systems Management Server (SMS) 346 systemy plików FAT/FAT32 415 szablon uprawnień Modyfikacja 192 szablon uprawnień Odczyt i wykonanie 192 szablon
 - konta użytkownika 118
 - obiekt użytkownika 80, 81
 - profil użytkownika 99
 - uprawnienia 192 szablon
 - użytkownika 80, 81, 89, 90

szyfrowanie odwracalne 74

Ś

ścieżka profilu 567

ściśła copologia nadrzędny/podrzędny 332

śledzenie lokalizacji drukarek 300, 301

T

tablica partycji GUID (GPT) 404

taśma kopii zapasowych 254, 255, 256, 646

zobacz także tworzenie kopii zapasowych danych

technologia maszyny wirtualnej 400 testowanie przydziału

dysków 422 topologia tcsi/piodiikc j.i . '>.'> } topologia wielości

werowa 332 topologie typu nadrzędny/podrzędny 332

topologie, usługa -SUS (Software Update [Servic.es](#)) 332, 333

tożsamości specjalne 127, 128 tryb Autor 39

Tryb awaryjny 382, 385. 386, 387 tryb Przywracanie

usługi katalogowej 639 tworzenie kont użytkownika za

pomocą skrypów 170

U

udostępnianie dtukowania 283, 284, 288

udostępnianie plików 659, 664

udostępnianie plików w trybie l'2P (peer-to peer) 539

ud/iały sieciowe 646

udziały ukryte 178, 229

ukierunkowanie na lokację 106

umowa EU1.A (F.nd User License Agreement) 347, 671

UNC (Universal Naming Convntion) 96, 178, 238

Uniwersalny kontroler hosta USB 521

UPN (główna nazwa użytkownika) 69, 107

UPnP (Universal Plug and Play) 56

uprawnienia

dodawanie 191

drukarka 293, 294, 316, 317

dziedziczony 192, 195

grupa 586

Internetowe usługi informacyjne (IIS) 219, 220

konfigurowanie 188, 192, 200, 202, 563

konta użytkownika 586

kopia zapasowa 253, 254

modyfikowanie 191

obiekt komputera 158

połączenie RDP-Tcp 675

ponowne przenoszenie 191

rozwiązywanie problemów 225, 227

szablony 192

zarządzanie 191, 192 uprawnienia

administratora 508 uprawnienia

bezpośrednie 196 uprawnienia czynne

177, 195, 198

ćwiczenie praktyczne 202, 203

określanie reguł 195, 196

wersja testowa 196, 198

zdefiniowany 229 **uprawnienia**

katalogu 219 uprawnienia NTFS 182,

188, 205

czynne 195, 198,202,203

ćwiczenia praktyczne 200, 204, 562, 563

dziedziczenie 192, 195

konfigurowanie 188, 192, 563, 577

lektura uzupełniająca 564

podsumowanie 205

pytania i odpowiedzi 204, 205, 230, 231, 578, 582

rozwiązywanie problemów 225, 227

własność zasobu 198, 199, 203, 204

zasobu IIS 219 uprawnienia specjalne 192

uprawnienia systemu plików 188, 205

czynne 195. 198,202,203

ćwiczenia praktyczne 200, 204, 562, 563

dziedziczenia 192, 195

informacje dla zdających egzamin 228, 233

konfigurowanie 188, 192, 200, 202, 563, 577

lektura uzupełniająca 564

najważniejsze pojęcia 229

podsumowanie 205, 227, 228

pytania i odpowiedzi 204, 205, 230, 231, 578, 582

rozwiązywanie problemów 225. 227, 583

własność zasobu 198, 199. 203, 204

uprawnienia udziału 99, 180, 181, 184

certyfikacja 183, 184

konfigurowanie 181, 182, 565

ograniczenia 182, 183

pytania i odpowiedzi 566, 570, 583, 587

rodzaje 181

rozwiązywanie problemów 226, 227, 583

w praktyce 183 uprawnienia Wykonaj 219

uprawnienia zapisu 192, 581, 582 uprawnienia

Zarządzanie drukarkami 294 uprawnienia

zasobów 198,199, 583, 586 uprawnienia

zezwalające 195, 196

uprawnienie Drukowanie 294
 uprawnienie Modyfikacja 181, 192, 569
 uprawnienie Odczyt 181, 569, 581, 582, 587
 uprawnienie Odmów 196, 202, 581
 uprawnienie Odmów odczytu 581
 uprawnienie Pełna kontrola 181, 192, 569, 683
 uprawnienie Przejmowanie na własność 199
 uprawnienie Zarządzanie dokumentami 294
 uprawnienie Zezwalać - Przejmuj na własność 199
 URI. (Uniform Resource Locators) 214, 217
 urząd certyfikacji (CA) 635, 636, 640
 urządzenia niezgodne z technologią PnP (Plug-and-Play) 505, 521
 urządzenia PnP (Plug-and-Play) 368, 371, 521
 urządzenia sprzętu .566, 389
zobacz także sterowniki; drukarki
 ćwiczenia praktyczne 372, 373, 379, 505, 506
 informacje dla zdających egzamin 386, 389
 instalowanie 368, 374, 534
 kody statusów 382, 383
 konfiguracja zasobu 378
 konfigurowanie 375, 380, 534
 lektura uzupełniająca 507
 lista IRI. 542
 monitorowanie 516
 najważniejsze pojęcia 387
 narzędzia przywracania sterownika 381, 382
 odinstalowanie 376, 387
