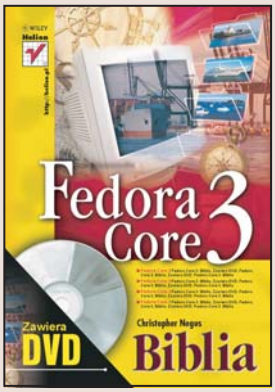
Fedora Core 3. Biblia



Autor: Christopher Negus
Tłumaczenie: Przemysław Szeremiota
ISBN: 83-7361-971-2
Tytuł oryginału: Red Hat Fedora Linux 3 Bible
Format: B5, stron: 1210

Doskonałe źródło wiedzy o najnowszej dystrybucji systemu Fedora Core

- Zaprzęgnij do pracy graficzne środowiska GNOME oraz KDE i skorzystaj z oprogramowania dołączonego do systemu
- Poznaj zasady administracji systemem, naucz się pracować z konsolą tekstową i zastosuj nowe mechanizmy bezpieczeństwa do ochrony komputera przed atakami z sieci
- Zainstaluj i skonfiguruj usługi sieciowe, serwer WWW i poczty elektronicznej oraz bazy danych

Fedora Core 3 to najnowsza wersja jednej z najpopularniejszych dystrybucji systemu Linux, znanej dawniej jako Red Hat. Obecnie nazwą Red Hat Linux opatrywane są dystrybucje rozprowadzane na zasadach komercyjnych, dystrybucję dostępną nieodpłatnie nazwano Fedora Core. Mimo zmiany polityki firmy Red Hat Inc. jej najnowszy produkt nadal pozostaje stabilnym i uniwersalnym systemem operacyjnym, wyposażonym we wszystkie nowe technologie, jakie pojawiły się w świecie Linuksa. Wykorzystano w nim najnowszą wersję jądra, doskonały mechanizm zabezpieczeń Security Enhanced Linux i najnowsze wersje oprogramowania dołączanego do kolejnych wersji tej dystrybucji Linuksa.

Książka „Fedora Core 3. Biblia" to kompletny przewodnik po najnowszej dystrybucji produktu firmy Red Hat Inc. Przeznaczona jest dla użytkowników, którzy rozpoczynają pracę z Linuksem i chcą poznać wszystkie jego możliwości, wykonując rzeczywiste zadania. Takie przedstawienie zawartych w książce wiadomości pozwala nie tylko na zapamiętanie sposobów realizacji określonych czynności, ale także na zrozumienie powiązań i wzajemnych zależności pomiędzy składnikami systemu.

Do książki dołączona została płyta DVD zawierająca najnowszą dystrybucję Fedora Core 3 wraz z setkami aplikacji i narzędzi.

Przekonaj się, że w przypadku systemów operacyjnych jakość nie musi być związana z wysoką ceną.

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

Spis treści

O Autorze **21**

Przedmowa **23**

Część I Rozpoczynamy pracę z systemem Fedora Core **33**

Rozdział 1. Wprowadzenie do systemu Fedora Core **35**

Fedora Core — wizytówka systemu 36
Czym jest Linux? 37
Uniksowe korzenie Linuksa 38
Ogólne cechy systemu Linux 41
Podstawowe zalety systemu Linux 42
Czym jest Red Hat Enterprise Linux i Fedora Core? 43
Firma Red Hat Inc. rozpoczyna projekt Fedora Project 44
Firma Red Hat Inc. skupia się na rozwoju dystrybucji Red Hat Enterprise Linux 45
Fedora Core czy Red Hat Enterprise Linux? 45
Dlaczego należy wybrać system Fedora Core lub Red Hat Enterprise Linux? 46
Nowości w dystrybucji Fedora Core 3 48
Jądro systemu Linux w wersji 2.6 50
System dźwiękowy ALSA 50
Technologia Security Enhanced Linux 50
Systemowe narzędzia konfiguracyjne 51
Serwer X i inne środowiska graficzne 52
Dodatkowe pakiety oprogramowania 52
Idea otwartej licencji oprogramowania 53
Podsumowanie 54

Rozdział 2. Instalacja systemu Fedora **55**

Szybka instalacja systemu Fedora Core 55
Instalacja systemu — krok po kroku 59
Instalacja systemu Fedora Core 3 59
Wybór metody instalacji 59
Wybór odpowiedniego sprzętu 62
Rozpoczynamy instalację 64
Fedora Setup Agent 75
Instalacja dodatkowych pakietów oprogramowania Fedora Core 77
Instalacja systemu Fedora Core — procedury specjalne 78
Inne metody rozpoczynania instalacji 78
Instalacja systemu Fedora z wykorzystaniem innych mediów 81

Rozpoczynanie instalacji VNC ... 85
Wykonywanie instalacji typu kickstart ... 86
Instalacja systemu Fedora Core — zagadnienia specjalne ... 92
Partycjonowanie dysków twardych ... 92
Odzyskiwanie wolnego miejsca z istniejących partycji ... 102
Zastosowanie programów rozruchowych GRUB lub LILO ... 105
Diagnozowanie i usuwanie problemów z instalacją ... 115
Podsumowanie ... 117

Rozdział 3. Uruchamianie środowiska graficznego ... 119
Logowanie w systemie Fedora ... 120
Uruchamianie pulpitu ... 122
Środowisko graficzne GNOME ... 132
Korzystanie z menedżera okien Metacity ... 133
Zastosowanie panelu GNOME ... 136
Korzystanie z menedżera plików Nautilus ... 141
Modyfikacja właściwości środowiska GNOME ... 144
Zarządzanie nośnikami wymiennymi ... 145
Narzędzia sieciowe GNOME ... 147
Opuszczanie środowiska GNOME ... 147
Przełączanie środowisk graficznych ... 148
Środowisko graficzne KDE ... 149
Uruchamianie środowiska KDE ... 149
Krótki opis pulpitu środowiska KDE ... 150
Zastosowanie menedżera plików Konqueror ... 153
Konfiguracja opcji menedżera plików Konqueror ... 160
Zarządzanie oknami ... 163
Konfiguracja pulpitu ... 165
Dodawanie aktywatorów aplikacji oraz typów MIME ... 168
Przygotowanie pulpitu do pracy ... 170
Po załadowaniu systemu nie uruchamia się środowisko graficzne ... 170
Konfiguracja karty graficznej i monitora ... 171
Konfiguracja kart graficznych pod kątem gier ... 173
Gdzie szukać dodatkowych informacji? ... 174
Podsumowanie ... 174

Rozdział 4. Polecenia systemu Linux ... 177
Powłoka systemu Linux ... 177
Kontrola sesji logowania ... 178
Sprawdzanie katalogów i uprawnień ... 179
Kontrola procesów systemu Linux ... 180
Kończenie pracy z powłoką ... 182
Powłoka systemu Linux ... 182
Korzystanie z powłoki systemowej ... 183
Odszukiwanie poleceń powłoki ... 184
Powtórne wykonywanie poleceń ... 187
Łączenie i rozwijanie poleceń ... 193
Zastosowanie zmiennych środowiskowych powłoki ... 196
Zarządzanie procesami pierwszo- i drugoplanowymi ... 200
Konfiguracja powłoki systemu ... 202
Praca z linuksowym systemem plików ... 206
Tworzenie plików i katalogów ... 208
Przenoszenie, kopiowanie i usuwanie plików ... 214

Edytor vi — przyjaciel czy wróg? ... 215
Pracujemy z edytorem vi ... 215
Nawigacja w dokumencie ... 219
Wyszukiwanie tekstu ... 219
Zastosowanie liczb w poleceniach ... 220
Podsumowanie ... 221

Część II Fedora w praktyce ... 223

Rozdział 5. Uruchamianie aplikacji ... 225
Fedora jako platforma aplikacyjna ... 226
Odpowiedniki aplikacji systemu Windows w systemie Linux ... 228
Pobieranie aplikacji dla systemu Fedora Core ... 230
A może poszukać na pulpicie?… ... 230
Poszukiwanie aplikacji w sieci internetowej ... 230
Pobieranie i instalowanie aplikacji za pomocą programu yum ... 232
Pobieranie oprogramowania dla systemu Linux ... 235
Konwencje nazywania pakietów oraz ich formaty ... 237
Korzystanie z innych formatów pakietów i dokumentów ... 239
Instalowanie aplikacji w systemie Fedora Core ... 241
Instalacja pakietów RPM i zarządzanie nimi ... 241
Kompilacja oraz instalacja aplikacji z kodu źródłowego ... 252
Uruchamianie aplikacji dla X Window System ... 255
Uruchamianie aplikacji z menu systemowego ... 255
Uruchamianie aplikacji z okna Uruchom program ... 256
Uruchamianie aplikacji z okna terminala ... 257
Uruchamianie zdalnych aplikacji X ... 258
Zastosowanie emulatorów do uruchamiania aplikacji z innych systemów operacyjnych ... 263
Uruchamianie aplikacji przeznaczonych dla systemu DOS ... 265
Zastosowanie pakietu WINE do uruchamiania aplikacji przeznaczonych dla systemu Windows ... 268
Zastosowanie pakietu ARDI Executor do uruchamiania aplikacji przeznaczonych dla komputerów Macintosh ... 274
Podsumowanie ... 275

Rozdział 6. Tworzenie dokumentów w systemie Fedora Core ... 277
Pakiet biurowy OpenOffice.org ... 278
Inne edytory tekstu ... 280
Pakiet StarOffice ... 281
Edytor tekstu AbiWord ... 282
Pakiet KOffice ... 282
Zastosowanie tradycyjnych narzędzi systemu Linux do publikacji dokumentów ... 283
Tworzenie dokumentów przy użyciu systemów składu Groff oraz LaTeX ... 285
Przetwarzanie tekstu przy użyciu systemu składu Groff ... 285
Przetwarzanie tekstu przy użyciu procesora TeX/LaTeX ... 296
Metody konwersji dokumentów ... 300
Tworzenie dokumentów typu DocBook ... 302
Kilka słów o SGML oraz XML ... 302
Drukowanie dokumentów w systemie Fedora Core ... 306
Korzystanie z domyślnej drukarki systemowej ... 307
Drukowanie plików z poziomu powłoki systemu ... 307

Kontrola stanu kolejek wydruku ... 308
Usuwanie zadań drukowania z kolejki ... 309
Sprawdzanie stanu drukarki ... 309
Wyświetlanie dokumentów przy użyciu pakietów Ghostscript oraz Acrobat ... 310
Zastosowanie poleceń ghostscript oraz gv ... 310
Zastosowanie przeglądarki Adobe Acrobat Reader ... 311
Programy graficzne w systemie Fedora ... 311
Przetwarzanie plików graficznych przy użyciu programu GIMP ... 312
Wykonywanie zrzutów ekranu ... 314
Przetwarzanie plików graficznych przy użyciu programu KolourPaint ... 315
Skanowanie dokumentów przy użyciu pakietu SANE ... 316
Podsumowanie ... 317

Rozdział 7. Gry i zabawy w systemie Fedora ... 319
Gry w systemie Linux? Ależ oczywiście! ... 320
Gdzie można znaleźć informacje na temat gier w systemie Linux? ... 320
Gry przeznaczone dla systemu Linux ... 321
Dobór karty graficznej obsługującej gry ... 322
Gry w środowisku X ... 323
Gry dla środowiska GNOME ... 323
Gry dla środowiska KDE ... 326
Gry komercyjne w systemie Linux ... 334
Gry firmy id Software ... 334
Pakiet TransGaming Cedega ... 336
Wersje demonstracyjne gier firmy Loki Software ... 339
Civilization: Call to Power ... 340
Myth II: Soulblighter ... 341
Heretic II ... 342
Neverwinter Nights ... 342
Podsumowanie ... 343

Rozdział 8. Fedora a multimedia ... 345
Odtwarzanie audio w systemie Linux ... 345
Konfiguracja karty dźwiękowej ... 348
Wybór odtwarzacza płyt Audio CD ... 349
Zastosowanie odtwarzacza MIDI ... 358
Konwersja oraz kompresowanie plików audio ... 359
Karty TV i kamery internetowe w systemie Linux ... 363
Oglądanie TV przy użyciu programu Tvtime ... 363
Prowadzenie wideokonferencji przy użyciu pakietu GnomeMeeting ... 366
Odtwarzanie wideo w systemie Linux ... 368
Odtwarzacz plików wideo xine ... 369
Odtwarzacz RealPlayer ... 372
Obsługa cyfrowych aparatów fotograficznych ... 373
Użycie aparatu cyfrowego w roli urządzenia przechowującego dane ... 374
Nagrywanie dysków Audio CD ... 375
Tworzenie płyt Audio CD przy użyciu polecenia cdrecord ... 376
Nagrywanie płyt CD i DVD za pomocą programu K3b ... 377
Zapisywanie zawartości płyt Audio CD na dysku ... 379
Tworzenie etykiet dysków CD przy użyciu polecenia cdlabelgen ... 380
Podsumowanie ... 382

Rozdział 9. Narzędzia umożliwiające korzystanie z sieci internetowej i sieci WWW 383
Korzystanie z narzędzi obsługi sieci WWW 384
Przeglądanie zasobów sieci WWW 385
Adresy URL 385
Strony WWW 387
Przeglądanie witryn WWW za pomocą aplikacji Mozilla 388
Korzystanie z przeglądarki Mozilla Firefox 398
Korzystanie z przeglądarek WWW pracujących w trybie tekstowym 401
Komunikacja z wykorzystaniem poczty elektronicznej 402
Podstawy obsługi poczty elektronicznej 403
Klient pocztowy Evolution 404
Klient pocztowy Mozilla Mail 407
Program pocztowy Thunderbird 410
Programy pocztowe pracujące w trybie tekstowym 411
Narzędzia odczytywania i zarządzania wiadomościami poczty elektronicznej 411
Korzystanie z grup dyskusyjnych 413
Obsługa grup dyskusyjnych z wykorzystaniem pakietu Mozilla 413
Program odczytywania wiadomości grup dyskusyjnych Pan 416
Korzystanie z komunikatorów internetowych — program Gaim 416
Korzystanie z poleceń zdalnego logowania, kopiowania i uruchamiania programów 417
Korzystanie z polecenia telnet do zdalnego logowania 418
Kopiowanie plików za pomocą FTP 419
Pobieranie plików za pomocą wget 425
Korzystanie z ssh do zdalnego logowania i uruchamiania poleceń 427
Zastosowanie polecenia scp do zdalnego kopiowania plików 428
Korzystanie z poleceń „r": rlogin, rcp i rsh 428
Podsumowanie 429

Część III Zarządzanie systemem Fedora 431

Rozdział 10. Podstawy zarządzania systemem 433
Użytkownik root 434
Jak zostać superużytkownikiem (polecenie su) 434
Polecenia i graficzne narzędzia administracyjne, pliki konfiguracyjne oraz dzienniki zdarzeń 436
Narzędzia administracyjne dysponujące graficznym interfejsem użytkownika 437
Polecenia administracyjne 440
Administracyjne pliki konfiguracyjne 441
Pliki dzienników administracyjnych 446
Korzystanie z innych kont administracyjnych 446
Administrowanie systemem Fedora 449
Konfiguracja urządzeń 450
Modyfikowanie konfiguracji sprzętowej z wykorzystaniem kudzu 450
Konfigurowanie modułów 451
Zarządzanie systemem plików i przestrzenią dyskową 454
Montowanie systemów plików 457
Korzystanie z polecenia mkfs do tworzenia systemu plików 464
Dodawanie dysku twardego 464
Zastosowanie macierzy RAID 467
Sprawdzanie przestrzeni systemowej 469

Monitorowanie wydajności systemu ... 471
Analiza wykorzystania komputera za pomocą narzędzia Monitor systemu ... 471
Monitorowanie wykorzystania procesora za pomocą top ... 472
Monitorowanie wykorzystania zasilania laptopów ... 473
Wybór alternatywnego oprogramowania ... 476
Wybór alternatywnych rozwiązań poczty elektronicznej i drukowania ... 476
Korzystanie z alternatywnych usług przesyłania poczty ... 478
Uaktualnianie oprogramowania Linux ... 478
Pobieranie uaktualnień ze zbiorów oprogramowania dla systemu Fedora Core ... 478
Narzędzie powiadamiające Red Hat Network ... 479
Rejestrowanie na stronie Red Hat Network ... 479
Pobieranie uaktualnień ... 481
Aktualizowanie systemu za pomocą programu yum ... 483
Korzystanie z Red Hat Network ... 484
Podsumowanie ... 484

Rozdział 11. Konfigurowanie kont użytkowników i zarządzanie nimi ... 487
Tworzenie kont użytkowników ... 488
Dodawanie użytkowników za pomocą useradd ... 488
Dodawanie kont użytkowników za pomocą narzędzia Menedżer użytkowników ... 492
Konfigurowanie ustawień domyślnych ... 494
Definiowanie początkowych skryptów logowania ... 496
Początkowy plik .bashrc ... 496
Początkowy plik .tcshrc ... 497
Konfigurowanie globalnych opcji powłoki systemowej ... 498
Konfigurowanie profili systemowych ... 499
Tworzenie przenośnych pulpitów ... 500
Obsługa użytkowników ... 501
Tworzenie skrzynki pocztowej wsparcia technicznego ... 501
Zmiana hasła użytkownika ... 502
Modyfikowanie ustawień kont użytkowników ... 503
Modyfikowanie ustawień konta użytkownika za pomocą polecenia usermod ... 503
Modyfikowanie ustawień kont użytkowników za pomocą okna Menedżer użytkowników ... 505
Usuwanie kont użytkowników ... 506
Usuwanie kont użytkowników z wykorzystaniem polecenia userdel ... 506
Usuwanie kont użytkowników za pomocą okna Menedżer użytkowników ... 507
Sprawdzanie wykorzystania przestrzeni dyskowej ... 508
Limit zasobów dyskowych jako metoda kontroli przestrzeni dyskowej ... 508
Korzystanie z polecenia du do kontroli wykorzystania dysku ... 512
Automatyczne usuwanie plików tymczasowych ... 513
Wysyłanie wiadomości e-mail do użytkowników ... 513
Podsumowanie ... 515