 opcje przekierowania 677, 679
 Panel sterowania 379
 podsumowanie 374, 380, 384, 386, 387
 przegląd 366, 367
 przywracanie po awarii 381, 382, 630, 631
 pytania i odpowiedzi 373, 374, 379, 380, 383, 384, 388, 389, 517, 542
 rozwiązywanie problemów 381, 384, 385, 386
 technologia PnP (Plug-and-Play) 368, 371
 tworzenie kopii zapasowej danych 644, 646
 wyłączanie 379, 387
 zadanie praktyczne 384, 385
 zarządzanie 504, 506
 urządzenia USB (Universal Serial Bus) 521
 usługa Active Directory 24, 26
 dane o stanie systemu 488
 domeny, drzewa i lasy 25, 35
 integracja drukarek 298, 301, 303
 książka adresowa system Windows 106
 lektura uzupełniająca 26
 listy kontroli dostępu (ACL) 26
 narzędzia wiersza poleceń 82, 88, 91, 131
 obiekty i jednostki organizacyjne (OU) 25

podmioty zabezpieczeń 555, 557
 przegląd 24
 przywracanie obiektów 639
 uwierzytelnienie 68
 wyszukiwanie obiektów 159, 160, 161
 zagadnienia związane z różnymi platformami 106, 107
 Zasada grupy 26
 usługa BITS (Background Intelligent Transfer Service) 336
 usługa FRS (File Replication Service) 24, 449
 usługa instalacji zdalnej (RIS) 149
 usługa LDM (Logical Disk Manager) 398
 usługa Menedżer dysku logicznego (LDM) 398
 usługa MMS (Microsoft Metadirectory Services) 19
 usługa NNTP (Network News Transfer Protocol) 637
 usługa Posłaniec 186
 usługa przeglądania 562
 usługa Rejestrowanie licencji 351, 353
 usługa Rejestrowanie zdalne 562
 usługa RPC (wywołanie procedury zdalnej) 311
 usługa RRAS (Routing i dostęp zdalny) 22, 562
 usługa Serwer 178
 usługa Software Update Synchronizacja 329
 usługa Stacja robocza 178
 usługa SUS (Software Update Services) 326, 344, 584
 administrowanie 329, 334
 aktualizacje- z uwzględnieniem .534, 335
 ćwiczenia praktyczne 585
 instalowanie 327, 329, 358, 359
 klient usługi Aktualizacje automatyczne 335, 337
 konfigurowanie 326, 327, 330, 331, 601
 monitorowanie 339
 podsumowanie 344, 361, 362
 przegląd 326, 595
 przywracanie serwera 342
 pytania i odpowiedzi 343, 363, 596, 603
 rozwiązywanie problemów 340, 341
 serwer usługi SUS (Software Update Services) 595
 składniki 327
 synchronizacja 333, 335, 359, 360
 topologie 332, 333
 tworzenie kopii zapasowej 341, 342
 witryna sieci Web 329, 330, 359
 zadania praktyczne 358, 360
 zdarzenia systemu 339, 340
 usługa Udostępnianie plików i drukarek w sieciach
 Microsoft Networks 178
 usługa VSS (Volume Shadow Copy Service) 234, 253, 262, 265, 274
 Usługa wiadomości błyskawicznych 56
 usługi -NET Web 637
 usługi dostępu zdalnego 23

Usługi metakatalogu 19 Usługi terminalowe 45, 46, 584
 aktualizacja poprzednich wersji 47
 folder macierzysty 669, 670
 konsola Konfiguracja 672
 licencje CAL 350, 609
 najnowsze informacje 49
 okno dialogowe Właściwości 73
 pytania i odpowiedzi 572, 576
 rozwiązywanie problemów 48, 49, 563, 571, 576
 składniki oprogramowania 46
 wykorzystywanie zarządzania zdalnego 610, 614
 usługi WMS (Windows Media Services) 23, 637
 ustawienia daty i godziny 30 ustawienia językowe 328, 331
 ustawienia regionalne 29 usuwanie • Konsola odzyskiwania 492
 konta komputera 163
 obiekty użytkownika 109
 uprawnienia 191
 usuwanie drukarek 299
 uwierzytelnienie 103, 112
 administrowanie 108, 109
 ćwiczenia praktyczne 110, 111
 inspekcja 107, 108
 konfiguracja zasady 103, 105, 110, 111
 podsumowanie 112
 pytania i odpowiedzi 112, 122, 569, 572
 rozwiązywanie problemów I 16, 168
 użytkownik 108, 109, 536
 wittyna protokołu FTP (FileTransfer Ptotocol) 218
 witryna sieci Web 218, 639, 642
 zagadnienia /wiązane z różnymi platformami 106, 107
 zasady blokady konta 105
 zasady haseł 104, 105 uwierzytelnienie anonimowe 218
 uwierzytelnienie anonimowe dla usługi FTP 218
 uwierzytelnienie Basic 218 uwierzytelnienie szyfrowane 2.18
 uwierzytelnienie usługi .NET Passport 218 uwierzytelnienie użytkownika 108, 109 uwierzytelnienie za pomocą certyfikatu 218, 635. 636, 640 użytkownicy
 instalacja urządzeń 371
 przydziały niestandardowe 421
 uwierzytelnienie 108, 109 Użytkownicy i komputery usługi Active Directory
 przenoszenie obiektów użytkowników 75
 tworzenie obiektu komputera 149, 154
 tworzenie obiektu użytkownika 68, 71

zarządzanie kontami grupy 130, 133 zarządzanie kontami użytkowników 72, 75, 554 zatwierdzanie konfiguracji serwera 32, 33

V

VSS (Volume Shadow Copy Service) 234, 253, 262, 265,

274

W

w pełni kwalifikowana nazwa domeny (FQDN) 331

wartość UseWUSever 340

wartość WUSever 340

WBEM (Web-Based Enterprise Management) 470

wersje systemu Windows Seiver 2003 17, 20

Datacenter Edition 19

Enterprise Edition 19

podsumowanie 20

pytania i odpowiedzi 19, 20, 34

Standard Edition 18

Web Edition 18

wersja 64-bitowa 19 wc/.el główny konsoli 36

Windows 2000 Professional 609 Windows Address

Book (WAB) 106 Windows Internet Namc Scryiie

(WINS) 23

Windows Management Instrnmeniation (WMI) 470, 475

interfejs wiersza poleceń 470, 473

konfiguracja zabezpieczeń 471

monitorowanie komputerów 473, 474

opis 470, 478

pobieranie danych z programu Podgląd zdarzeń 474

podsumowanie 475

pytania i odpowiedzi 474, 475, 481 Windows Management

Inteiface Command-iinc (WMK 470, 475

administracja 471, 473

aliasy 472

monitorowanie komputerów 473, 474

opis 470, 471, 478

porównanie trybu interaktywnego i nicinteraktywne 471

zlecenia 472, 473 Windows

Messenger 52, 53, 575 Windows NT 4

431 Windows Server 2003

administracja 34, 63

aktualizacja 431

aktywacja 21, 30, 31, 35

dane o stanie systemu 486, 489

- Datacenter Edition 19
- Enterprise Edition 19, 34
- konfiguracja 22, 24, 31, 33
- Konsola odzyskiwania 492, 494
- monitorowanie 446, 481, 516
- narzędzia wiersza poleceń 82, 88
- odporność na uszkodzenia 21, 22, 27, 31, 395, 396, 425, 435, 648
- poziomy funkcjonalności domeny 124
- Serwer terminali 668, 683
- Standard Edition 19, 34
- sterowniki dostarczane wraz z 368
- usługa Active Directory 24, 26
- usługa SUS (Software Update Services) 326, 344, 584
- Web Edition, 19, 34
- wdrażanie macierzy RAID 425
- witryna sieci Web firmy Microsoft 17
- zasady zabezpieczeń 103 Windows Server 2003
- Resource Kit 153 Windows System Resource Manager (WSRM) 19 Windows Update Server 326, 327, 595, 602
- wirusy 637, 641
- witryna sieci Web firmy Microsoft 17
- witryny sieci Web
 - administracja usługi SUS (Software Update Services) 327
 - administrowanie środowiskiem sieci Web 213, 214
 - konfigurowanie i zarządzanie 215, 217
 - ograniczanie dostępu 638, 641
 - ograniczanie połączeń 638, 639, 641
 - opcje uwierzytelnienia 218, 639, 642
- witryny usługi FTP (File Transfer Protocol)
 - administrowanie 217, 637
 - opcje uwierzytelnienia 218
- włamywacze 636 własność 198, 199, 203, 204, 229 własność zasobu 198, 199, 203, 204 właściwości
 - drukarka 283, 284, 293, 297
 - konta komputera 159, 161
 - konta użytkownika 73, 74
- właściwości konta 73, 74 właściwości
 - użytkownika 69, 70, 71 włączanie
 - inspekcja 208
 - konta komputera 164, 165
 - konta użytkownika 108 WMI; *zobacz* Windows Management Instrumentation
 - (WMI) WMIC; *zobacz* Windows Management Interface Command-line (WMIC)
- wolny nośnik 255
- wolumin systemowy (Sysvol) 24
 - folder Sysvol 488
 - odporność na uszkodzenia 430
- woluminy
 - defragmentacja 417
 - formatowanie 405
 - instalowany 395, 405, 406, 412, 508
 - konfigurowanie 403, 406
 - konservacja 415, 423
 - litery dysku 405, 406, 412
 - rozszerzanie 406, 407, 412
 - tworzenie 404, 405 woluminy dublowane 395, 399, 426, 428, 648
 - odporność na uszkodzenia 649, 651
 - przywracanie 426, 428
 - tworzenie 426
 - woluminy RAID-5 429, 430
 - wydajność dysku 532
 - zdefiniowany 440 woluminy instalowane 395, 405, 406, 412, 508 woluminy logiczne 394, 395
 - dyski dynamiczne 397, 399
 - dyski podstawowe 397 woluminy łączone 398, 440, 530 woluminy proste 398, 440 woluminy RAID-0; *zobacz* woluminy rozłożone woluminy RAID-1; *zobacz* woluminy dublowane woluminy RAID-5; *zobacz* woluminy rozłożone z parzystością woluminy rozłożone 398, 425, 426
 - definicja 440
 - odporność na uszkodzenia 651
 - optymalizacja wydajności 524
 - ponowne tworzenie 654, 661
 - przywracanie 426
 - tworzenie 425, 426 woluminy rozłożone z parzystością 395, 396, 399, 428, 430, 524, 648
 - konfigurowanie 428, 429
 - optymalizacja wydajności 524
 - przywracanie 429, 660, 664
 - definicja 429, 430, 440 woluminy rozszerzone 406, 407, 412 wpis kontroli dostępu (ACE) 188 WSRM (Windows System Resource Manager) 19 wstępnie skonfigurowane profile użytkowników 96, 97, 99, 101 Wszystkie urządzenia i podsumowanie raportu 522 wybór plików kopii zapasowej 258, 259 wykaz, kopia zapasowa 255, 256