Rozdział 12. Automatyzacja zadań systemowych ... 517
Skrypty powłoki systemowej ... 518
Uruchamianie i debugowanie skryptów powłoki ... 518
Zmienne powłoki ... 519
Wykonywanie operacji arytmetycznych w skryptach powłoki ... 521
Wykorzystywanie struktur programistycznych w skryptach powłoki ... 522
Kilka przydatnych poleceń zewnętrznych ... 527
Tworzenie prostych skryptów powłoki ... 529

Inicjalizacja systemu ... 530
Uruchamianie procesu init ... 531
Plik inittab ... 531
Uruchamianie i zamykanie systemu ... 535
Uruchamianie skryptów startowych ... 535
Zrozumienie skryptów startowych ... 536
Zrozumienie działania skryptów startowych ... 538
Zmiana zachowania skryptu startowego ... 540
Reorganizacja i usuwanie skryptów poziomu uruchamiania ... 541
Dodawanie skryptów startowych własnych usług ... 542
Zarządzanie usługami xinetd ... 543
Manipulowanie poziomami uruchamiania ... 544
Planowanie zadań systemowych ... 546
Korzystanie z at.allow i at.deny ... 546
Określanie czasu uruchamiania zadań ... 546
Przekazywanie zaplanowanych zadań ... 546
Przeglądanie zaplanowanych zadań ... 548
Usuwanie zaplanowanych zadań ... 548
Korzystanie z polecenia batch ... 548
Korzystanie z narzędzia cron ... 549
Podsumowanie ... 552

Rozdział 13. Tworzenie kopii bezpieczeństwa i przywracanie plików ... 553

Wykonywanie podstawowej archiwizacji przy użyciu narzędzia rsync ... 554
Lokalna archiwizacja plików ... 555
Zdalna archiwizacja plików ... 556
Wybór strategii tworzenia kopii bezpieczeństwa ... 557
Pełna kopia bezpieczeństwa ... 557
Przyrostowa kopia bezpieczeństwa ... 558
Tworzenie kopii lustrzanej ... 558
Sieciowa kopia bezpieczeństwa ... 558
Wybór nośnika kopii bezpieczeństwa ... 559
Taśma magnetyczna ... 560
Zapisywalne dyski CD ... 562
Zapisywalne dyski DVD ... 565
Tworzenie kopii bezpieczeństwa na dysku twardym ... 566
Instalowanie mirrordir do klonowania katalogów ... 567
Klonowanie katalogu za pomocą mirrordir ... 567
Automatyczne tworzenie kopii lustrzanych ... 568
Tworzenie kopii bezpieczeństwa za pomocą polecenia dump ... 568
Tworzenie kopii bezpieczeństwa ... 569
Poziomy operacji dump ... 571
Automatyzacja tworzenia kopii bezpieczeństwa z wykorzystaniem narzędzia cron ... 572
Przywracanie plików z kopii bezpieczeństwa ... 574
Przywracanie całego systemu plików ... 574
Odzyskiwanie poszczególnych plików ... 576
Konfigurowanie narzędzia Amanda do wykonywania sieciowych kopii bezpieczeństwa ... 578
Tworzenie pliku amanda.conf ... 580

Tworzenie pliku disklist ... 582
Dodawanie usług sieciowych narzędzia Amanda ... 582
Wykonywanie kopii bezpieczeństwa narzędziem Amanda ... 583
Korzystanie z narzędzia archiwizacji pax ... 584
Podsumowanie ... 587

Rozdział 14. Bezpieczeństwo systemu ... 589
Haker a włamywacz ... 589
Metody ataku ... 590
Ochrona przed atakami „odmowa usługi" ... 591
Mailbombing ... 591
Blokowanie spamu ... 593
Smurfing — wzmożony atak ... 594
Metody obrony przed atakami DDoS ... 595
Obrona przed atakami intruzów ... 599
Analizowanie dostępu do usług sieciowych ... 599
Blokowanie usług sieciowych ... 600
Korzystanie z pośrednictwa TCP ... 602
Ochrona sieci z wykorzystaniem zapór sieciowych ... 604
Konfigurowanie zapory filtrującej — iptables ... 605
Wykrywanie włamań na podstawie plików dzienników ... 617
Rola syslogd ... 619
Przekierowywanie wiadomości dzienników za pomocą syslogd ... 619
Zrozumienie wiadomości logfile ... 620
Monitorowanie plików dzienników z wykorzystaniem LogSentry ... 621
Pobieranie i instalowanie LogSentry ... 622
Instalowanie LogSentry ... 622
Uruchamianie LogSentry ... 623
Korzystanie z LogSentry ... 623
Dopasowywanie LogSentry do potrzeb danego systemu ... 624
Ochrona hasłem ... 630
Wybór dobrego hasła ... 631
Korzystanie z pliku haseł ukrytych ... 632
Wykorzystanie metod szyfrowania ... 634
Kryptografia symetryczna ... 634
Kryptografia klucza publicznego ... 635
Protokół SSL (ang. Secure Socket Layer) ... 635
Korzystanie z pakietu Secure Shell ... 643
Uruchamianie usługi SSH ... 644
Korzystanie z poleceń ssh, sftp i scp ... 644
Korzystanie z poleceń ssh, sftp i scp bez podawania hasła ... 646
Ochrona komputera z wykorzystaniem PortSentry ... 647
Pobieranie i instalowanie PortSentry ... 647
Korzystanie z PortSentry ... 648
Konfigurowanie PortSentry ... 648
Testowanie PortSentry ... 653
Śledzenie włamań PortSentry ... 654
Przywracanie dostępu ... 655
Podsumowanie ... 655

Część IV Konfiguracja usług sieciowych serwera Fedora 657

Rozdział 15. Konfiguracja sieci lokalnej LAN 659

Sieci lokalne 659
Konfiguracja urządzeń sieci lokalnej 660
Konfigurowanie protokołu TCP/IP sieci lokalnej 665
Tworzenie i konfiguracja bezprzewodowej sieci lokalnej 670
Sieci bezprzewodowe 671
Dobór komponentów sieci bezprzewodowych 673
Instalacja sterownika interfejsu sieci bezprzewodowej 676
Instalowanie oprogramowania sieci bezprzewodowej 678
Konfiguracja bezprzewodowej sieci lokalnej 679
Pomiar zasięgu sieci 685
Modyfikowanie ustawień związanych z obsługą sieci bezprzewodowych 685
Adresy IP 687
Klasy adresów IP 687
Maski sieciowe 688
Routing bezklasowy CIDR (ang. Classless Inter-Domain Routing) 689
Uzyskiwanie adresów IP 690
Rozwiązywanie problemów z siecią lokalną 691
Czy system Linux w trakcie uruchamiania odnalazł sterownik karty sieciowej? 691
Czy można się połączyć z innym komputerem znajdującym się w sieci lokalnej? 692
Czy karta sieciowa Ethernet jest aktywna? 693
Rozwiązywanie problemów z bezprzewodowymi sieciami lokalnymi 694
Monitorowanie natężenia ruchu w sieci lokalnej LAN przy użyciu programu Ethereal 698
Podsumowanie 703

Rozdział 16. Podłączenie do internetu 705

Struktura internetu 706
Domeny internetowe 708
Nazwy i adresy IP komputerów 710
Routing 711
Usługa proxy 712
Łączenie się z internetem za pomocą modemu 712
Uzyskiwanie wymaganych parametrów 712
Konfiguracja połączenia PPP 714
Tworzenie połączenia telefonicznego przy użyciu kreatora Internet Configuration Wizard 714
Uruchamianie połączenia PPP 717
Uruchamianie połączenia PPP na żądanie 717
Testowanie połączenia PPP 718
Połączenie sieci lokalnej z internetem 724
Konfiguracja komputera z systemem Fedora Core jako routera 725
Konfiguracja funkcji routingu systemu Fedora Core 726
Konfiguracja klientów 729
Konfiguracja klientów wyposażonych w system Windows 730
Konfiguracja wirtualnej sieci prywatnej VPN (ang. Virtual Private Network) 731
Protokół IPsec 732
Zastosowanie protokołu IPsec 733
Zastosowanie protokołu IPsec w dystrybucji Fedora Core 734

Konfiguracja komputera z systemem Fedora Core jako serwera proxy ... 735
Uruchamianie modułu squid ... 736
Prosty plik konfiguracyjny squid.conf ... 738
Modyfikacja pliku konfiguracyjnego serwera Squid ... 739
Diagnozowanie serwera Squid ... 744
Konfiguracja klientów proxy ... 745
Konfiguracja przeglądarki Mozilla pod kątem wykorzystania usługi proxy ... 746
Konfiguracja przeglądarki Internet Explorer pod kątem wykorzystania usługi proxy ... 747
Konfiguracja innych przeglądarek pod kątem wykorzystania usługi proxy ... 748
Podsumowanie ... 749

Rozdział 17. Konfiguracja serwera druku ... 751
CUPS (Common UNIX Printing Service) ... 752
Konfiguracja drukarek ... 753
Konfiguracja drukarek lokalnych ... 754
Konfigurowanie drukarek sieciowych ... 757
Usługa wydruku CUPS ... 762
Administrowanie usługą CUPS przy użyciu przeglądarki internetowej ... 762
Konfigurowanie serwera CUPS (plik cupsd.conf) ... 764
Konfigurowanie opcji drukarki CUPS ... 766
Polecenia obsługujące drukowanie ... 767
Drukowanie przy użyciu programu lpr ... 767
Wyświetlanie statusu przy użyciu programu lpc ... 768
Usuwanie zadań wydruku przy użyciu polecenia lprm ... 768
Konfiguracja serwerów wydruku ... 769
Konfigurowanie współdzielonej drukarki CUPS ... 769
Konfiguracja drukarki udostępnionej przez serwer Samba ... 771
Podsumowanie ... 773

Rozdział 18. Konfiguracja serwera plików ... 775
Dlaczego warto skonfigurować serwer plików? ... 775
Konfiguracja serwera plików NFS ... 776
Udostępnianie systemu plików przez serwer NFS ... 778
Systemy plików NFS ... 785
Odmontowanie systemu plików NFS ... 791
Inne interesujące możliwości usługi NFS ... 792
Konfiguracja serwera plików Samba ... 793
Instalacja pakietu Samba ... 794
Konfigurowanie prostego serwera plików Samba ... 794
Konfigurowanie serwera Samba przy użyciu narzędzia SWAT ... 798
Pliki i polecenia serwera Samba ... 808
Konfigurowanie klientów serwera Samba ... 811
Rozwiązywanie problemów z serwerem Samba ... 814
Podsumowanie ... 816

Rozdział 19. Konfiguracja serwera poczty ... 817
Omówienie protokołu SMTP i serwera sendmail ... 818
Instalacja i uruchomienie serwera sendmail ... 819
Uruchamianie serwera sendmail ... 819
Inne programy ... 820
Rejestracja zdarzeń związanych z działaniem serwera sendmail ... 821

Konfiguracja serwera sendmail ... 822
Uzyskanie nazwy domeny ... 823
Określanie podstawowych ustawień serwera sendmail (plik sendmail.mc) ... 824
Definiowanie dostępu do wiadomości wychodzących ... 828
Konfigurowanie wirtualnych serwerów ... 829
Konfigurowanie kont wirtualnych użytkowników ... 830
Dodawanie kont użytkowników ... 831
Uruchomienie serwera sendmail i wygenerowanie plików bazy danych ... 832
Przekierowywanie wiadomości ... 833
Serwer Postfix ... 835
Rozpoznawanie spamu przy użyciu programu SpamAssassin ... 836
Zastosowanie programu SpamAssassin na własnym serwerze pocztowym ... 837
Konfigurowanie klienta pocztowego pod kątem filtracji spamu ... 839
Pobieranie wiadomości z serwera poczty (protokoły IMAP i POP3) ... 840
Dostęp do skrzynek pocztowych serwera poczty działającego w systemie Linux ... 841
Konfiguracja usług POP3 i IMAP przy użyciu usługi dovecot ... 842
Pobieranie wiadomości z poziomu przeglądarki internetowej przy użyciu narzędzia Squirrelmail ... 843
Administrowanie listą dystrybucyjną przy użyciu narzędzia mailman ... 845
Podsumowanie ... 847

Rozdział 20. Konfiguracja serwera FTP ... 849

Serwery FTP ... 850
Funkcje serwera FTP ... 850
Typy użytkowników serwera FTP ... 851
Zastosowanie serwera vsFTPd ... 852
„Szybkie" uruchomienie serwera vsFTPd ... 852
Konfiguracja serwera vsFTPd ... 853
Dodatkowe informacje na temat serwerów FTP ... 858
Podsumowanie ... 859

Rozdział 21. Konfiguracja serwera WWW ... 861

Podstawowe informacje na temat serwerów WWW ... 862
Serwer Apache ... 862
Serwer TUX ... 863
Inne serwery WWW przeznaczone dla systemu Fedora Core ... 864
„Szybkie" uruchomienie serwera Apache ... 865
Konfiguracja serwera Apache ... 867
Konfiguracja serwera WWW (plik httpd.conf) ... 868
Konfigurowanie modułów i powiązanych z nimi usług (pliki /etc/httpd/conf.d/*.conf) ... 898
Zatrzymywanie i uruchamianie serwera Apache ... 899
Monitorowanie pracy serwera ... 901
Wyświetlanie informacji na temat serwera ... 901
Wyświetlanie statusu serwera ... 901
Dodatkowa kontrola dostępu do strony Server Info i Server Status ... 903
Rejestrowanie błędów ... 903
Rejestrowanie żądań ... 904
Analiza danych przetwarzanych przez serwer WWW ... 905
Podsumowanie ... 906

Rozdział 22. Konfiguracja serwera adresowego LDAP 907
Protokół LDAP 908
Definiowanie informacji w schematach 909
Tworzenie struktury katalogów LDAP 910
Zastosowanie serwera OpenLDAP 911
Instalowanie pakietów serwera OpenLDAP 911
Konfigurowanie serwera OpenLDAP (plik slapd.conf) 911
Uruchamianie usługi serwera OpenLDAP 913
Tworzenie książki adresowej LDAP 914
Inne zadania związane z konfigurowaniem katalogu LDAP 918
Korzystanie z książki adresowej przy użyciu programu Mozilla Mail 920
Podsumowanie 921

Rozdział 23. Konfiguracja serwera DHCP i NIS 923
Zastosowanie protokołu DHCP (ang. Dynamic Host Configuration Protocol) 924
Konfigurowanie serwera DHCP 924
Konfiguracja zapory sieciowej pod kątem serwera DHCP 925
Konfiguracja pliku dhcpd.conf 925
Uruchamianie serwera DHCP 931
Konfiguracja klienta DHCP 932
Usługa NIS (ang. Network Information Service) 934
Konfiguracja komputera z systemem Fedora Core jako klienta NIS 936
Określenie nazwy domeny NIS 936
Konfiguracja pliku /etc/yp.conf 937
Konfiguracja modułów klienta NIS 938
Kontrola poprawności działania usługi NIS 938
Zastosowanie map usługi NIS 939
Konfiguracja komputera z systemem Fedora Core jako serwera nadrzędnego NIS 940
Tworzenie map usługi NIS 940
Konfiguracja komputera z systemem Fedora Core jako serwera podrzędnego NIS 944
NIS a usługi katalogowe Windows 945
Podsumowanie 945

Rozdział 24. Konfiguracja serwera baz danych MySQL 947
Pakiety serwera MySQL 948
Konfiguracja serwera MySQL 948
Zastosowanie konta użytkownika i grupy o nazwie mysql 949
Tworzenie kont administracyjnych 949
Definiowanie opcji serwera MySQL 950
Zastosowanie przykładowych plików my.cnf 955
Uruchomienie serwera MySQL 957
Kontrola poprawności działania serwera MySQL 957
Praca z bazami danych serwera MySQL 958
Uruchomienie polecenia mysql 958
Tworzenie bazy danych przy użyciu polecenia mysql 960
Wprowadzanie danych do tabeli bazy danych serwera MySQL 961
Tabele bazy danych serwera MySQL 964
Wyświetlanie danych zawartych w bazie danych MySQL 969
Wyświetlanie wszystkich lub wybranych rekordów 970
Wyświetlanie wybranych kolumn 971
Sortowanie danych 971

Modyfikowanie tabel oraz ich rekordów ... 972
Modyfikacja struktury tabel bazy danych MySQL ... 972
Aktualizowanie i usuwanie rekordów bazy danych serwera MySQL ... 973
Dodawanie i usuwanie użytkowników ... 974
Dodawanie użytkowników i nadawanie im uprawnień ... 974
Odbieranie uprawnień ... 975
Wykonywanie kopii zapasowych baz danych ... 976
Kontrola i naprawianie baz danych ... 976
Podsumowanie ... 978

Rozdział 25. Publiczne udostępnianie usług sieciowych przy użyciu serwera DNS ... 979
Określenie przeznaczenia serwera ... 980
Korzystanie z usług zewnętrznych firm internetowych ... 980
Podłączenie serwera publicznego ... 981
Wybór dostawcy usług internetowych ... 982
Rejestracja nazwy domeny ... 984
Konfiguracja serwera publicznego ... 987
Konfiguracja sieci ... 987
Konfiguracja serwerów ... 988
Zarządzanie zabezpieczeniami ... 989
Instalacja i konfiguracja serwera DNS ... 991
Serwer DNS ... 992
Serwer DNS — przykład ... 995
„Szybkie" uruchomienie serwera DNS ... 996
Kontrola poprawności pracy serwera DNS ... 1005
Dodatkowe źródła informacji na temat serwera BIND ... 1006
Podsumowanie ... 1006