wyłączanie
 konta komputera 164, 165
 konta użytkownika 71, 109
 urządzenia sprzętu 379, 387 wyłączanie
 plików z kopii zapasowej 258 wyszukiwanie
 dane usługi WMI w programie Podgląd zdarzeń 474
 drukarki 285
 foldery udostępnione 180, 181
 obiekty komputerów 159, 160
 pakiety serwisowe 345, 346, 357
 wzór odniesienia 457

X

XML (Kxtensible Markup Language) 53, 217

Z

Zaawansowane uwierzytelnienie szyfrowane 218
 zabezpieczenia
 drukarka 293, 294, 309
 folder udostępniony 180
 hasła 70, 71
 Inrcrnetowe usługi informacyjne (IIS) 218, 220, 221
 Konsola odzyskiwania 494
 kopia zapasowa 253, 254, 261
 podmioty 555, 557
 Pomoc zdalna 53, 54, 55
 Serwer terminali 669
 uwierzytelnienie 103, 112
 własność zasobu 198, 199
 zagadnienia dotyczące różnych platform 106, 107
 zasady 103. 105
 zadanie praktyczne
zobacz także ćwiczenia praktyczne
 dane i dostęp do sieci intranet 224
 drukarki 315, 318
 foldery udostępnione 223
 konta grup 140
 konta komputerów 169, 170
 konta użytkowników 113, 115
 monitorowanie wydajności 475, 476
 narzędzia administracyjne 58, 59
 Pakiety serwisowe 357. 358
 pamięć dyskowa 434, 436
 sterowniki 384, 385
 tworzenie kopii zapasowej danych 270, 271
 urządzenia sprzętu 384, 385

usługa SUS (Software Update Services) 358, 360
 zakładka Aplikacje, Menedżer zadań 464 zakładka COM+,
 okno dialogowe Właściwości 73 zakładka Członek grupy
 73 zakładka Dysk 370
 zakładka Konta, okno dialogowe Właściwości 72, 73, 74
 zakładka Ogólne, okno dialogowe Właściwości 72 zakładka
 Procesy, Menedżer zadań 465, 466 zakładka Profil, okno
 dialogowe Właściwości 72 zakładka Sieć, Menedżer zadań 466,
 467 zakładka Telefonowanie, okno dialogowe Właściwości 73
 zakładka Udostępnianie 178 zakładka Użytkownicy, Menedżer
 zadań 467 zakładka Wydajność, Menedżer zadań 466 •zakładka
 Zasoby 377 ■zakres grupy 125, 126 zapisywanie danych o
 wydajności 461 zapisywanie wyszukiwania 285 /apoiiy
 ogniowe 56 zarządzanie dyskami 508
 ćwiczenia praktyczne 505
 interfejs konsoli 402, 403
 narzędzia wiersza poleceń 408, 4 10
 optymalizacja wydajności 524
 pytania i odpowiedzi 508, 51 5
 zarządzanie zdalne 610
 ćwiczenia praktyczne 585
 konsola MMC (Microsoft Management Console) 42, 43
 pytania i odpowiedzi 611, 614
 Serwer terminali 682, 683
 Zasada grupy 26
 aplikacja 603
 instalowanie pakietów serwisowych 346, 358, 595
 konfiguracja usługi Aktualizacje automatyczne 337, 338
 opcje programu Pomoc zdalna 54, 55
 pytania i odpowiedzi 535, 536, 539, 540, 542
 Usługi terminalowe 673
 ustawienia przekierowania danych klient/serwer 572, 575
 włączanie inspekcji 208 zasada Przeprowadź inspekcję
 dostępu do obiektu 229 zasada Zezwalaj wyłącznie na
 stosowanie lokalnych profili
 użytkownika 95
 zasady
zobacz także Zasada grupy
 aktualizacja 337, 338
 blokady konta 105
 hasło 104, 105, 572
 inspekcja 107, 108
 zabezpieczenia 103, 105

zasady dotyczące przekietowania folderu 93
 zastępowanie dziedziczenia 193, 194
 „zaśmiecone” dyski 533
 Zaufania i domeny usługi Active Directory 547, 557
 zdarzenia logowania 111, 115, 116
 zerowanie
 hasła 26, 109, 547
 konta komputera 165, 171, 172, 547, 586, 587 zestaw
 ASR (Automatyczne odzyskiwanie systemu) 633
 zobacz także Automatyczne odzyskiwanie systemu
 lisia plików 491
 odzyskiwanie danych z 642
 tworzenie 489, 490, 495 zestaw narzędzi
 defragmentacji 416, 417 zewnętrzne obiekty
 GPO 540
 Zintegrowane uwierzytelnienie systemu Windows 218
 zlecenia, usługa WMIC (Windows Management Interfacc
 Command-line) 472, 473
 zmiana nazwy
 kompuieiy I 51
 obiekty użytkownika 109 znak
 <S> (at) 258 znak dolara (\$) 178.570
 zwykle kopii- zapasowe 239, 274
 przyrostowe kopie zapasowe 241
 różnicowe kopie zapasowe 240, 241
 wykonywanie ćwiczeń praktycznych 242

Ż

żądania p.zciwań (HU..) 368, 541, 542



Szanowni Państwo,

Wraz z firmą Microsoft chcielibyśmy Państwu przedstawić informacje na temat produktów rodziny **Microsoft Technet** - technicznej encyklopedii dostępnej na płytach CD lub DVD, dostarczanej w formie rocznej subskrypcji. Pierwsza przesyłka zawiera około 50 płyt w wygodnym segregatorze wysyłanym pod adres wskazany podczas rejestracji produktu. Dodatkowo co miesiąc subskrybent otrzymuje przesyłki zawierające kilkanaście płyt z uaktualnieniami do posiadanych już informacji, co pozwala mu korzystać z zawsze bieżących informacji.

Produkty te są skarbnicą wiedzy technicznej, niezbędnej każdemu administratorowi. Stanowią także znakomite uzupełnienie narzędzi MSDN.

Zapraszamy już teraz do zakupu:

- » **MS Technet 2000 Single User** - zawiera poprawki oprogramowania (paten), Service Pack, Sterowniki, Knowledge Base, 12 comiesięcznych przesyłek aktualizacyjnych;
- « **MS Technet 2000 Single Sen/er** - zawiera poprawki oprogramowania (patch), Service Pack, Sterowniki, Knowledge Base, licencje dla użytkowników sieciowych, 12 comiesięcznych przesyłek aktualizacyjnych;

Zamówienia można składać na stronie <http://www.promise.com.pl/Sklep/>, bądź na numer faksu (22) 826 40-15.

Dodatkowych informacji na temat Microsoft Technet udziela Agnieszka StyśZeiglic pod numerem telefonu (22) 654-61-12. Mogą je Państwo również uzyskać na stronie internetowej <http://www.promise.com.pl/msdn/>.

Microsoft Developer

Serdecznie zapraszamy Państwa do subskrypcji **DevFlash** - elektronicznego biuletynu dla programistów. Miesięcznik jest redagowany przez pracowników polskiego oddziału Microsoft. Znajdą w nim Państwo informacje techniczne zaczerpnięte z bazy wiedzy Microsoft Developer Network, najbardziej aktualne wiadomości dla każdego twórcy oprogramowania jak i informacje poświęcone wydarzeniom lokalnym.

Tak, więc jeżeli chcą Państwo:

- » otrzymywać zaproszenia na konferencje Microsoft Developer Days,
- » być na bieżąco informowani o innych seminariach dla programistów,
- » wiedzieć więcej o najnowszych wersjach naszych technologii i platformie .NET,
- oraz uzyskiwać informacje o specjalnych promocjach i programach dla deweloperów w Polsce,

zapraszamy do subskrypcji biuletynu DevFlash pod adresem:

<http://www.microsoft.com/poland/developer/devflash/>



MSDN to podstawowe narzędzia dla każdego programisty i kompleksowe środowisko do tworzenia oraz testowania aplikacji

Subskrypcja **Microsoft Developer Network** pozwala programiście być zawsze na bieżąco z najnowszymi trendami programistycznymi

Wybierając subskrypcję MSDN (Microsoft Developer Network) zapewnią Państwo wszystko, co jest potrzebne do tworzenia aplikacji WWW oraz aplikacji dla środowiska Microsoft Windows, między innymi, dostęp do najnowszej wersji Microsoft Visual Studio .NET, biblioteki wiedzy oraz pomocy technicznej. Subskrypcja MSDN dostarcza najnowsze wersje oprogramowania przez rok lub 2 lata, przy czym po upływie tego czasu mogą Państwo nadal korzystać z produktów objętych umową licencyjną lub przedłużyć swoją umowę ze zniżką.