Rozdział 26. Współpraca systemów Macintosh z serwerem Linux ... 1009
System Mac OS X od wnętrza ... 1010
Usługi sieciowe systemu Mac OS X ... 1011
Zastosowanie protokołu AppleTalk (pakiet netatalk) w systemie Mac OS X ... 1012
Zastosowanie protokołu AppleTalk w systemach Mac OS 8 i OS 9 ... 1013
Serwer Samba (komputery z systemami Windows i Linux) ... 1014
Współużytkowanie aplikacji środowiska graficznego X ... 1015
Konfigurowanie serwera AppleTalk w systemie Linux ... 1015
Co należy wiedzieć przed uruchomieniem serwera netatalk? ... 1016
Konfigurowanie serwera netatalk ... 1017
Zabezpieczanie udziałów serwera netatalk ... 1022
Rozwiązywanie problemów z serwerem netatalk ... 1029
Dostęp do serwerów NFS z komputerów z systemem Mac ... 1030
Łączenie się z serwerem NFS przy użyciu okna Connect to Server ... 1031
Łączenie się z serwerem NFS z poziomu wiersza poleceń ... 1032
Podsumowanie ... 1033

Część V Nowe technologie ... 1035

Rozdział 27. Zapoznanie się z jądrem systemu Linux w wersji 2.6 ... 1037
Podstawowe informacje na temat jądra ... 1038
Sprawdzenie aktualnie używanego jądra ... 1038
Katalog /sys ... 1040

Innowacje związane z wydajnością stacji roboczych ... 1040
Innowacje związane z obsługą laptopów ... 1042
Innowacje związane z wydajnością serwerów ... 1042
Innowacje związane z obsługą sprzętu ... 1043
Obsługa urządzeń USB ... 1043
Korzystanie ze starszych urządzeń ... 1044
Zastosowanie jądra w wersji 2.6 poza systemem Fedora Core ... 1044
Uruchamianie jądra w wersji 2.6 na urządzeniach wbudowanych ... 1045
Zastosowanie jądra systemu Linux w wersji 2.6 w innych architekturach ... 1045
Podsumowanie ... 1046

Rozdział 28. Zastosowanie technologii Security Enhanced Linux ... 1047
Technologia Security Enhanced Linux ... 1048
Typy i role w SELinux ... 1049
Użytkownicy ... 1049
Reguły ... 1050
Narzędzia SELinux ... 1050
Zastosowanie technologii SELinux w systemie Fedora Core 3 ... 1051
Instalacja oprogramowania SELinux ... 1051
Sprawdzanie aktywności technologii SELinux ... 1052
Kontrola stanu rozszerzenia SELinux ... 1053
Modyfikowanie zestawów reguł SELinux ... 1055
Dodatkowe informacje na temat technologii SELinux ... 1056
Podsumowanie ... 1057

Dodatki ... 1059

Dodatek A Zawartość płyty DVD ... 1061

Dodatek B Pakiety RPM systemu Fedora Core 3 ... 1065

Dodatek C Uruchamianie usług sieciowych ... 1125

Dodatek D Publiczna licencja GNU ... 1147

Skorowidz ... 1153

Rozdział 13.
Tworzenie kopii bezpieczeństwa i przywracanie plików

W tym rozdziale:

- Wykonywanie podstawowej archiwizacji
- Wybór strategii tworzenia kopii bezpieczeństwa
- Wybór nośnika kopii bezpieczeństwa
- Tworzenie kopii bezpieczeństwa na dysk twardy
- Tworzenie kopii bezpieczeństwa za pomocą polecenia `dump`
- Automatyczne tworzenie kopii bezpieczeństwa narzędziem *cron*
- Przywracanie plików z kopii bezpieczeństwa
- Tworzenie kopii bezpieczeństwa przez sieć
- Wykonywanie sieciowych kopii zapasowych większej liczby komputerów
- Korzystanie z narzędzia *pax archiving*

Jeśli kiedykolwiek zdarzyło Ci się przeżyć awarię dysku twardego, wiesz, jak poważne może mieć to konsekwencje. Możesz utracić niezwykle ważne dane. Prawie na pewno spędzisz niezliczone godziny, próbując na nowo zainstalować system operacyjny i aplikacje. Nie jest to ciekawe, ani zabawne doświadczenie. Wystarczy, że zdarzy się tylko raz, a nauczysz się, jak wielkie znaczenie ma regularne wykonywanie kopii zapasowych ważnych danych.

Obecnie coraz lepsze i szybsze narzędzia do tworzenia kopii zapasowych mogą pomóc w uproszczeniu procesu wykonywania kopii bezpieczeństwa danych. System Fedora Linux obsługuje wiele różnych rodzajów nośników — takich jak nagrywalne dyski CD-ROM (np. CD-R), DVD (np. DVD+RW i DVD-RW) i taśmy magnetyczne — umożliwiających tworzenie kopii zapasowych. Korzystając z narzędzi, takich jak `cron`, możesz tak skonfigurować system, aby tworzenie kopii zapasowych było regularne i automatyczne.

Niniejszy rozdział opisuje sposób tworzenia strategii oraz wyboru nośników dla kopii zapasowych w systemie Fedora Linux. Dowiesz się, jak automatycznie tworzyć kopie zapasowe oraz kopie zapasowe przez sieć. Opiszę również sposoby przywracania z kopii bezpieczeństwa poszczególnych plików lub całego systemu plików przy użyciu narzędzi, takich jak polecenie `restore`.

Wykonywanie podstawowej archiwizacji przy użyciu narzędzia rsync

Tania przestrzeń dysków twardych, szybkie połączenia sieciowe i kilka naprawdę solidnych nowych narzędzi — wszystko to sprawiło, że użytkownicy systemu Linux otrzymali kilka wartościowych metod archiwizacji danych zastępujących wysłużone rozwiązanie oparte na niezawodnych przenośnych nośnikach, takich jak taśmy i dyski CD. W celu zarchiwizowania prywatnych danych lub znajdujących się na komputerze niewielkiej firmy można będzie skorzystać z przykładów zawartych w tym podrozdziale, prezentują one proste metody tworzenia pewnych kopii zapasowych danych.

Aby wykonać procedurę archiwizacji, musisz dysponować wolną przestrzenią dyskową, która przynajmniej nieznacznie przekracza pojemność dysku twardego, dla którego zostanie sporządzona kopia zapasowa danych. Wolna przestrzeń dyskowa może:

- **znajdować się na innej partycji dysku** — przez umieszczenie kopii zapasowej na oddzielnej partycji uzyskamy dodatkowe zabezpieczenie danych na wypadek uszkodzenia archiwizowanej partycji; jednak zabezpieczenie to nie chroni przed awarią całego dysku twardego,
- **znajdować się na innym dysku twardym** — przez umieszczenie kopii zapasowej na innym dysku twardym uzyskamy dodatkowe zabezpieczenie danych na wypadek awarii dysku, które jednak nie uchroni danych, gdy komputer padnie ofiarą kataklizmu (np. uderzenia pioruna, powodzi itp.),
- **znajdować się na innym komputerze** — przez wykonanie archiwizacji za pośrednictwem sieci możliwe jest wykonanie kopii zapasowej danych umieszczonych na innym komputerze, znajdującym się w znacznej odległości od komputera źródłowego, a przy okazji zwiększenie pewności. Możliwe jest wykonanie archiwizacji danych znajdujących się na komputerze stojącym na korytarzu lub na drugim końcu kraju.

Właściwa procedura archiwizacji jest wykonywana przy użyciu polecenia `rsync`. Przypomina ono polecenie zdalnego kopiowania `rcp`. Zasadniczo polecenie `rsync` pozwala skopiować pliki z jednego miejsca w drugie. Jednak oferuje też kilka przydatnych dodatkowych funkcji, które umożliwiają wykonanie następujących czynności.

- **Przesyłanie jedynie różnic zaistniałych w plikach** — jeśli rozpocznie się przesyłanie pliku, który był już poddany tej operacji w ramach wcześniejszej archiwizacji, to polecenie `rsync` w celu określenia różnic zaistniałych między starą i nową wersją pliku zastosuje algorytm szukania sumy kontrolnej, a następnie prześle jedynie te dane, które będą różniły obie wersje pliku.

- **Bezpieczne przesyłanie danych** — polecenie `rsync` w połączenie z narzędziem `ssh` lub inną zdalną powłoką systemową zaszyfruje dane, a zatem będą one mogły zostać przesłane w sieci w bezpieczny sposób.
- **Zarządzanie prawami właściciela** — przesyłane pliki mogą utrzymać swoje oryginalne uprawnienia, prawa właściciela i członkostwo w grupach. Ze względu na to, że prawo właściciela jest oparte na liczbowych identyfikatorach UID i GID, konieczne jest utworzenie na docelowym komputerze identycznych jak na komputerze źródłowym kont użytkowników i grup, aby po skopiowaniu plików ich właścicielami byli ci sami użytkownicy i grupy.

W kolejnych podrozdziałach znajdziesz przykłady zastosowania polecenia `rsync`.

Lokalna archiwizacja plików

Pierwszy przykład prezentuje prostą archiwizację prywatnych plików użytkownika. Skopiowana zostanie zawartość katalogu */home/kuba* (wszystkie pliki i podkatalogi) do innego katalogu znajdującego się na tym samym komputerze. Docelowy katalog może znajdować się na oddzielnej partycji (w rozdziale 2. zawarto informacje na temat tworzenia niezależnych partycji), innym dysku twardym (w rozdziale 10. umieszczono więcej informacji dotyczących dysków twardych) lub w zdalnym systemie plików NFS (w rozdziale 18. można znaleźć informacje na temat podłączania tego typu systemu plików).

```
# rsync -av /home/kuba /mnt/backup/homes/
```

Zauważ, że nazwa katalogu */home/kuba* nie kończy się znakiem ukośnika (jak w */home/kuba/*). Dzięki temu program `rsync` skopiuje pliki znajdujące się w tym katalogu do katalogu docelowego o nazwie *kuba* (*/mnt/backup/homes/kuba*). Gdyby nazwę katalogu źródłowego zakończyć ukośnikiem, pliki z katalogu źródłowego zostałyby skopiowane wprost do */mnt/backup/homes*.

W powyższym przykładzie cała zawartość katalogu */home/kuba* została skopiowana do katalogu */mnt/backup/homes/kuba*. Kopiowane są wszystkie typy plików, podkatalogi, łącza i urządzenia. Po zastosowaniu opcji `-a` dla kopiowanych plików zostaną zachowane wszystkie prawa właściciela, uprawnienia i czasy utworzenia.

Jeśli katalog */mnt/backup/homes/* znajduje się na oddzielnym dysku, cała zawartość katalogu */home/kuba* będzie istniała w dwóch różnych miejscach tego samego komputera. Jeśli udostępniony katalog */mnt/backup/homes/* jest częścią systemu plików NFS (z włączonym prawem zapisu), kopia zapasowa plików zostanie utworzona na innym komputerze.

Ponieważ w przytoczonym przykładzie jest wykonywana kopia zapasowa prywatnych plików, które niezbyt często są modyfikowane, po upływie kilku dni, w ciągu których pliki były przetwarzane, ponownie można wykonać dokładnie takie samo polecenie.

```
# rsync -av /home/kuba /mnt/backup/homes/
```

Tym razem w docelowym katalogu znajdą się wszystkie nowe pliki, natomiast poprzednio zarchiwizowane pliki zostaną uaktualnione o zmiany dokonane w plikach źródłowych. Wszystkie pliki usunięte z katalogu domowego w dalszym ciągu pozostaną w docelowym katalogu (jeśli się tego wyraźnie nie określi, polecenie `rsync` nie wykluczy z kopii

zapasowej plików usuniętych z katalogu źródłowego). Efektem ponownie wykonanego polecenia `rsync` będzie pełna kopia bieżącej zawartości katalogu */home/kuba* poszerzona o wszystkie pliki z niego usunięte.

Jeśli chcesz, aby usuwanie plików z katalogu domowego (źródłowego) powodowało też usuwanie ich kopii zapasowych z katalogu docelowego, uzupełnij wywołanie polecenia `rsync` opcją `--delete`.

Zdalna archiwizacja plików

Poprzedni przykład prezentował szybką instruktażową metodę archiwizacji. Kopię zapasową ważniejszych danych koniecznie trzeba umieścić na innym komputerze i powtarzać operację archiwizowania w regularnych odstępach czasu. Można to osiągnąć przy użyciu polecenia `rsync` współpracującego z narzędziami `ssh` i `cron`.

Przez zastosowanie narzędzia `ssh` w roli warstwy transportowej uzyskujemy gwarancję szyfrowania danych w trakcie ich przesyłania. Ze względu na to, że usługa `sshd` powiązana z narzędziem `ssh` domyślnie jest aktywna w wielu wersjach systemów Red Hat Linux i Fedora Linux, w celu przeprowadzenia archiwizacji wymagane jest jedynie konto i hasła użytkownika systemu zdalnego komputera. Jeśli tylko ze zdalnym komputerem można połączyć się za pomocą narzędzia `ssh` i zainstalowano na nim program `rsync`, przy jego użyciu można skopiować pliki do komputera. Oto przykład:

```
# rsync -azv -e ssh /home/kuba/ komp1:/mnt/backup/homes/
root@komp1's password: *******
building file list ... done
```

W tym przykładzie zdalny komputer jest identyfikowany przez nazwę `komp1` umieszczoną przed zdalnym katalogiem i oddzieloną od niego znakiem dwukropka. Użyto też innych opcji. Do opcji `-a` (realizuje archiwizację) i `-v` (tryb pełnej informacji) została dodana opcja `-z` odpowiedzialna za kompresję danych (po kompresji przesyłanie danych jest bardziej efektywne). Dodatkowo użyto opcji `-e ssh`, która przy przesyłaniu danych wymusza zastosowanie przez polecenie `rsync` narzędzia `ssh`. Prośba o podanie hasła została wyświetlona przez narzędzie `ssh`.

Powyższe polecenie może być wykonywane za każdym razem, gdy musimy dokonać archiwizacji danych. Jednak bardziej efektywna metoda wykonywania tego polecenia polega na zdefiniowaniu go jako zadania dla narzędzia `cron`. Dzięki temu kopie zapasowe danych będą tworzone automatycznie i regularnie co jakiś czas.

Jeśli polecenie `rsync` ma być uruchamiane automatycznie, nie może oczekiwać na podanie hasła. Trzeba wtedy wykonać następującą procedurę:

1. Skonfiguruj tak narzędzie `ssh`, aby przy logowaniu nie wymagało podania hasła od użytkownika zamierzającego wykonać kopię zapasową danych (więcej informacji na ten temat można znaleźć w rozdziale 14.).
2. Określ, jak często ma być przeprowadzana archiwizacja. Jeśli np. polecenie `rsync` ma być wykonywane raz dziennie, jako użytkownik *root* utwórz plik `/etc/cron.daily/moja_kopia_zapasowa`.

3. Dla pliku ustaw uprawnienie umożliwiające jego uruchamianie.

```
# chmod 755 /etc/cron.daily/moja_kopia_zapasowa
```

4. W pliku *moja_kopia_zapasowa* umieść następujące polecenie:

```
rsync -azv -e ssh /home/kuba/ kuba@komp1:/mnt/backup/homes/
```

Warto zauważyć, że w powyższym poleceniu podałem użytkownika `kuba`, którego konto zostanie użyte przy logowaniu na zdalnym komputerze `komp1`. W miejsce użytkownika `kuba` należy wstawić nazwę użytkownika, któremu w kroku 1. zostanie umożliwione archiwizowanie danych bez konieczności podawania hasła przy logowaniu.

Od teraz kopia zapasowa danych umieszczana na zdefiniowanym komputerze będzie wykonywana raz dziennie.

Przy użyciu wcześniej zawartego polecenia realizującego podstawową archiwizację danych można też wykonywać bardziej złożone operacje. W szczególności można rozważyć zdefiniowanie operacji wykonywania migawki. Migawka umożliwia przywrócenie z kopii zapasowej pliku z określoną datą i czasem utworzenia. Na stronie internetowej Mike'a Rubela (*http://www.mikerubel.org/computers/rsync_snapshots*) znajduje się znakomita procedura o nazwie *Easy Automated Snapshot-Style Backups with Linux and Rsync* służąca do wykonywania migawek za pomocą polecenia `rsync`.

Wybór strategii tworzenia kopii bezpieczeństwa

Kusząca jest możliwość wykonywania kopii zapasowej danych w szybki i prosty sposób, jednak ważniejsze dane wymagają dokładniejszego planowania i większej przezorności. Znamy kilka metod tworzenia kopii bezpieczeństwa danych. Musisz zadać sobie kilka pytań, aby zdecydować, która metoda jest w Twoim przypadku najlepsza. Oto kwestie, które musisz wziąć pod uwagę.

- Ile czasu może upłynąć w przypadku awarii do chwili odzyskania danych?
- Czy musimy przywracać starsze wersje plików, czy wystarczy najbardziej aktualna?
- Czy musimy tworzyć kopię zapasową plików na jednym komputerze, czy na wielu komputerach podłączonych do sieci?

Odpowiedzi na te pytania będą pomocne przy podejmowaniu decyzji, jak często wykonywać pełne kopie zapasowe, a jak często wystarczy przyrostowa kopia zapasowa. Jeśli dane są niezwykle ważne, możesz nawet uznać, że muszą być kopiowane nieustannie przy wykorzystaniu technologii kopii *lustrzanych dysków*. Kolejne podpunkty opisują różne metody tworzenia kopii bezpieczeństwa.

Pełna kopia bezpieczeństwa

Pełna kopia bezpieczeństwa przechowuje każdy plik z archiwizowanego dysku lub partycji. Gdyby dysk uległ awarii, możesz odtworzyć system, przywracając całą kopię bezpieczeństwa na nowym dysku. Niezależnie od tego, którą strategię tworzenia kopii bezpieczeństwa wybierzesz, powinna ona w jakimś stopniu obejmować tworzenie pełnej

kopii bezpieczeństwa. Możesz tworzyć pełne kopie bezpieczeństwa codziennie lub tylko raz w tygodniu, jest to uzależnione od tego, jak często dodajesz lub modyfikujesz pliki w systemie, a także zależy od pojemności nośnika, który wykorzystujesz do zapisywania kopii bezpieczeństwa.