Jest pięć poziomów subskrypcji MSDN, które można dopasować do własnych potrzeb i możliwości. Szczegółowe informacje na temat każdego i poziomów znajdują Państwo pod adresem <http://www.microsoft.com/poland/msdn/poziomy.htm>

W subskrypcji można znaleźć między innymi:

- » Visual Studio .NET w wersji zależnej od poziomu MSDN
- » zestawy serwerów Microsoft.
- » systemy operacyjne Microsoft, pakiety SDK, DDK
- » MSDN Library (aktualizacje kwartalne)
- » wsparcie techniczne

Zasady dystrybucji: Pierwsza wysyłka zawiera aktualne wersje wymienionych wyżej zasobów, aktualizacje, wersje beta i nowe produkty są dostarczane kwartalnie lub można je pobrać ze specjalnie przygotowanych witryn dla użytkowników MSDN.

Jeżeli zainteresowała Państwa nasza oferta, prosimy do kontakt:

APN Promise
Ul. Zielna 39
00-108 Warszawa
Tel./fax (0 prefix 22) 654-61-12

Więcej informacji na temat MSDN znajdują Państwo na stronie:

<http://www.microsoft.com/poland/msdn/> lub <http://www.promise.com.pl/msdn/>.

Certyfikaty MCSA i MCSE dotyczące systemu Microsoft Windows Server 2003

Certyfikat MCSE (Microsoft Certified Systems Engineer) jest podstawowym certyfikatem dla fachowców analizujących wymagania biznesu, projektujących i wprowadzających infrastrukturę rozwiązań biznesowych bazujących na platformach systemu Microsoft® Windows Server™ 2003 i Microsoft Windows Server System. Implementacje te dotyczą instalowania, konfigurowania oraz rozwiązywania problemów systemów sieciowych.

Certyfikat MCSA (Microsoft Certified Systems Administrator) potwierdza osiągnięty poziom umiejętności i wiedzy potrzebnej do prawidłowego wprowadzenia, zarządzania i rozwiązywania problemów spotykanych w środowisku systemów Windows Server 2003.

Informacje dotyczące materiałów do przestudiowania, ćwiczeń oraz certyfikatów związanych z systemem Microsoft Windows Server 2003 można znaleźć pod adresem: <http://www.microsoft.com/traincert>

Wymagania obowiązkowe certyfikatów MCSA/MCSE

MCSA

Trzy egzaminy obowiązkowe, wliczając w to:

- Dwa egzaminy dotyczące systemów sieciowych (Networking System) ■
- Jeden egzamin dotyczący systemu operacyjnego klienta (Client Operating System)

MCSE

Sześć egzaminów obowiązkowych, wliczając w to:

- Cztery egzaminy dotyczące systemów sieciowych (Networking System)
- Jeden egzamin dotyczący systemu operacyjnego klienta (Client Operating System)
- Jeden egzamin dotyczący projektowania

Egzaminy dotyczące systemów sieciowych (Networking System)

MCSA (wymagane dwa egzaminy)	MCSE (wymagane cztery egzaminy)	Egzaminy obowiązkowe: systemy sieciowe	Materiały do studiowania opracowane przez Microsoft Press	ISBN
✓	✓	Egzamin 70-290: Zarządzanie i obsługa środowiska Windows Server 2003	MCSA/MCSE Zestaw szkoleniowy (Egzamin 70-290): Zarządzanie i obsługa środowiska Windows Server 2003 ⁴ MCSE Zestaw szkoleniowy: Microsoft Windows Server 2003 Core Requirements, Egzaminy 70-290, 70-291, 70-293, 70-294	0-7356-1437-7 83-88440-40-3 0-7356-1953-0
✓	✓	Egzamin 70-291: Wdrażanie, zarządzanie i obsługa infrastruktury sieciowej Windows Server 2003	MCSA/MCSE Zestaw szkoleniowy (Egzamin 70-291): Wdrażanie, zarządzanie i obsługa Infrastruktury sieciowej Windows Server 2003 ³ MCSE Zestaw szkoleniowy: Microsoft Windows Server 2003 Core Requirements, Egzaminy 70-290, 70-291, 70-293 i 70-294	0-7356-1437-3 83U8440-43-8 0-7356-1953-0
	✓	Egzamin 70-293: Planowanie i obsługa infrastruktury sieciowej Windows Server 2003	MCSE Zestaw szkoleniowy (Egzamin 70-293): Planowanie i obsługa infrastruktury sieciowej Windows Server 2003 ⁴ MCSE Zestaw szkoleniowy: Microsoft Windows Server 2003 Core Requirements, Egzaminy 70-290, 70-291, 70-293, 70-294	0-7356-1893-3 83 88440446 0735619530
	✓	Egzamin 70-294: Planowanie, wdrażanie i obsługa infrastruktury Active Directory Windows Server 2003	MCSE Zestaw szkoleniowy (Egzamin 70-294): Planowanie, wdrażanie i obsługa infrastruktury Active Directory Windows Server 2003 ³ MCSE Zestaw szkoleniowy: Microsoft Windows Server 2003 Core Requirements, egzaminy 70-290, 70-291, 70-293, 70-294	0-7356-1437-3 83-88440-454 0735619530