Przyrostowa kopia bezpieczeństwa

Przyrostowa kopia bezpieczeństwa zawiera tylko pliki utworzone lub modyfikowane po wykonaniu ostatniej pełnej kopii bezpieczeństwa. Wybór tworzenia przyrostowej kopii bezpieczeństwa pozwala zaoszczędzić miejsce na nośniku. Tworzenie przyrostowych kopii bezpieczeństwa jest również mniej czasochłonne, ponieważ archiwizowane są jedynie te dane, które uległy zmianie od czasu wykonywania ostatniej operacji sporządzania kopii zapasowej (pełnej lub przyrostowej). Tworzenie przyrostowych lub innego typu częściowych kopii zapasowych może być ważne, gdy w dni robocze system jest bardzo obciążony i sporządzanie pełnej kopii zapasowej obniżyłoby jego wydajność. W takim przypadku warto zaplanować tworzenie pełnej kopii bezpieczeństwa podczas weekendu.

Tworzenie kopii lustrzanej

Przywrócenie danych z pełnej lub przyrostowej kopii bezpieczeństwa wymaga czasu, a zdarza się, że nie możesz sobie pozwolić na wyłączenie systemu ani na chwilę. Duplikując dane i pliki systemowe na dodatkowym dysku twardym, możesz znacznie skrócić czas przywrócenia systemu do pracy w przypadku awarii jednego z dysków.

W trakcie tworzenia kopii lustrzanej system nieustannie aktualizuje dysk będący kopią lustrzaną dysku głównego. W wersji tworzenia kopii lustrzanej o nazwie RAID 1 (tego typu macierz omówiono w rozdziale 10.) duplikowany dysk jest zapisywany w tym samym czasie co dysk główny, jeśli główny dysk ulegnie awarii, to kopia lustrzana może niezwłocznie przejąć jego rolę. Taki system jest nazywany *odpornym na uszkodzenia* (*fault-tolerant*); jest to rozwiązanie wskazane w wypadku serwera, który musi być nieustannie dostępny.

Sieciowa kopia bezpieczeństwa

Wszystkie opisane wcześniej metody wykonywania kopii bezpieczeństwa mogą być również wykorzystywane do wykonywania kopii bezpieczeństwa przez sieć. Zaletą tego sposobu jest możliwość wykorzystywania pojedynczego urządzenia do tworzenia kopii bezpieczeństwa wielu komputerów podłączonych do sieci. Jest to rozwiązanie znacznie tańsze i wygodniejsze niż instalowanie napędu taśm lub innego urządzenia tworzenia kopii bezpieczeństwa w każdym komputerze w sieci. Jeśli chcesz tworzyć kopie bezpieczeństwa wielu komputerów, potrzebne Ci będzie urządzenie o dużej wydajności. W takim wypadku warto zastanowić się nad zainstalowaniem mechanicznej ładowarki taśm, nagrywarki płyt DVD-RW lub zmieniarki dysków CD-ROM z możliwością nagrywania wielu płyt bez konieczności interwencji ze strony operatora.

Możliwe jest nawet tworzenie pewnego rodzaju kopii lustrzanej przez sieć. Na przykład serwer WWW może przechowywać duplikat danych na innym serwerze. Jeśli pierwszy z serwerów ulegnie awarii, wystarczy prosta zmiana adresu TCP/IP, aby przekierować ruch do drugiego serwera. Po naprawie pierwszego serwera dane mogą być przywrócone z serwera będącego jego kopią lustrzaną.

Wybór nośnika kopii bezpieczeństwa

Kiedy już wiesz, jaką strategię tworzenia kopii bezpieczeństwa chcesz zastosować, czas na wybranie nośnika. W systemach Fedora Core możesz korzystać z kilku różnych typów urządzeń i nośników do tworzenia kopii bezpieczeństwa. Każdy z nich ma swoje wady i zalety.

Wybór rodzaju nośnika w znacznym stopniu jest zależny od ilości danych, które chcesz archiwizować, czasu przechowywania kopii bezpieczeństwa oraz częstotliwości odzyskiwania danych. Niebagatelne znaczenie ma również kwota, którą możesz na ten cel przeznaczyć. Tabela 13.1 zawiera porównanie najbardziej popularnych rodzajów nośników kopii bezpieczeństwa.

Tabela 13.1. *Porównanie popularnych nośników kopii bezpieczeństwa*

Nośnik kopii bezpieczeństwa	Zalety	Wady
Taśma magnetyczna	Duża pojemność, niski koszt archiwizowania dużych ilości danych	Dostęp sekwencyjny, dlatego odzyskiwanie pojedynczych plików może trwać dłużej
Nagrywany dysk CD-ROM	Nośnik o dostępie swobodnym, dzięki czemu odzyskanie poszczególnych plików jest proste. Kopie bezpieczeństwa mogą być przywracane z dowolnego dysku CD-ROM	Ograniczona pojemność (około 700 MB na jednym dysku)
Nagrywany dysk DVD	Nośnik o dostępie swobodnym (podobnie jak dysk CD-ROM) o sporej pojemności wynoszącej 4,7 GB (jednak rzeczywista pojemność może być mniejsza)	Co prawda, ceny napędów DVD-RW i dysków DVD-R są stosunkowo wysokie, ale cały czas się obniżają. Tego typu urządzenia są mniej popularne od napędów CD-ROM
Dodatkowy dysk twardy	Pozwala na szybsze i częstsze tworzenie kopii bezpieczeństwa. Przywrócenie danych po awarii jest bardzo szybkie. Brak konieczności wymiany nośników. Dane mogą być odszukane i przywrócone bardzo szybko. Drugi dysk może być wirtualnym klonem pierwszego dysku, dzięki czemu w wypadku awarii możesz uruchomić system z drugiego dysku	Dane nie mogą być przechowywane poza miejscem instalacji systemu, dlatego istnieje niebezpieczeństwo utraty wszystkich danych w przypadku, gdy cały serwer ulegnie zniszczeniu. Metoda nie nadaje się do przechowywania danych archiwalnych wielu wersji plików. Ilość miejsca na dysku twardym jest przecież ograniczona i w końcu się ono wyczerpie. Ograniczenie to można obejść, stosując wymienne dyski twarde i regularnie wymieniając dyski kopii zapasowej

Kolejny podrozdział opisuje sposób korzystania z taśm magnetycznych oraz nagrywanych dysków CD-ROM i DVD jako nośników kopii zapasowej. W dalszej części rozdziału dowiesz się, jak wykorzystać dyski twarde w charakterze nośników kopii zapasowych.

Taśma magnetyczna

Taśma magnetyczna to najbardziej popularny nośnik wykorzystywany do tworzenia kopii bezpieczeństwa dużej ilości danych. Taśmy oferują tani i wygodny sposób archiwizowania plików. Dzisiejsze szybkie napędy taśm mogą zapisywać wiele gigabajtów danych na zadziwiająco małej taśmie, dzięki czemu ogromne ilości danych mogą być bezpiecznie przechowywane.

Główną wadą taśm magnetycznych jest fakt, że jest to nośnik o dostępnie sekwencyjnym. Oznacza to, że taśmy są odczytywane i zapisywane od początku do końca i odszukanie konkretnego pliku może być bardzo czasochłonne. Dlatego taśma najlepiej nadaje się do tworzenia kopii bezpieczeństwa całego systemu, ale nie jest najlepszym wyborem, w sytuacji gdy często konieczne jest odzyskiwanie pojedynczych plików.

System Fedora może obsługiwać szeroką gamę napędów taśm. Większość napędów taśmowych SCSI będzie współpracowała z podstawowym jądrem systemu Linux. Jądro obsługuje też już wprost wiele napędów taśmowych IDE, nie wymagając odwoływania się do nich w trybie emulacji SCSI. Niektóre napędy wymagają jednak instalacji dodatkowego oprogramowania.

Wykorzystanie narzędzi ftape do obsługi taśm magnetycznych

Jeśli napęd taśm jest podłączony do kabla sterownika IDE, potrzebny będzie sterownik `ftape`, aby się do niego odwoływać. Na szczęście ładowalny moduł `ftape` jest dostępny wraz z jądrem 2.6 systemu Linux. Podczas uruchamiania system Linux powinien automatycznie wykryć napęd taśm i załadować sterownik `ftape`. Aby sprawdzić, czy system załadował sterownik napędu taśm, wpisz następujące polecenie po uruchomieniu komputera:

```
dmesg | grep ftape
```

Powoduje ono przeszukanie ostatnich wiadomości jądra pod kątem słowa `ftape`. Jeśli moduł `ftape` został załadowany, powinieneś zobaczyć następujące informacje:

```
ftape v3.04d 25/11/97
[000] ftape-init.c (ftape_init) - installing QIC-117 floppy tape hardware drive... .
[001] ftape-init.c (ftape_init) - ftape_init @ 0xd08b0060.
[002] ftape-buffer.c (add_one_buffer) -  buffer nr #1 @ c1503914, dma area @ c02c0000.
[003] ftape-buffer.c (add_one_buffer) -  buffer nr #2 @ c1503c44, dma area @ c0298000.
[004] ftape-buffer.c (add_one_buffer) -  buffer nr #3 @ c50abaac, dma area @ c0328000.
[005] ftape-calibr.c (time_inb) - inb() duration: 1109 nsec.
[006] ftape-calibr.c (ftape_calibrate) - TC for 'ftape_udelay()' = 310 nsec
     (at 20479 counts).
[007] ftape-calibr.c (ftape_calibrate) - TC for 'fdc_wait()' = 2208 nsec
     (at 2559 counts).
```

Jeśli moduł nie został załadowany, sprawdź, czy obsługa modułu `ftape` i określonego napędu taśm jest wkompilowana jako część jądra. Powinno być możliwe dołączenie modułu `ftape` jako modułu ładowalnego.

W większości przypadków do urządzenia `ftape` można się odwołać, jak do dowolnego urządzenia SCSI. Podstawowa różnica polega na tym, że plik urządzenia `ftape` zawiera litery *qft* (ang. *QIK Floppy Tape*), gdy tymczasem taśma SCSI zawiera *st*. Np. plik urządzenia dla pierwszej taśmy SCSI w systemie to prawdopodobnie */dev/st0*; plik urządzenia dla pierwszego napędu taśm — */dev/qft0*.

Wszystkie standardowe programy obsługi taśm i archiwizacji powinny działać poprawnie dla obu rodzajów urządzeń. Niemniej jednak istnieje kilka dodatkowych programów, które możesz uznać za przydatne do obsługi napędu taśm. Programy te znajdują się w pakiecie `ftape-tools` pod adresem *ftp://metalab.unc.edu/pub/Linux/Kornel/tapes/*. Pobierz plik o nazwie *ftape-tools-1.09.tar.gz*. Jeśli dostępna jest nowsza wersja, możesz ją pobrać zamiast podanej. Rozpakuj pakiet `ftape` za pomocą polecenia `tar`:

```
$ tar -xzvf ftape-tools-1.09.tar.gz
```

Pakiet zostanie rozpakowywany do katalogu *ftape-tools-1.09*. Użyj polecenia `cd`, aby przejść do tego katalogu i uruchom skrypt `./configure`, by przygotować pliki uruchomieniowe pakietu. Następnie skompiluj pakiet przy użyciu polecenia `make`:

```
$ ./configure
$ make
```

Teraz nadaj uprawnienia użytkownikowi *root*, korzystając z polecenia `su`, i wpisz polecenie `make install`, aby zainstalować programy *ftape-tools* oraz instrukcje w odpowiednich katalogach:

```
# make install
```

Testowanie napędu taśm magnetycznych

Jesteś już gotowy do testowania napędu taśm. Włóż czystą taśmę do napędu taśm i wpisz następujące polecenie:

```
$ mt -f /dev/qft0 rewind
```

Powinieneś usłyszeć dźwięk przesuwania taśmy podczas przewijania przez system. Jeśli taśma jest już przewinięta, będzie to bardzo krótkotrwała czynność. Polecenie `mt` dostępne jako jedno z narzędzi pakietu `ftape-tools` jest wykorzystywane do skanowania, przewijania i wyładowywania taśm magnetycznych w napędzie taśm.

Formatowanie taśm magnetycznych

Pakiet `ftape-tools` zawiera również narzędzie do formatowania taśm. Większość taśm jest formatowana przed dostarczeniem ich do klienta. W przypadku gdy masz starszy sterownik napędu taśm, który korzysta z taśm niesformatowanych, użyj polecenia `ftformat`, aby je sformatować:

```
$ /usr/local/bin/ftformat -f /dev/qft0
```

Zwykle parametr `-f` podany wraz z nazwą urządzenia jest jedynym parametrem, który musisz podać. Niemniej jednak warto przeczytać instrukcję obsługi polecenia `ftformat`, aby dowiedzieć się więcej na temat opcji i możliwości tego polecenia.

Zapisywalne dyski CD

Innym nośnikiem kopii bezpieczeństwa, który zyskuje coraz większą popularność, jest dysk CD, na który można nagrać dane. Zapisywalne dyski CD mają kilka zalet, które powodują, że są one lepsze od taśm magnetycznych. Główną zaletą jest fakt, że zapisywalny dysk CD jest nośnikiem swobodnego dostępu. Oznacza to, że na dysku CD możesz szybko odszukać potrzebny plik bez konieczności sekwencyjnego skanowania całej zawartości. Jest to szczególnie przydatne, gdy musisz zachować historię zmian często modyfikowanych plików (takich jak kod źródłowy dla projektu oprogramowania lub wersje robocze dokumentów prawniczych).

Inną zaletą jest niezwykle długi czas przechowywania dysków CD. Jeśli chcesz zachować archiwalne wersje kopii bezpieczeństwa, zapisywalny dysk CD jest dobrym wyborem. Jeśli kopie bezpieczeństwa mają być przechowywane przez krótki czas, powinieneś zastanowić się nad wykorzystaniem dysku CD wielokrotnego zapisu. Dysk CD wielokrotnego zapisu (CD-RW, w odróżnieniu od nagrywanego dysku CD-R) może być wielokrotnie formatowany i wykorzystywany do przechowywania nowych wersji kopii bezpieczeństwa.

Największą wadą jest pojemność dysku CD, który może przechowywać maksymalnie 700 MB danych. Dla porównania, taśmy magnetyczne mogą przechowywać wiele gigabajtów danych, natomiast dyski DVD do 4,7 GB. Przykładowo taśmy DAT DDS-3 są w stanie po zastosowaniu kompresji pomieścić 24 GB danych, natomiast taśmy AIT-2 o szerokości 8 mm maksymalnie 100 GB.

Instalowanie pakietu cdrecord

Aby zapisywać dyski CD-ROM w systemie Fedora, musisz zainstalować pakiet `cdrecord`. Pakiet ten zawiera elementy, takie jak `cdrecord`, `devdump`, `isodump`, `isoinfo`, `isovfy` i `readcd`. Pakiet `cdrecord` jest częścią dystrybucji Fedora Core.

Pakiet `cdrecord` wymaga korzystania z napędu CD-ROM standardu SCSI. Jeśli masz napęd CD-ROM IDE/ATAPI, nie jest już konieczne konfigurowanie go, tak aby emulował napęd SCSI. W poprzednich wersjach systemów Red Hat Linux i Fedora Core emulacja napędu SCSI była uaktywniana automatycznie.

Zapisywanie dysków CD-ROM

Ponieważ dane zapisane na dysku CD-ROM nie mogą być później modyfikowane, musisz sformatować dysk CD-ROM i zapisać na nim pliki w jednym kroku. Jeśli najpierw sformatujesz dysk, to zostaniesz z pustym systemem plików na dysku CD-ROM, na którym nie możesz już nic więcej zapisać.

Pierwszym krokiem jest utworzenie obrazu systemu plików CD jako pliku na komputerze. Możesz to zrobić za pomocą polecenia `mkisofs`. Wyobraź sobie, że chcemy utworzyć kopię bezpieczeństwa katalogu domowego użytkownika *mary*. Wywołamy polecenie `mkisofs` i przekażemy jako argument nazwę obrazu systemu plików, jaki chcemy utworzyć, oraz katalog, który ma być jego źródłem:

```
$ mkisofs -R -o /var/tmp/mary.iso /home/mary
```

Utworzony zostanie obraz systemu plików ISO9660 w pliku o nazwie *mary.iso* znajdującym się w katalogu */var/temp*. Opcja `-R` powoduje, że zostaną użyte prawa własności i długie nazwy plików stosowane w systemie Linux. Jeśli partycja */var* ma zbyt mało wolnej przestrzeni, aby zapisać obraz, wybierz inną lokalizację.

Domyślnie polecenie `mkisofs` zachowuje informacje o właścicielu i prawach do dostępu plików i katalogów, które zapisuje w postaci obrazu systemu plików. Takie podejście jest prawidłowe, jeśli tworzysz kopię bezpieczeństwa, ale nie sprawdza się, gdy chcesz wykreować dystrybucyjny dysk CD. W takim przypadku użyj opcji `-r` jako pierwszego parametru polecenia `mkisofs`. Pliki będą zapisane z prawami odczytu dla wszystkich użytkowników, a w razie potrzeby z prawami do wykonywania.