Egzaminy dotyczące systemów operacyjnych klienta (Client Operating System)

MCSA (jeden do wyboru)	MCSE (jeden do wyboru)	Egzaminy obowiązkowe: system operacyjny klienta	Materiały do studiowania opracowane przez Microsoft Press	ISBN
✓	✓	Egzamin 70-270: Instalowanie, konfigurowanie i administracja Windows XP Professional	MCSE Zestaw szkoleniowy (Egzamin 70-270): Windows XP Professional ⁶	0-7356-1429-6 83S8440-27-6
✓	✓	Egzamin 70-210 ⁵ : Instalowanie, konfigurowanie i administracja Windows® 2000 Professional	MCSA/MCSE Zestaw szkoleniowy (Egzamin 70-210): Microsoft Windows 2000 Professional, wydanie drugie	07356-176&X

Egzaminy dotyczące projektowania

MCSA (nie dotyczy)	MCSE (jeden do wyboru)	Egzaminy obowiązkowe: projekt	Materiały do studiowania opracowane przez Microsoft Press	ISBN
	✓	Egzamin 70-297 ¹ : Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure	MCSE Zestaw szkoleniowy (Egzamin 70-297): Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure	0-7356-1970-4
	✓	Egzamin 70-298 ² : Designing Security for a Microsoft Windows Server 2003 Network	MCSE Zestaw szkoleniowy (Egzamin 70-298): Designing Security for a Microsoft Windows Server 2003 Network	0-7356-1969-7

Nie istnieją żadne dodatkowe egzaminy obowiązkowe lub do wyboru wymagane dla uzyskania certyfikatów MCSA dotyczących systemu Windows 2000 dla osób, które zdały egzamin 70-292 lub wymagane dla uzyskania certyfikatów MCSE (system Windows 2000) dla osób, które zdały egzaminy 70-292 i 70-296.

egzamin kwalifikujący

Egzaminy do wyboru (wymagany jeden egzamin)

Można wybrać jeden z wymienionych poniżej tematów

MCSA (jeden do wyboru)	MCSE Geden do wyboru)	Egzaminy do wyboru	Materiały do studiowania opracowane przez Microsoft Press®	ISBN
✓	✓	Egzamin 70-227 ¹ : Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server 2000, Enterprise Edition	MCSE Zestaw szkoleniowy (Egzamin 70-227): Microsoft Internet Security and Acceleration Server 2000	0-7356-1347-8
✓	✓	Egzamin 70-228 ¹ : Installing, Configuring, and Administering Microsoft SQL Server 2000 Enterprise Edition	MCSA/MCSE/MCDBA Zestaw szkoleniowy (Egzamin 70-228): Microsoft SQL Server 2000 System Administration, Second Edition	0-7356-1961-1
	✓	Egzamin 70-229 ¹ : Designing and Implementing Databases with Microsoft SQL Server 2000 Enterprise Edition	MCAD/MCSE/MCDBA Zestaw szkoleniowy (Egzamin 70-229): Microsoft SQL Server 2000 Database Design and Implementation, Second Edition	0-7356-1960-3
✓	✓	Egzamin 70-284: Implementing and Managing Microsoft Exchange Server 2003	MCSA/MCSE Zestaw szkoleniowy (Egzamin 70-284): Implementing and Managing Microsoft Exchange Server 2003	0-7356-1899-2
	✓	Egzamin 70-297 ³ : Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure	MCSE Zestaw szkoleniowy (Egzamin 70-297): Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure	0-7356-1970-0
	✓	Egzamin 70-298 ³ : Designing Security for a Microsoft Windows Server 2003 Network	MCSE Zestaw szkoleniowy (Egzamin 70-298): Designing Security for a Microsoft Windows Server 2003 Network	0-7356-1969-7