Jeśli posiadasz nagrywarkę CD standardu ATAPI, nie będzie już wymagany dla napędu identyfikator SCSI ID, aby za jej pomocą było możliwe zapisywanie danych. Zamiast identyfikatora można podać nazwę urządzenia (np. `dev=/dev/cdrom`). Jeśli jednak dysponujesz nagrywarką CD SCSI, trzeba sprawdzić, jaki jest numer szyny SCSI, numer identyfikacyjny urządzenia oraz numer *LUN* (ang. *Logical Unit Number*) napędu, zanim będzie możliwe zapisanie pliku obrazu na dysku CD. Jeśli nie masz szyny SCSI w komputerze, emulowany numer szyny SCSI będzie prawdopodobnie wynosił zero. Następnie musisz się dowiedzieć, jakiego identyfikatora urządzenia SCSI używa napęd CD-ROM. Przywołaj polecenie `cdrecord` z parametrem `-scanbus`:

```
# cdrecord -scanbus
```

Powinny pojawić się takie informacje:

```
Cdrecord 2.0 (i686-pc-linux-gnu) Copyright (C) 1995-2002 Jörg Schilling
Linux sg driver version: 3.1.25
Using libscg version 'schily-0.7'
scsibus0:
0,0,0   0)  'Memorex ' 'CRW-1622 ' 'D4.0' Removable CD-ROM
0,0,1   1)  *
0,0,2   2)  *
0,0,3   3)  *
0,0,4   4)  *
0,0,5   5)  *
0,0,6   6)  *
0,0,7   7)  *
```

Z podanych informacji wynika, że napęd CD-ROM wykorzystuje identyfikator SCSI zero. W tym wypadku numer LUN powinien również wynosić zero, więc znamy już trzy potrzebne wartości. Możemy je podać jako argumenty polecenia `cdrecord` będącego częścią parametru `dev`.

Pierwszy podawany jest numer szyny SCSI, następnie identyfikator urządzenia, a na samym końcu — numer LUN. Całe polecenie powinno mieć następującą postać:

```
# cdrecord -v speed=2 dev=0,0,0 -data /var/tmp/mary.iso
```

W przypadku nagrywarki CD ATAPI identyfikowanej przez urządzenie `/dev/cdrom` polecenie może wyglądać następująco:

```
# cdrecord -v speed=2 dev=/dev/cdrom -data /var/tmp/mary.iso
```

Do polecenia dołączyliśmy kilka dodatkowych parametrów. Parametr `-v` informuje polecenie, aby wyświetlało informacje na ekranie. Parametr `speed` mówi, z jaką prędkością należy nagrywać dysk (w naszym wypadku jest to X2). Można pominąć parametr `speed=2` i umożliwić programowi `cdrecord` automatyczne wykrycie prędkości zapisu posiadanej nagrywarki CD. Parametr `-data` określa, że kolejny parametr jest nazwą obrazu systemu plików, który ma zostać zapisany na dysk CD-ROM. Użycie opcji `-eject` spowoduje wysunięcie z napędu dysku CD-ROM po zakończeniu operacji. Podczas nagrywania dysku polecenie `cdrecord` powinno wyświetlać informacje dotyczące statusu wykonywanej czynności:

```
cdrecord: No write mode specified.
cdrecord: Assuming -tao mode.
cdrecord: Future versions of cdrecord may have driver dependent defaults.
cdrecord: Continuing in 5 seconds...
Cdrecord-Clone 2.01a27-dvd (i686-pc-linux-gnu) Copyright (C) 1995-2004 Jorg Schelling
TOC Type: 1 = CD-ROM
scsidev: '/dev/cdrom'
devname: '/dev/cdrom'
scsibus: -2 target: -2 lun: -2
Warning: Open by 'devname' is unintentional and not supported.
Linux sg driver version: 3.5.27
Using libscg version 'schily-0.8'
cdrecord: Warning: using inofficial libscg transport code version
(schily - Red Hat-scsi-linux-sg.c-1.80-RH '@(#)scsi-linux-sg.c
1.80 04/03/08 Copyright 1997 J. Schilling').
SCSI buffer size: 64512
atapi: 1
Device type         : Removable CD-ROM
Version             : 0
Response_Format     : 1
Vendor_info         : 'Memorex'
Identifikation      : 'CRW-1622'
Revision            : 'D4.0'
Device seems to be  : Generic mmc CD-RW
Using generic SCSI-3/mmc CD-R/CD-RW driver (mmc_cdr)
Driver flags        : SWABAUDIO
Drive buf size      : 786432 = 768 KB
FIFO size           : 4194304 = 4096 KB
Track 01: data     0 MB
Total size:        0 MB (00:04.02) = 302 sectors
Lout start:        1 MB (00:06/02) = 302 sectors
Currect Secsize:   2048
ATIP info from disk:
  Indicated writing power: 5
  Is not unrestricted
  Is not erasable
  Disk sub type: Medium Type B, low Beta category (B-) (4)
  ATIP start of lead in:  -12369 (97:17/06)
  ATIP start of lead out: 359849 (79:59/74)
Disk type:        Short strategy type (Phthalocyanine or similar)
Manuf. index:  69
Manufacturer: Moser Baer India Limited
Manufacturer is guessed because of the orange forum embargo.
The orange forum likes to get money for recent information.
The information for this media may not be correct.
Blocks total: 359849 Blocks current: 359849 Blocks remaining: 359547
```

```
Starting to write CD/DVD At speed 4 in real TAO mode for single session.
Last chance to quit, starting real write in 0 seconds. Operation starts.
Waiting for reader process to fill input buffer ... input buffer ready.
trackno=0
Performing OPC...
Starting new track at sector: 0
Track 01:  90 of 90 MB written (fifo 100%)
Track 01: Total bytes read/written: 94928896/94928896 (46352 sectors) .
Writing time: 319.345s
Fixating...
Fixating time: 133.349s
cdrecord: fifo had 1496 puts and 1496 gets.
cdrecord: fifo was 0 times empty and 1424 times full, min fill was 95%.
```

Po zakończeniu zapisywania dysku CD-ROM przez polecenie `cdrecord` przywrócony zostanie wiersz poleceń powłoki systemowej oraz usunięty plik obrazu systemu plików */var/tmp/mary.iso*. Opisz odpowiednio dysk CD-ROM i umieść go w bezpiecznym miejscu.

Jeśli będziesz potrzebował dowolnego pliku zapisanego na dysku CD-ROM, to wystarczy go umieścić w napędzie. Jeśli po włożeniu płyty nie zostanie automatycznie wyświetlona jego zawartość, należy wykonać polecenie `mount /media/cdrecorder`. Wyświetl zawartość katalogu */media/cdrecorder* i przekopiuj z niego żądane pliki.

Więcej informacji na temat polecenia `cdrecord` znajdziesz w rozdziale 8. Z instrukcji CD-Writing-HOWTO dowiesz się więcej na temat instalowania i wyszukiwania błędów obsługi napędów CD-ROM. Jeśli używasz środowisk graficznych dystrybucji Fedora Core, zapewne będziesz wolał korzystać z graficznych narzędzi nagrywania dysków CD. W rozdziale 8. opisano jedno z takich narzędzi, nadające się do nagrywania płyt CD i DVD.

Zapisywalne dyski DVD

Dysponując napędem obsługującym zapisywalne dyski DVD przy użyciu polecenia `dvdrecord`, możesz zapisać na nich kopię zapasową danych. Procedura jest prawie taka sama jak w przypadku archiwizacji danych na dyskach CD z tym, że występują następujące różnice:

- zamiast polecenia `cdrecord` jest używane `dvdrecord` (mimo to mogą one posiadać prawie identyczne interfejsy),
- na każdym dysku można zapisać więcej danych (4,7 GB przy 700 MB),
- zarówno nagrywarka dysków DVD, jak i same nośniki danych są znacznie droższe od napędów i dysków CD.

Gdy producenci podają wartość 4,7 GB, mają na myśli gigabajt równy 1000, a nie 1024 MB. A zatem, na dysku DVD można jedynie zapisać około 4,4 GB danych.

Polecenie `dvdrecord` umożliwia nagrywanie danych na dyskach DVD przy użyciu dowolnej nagrywarki DVD kompatybilnej ze standardem *MMC* (ang. *Multimedia Command*). W trakcie pisania programu `dvdrecord` testowano go przy użyciu nagrywarki DVD firmy Pioneer (model DVR-A03).

Aby utworzyć plik obrazu systemu plików (przy użyciu polecenia `mkisofs`) i zlokalizować napęd dysków DVD-R, należy postępować zgodnie z procedurą zamieszczoną w podrozdziale „Zapisywalne dyski CD-ROM", a następnie w celu zapisania danych na dysku DVD wykonać polecenie `dvdrecord`. Poniżej zawarto przykład użycia programu `dvdrecord` do zapisania na dysku DVD pliku obrazu systemu plików o nazwie *bigimage.cd*:

```
# dvdrecord -v speed=2 dev=/dev/cdrom -data bigimage.cd
```

W przygotowaniu obrazów płyt DVD przydatne może być narzędzie o nazwie `growisofs`. Program ten łączy funkcje `mkisofs` (programu do tworzenia obrazów systemów plików) i oprogramowania nagrywającego owe obrazy na płytach.

Tworzenie kopii bezpieczeństwa na dysku twardym

Jak już wspominałem na początku rozdziału przy okazji omawiania procedury wykonywania prostej archiwizacji, przenośne nośniki danych, takie jak taśmy lub dyski CD, nie są jedynymi dostępnymi rozwiązaniami tworzenia kopii bezpieczeństwa danych. Może się okazać, że warto zainstalować w systemie drugi dysk twardy i wykorzystać go do tworzenia kopii bezpieczeństwa. Takie rozwiązanie ma pewną przewagę nad sposobami opisanymi wcześniej.

- Kopia bezpieczeństwa może być wykonywana szybko i podczas czasu pracy; dzięki temu zapisane na niej dane będą bardziej aktualne na wypadek awarii.
- Nośnik nie musi być dodatkowo podłączany do systemu, dlatego dane mogą być odzyskiwane szybciej i bardziej efektywnie.
- Możesz skonfigurować drugi dysk jako wirtualny klon pierwszego. Jeśli pierwszy dysk ulegnie awarii, możesz uruchomić system z drugiego dysku bez konieczności instalowania dodatkowych urządzeń. Oprogramowanie obsługi kopii lustrzanych pozwala zautomatyzować ten proces.
- Nowe i atrakcyjne cenowo przenośne dyski twarde (z uwzględnieniem modeli podłączanych za pomocą interfejsów USB i FireWire) oferują wygodny w użyciu przenośny nośnik danych, o którym zwykle myślano zupełnie odwrotnie.

Istnieje jednak kilka wad tworzenia kopii bezpieczeństwa na dysku twardym. Przykładowo, metoda nie nadaje się do przechowywania archiwów historycznych wielu wersji plików, ponieważ dysk twardy zostanie w końcu zapełniony. Jednak problem ten może zostać znacząco zmniejszony przez migawki (przechowujące zmiany dokonane w plikach) tworzone przy użyciu narzędzia `rsync`.

Najprostszą formą tworzenia kopii bezpieczeństwa na drugim dysku twardym jest kopiowanie ważnych plików na inny dysk za pomocą polecenia `cp` lub `tar`. Najbardziej wyrafinowaną metodą jest wykorzystanie oprogramowania RAID do utworzenia odpornego na awarie systemu kopii lustrzanych. Jeśli nie potrzebujesz wysokiego poziomu bezpieczeństwa przed utratą danych, które oferuje kopia lustrzana RAID, ale chciałbyś mieć pod ręką dokładny i gotowy do użytku duplikat danych, istnieje alternatywa — pakiet `mirrordir`.

Instalowanie mirrordir do klonowania katalogów

Pakiet `mirrordir` pozwala na tworzenie kopii lustrzanej dysków twardych. *Mirrordir* to użyteczne narzędzie, które umożliwia wykonanie i przechowywanie dokładnej kopii hierarchii katalogów. Oficjalną stronę tego pakietu znajdziesz pod adresem *http://mirrordir.sourceforge.net*. Możesz pobrać pakiet, klikając przycisk *Download RPM*.

Gdy już pobrałeś plik, zainstaluj go tak samo jak instalujesz dowolny *rpm*. Jeśli np. zapisałeś plik *rpm* w katalogu */tmp*, możesz wpisać polecenie:

```
# rpm -Uhv /tmp/mirrordir*rpm
```

Klonowanie katalogu za pomocą mirrordir

Po zainstalowaniu *mirrordir* możesz go użyć do klonowania katalogu. Załóżmy, że masz drugi dysk twardy zawierający na tyle dużą partycję, że możesz tam zapisać kopię swojej partycji */home*. Pierwszym krokiem jest utworzenie katalogu, w którym możesz podłączyć partycję, oraz jej podłączenie. Zaloguj się jako użytkownik *root* i wpisz polecenie:

```
# mkdir -p /mirror/home
# mount /dev/hdb5 /mirror/home
```

W tym przykładzie podłączamy piątą partycję (`5`) drugiego dysku twardego (`hdb`) — to wyjaśnia nazwę urządzenia `/dev/hdb5`. Litera `b` odnosi się do drugiego dysku, a `5` — do numeru partycji. W Twoim przypadku może to być inny dysk lub partycja. Wtedy odpowiednio zmodyfikuj nazwę. Zakładając, że polecenie `mount` bezproblemowo podłączyło dysk, możesz już kopiować swoją partycję */home*. Wpisz następujące polecenie:

```
# mirrordir /home /mirror/home
```

Użycie tego polecenia powoduje, że zawartość katalogu */home* jest duplikowana w katalogu */mirror/home*.

Musisz uważać na kolejność podawania parametrów. Jeśli ją odwrócisz, cała zawartość katalogu */home* zostanie usunięta! Stanie się tak, ponieważ zastąpisz pustym katalogiem zawartość swojego katalogu */home*.

Teraz już masz kopię bezpieczeństwa całej partycji */home*. Możesz ponownie uruchomić polecenie `mirrordir` w przyszłości i ponownie wykona ono dokładną kopię katalogu */home* w katalogu */mirror/home*. Do katalogu */mirror/home* zostaną skopiowane tylko te pliki, które zostały utworzone lub zmodyfikowane od ostatniego uruchomienia polecenia `mirrordir`. Z katalogu */mirror/home* zostaną usunięte pliki, które znikły z katalogu */home*. Dzięki temu kopia lustrzana będzie zawsze aktualna bez konieczności kopiowania całej partycji */home* za każdym razem. Jeśli dysk z partycją */home* ulegnie awarii, możesz zastąpić go innym, a następnie przekopiować system plików z kopii lustrzanej za pomocą polecenia `mirrordir` z odwróconymi parametrami:

```
# mirrordir /mirror/home /home
```

Możesz przywrócić system do pracy jeszcze szybciej, zamieniając lustrzaną partycję na aktualną. Przejdź do edycji pliku */etc/fstab* i zmień nazwę urządzenia na */home*, aby wskazywało katalog zawierający kopię lustrzaną. Teraz odłącz i podłącz na nowo partycję

/home (lub uruchom na nowo komputer) i katalog kopii lustrzanej będzie widoczny jako katalog */home*. Użytkownicy nie mają szans zorientować się, że coś się zmieniło. Możesz nawet rozważyć pomysł tworzenia kopii lustrzanej każdej partycji na głównym dysku. Wtedy nawet w przypadku awarii całego dysku możesz przywrócić poprawną pracę systemu bardzo szybko. Po prostu zastąp uszkodzony dysk kopią lustrzaną i możesz dalej pracować.

Automatyczne tworzenie kopii lustrzanych

Aby zautomatyzować proces tworzenia kopii lustrzanych, możesz napisać niewielki skrypt, który podłącza partycję lustrzaną, uruchamia polecenie `mirrordir` i odłącza partycję. Jeśli pozostawisz partycję z kopią lustrzaną odłączoną, kiedy z niej nie korzystasz, zmniejszasz ryzyko omyłkowego usunięcia danych z tej partycji. Utwórz skrypt `mirror.sh` i umieść go w katalogu */usr/local/sbin*. Przedstawiony poniżej skrypt powinien się doskonale do tego celu nadawać:

```
#!/bin/sh
#
# mirror.sh: Odwzorowuje partycję /home na drugim dysku twardym
#
/bin/mount /dev/hdb5 /mirror/home
mirrordir /home /mirror/home
/bin/umount /mirror/home
```

Teraz wskaż ten skrypt jako zadanie do wykonania dla procesu `cron`. W tym celu uruchom polecenie `cron` z parametrem `-e`. Wywołany zostanie edytor zawierający listę zadań procesu `cron`. Dodaj następującą linię na końcu listy:

```
0  *  *  *  * /usr/local/sbin/mirror.sh
```

Zapisz zmiany i zamknij edytor. Wpis powoduje, że skrypt jest uruchamiany raz na godzinę. Jeśli zdecydujesz się kreować kopie lustrzane pozostałych partycji, możesz to zrobić w prosty sposób, tworząc odpowiednie punkty montowania i dodając odpowiednie sekcje w skrypcie `mirror.sh`.

Wadą tworzenia lustrzanych kopii dysków jest to, że przypadkowa modyfikacja albo uszkodzenie danych przechowywanych w odzwierciedlanym katalogu domowym odzwierciedli to uszkodzenie w kopii — chyba że odpowiednio szybko wychwycisz błąd i zablokujesz niepożądaną synchronizację kopii.

Tworzenie kopii bezpieczeństwa za pomocą polecenia dump

Polecenie `dump` jest jednym z najczęściej używanych narzędzi wykonywania kopii bezpieczeństwa systemów Unix. Historia polecenia sięga początków systemu Unix i dlatego jest standardowym elementem prawie każdej wersji tego systemu. Pakiet `dump` jest również częścią systemów Red Hat Linux i Fedora Core. Jeśli nie został zainstalowany domyślnie w czasie pierwszego uruchomienia systemu Linux, możesz zainstalować go z pakietu RPM `dump` znajdującego się na instalacyjnej płycie DVD dystrybucji Fedora Core.

Polecenia `dump` i `restore` przez wiele lat były szeroko stosowane, jednak obecnie nie są uważane za szczególnie niezawodne i solidne narzędzia archiwizujące i przywracające dane. Opis obu narzędzi zamieszczono tu ze względu na starsze nośniki archiwizujące i skrypty automatyzujące, które w dalszym ciągu korzystają z tych poleceń.

Pakiet `dump` zawiera kilka poleceń. Możesz przejrzeć instrukcje, aby dowiedzieć się więcej na ten temat, ale tabela 13.2 zawiera krótki opis programów.

Tabela 13.2. *Programy pakietu dump*

Polecenie	Opis
`dump`	Tworzy archiwalną kopię bezpieczeństwa całych partycji dysku lub wybranych katalogów
`restore`	Może być użyte do przywrócenia całego archiwum lub poszczególnych plików z archiwum na dysk twardy
`rmt`	Program wykorzystywany przez polecenia `dump` i `restore` do kopiowania plików przez sieć. Nigdy nie należy używać tego polecenia samodzielnie

Tworzenie kopii bezpieczeństwa

Tworząc kopię bezpieczeństwa systemu plików przy użyciu polecenia `dump`, musisz podać parametry określające poziom, nośnik oraz system plików, którego kopia ma być tworzona. Możesz również podać parametry dodatkowe określające rozmiar nośnika kopii bezpieczeństwa, metodę żądania wprowadzenia kolejnej taśmy oraz zapisanie czasu i statusu wykonanego zrzutu systemu plików.

Pierwszym parametrem polecenia `dump` jest zawsze lista jednoliterowych kodów opcji. Zaraz za nią występuje oddzielona spacją lista argumentów wymaganych przez te opcje. Argumenty występują w tym samym porządku co wymagające ich podania opcje. Ostatnim parametrem jest zawsze system plików lub katalog, którego kopia bezpieczeństwa jest tworzona.

```
# dump opcje argumenty system_plików
```

Tabela 13.3 przedstawia jednoliterowe kody opcji polecenia `dump`.

Typowe polecenie `dump` może wyglądać analogicznie do następującego:

```
# dump 0uBf 500000 /dev/gft0 /dev/hda6
```

Skutkiem tego polecenia jest wykonanie przez polecenie `dump` na poziomie zero (pełna kopia bezpieczeństwa) kopii bezpieczeństwa systemu plików */dev/hda6* oraz zapisanie tej kopii w napędzie taśm */dev/qft0* i zapamiętanie wyników w pliku */etc/dumpdates*. Opcja `B` jest użyta w celu zwiększenia oczekiwanej liczby bloków taśmy do 500000, w przeciwnym razie polecenie `dump` poprosi o włożenie nowej taśmy do napędu wcześniej niż rzeczywiście będzie to konieczne. Polecenie `dump` wyświetla wiadomości o stanie wykonania polecenia na ekranie, informując administratora, na jakim etapie wykonania znajduje się kopia bezpieczeństwa i podając przewidywany czas do ukończenia operacji. Informacje o wynikach wykonania polecenia mają postać, jak na stronie 569:

Tabela 13.3. *Opcje polecenia dump*

Opcje polecenia dump	Opis
`0-9`	Poziom operacji `dump`. Wybranie poziomu `0` powoduje utworzenie kopii bezpieczeństwa wszystkich plików (pełna kopia bezpieczeństwa). Wyższa wartość tworzy kopię bezpieczeństwa tylko tych plików, które zostały zmodyfikowane lub utworzone od ostatniej kopii bezpieczeństwa o tym samym lub niższym numerze (przyrostowa kopia bezpieczeństwa). Domyślną opcją jest opcja `9`
`-B` *`liczba_ zapisów`*	Liczba zapisów kopii bezpieczeństwa na woluminie. Ogólnie dotyczy to ilości danych, które zmieszczą się na taśmie. Opcja wymaga podania argumentu o wartości numerycznej
`-b` *`ilość_kb_ w_rekordzie`*	Ilość kilobajtów w jednym rekordzie kopii bezpieczeństwa. Przydatna informacja w połączeniu z opcją `B`. Opcja wymaga podania argumentu o wartości numerycznej
`-h` *`poziom`*	Pliki mogą być oznaczone atrybutem `nodump`. Ta opcja określa poziom operacji `dump`, przy którym uwzględniany jest atrybut `nodump`. Opcja przyjmuje wartości `0` – `9`
`-f` *`plik`*	Nazwa pliku lub urządzenia, w którym ma być zapisana kopia bezpieczeństwa. Może to być nawet plik lub urządzenie dostępne na zdalnej maszynie
`-d` *`gęstość`*	Definiuje gęstość zapisu taśmy. Domyślna wartość to 1600 bitów na cal. Opcja wymaga podania argumentu o wartości numerycznej
`-n`	Kiedy polecenie `dump` wymaga dodatkowego działania ze strony operatora (takiego jak wymiana taśmy), to przesyła wiadomość do wszystkich użytkowników w grupie operatorów. Użycie tej opcji nie wymaga podania dodatkowych argumentów
`-s` *`długość_ w_stopach`*	Określa długość taśmy w stopach. Wartość jest zależna o gęstości zapisu taśmy (opcja `d`) i rozmiaru rekordu kopii bezpieczeństwa (opcje `B` i `b`). Wymaga podania argumentu o wartości numerycznej
`-u`	Zapisuje aktualną kopię bezpieczeństwa w pliku */etc/dumpdates*. Jest to dobre rozwiązanie, szczególnie w przypadku tworzenia przyrostowych kopii bezpieczeństwa
`-t` *`data`*	Określa datę i czas, w oparciu o które wykonywane są przyrostowe kopie bezpieczeństwa. Wszystkie pliki modyfikowane lub tworzone później zostaną zapisane w kopii bezpieczeństwa. Użycie tej opcji powoduje pominięcie przez polecenie `dump` pliku */etc/dumpdates*. Wymaga podania pojedynczego argumentu — daty w formacie określonym w instrukcji `ctime`
`-W`	Użycie tej opcji powoduje, że polecenie `dump` wyświetla listę systemów plików, które mają zostać zapisane w kopii bezpieczeństwa. Lista tworzona jest w oparciu o zawartość plików */etc/dumpdates* i */etc/fstab*
`-w`	Działa analogiczne jak opcja `W`, ale wyświetla listę pojedynczych plików, które mają zostać zapisane w kopii bezpieczeństwa

```
DUMP: Date of this level 0 dump: Thu Aug 15 23:33:37 2002
DUMP: Dumping /dev/hda6 (/home) to /dev/qft0
DUMP: Exclude ext3 journal inode 8
DUMP: Label: /home
DUMP: mapping (Pass I) [regular files]
DUMP: mapping (Pass II) [directories]
DUMP: estimated 93303 tape blocks on 0.19 tape(s).
DUMP: Volume 1 started with block 1 at: Thu Aug 15 23:33:47
DUMP: dumping (Pass III) [directories]
DUMP: dumping (Pass IV) [regular files]
DUMP: Closing /dev/qft0
DUMP: Volume 1 comp[leted At: Thu Aug 15 23:35:35 2002
DUMP: Volume 1 94360 tape blocks (92.15MB)
DUMP: Volume 1 took 0:01:48
DUMP: Volume 1 transfer rate: 873 kB/s
DUMP: 94360 tape blocks (92.15MB) on 1 volume(s)
DUMP: finished In 108 seconds, throughput 873 kBytes/sec
DUMP: Date of this level 0 dump: Thu Aug 16 23:33:37 2001
DUMP: Date of this dump completed: Thu Aug 16 23:33:37 2001
DUMP: Average transfer rate: 873 kB/s
DUMP: DUMP is DONE
```

Poziomy operacji dump

Polecenie `dump` może tworzyć kopię bezpieczeństwa wszystkich plików w systemie plików lub kopię bezpieczeństwa tylko wybranych plików, które były ostatnio modyfikowane. Parametr poziomu operacji `dump` jest wykorzystywany do określenia sposobu wykonywania kopii bezpieczeństwa. Poziom `0` określa tworzenie pełnej kopii bezpieczeństwa wszystkich plików w systemie plików. Określenie wyższego poziomu (`1` – `9`) powoduje zapisywanie kopii bezpieczeństwa tylko tych plików, które były modyfikowane lub utworzone od ostatniej operacji `dump`. Polecam wykorzystanie poziomów operacji `dump` do utworzenia harmonogramu pełnych i przyrostowych kopii bezpieczeństwa, zgodnie z przykładem przedstawionym w tabeli 13.4.

Tabela 13.4. *Zalecany harmonogram tworzenia kopii bezpieczeństwa*

Dzień tygodnia	Poziom operacji dump
Niedziela	Poziom 0 (pełna kopia bezpieczeństwa). Wysuń taśmę z napędu po zakończeniu operacji
Poniedziałek	Poziom 9 (przyrostowa kopia bezpieczeństwa)
Wtorek	Poziom 8 (przyrostowa kopia bezpieczeństwa)
Środa	Poziom 7 (przyrostowa kopia bezpieczeństwa)
Czwartek	Poziom 6 (przyrostowa kopia bezpieczeństwa)
Piątek	Poziom 5 (przyrostowa kopia bezpieczeństwa)
Sobota	Poziom 4 (przyrostowa kopia bezpieczeństwa)

Zwróć uwagę, że po wykonaniu pełnej kopii bezpieczeństwa w niedzielę następnego dnia tworzona jest przyrostowa kopia bezpieczeństwa na poziomie 9 i kolejno każdego dnia jest wykonywana przyrostowa kopia bezpieczeństwa o jeden poziom niżej. Dzięki temu

wszystkie pliki, które uległy modyfikacji od niedzieli, zostaną zapisane na każdej przyrostowej kopii bezpieczeństwa. Z tego powodu każda przyrostowa kopia bezpieczeństwa jest większa od poprzedniej; zawiera ona wszystkie pliki z poprzedniej przyrostowej kopii bezpieczeństwa oraz pliki, które od tego czasu uległy modyfikacji. Może się to wydawać marnotrawstwem miejsca na taśmie, ale pozwala zaoszczędzić wiele czasu i wysiłku, gdyby zaistniała potrzeba odtworzenia systemu plików.

Wyobraźmy sobie np., że dysk twardy uległ awarii w piątek. Po zastąpieniu go nowym dyskiem możesz przywrócić cały system plików, wykonując dwa kroki: przywracasz pełną kopię bezpieczeństwa z poprzedniej niedzieli, a następnie przywracasz zmodyfikowane od tego czasu dane z przyrostowej kopii bezpieczeństwa wykonanej w czwartek. Jest to możliwe dzięki temu, że czwartkowa kopia przyrostowa zawiera wszystkie dane z taśm poniedziałkowej, wtorkowej i środowej, jak również pliki, które zostały zmodyfikowane później. Jeśli poziomy operacji `dump` wzrastałyby w kolejne dni (poziom 1 w poniedziałek, poziom 2 we wtorek itd.), wszystkie przyrostowe kopie bezpieczeństwa musiałyby być przywracane, aby odtworzyć cały system plików do najbardziej aktualnego stanu.

Automatyzacja tworzenia kopii bezpieczeństwa z wykorzystaniem narzędzia cron

Możesz zautomatyzować wykonanie większości kopii zapasowych za pomocą skryptów powłoki i demona `cron`. Użyj polecenia `su`, aby nadać sobie prawa użytkownika *root*, a następnie przy użyciu polecenia `cd` przejdź do katalogu */usr/local/bin*. Użyj dowolnego edytora tekstów do utworzenia skryptu powłoki o nazwie `backups.sh`, który ma następującą postać:

```
#!/bin/sh
#
# backups.sh – Prosty skrypt tworzenia kopii
# zapasowej, autorstwa Thada Phetteplace
#
# Przedstawiony skrypt wymaga podania jednego
# parametru, poziomu operacji dump.
# Jeśli poziom operacji dump nie jest podany,
# automatycznie przyjmowana jest wartość zero.
# Dla poziomu zero (pełna kopia bezpieczeństwa)
# taśma jest przewijana i wysuwana z napędu.
#
if [ $1 ]; then
        level=$1
else
        #
        # Nie podano poziomu wykonania operacji, dlatego
        # domyślnie wybierana jest wartość zero.
        #
        level="0"
fi

/sbin/dump $level'uf' /dev/nrft0 /
/sbin/dump $level'uf' /dev/nrft0 /home
```

```
/sbin/dump $level'uf' /dev/nrft0 /var
/sbin/dump $level'uf' /dev/nrft0 /usr
#
# Jeśli wykonywana jest pełna kopia bezpieczeństwa,
# przewiń i wysuń taśmę z napędu po zakończeniu operacji.
#
if [ $level = "0" ] ; then
       /bin/mt -f /dev/nrft0 rewind
       /bin/mt -f /dev/nrft0 offline
fi
```

Możesz zmodyfikować skrypt w taki sposób, aby tworzył kopie bezpieczeństwa konkretnych partycji, ale oprócz tego skrypt nie wymaga dodatkowych zmian i powinien działać poprawnie. Po zapisaniu pliku i zamknięciu edytora tekstów zmień uprawnienia do pliku w taki sposób, aby mógł on być uruchamiany tylko przez użytkownika *root*:

```
# chmod 700 backups.sh
```

Teraz, jeśli jesteś zalogowany jako użytkownik *root*, to za pomocą skryptu *backups.sh* możesz utworzyć kopię bezpieczeństwa całego systemu plików. Skrypt wymaga podania jednego parametru, którym jest poziom operacji `dump`. Jeśli go nie podasz, automatycznie wybrany zostanie poziom zero. Dlatego następujące polecenia spowodują wykonanie takiej samej kopii bezpieczeństwa:

```
# backups.sh
# backups.sh 0
```

Może zaistnieć konieczność dopasowania skryptu do potrzeb Twojego systemu. Ja np. korzystam z napędu taśm */dev/nrft0*. W Twoim wypadku może to być inny napęd. Niezależnie od tego, jakiego urządzenia używasz, powinieneś używać wersji nazwy urządzenia rozpoczynającej się od `n`. Dzięki temu system wie, że po zakończeniu kopiowania danych na taśmę nie powinien przewijać tej taśmy. Widać w przykładzie, że użyłem polecenia `/dev/nrft0` zamiast `/dev/rst0`. Gdybym użył `/dev/rst0`, każda kolejna kopia przyrostowa zastępowałaby zapisaną wcześniej kopię.

Możesz również zmienić partycje, których kopie bezpieczeństwa są wykonywane oraz poziom operacji `dump`, przy którym taśma jest wysuwana z napędu. Często stosowaną praktyką jest wysuwanie taśmy po wykonaniu ostatniej kopii przyrostowej, czyli przed wykonaniem kolejnej pełnej kopii bezpieczeństwa.

Największą zaletą tego skryptu jest łatwość jego modyfikacji w zakresie automatycznego uruchamiania tego skryptu przez system. Wystarczy dodać kolejne wpisy w pliku *crontab*, a demon `cron` będzie uruchamiał skrypt w podanych terminach. Jeśli jesteś zalogowany jako użytkownik *root*, wpisz polecenie `crontab` z parametrem `-e`:

```
# crontab -e
```

Spowoduje to otwarcie pliku *crontab* w edytorze tekstów. Dodaj następujące wpisy na końcu pliku:

```
0 22 * * 0 /usr/local/bin/backup.sh 0
0 22 * * 1 /usr/local/bin/backup.sh 9
0 22 * * 2 /usr/local/bin/backup.sh 8
0 22 * * 3 /usr/local/bin/backup.sh 7
```

```
0 22 * * 4 /usr/local/bin/backup.sh 6
0 22 * * 5 /usr/local/bin/backup.sh 5
0 22 * * 6 /usr/local/bin/backup.sh 4
```

Zapisz i zamknij plik. Demon `cron` uruchomi skrypt o godzinie 22:00 każdego dnia tygodnia. Przedstawiony przykład wykorzystuje omówiony wcześniej schemat harmonogramu. Pełna kopia bezpieczeństwa jest wykonywana w niedzielę i po jej utworzeniu taśma jest wysuwana. Nowa taśma powinna zostać załadowana w poniedziałek i kolejne przyrostowe kopie bezpieczeństwa będą zapisywane na niej przez pozostałe dni tygodnia. Następna pełna kopia bezpieczeństwa zostanie zapisana na tej taśmie pod koniec tygodnia, chyba że w niedzielę ktoś wyjmie zapisaną taśmę i przed godziną 22:00 zastąpi ją inną.

Przywracanie plików z kopii bezpieczeństwa

Polecenie `restore` jest wykorzystywane do przywracania plików z taśmy lub z innego nośnika zawierających kopię bezpieczeństwa wykonaną przy użyciu programu `dump`. Możesz użyć polecenia `restore` do przywrócenia całego systemu plików lub wybrania pojedynczych plików, które mają zostać przywrócone. Polecenie odzyskuje pliki z określonego nośnika i kopiuje je do bieżącego katalogu (katalogu, z którego uruchamiane jest polecenie `restore`), możliwe jest dodatkowo odzyskanie struktury katalogów. Podobnie jak w przypadku polecenia `dump`, pierwszy parametr przekazywany do polecenia `restore` to lista jednoznakowych kodów opcji przedstawionych w tabeli 13.5.

Przywracanie całego systemu plików

Powróćmy do omówionego wcześniej przykładu piątkowej awarii dysku. Zainstalowałeś pachnący nowością dysk twardy i masz pod ręką taśmy z kopiami bezpieczeństwa. Czas przywrócić pliki. Dla potrzeb tego przykładu zakładam, że dysk, który uległ awarii, zawierał tylko partycję */home* i system Fedora działa bez zakłóceń. Jeśli jednak zawierał on system operacyjny Fedora Core, musisz zacząć od ponownego zainstalowania systemu i dopiero po zakończeniu tej operacji możesz przejść do odzyskiwania plików z kopii bezpieczeństwa.