MCSA (jeden do wyboru)	MCSE (jeden do wyboru)	Egzaminy CompTIA	Materiały do studiowania opracowane przez Microsoft Press ^{*1}	ISBN
✓	✓	CompTIA Security [*]	Security Certification Training Kit	0-7356-1822-4
		CompTIA A+ oraz CompTIA Network [*]	At Certification Training Kit, Third Edition	0-7356-1265-X
✓			Faster Smarter MC Certification Network i Certification Training Kit Faster Smarter Network [*] Certification	0-7356-1915-8
		CompTIA A+ oraz CompTIA Server ⁺	At Certification Training Kit, Third Edition	0-7356-1932-5
✓			Faster Smarter At Certification	0-7356-1915-8
			Senior Certification Training Kit	0-7356-1272-2

Aktualizacje egzaminów

Dla uzyskania certyfikatów MCSA lub MCSE dotyczących systemu Windows 2000 można zdawać następujące egzaminy będące alternatywą wymagań obowiązkowych. Informacje szczegółowe zamieszcza witryna: mm.mwiosyl.com/training

MCSA (Jeden egzamin)	MCSE (Dwa egzaminy)	Aktualizacja egzaminu	Materiały do studiowania opracowane przez Microsoft Press	ISBN
✓	✓	Egzamin 70-292: Managing and Maintaining a Microsoft Windows Server 2003 Environment for an MCSA Certified on Windows® 2000	MCSA/MCSE Zestaw szkoleniowy (Egzaminy 70-292 i 70-296): Upgrading Your Certification to Microsoft Windows Server 2003 Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 Environment	0-7356-1971-9
	✓	Egzamin 70-296: Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Environment for an MCSE Certified on Windows 2000	MCSA/MCSE Zestaw szkoleniowy (Egzaminy 70-292 i 70-296): Upgrading Your Certification to Microsoft Windows Server 2003 Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 Environment	0-7356-1971-9

¹ Kandydaci, którzy zdali egzaminy dotyczące systemu Windows NT 4.0 70-067, 70-068 oraz 70-073 mieli okazję zdawać egzamin 70-240: Microsoft Windows 2000 Accelerated Egzamin dla certyfikatu MCP dotyczącego systemu Microsoft Windows NT 4.0. Dzięki zaliczeniu tego egzaminu kandydat spełniał wymagania egzaminu MCSE 70-210. Egzaminu 70-240 nie można już zdawać.

² Egzaminy 70-297 i 70-298 w jednym przypadku mogą być zaliczane jako obowiązkowe, a w innym jako egzaminy do wyboru.

³ Egzaminy 70-297 i 70-298 w jednym przypadku mogą być zaliczane jako obowiązkowe, a w innym jako egzaminy do wyboru.

⁴ Pozycje te są dostępne w języku polskim - drugi numer ISBN.

Wymagania systemowe

Wymagania dla urządzeń sprzętu

Przeprowadzenie ćwiczeń zamieszczonych w części 1 wymaga spełnienia następujących wymagań minimalnych:

- System Microsoft Windows Server 2003 Enterprise Edition (180-dniowa wersja testowa systemu Windows Server 2003 Enterprise Edition została dołączona na dysku CD-ROM).
- System Microsoft Windows XP Professional - opcja (system nie został zamieszczony na dysku CD-ROM; oprogramowanie to jest wymagane jedynie podczas wykonywania opcjonalnych ćwiczeń praktycznych).
- Procesor minimum 133 MHz dla komputerów bazujących na serii x86 oraz minimum 733 MHz dla komputerów bazujących na procesorach Itanium (zaleca się srosowanie procesora pracującego z prędkością 733 MHz).
- Minimum 128 MB pamięci RAM (zalecane 256 MB).
- Przestrzeń dyskowa dla instalacji: 1,5 GB dla komputerów bazujących na serii x86 oraz 2,0 GB dla komputerów bazujących na procesorach Itanium.
- Monitor o rozdzielczości 800 x 600 lub wyższej.
- Napęd dysków CD-ROM lub DVD-ROM.
- Mysz Microsoft Mouse lub kompatybilne urządzenie.

Aby można było przeglądać książki elektroniczne (ebook) za pomocą komputera Pocket PC, musi on spełniać następujące minimalne wymagania systemowe:

- System Microsoft Pocket PC 2002 lub późniejsze wersje.
- Program Adobe Acrobat Reader 1.0 lub jego wersje późniejsze (wymagania systemowe dotyczące uruchamiania programu Acrobat Reader w systemie Pocket PC zamieszczone są na witrynie sieci Web firmy Adobe).
- Program ActiveSync 3.1 lub jego wersje późniejsze.
- 16 MB pamięci RAM (zalecane 32 MB)
- Wbudowana lub dodatkowa karta pamięci typu „flash”, zalecana karta to CompactFlash lub Secure Digital Media Card

Instrukcje dotyczące odinstalowania programu

Ważność dołączonej wersji systemu Microsoft Windows Server 2003 Enterprise Edition wygasa po 180 dniach od instalacji. Jeśli użytkownik decyduje się przerwać wykorzystywanie tego oprogramowania, powinien ponownie zainstalować pierwotny system operacyjny. Być może trzeba będzie ponownie formatować dysk.