Zanim zaczniesz odzyskiwać pliki na swój nowy dysk twardy, musisz na nim utworzyć pusty system plików. Do tego celu możesz użyć polecenia `mkfs`. Pozwala ono na podanie różnego rodzaju parametrów, ale zwykle musisz jedynie wpisać nazwę urządzenia, na którym ma powstać system plików. Dlatego, aby przygotować nowy dysk twardy, wpisz polecenie:

```
# mkfs /dev/hda6
```

Innym rozwiązaniem, ponieważ nasz katalog */home* jest wymieniony w pliku */etc/fstab*, jest możliwość określenia punktu montowania `/home`, a polecenie `mkfs` odszuka odpowiednie urządzenie. Dlatego przedstawione wcześniej polecenie może być zastąpione przez następujące:

```
# mkfs /home
```

Tabela 13.5. *Opcje polecenia restore*

Opcje polecenia restore	Opis
`-r`	Przywracanie całego archiwum
`-C`	Porównywanie zawartości zrzuconego pliku z plikami na dysku. Opcja wykorzystywana do sprawdzenia, czy operacja przywracania danych została zakończona pomyślnie
`-R`	Rozpocznij proces przywracania od określonej taśmy w przypadku kopii bezpieczeństwa składającej się z wielu taśm. Opcja wykorzystywana do ponownego uruchomienia procesu przywracania, który został przerwany
`-X` *lista_ plików*	Odzyskiwane są z archiwum tylko określone pliki lub katalogi. Opcja wymaga podania jednego argumentu — listy plików lub katalogów, które mają zostać odzyskane
`-T` *plik*	Wyświetla zawartość zrzuconego archiwum. Jeśli plik lub katalog jest podany jako argument, wyświetla tylko informacje dotyczące wystąpienia tego pliku, katalogu lub zawartości tego katalogu
`-i`	Przywraca pliki w trybie interaktywnym
`-b` *rozmiar_ bloku*	Określa rozmiar bloku zrzutu w kilobajtach. Opcja wymaga podania argumentu numerycznego
`-D` *system_ plików*	Określa nazwę systemu plików, który ma być porównany przy wykorzystaniu opcji `C`. Nazwa systemu plików jest przekazywana jako argument
`-F` *skrypt*	Określa nazwę archiwum, z którego należy przywrócić dane. Opcja wymaga podania argumentu alfanumerycznego
`-h`	Jeśli użyta została ta opcja, polecenie `restore` odtwarza katalogi oznaczone do rozpakowania, ale nie rozpakowuje ich zawartości
`-m`	Pliki są odzyskiwane w oparciu o numer i-węzła zamiast uwzględniania nazwy. Opcja nie jest zbyt często wykorzystywana
`-N`	Zamiast rozpakowywania plików, wyświetlane są ich nazwy
`-s` *numer_ pliku*	Określa plik zrzutu, od którego polecenie ma zacząć przywracanie danych w przypadku taśmy z wieloma systemami plików. Opcja wymaga podania argumentu w formacie numerycznym
`-T` *katalog*	Informuje polecenie `restore`, gdzie należy zapisywać ewentualne pliki tymczasowe. Opcja przydatna, jeśli system został uruchomiony z dyskietki (na której nie ma miejsca na pliki tymczasowe)
`-v`	Pozwala na wypisywanie większej ilości informacji. Polecenie `restore` wyświetla informacje o każdym pliku, który jest przywracany
`-y`	Polecenie `restore` będzie kontynuować działanie po napotkaniu uszkodzonego bloku, zamiast czekać na potwierdzenie użytkownika, że proces ma być kontynuowany

Należy zachować szczególną ostrożność podczas korzystania z polecenia `mkfs`. Jeśli podasz niewłaściwą nazwę urządzenia, możesz niechcący usunąć wszystkie dane z istniejącego systemu plików.

Po utworzeniu systemu plików na nowym dysku podłącz partycję do tymczasowego punktu montowania.

```
# mkdir /mnt/test
# mount /dev/hda6 /mnt/test
```

Powoduje to podłączenie nowego systemu plików do katalogu */mnt/test*. Teraz przejdź do tego katalogu (`cd /mnt/test`) i użyj polecenia `restore`, aby odzyskać cały system plików z taśmy z kopią bezpieczeństwa. Oczywiście przy założeniu, że umieściłeś odpowiednią taśmę w napędzie taśm.

```
# cd /mnt/test
# restore rf /dev/nrft0
```

Po zakończeniu przywracania plików możesz odłączyć partycję i podłączyć ją w odpowiednim punkcie montowania. Jeśli odzyskałeś system plików na inną partycję fizyczną niż ta, na której wcześniej się znajdował, upewnij się, że odpowiednio zmodyfikowałeś plik */etc/fstab*, aby odpowiednia partycja została podłączona przy kolejnym uruchomieniu systemu.

Odzyskiwanie poszczególnych plików

Polecenie `restore` może być wykorzystane do przywracania poszczególnych plików i katalogów. Używając polecenia `restore` w trybie interaktywnym, możesz kolejno wpisać zestaw poleceń `restore` do selektywnego przywracania plików. Aby uruchomić polecenie `restore` w trybie interaktywnym, użyj parametru `i` zamiast parametru `r`:

```
# restore if /dev/nrst0
```

Polecenie `restore` odczyta indeks plików z taśmy kopii bezpieczeństwa i wyświetli znak zachęty polecenia `restore`. Możesz wpisać polecenia pozwalające wybrać pliki i katalogi, które mają zostać przywrócone. Możesz przemieszczać się w strukturze katalogów indeksu kopii bezpieczeństwa w taki sam sposób w jaki przemieszczasz się w systemie plików przy użyciu wiersza poleceń powłoki systemowej. Interaktywna wersja polecenia `restore` oferuje nawet własne wersje poleceń `cd` i `ls`, co pokazano w tabeli 13.6.

Załóżmy, że użytkownik *joe* niechcący usunął podkatalog *Mail* z własnego katalogu domowego. Tak się składa, że Joe jest Twoim przełożonym, więc musisz pilnie odzyskać jego pliki. Oto sposób, w jaki możesz się uporać z tym zadaniem.

Umieść odpowiednią taśmę w napędzie i zaloguj się jako użytkownik *root*. Użyj polecenia `cd`, aby przejść do katalogu głównego partycji */home*, a następnie uruchom polecenie `restore` w trybie interaktywnym:

```
# cd /home
# restore if /dev/nrft0
```

Sprawdź, czy masz taśmę z kopią bezpieczeństwa partycji */home*, wpisując polecenie `ls`. Powinieneś zobaczyć listę katalogów odpowiadającą użytkownikom, których katalogi domowe znajdują się w katalogu */home*:

```
restore > ls
.:
bob/      jane/       joe/      lost+found/       mary/      thad/
```

Tabela 13.6. *Interaktywne polecenia restore*

Polecenie	Opis
`add`	Dodaje plik lub katalog do listy plików, które mają być odzyskane. Jeśli katalog ma być odzyskany, wszystkie katalogi i pliki znajdujące się wewnątrz również zostaną odzyskane
`cd`	Zmienia bieżący katalog widoczny w archiwum. Działa analogicznie jak polecenie `cd` używane w wierszu poleceń powłoki systemowej
`delete`	Usuwa plik lub katalog z listy plików, które mają zostać odzyskane. Usunięcie katalogu z listy powoduje usunięcie z listy wszystkich katalogów i plików, które znajdują się wewnątrz
`extract`	Odzyskuje z archiwum wszystkie zaznaczone pliki i katalogi i zapisuje je w systemie plików
`help`	Wyświetla listę dostępnych poleceń
`ls`	Wyświetla zawartość bieżącego katalogu. Jeśli nazwa katalogu jest podana jako argument, wyświetla zawartość tego katalogu. Pliki lub katalogi oznaczone do odzyskania powinny rozpoczynać się znakiem *
`pwd`	Wyświetla pełną nazwę ścieżki bieżącego katalogu archiwum
`quit`	Kończy tryb interaktywnego przywracania danych
`setmodes`	Pliki nie są przywracane; uzgadniane są tryby istniejących plików na dysku docelowym z trybami zapisanymi w pliku zrzutu. Takie rozwiązanie jest przydatne, jeśli przywracane są dane z kopii bezpieczeństwa, której wykonywanie zostało przerwane przed zakończeniem
`verbose`	Wyświetla informacje dotyczące procesu przywracania podczas jego trwania. Wyświetlane wyniki zawierają informację o każdym pliku, który jest przywracany

Tak, teraz widać, że to jest partycja */home*. Przejdź do katalogu domowego użytkownika *joe* za pomocą polecenia `cd`. Użyj ponownie polecenia `ls`, aby zobaczyć zawartość jego katalogu domowego:

```
restore > cd joe
restore > ls
./joe:
.mozilla/    Desktop/    report.html
.tcshrc          Mail/       letter.txt
.xinitrc         News/       www/
```

Teraz zaznacz, że katalog *Mail* powinien zostać odzyskany, korzystając z polecenia `add`:

```
restore > add Mail
```

Jeśli ponownie użyjesz polecenia `ls`, zobaczysz, że nazwa katalogu *Mail* jest poprzedzona znakiem `*`, co oznacza, że został on zaznaczony i ma być odzyskany.

```
restore > ls
./joe:
.mozilla/  Desktop/     report.html
.tcshrc        *Mail/        letter.txt
.xinitrc        News/        www/
```

Teraz użyj polecenia `extract`, aby rozpocząć proces przywracania. Polecenie `restore` poprosi o podanie numeru taśmy, od którego należy rozpocząć przywracanie. Nasza kopia bezpieczeństwa mieści się na jednej taśmie, więc wpisz numer `1`. Jeśli pojawi się pytanie

`set owner/mode for '.'?`, daj odpowiedź twierdzącą, wciskając klawisz *y*, a później klawisz *Enter*. Następnie przywrócone zostaną uprawnienia (jeśli zachodzi taka konieczność) do katalogu, który jest przywracany. W naszym przypadku nie ma to kluczowego znaczenia, ale zawsze powinieneś dawać odpowiedź twierdzącą, jeśli odzyskujesz pełną kopię bezpieczeństwa. Teraz na ekranie powinny być widoczne następujące informacje:

```
restore > extract
You have not read any tapes yet.
Unless you know which volume your file(s) are on you
should start with the last volume and work toward the first.
Specify next volume #: 1
set owner/mode for '.'? [yn] y
restore >
```

W tym momencie pliki są już przywrócone na dysk i możesz zamknąć program `restore` poleceniem `quit`. To wszystko, co było do zrobienia. Znasz już podstawy wykorzystania poleceń `dump` i `restore`.

Konfigurowanie narzędzia Amanda do wykonywania sieciowych kopii bezpieczeństwa

Pakiet `Amanda` (ang. *Advanced Maryland Automatic Network Disk Archiver*) pozwala przy użyciu jednego napędu taśmowego o dużej pojemności zainstalowanego na serwerze zarchiwizować za pośrednictwem sieci pliki znajdujące się na wielu komputerach. Pakiet *Amanda* obejmuje całą gamę poleceń. Instrukcja obsługi tego pakietu zawiera szczegółowe informacje na temat poleceń przedstawionych w tabeli 13.7.

Polecenie `amdump` będzie najczęściej wykorzystywane, ale zanim zaczniemy go używać, musimy skonfigurować pewne ustawienia zarówno na serwerze kopii bezpieczeństwa (system, do którego podłączony jest napęd taśm), jak i na stacjach klienckich (systemy, które zapisują swoje kopie bezpieczeństwa).

Tworzenie katalogów Amanda

Musisz utworzyć katalogi, które będą przechowywały pliki konfiguracyjne narzędzia *Amanda* oraz zapisywane przez narzędzie pliki dzienników. Pliki konfiguracyjne są zapisywane w katalogu */etc/amanda*, a pliki dzienników — w katalogu */var/lib/amanda*. W obu wypadkach powinieneś zalogować się jako użytkownik `amanda` i utworzyć podkatalogi wewnątrz tych katalogów, po jednym dla każdego harmonogramu tworzenia kopii bezpieczeństwa, który będziesz uruchamiać, oraz plik indeksu, co pokazano poniżej.

```
# su - amanda
$ mkdir -p /var/lib/amanda/normal/index
$ mkdir -p /etc/amanda/normal
```

Ze względów bezpieczeństwa należałoby wykonywać zadania administracyjne narzędzia *Amanda* z poziomu specjalnego konta użytkownika *amanda*. W tym celu z poziomu użytkownika *root* należy nadać hasło dla konta *amanda* za pomocą polecenia `passwd amanda`. Jednak lepszym rozwiązaniem może być nienadawanie hasła kontu *amanda*. Wtedy w celu wykonania zadań za pomocą narzędzia *Amanda* (bez podawania dodatkowego hasła) wystarczy z konta użytkownika *root* wykonać polecenie `su - amanda`. Dalsza część przedstawionej procedury zakłada, że jesteś już zalogowany jako *amanda*.

Tabela 13.7. *Polecenia wykonywania kopii bezpieczeństwa narzędzia Amanda*

Polecenie	Opis
`amdump`	Wykonuje automatyczne kopie bezpieczeństwa *Amanda*. Zwykle jest uruchamiane przez narzędzie *cron* na komputerze, który zarządza napędem taśm i wykonaniem kopii bezpieczeństwa systemów klienckich. Polecenie `amdump` zapisuje na taśmie kopie bezpieczeństwa wszystkich dysków wymienionych w pliku *disklist* lub, jeśli wystąpi problem, na dysku tymczasowym. Po wykonaniu wszystkich kopii bezpieczeństwa polecenie `amdump` przesyła pocztą elektroniczną wiadomość zawierającą informacje o udanych i nieudanych operacjach
`amflush`	Przenosi kopie bezpieczeństwa z dysku tymczasowego na taśmę. Polecenie `amflush` jest uruchamiane po przekazaniu przez polecenie `amdump` informacji, że kopia bezpieczeństwa nie może być zapisywana na taśmę. W takiej sytuacji kopie bezpieczeństwa pozostają na dysku tymczasowym. Po rozwiązaniu problemu z napędem taśm należy uruchomić polecenie `amflush` w celu przepisania kopii bezpieczeństwa z dysku tymczasowego na taśmę
`amcleanup`	Porządkuje dane po przerwanym poleceniu `amdump`. Polecenie musi być uruchomione, tylko wtedy gdy z jakiegoś powodu polecenie `amdump` nie mogło zostać zakończone pomyślnie. Zwykle ma to miejsce, kiedy serwer taśm wygeneruje błąd podczas uruchamiania polecenia `amdump`
`amrecover`	Oferuje interaktywny interfejs umożliwiający przeglądanie plików indeksu *Amanda* i wybór taśm, z których pliki mają być przywracane. Polecenie `amrecover` może również uruchamiać polecenie `amrestore` oraz systemowy program przywracania danych (na przykład `tar`)
`amrestore`	Odczytuje taśmy *Amanda*, wyszukując żądanych kopii bezpieczeństwa. Polecenie `amrestore` pozwala wykonywać wszystkie operacje, począwszy od interaktywnego przywracania pojedynczych plików po przywracanie pełnej kopii bezpieczeństwa wszystkich partycji uszkodzonego dysku
`amlabel`	Zapisuje na taśmie nagłówek pakietu *Amanda*. Wszystkie taśmy *Amanda* muszą być oznaczone za pomocą polecenia `amlabel`. Polecenia `amdump` i `amflush` nie pozwalają zapisywać na taśmach, które nie mają odpowiedniego nagłówka
`amcheck`	Sprawdza, czy właściwa taśma jest umieszczona w napędzie taśm oraz czy wszystkie systemy plików we wszystkich systemach klienckich są gotowe do wykonania kopii bezpieczeństwa. Polecenie może być uruchamiane przez narzędzie `cron` przed poleceniem `amdump`, dzięki czemu administrator otrzyma wiadomość z ostrzeżeniem, że operacja się nie powiedzie, jeśli nie wykona określonej czynności w celu rozwiązania problemu
`amadmin`	Odpowiada za wykonanie zadań administracyjnych, takich jak odszukiwanie taśm potrzebnych do odtworzenia systemu plików, wybór odpowiednich dysków do wykonania pełnej kopii bezpieczeństwa oraz sprawdzanie harmonogramu wykonywanych prac
`amtape`	Odpowiada za obsługę narzędzia do zmieniania taśm w napędzie. Umożliwia załadowanie odpowiednich taśm, wysuwanie taśm z napędu i skanowanie magazynu taśm
`amverify`	Sprawdza, czy na taśmach *Amanda* nie występują błędy (dotyczy to jedynie kopii bezpieczeństwa w formacie GNU tar)
`amrmtape`	Usuwa taśmę z listy taśm oraz z bazy danych *Amanda*
`amstatus`	Podaje status uruchomionego polecenia `amdump`

Dla celów tego przykładu utworzyłem konfigurację wykonania kopii bezpieczeństwa *normal*, która zapisuje dane z kilku komputerów. Możesz zdecydować się na utworzenie konfiguracji kopii bezpieczeństwa, która będzie zapisywała partycje zawierające system operacyjny. Wtedy będziesz mógł uruchamiać wykonanie kopii bezpieczeństwa przed uaktualnieniem systemu operacyjnego.

Musisz również określić dysk tymczasowy, którego może używać narzędzie *Amanda* do tymczasowego kolejkowania kopii bezpieczeństwa przed zapisaniem ich na dysk. Katalog ten powinien zawierać dużo wolnej przestrzeni. Na moim serwerze znajduje się duża partycja */home*, dlatego tam właśnie umieściłem katalog *Amanda*:

```
# mkdir /home/amanda
# chmod 700 /home/amanda
# chown amanda /home/amanda
# chgrp disk /home/amanda
```

Tworzenie pliku amanda.conf

Jako użytkownik *amanda* musisz utworzyć dwa pliki konfiguracyjne dla narzędzia *Amanda* i zapisać je w katalogach */etc/amanda/normal*: *amanda.conf* i *disklist*. Możesz zacząć od skopiowania przykładowych plików z katalogu */etc/amanda/DailySet1*:

```
$ cd /etc/amanda/DailySet1
$ cp amanda.conf disklist /etc/amanda/normal
```

Plik *amanda.conf* definiuje wiele ogólnych wartości konfiguracyjnych, a plik *disklist* określa, które komputery i partycje mają być zapisywane w kopii bezpieczeństwa. Plik *amanda.conf* jest dosyć złożony, ale na szczęście większość definiowanych wartości może pozostać w domyślnej formie. Oto uproszczony przykład pliku *amanda.conf* wraz z dołączonymi komentarzami:

```
#
# amanda.conf - przykładowy plik konfiguracyjny
# Amanda. Przedstawiony plik to kolejna z wersji rzeczywistego pliku
# konfiguracyjnego wykorzystywana przez CS.UMD.EDU.

org "GLACI"         # nazwa organizacji wykorzystywana przez raporty
mail to "amanda"    # uruchamiane przez amdump
dumpuser "amanda"   # użytkownik, na prawach którego
                    # uruchamiany jest dump

# Określ nazwę napędu i (lub) lub zmieniarki taśm. Jeśli nie
# masz zmieniarki i nie chcesz wykorzystywać więcej niż
# jednej taśmy podczas jednej sesji amdump, umieść
# znak komentarza na początku definicji tpchanger.

runtape 1                # ilość taśm wykorzystywanych
                         # podczas pojedynczej
                         # sesji amdump
tapedev "/dev/nrft0"     # wykorzystanie napędu taśm bez przewijania
rawtapedev "/dev/nrft0"  # wykorzystanie samodzielnego
                         # urządzenia (tylko ftape)

tapetype HP-DAT # rodzaj taśmy
            # (przejdź do sekcji tapetypes poniżej)
labelstr "^normal[0-9][0-9]*$" # określa, że wszystkie typy taśm są odpowiednie
```

```
# Określa dysk tymczasowy. Jest on wykorzystywany
# jako tymczasowa przestrzeń przechowywania dla
# zrzutów przed zapisaniem ich na taśmę i jest to
# rozwiązanie zalecane w większości wypadków.

holdingdisk hd1 {
  comment "main holding disk"
  directory "/home/amanda"   # lokalizacja dysku tymczasowego
  use 290 Mb         # ilość przestrzeni dostępnej do wykorzystania
  chunksize -1               # rozmiar jednostki
  }

# Poniżej przedstawione słowo kluczowe infofile jest tutaj
# zamieszczone tylko ze względów historycznych, ponieważ
# obecnie powinien to być katalog (chyba, że wybrany został
# format bazy danych inny niż domyślne ustawienie 'text')

infofile  "/usr/adm/amanda/normal/curinfo"   # database DIRECTORY
logdir "/usr/adm/amanda/normal"              # log directory
indexdir "/usr/adm/amanda/normal/index"      # index directory

# tapetypes

# Definicja rodzaju wykorzystywanej taśmy wskazanej
# w definicji "tapetype" znajdującej się powyżej. Niektóre
# typowe rodzaje taśm zostały wymienione w tej sekcji.
# Typ taśmy informuje narzędzie amanda, ile MB zmieści się na taśmie,
# jak duże są znaczniki plików i jak szybki jest napęd taśm.

define tapetype HP-DAT {
      comment "DAT tape drives"
      # dane dostarczone przez Roba Browninga rbl@cs.utexas.edu
      length 1930 mbytes
      filemark 111 kbytes
      speed 468 kbytes
}

# dumptypes
#
# Odwołania do tej sekcji są umieszczone
# w pliku zawierającym listę dysków.

define dumptype global {
      comment "Gobal definitions"
      # Definicja przydatna do określania parametrów globalnych,
      # dzięki czemu nie musisz ich zapisywać wszędzie.
}

define dumptype always-full {
     global
     comment "Full dump of this filesystem always"
     compress none
     priority high
     dumpcycle 0
}
```

Przykładowy plik *amanda.conf* został napisany w oparciu o bardziej obszerny przykład znajdujący się w katalogu */etc/amanda/DailySet1*. Przykładowy plik *amanada.conf* zawiera dodatkowe informacje dotyczące dostępnych opcji konfiguracyjnych. Więcej informacji znajdziesz również w instrukcji pakietu *Amanda* (wpisz polecenie `man amanda`). Dodatkowe instrukcje znajdziesz w katalogu */usr/share/doc/amanda-server**. W skrócie, musisz wykonać następujące kroki.

- Zmodyfikuj nazwę organizacji dla potrzeb generowanych raportów.
- Zmień nazwy urządzeń dla poleceń `tapedev` i `rawtapedev`, aby odpowiadały nazwom napędów taśm w systemie.
- Wybierz wpis typu taśmy odpowiedni dla Twojego napędu taśm.
- Zmień nazwę katalogu określonego w sekcji dotyczącej dysku tymczasowego przechowywania danych, aby odpowiadała nazwie utworzonego wcześniej katalogu.

Tworzenie pliku disklist

Musisz również utworzyć plik *disklist* w katalogu */etc/amanda/normal*. Zawiera on listę systemów i partycji dysków, które będą umieszczone na kopii bezpieczeństwa. Informacja `always-full` jest zamieszczona na końcu każdego wpisu, dzięki czemu narzędzie *Amanda* wie, jakiego typu kopia bezpieczeństwa ma zostać wykonana. Określa ona tworzenie pełnych zamiast przyrostowych kopii bezpieczeństwa.

```
# przykładowy plik zawierający listę dysków Amanda2
#
# Format pliku to:
#
# hostname diskdev dumptype [spindle [interface]]
#
# zawiera informacje o typach zrzutów określonych
# przed administratora w pliku amanda.conf.

damian hda5 always-full
damian hda6 always-full
damian hda7 always-full
damian hda8 always-full

daria hda5 always-full
daria hda6 always-full
daria hda7 always-full
daria hda1 always-full
daria hda2 always-full
```

Przykładowy plik odpowiada za tworzenie kopii bezpieczeństwa dwóch komputerów, *damian* i *daria*. Porządek wykonywania kopii bezpieczeństwa odpowiada ważności zapisywanych danych — najważniejsze dane są zapisywane na początku. Dzięki temu, jeśli zabraknie miejsca na taśmie, najważniejsze dane będą już na niej zapisane.

Dodawanie usług sieciowych narzędzia Amanda

Narzędzie *Amanda* jest zaprojektowane do wykonywania kopii bezpieczeństwa przez sieć. Następujące usługi `amanda` są zdefiniowane w pliku */etc/services*:

```
amanda 10080/udp
amanda 10080/tcp
```

```
amandaidx 10082/tcp
amidxtape 10083/tcp
```

Na serwerze amanda

Aby udostępnić następujące usługi systemu Fedora Core w sieci, musisz skonfigurować demona `xinetd`, aby nasłuchiwał żądań nadchodzących do tych usług. W tym celu, wykonując jako użytkownik *root* poniższe polecenia, powinieneś uaktywnić usługi `amandaidx` i `amidxtape`.

```
# chkconfig amidxtape on
# chkconfig amandaidx on
```

Dzięki temu narzędzie *Amanda* może przyjmować zgłoszenia od systemów klienckich i uruchamiać proces wykonywania kopii bezpieczeństwa bez interwencji użytkownika. Demon `xinetd` musi zostać powiadomiony o konieczności ponownego odczytania plików */etc/xinetd.d*, zanim zmiany zostaną wprowadzone w systemie. Możesz to zrobić, wpisując następujące polecenie z konta użytkownika *root*:

```
# /etc/init.d/xinetd reload
```

Na każdej stacji klienckiej amanda

Musisz skonfigurować pliki *.amandahosts* w katalogu */var/lib/amanda* na każdej stacji klienckiej, której kopia bezpieczeństwa będzie wykonywana przez serwer *amanda*. Plik powinien zawierać pełną nazwę serwera kopii bezpieczeństwa wraz z nazwą domeny, który będzie się łączył ze stacją. Na początku w pliku jako serwer kopii zapasowych zdefiniowany jest jedynie lokalny komputer. W celu przypisania takiej roli innemu komputerowi należy wykonać następujące polecenie (kiedy zalogujesz się jako użytkownik *amanda*, w miejsce łańcucha `amandahost` zostanie wstawiona nazwa serwera kopii zapasowych):

```
$ echo amandahost >> /var/lib/amanda/.amandahosts
```

Musisz się upewnić, że demon klienta *amanda* jest skonfigurowany do uruchamiania na stacji klienckiej. W tym celu jako użytkownik *root* wykonaj następujące polecenie:

```
# chkconfig amanda on
```

Ustawienie to pozwala stacji klienckiej *amanda* komunikować się z serwerem *amanda*. Znowu musisz powiadomić proces demona `xinetd` o konieczności ponownego wczytania plików */etc/xinetd.d*, aby zmiany zostały zapamiętane. W tym celu należy z konta użytkownika *root* wpisać następujące polecenie:

```
# /etc/init.d/xinetd reload
```

Wykonywanie kopii bezpieczeństwa narzędziem Amanda

Teraz, kiedy już wszystkie ustawienia zostały skonfigurowane, możesz przejść do wykonania kopii bezpieczeństwa za pomocą narzędzia *Amanda*. Z konta użytkownika *root* wpisz następujące polecenie:

```
# /usr/sbin/amdump normal
```

Uruchomione zostaje polecenie amdump zaczynające działanie od odczytania plików konfiguracyjnych, które znajdzie w utworzonym wcześniej katalogu */etc/amanda/normal*. Następnie przechodzi do odczytania listy systemów i partycji z pliku *disklist*, wykonując kopie bezpieczeństwa każdej partycji zgodnie z ich porządkiem występowania na liście. Wyniki wykonania polecenia amdump są zapisywane w katalogu */var/lib/amanda/normal*. Przejrzyj pliki, które tam znajdziesz, aby sprawdzić wyniki wykonania kopii bezpieczeństwa. (W poprzednim podrozdziale znajdziesz informacje dotyczące tworzenia pliku *disklist*, co pozwoli na łatwiejsze zrozumienie procesu wykonywanego przez polecenie amdump).

Możesz oczywiście zautomatyzować ten proces przy użyciu narzędzia cron. Aby utworzyć harmonogram uruchamiania polecenia amdump, podobny do harmonogramu polecenia dump omówionego w poprzedniej części rozdziału, wykonaj opisane dalej kroki. Z konta użytkownika *root* wpisz polecenie crontab z parametrem -e:

```
# crontab -e
```

Spowoduje to uruchomienie pliku *crontab* w edytorze tekstów. Umieść następujące wpisy na końcu pliku:

```
0 22 * * 0 /usr/sbin/amdump normal
0 22 * * 1 /usr/sbin/amdump incremental
0 22 * * 2 /usr/sbin/amdump incremental
0 22 * * 3 /usr/sbin/amdump incremental
0 22 * * 4 /usr/sbin/amdump incremental
0 22 * * 5 /usr/sbin/amdump incremental
0 22 * * 6 /usr/sbin/amdump incremental
```

Zapisz plik i zamknij edytor tekstów. Demon crond uruchomi polecenie amdump każdego dnia tygodnia o godzinie 22:00. W przedstawionym przykładzie przyjęto założenie, że utworzona została druga konfiguracja dla wykonywania kopii przyrostowej. W tym celu należy utworzyć podkatalog o nazwie *incremental* w katalogu */etc/amanda* i zapisać w nim odpowiednio zmodyfikowane pliki *amanda.conf* i *disklist*. Musisz również utworzyć podkatalog o nazwie *incremental* w katalogu */usr/adm/amanda*, gdzie narzędzie *Amanda* będzie zapisywać dzienniki zdarzeń.

Prawidłowe skonfigurowanie wszystkich elementów może zająć Ci dłuższą chwilę, ale po ich ustawieniu narzędzie *Amanda* może znacznie uprościć wykonywanie i zarządzanie sieciowymi kopiami bezpieczeństwa. *Amanda* może okazać się zbyt złożonym narzędziem dla małej firmy, ale w przypadku dużej sieci korporacyjnej pozwala systemowi Fedora Linux działać w charakterze sieciowego serwera kopii bezpieczeństwa.

Korzystanie z narzędzia archiwizacji pax

Na przestrzeni lat powstało wiele systemów operacyjnych typu Unix, co doprowadziło do utworzenia całej gamy podobnych, ale niezgodnych ze sobą formatów archiwizowania plików. Nawet narzędzia o tej samej nazwie mogą wykorzystywać nieznacznie różniące się od siebie formaty zapisu w różnych systemach. Tego typu niezgodności mogą powodować wystąpienie poważnych problemów podczas archiwizowania i odzyskiwania danych w środowisku wielosystemowym. Na szczęście istnieje rozwiązanie tego problemu.

Program `pax` to narzędzie w standardzie POSIX, które może odczytywać i zapisywać szeroką gamę formatów archiwalnych. Pakiet RPM dla narzędzia `pax` jest częścią systemu Fedora Core. Jeśli pakiet RPM nie jest zainstalowany, skopiuj plik *pax-** z dystrybucyjnego CD-ROM-u nr 1 lub pobierz go z witryny FTP Fedora Linux, a następnie użyj polecenia `rpm`, aby go zainstalować.

```
# rpm -Uhv pax-*
```

Pamiętaj, że musisz być zalogowany jako użytkownik *root* podczas instalowania oprogramowania przy użyciu polecenia `rpm`.

Narzędzie `pax` przyjmuje wiele opcji wiersza poleceń. Ostatnim parametrem jest zwykle nazwa pliku lub katalogu, który ma zostać zarchiwizowany. Możesz używać znaków „*” lub „?” do określenia większej liczby plików lub katalogów. Najczęściej używane opcje to `-r` lub `-w` wykorzystywane do określenia odczytu lub zapisu archiwum. Są one zwykle wykorzystywane w połączeniu z parametrem `-f`, który pozwala określić nazwę pliku archiwum.

Różne kombinacje polecenia `pax` umożliwiają rozpakowanie dowolnego archiwum, tworzenie archiwum, wyświetlenie zawartości archiwum, a nawet skopiowanie całej hierarchii katalogów z jednego miejsca w inne. Tabela 13.8 przedstawia kilka przykładów wykorzystania polecenia `pax`.

Tabela 13.8. *Przykłady wykorzystania polecenia pax*

Zastosowania polecenia pax	Opis
`pax -f mojepliki`	Wyświetla zawartość archiwum o nazwie *mojepliki*
`pax -r -f mojepliki`	Rozpakuj zawartość archiwum o nazwie *mojepliki*
`pax -w -f mojepliki /etc`	Tworzy archiwum o nazwie *mojepliki* zawierające wszystko, co znajduje się w katalogu */etc*
`pax -w -f mojepliki *.txt`	Archiwizuje w bieżącym katalogu wszystkie pliki, które mają rozszerzenie *.txt*
`pax -r -w /starykatalog /nowykatalog`	Kopiuje zawartość katalogu */starykatalog* do katalogu */nowykatalog*
`pax -w -B 1440000 -f /dev/fd0 *`	Archiwizuje zawartość bieżącego katalogu na wiele dyskietek
`pax -w -x cpio -f mojepliki`	Archiwizuje zawartość bieżącego katalogu w pliku o nazwie *mojepliki*, korzystając z formatu *cpio*
`pax -r -U maria -f kopiebezpieczenstwa`	Rozpakowuje wszystkie pliki, których właścicielem jest użytkownik *maria* z archiwum o nazwie *kopiebezpieczenstwa*

Zwróć uwagę, że jeśli pominiesz zarówno opcję `-r`, jak i `-w`, to możesz wyświetlić przy użyciu polecenia `pax` zawartość archiwum. Jeśli użyjesz obydwu opcji, `-r` i `-w`, powinieneś pominąć opcję `-f` i określić katalogi źródłowe i docelowe. Wynikiem użycia takiego polecenia będzie odzwierciedlanie zawartości katalogu źródłowego w katalogu docelowym.

Możesz zastosować dodatkowe parametry, aby jeszcze bardziej zmienić działanie polecenia `pax`. Spróbuj użyć opcji `-x` w połączeniu z opcją `-w`, aby określić konkretny typ archiwum, które ma zostać utworzone. Możesz również użyć opcji `-B`, aby podać ilość bajtów, które mają być zapisane w każdym wolumenie archiwum składającego się z wielu wolumenów.

Tabela 13.9 opisuje w skrócie parametry polecenia `pax`.

Tabela 13.9. *Opcje polecenia pax*

Opcje polecenia pax	Opis
`-r`	Odczytuje pliki z archiwum
`-w`	Zapisuje pliki w archiwum
`-a`	Dopisuje pliki do istniejącego archiwum
`-b` *rozmiar_bloku*	Określa rozmiar bloku danych w archiwum. Podana liczba musi być wielokrotnością liczby 512
`-c` *wzorzec*	Dopasowuje wszystkie pliki z wyjątkiem plików pasujących do określonego wzorca
`-d`	Dopasowuje nazwy plików do podanego wzorca nazw plików lub katalogów, bez uwzględniania całej ścieżki
`-f` *archiwum*	Określa nazwę archiwum
`-i`	Zmienia nazwy plików podczas archiwizowania
`-k`	Nie pozwala zastępować istniejących plików
`-l`	W trybie kopiowania (`-r -w`) łączy pliki za pomocą sztywnych dowiązań
`-n` *wzorzec*	Dopasowuje tylko pierwszy plik, który odpowiada określonemu wzorcowi
`-o` *opcje*	Opcje dodatkowe wymagane przez wykorzystywany format archiwizacji
`-p` *łańcuch*	Określa charakterystykę pliku, która powinna być zachowana podczas archiwizowania lub kopiowania. Więcej informacji na temat znajdziesz w instrukcji polecenia `pax`
`-s` *nowyłańcuch*	Zmienia nazwy plików archiwalnych, wykorzystując podane wyrażenie
`-t`	Zachowuje informacje o czasach dostępu do plików archiwalnych
`-u`	Pliki nie są zastępowane starszymi wersjami
`-v`	Podczas działania polecenia wyświetlane są na ekranie informacje
`-x` *format*	Określa format archiwum. Akceptowane formaty to `cpio`, `bcpio`, `sv4cpio`, `sv4crc`, `tar` i `ustar`. Domyślnym formatem tworzenia archiwum jest format `ustar`. Polecenie `pax` automatycznie wykrywa prawidłowy format pliku podczas odczytywania archiwum
`-z`	Wskazuje, że archiwum ma zostać spakowane i rozpakowane za pomocą narzędzia `gzip`
`-B` *bajty*	Określa liczbę bajtów dla każdego wolumenu archiwum. Używamy tej opcji do tworzenia archiwum na zdalnych nośnikach składających się z wielu wolumenów
`-D`	Nie zastępuje istniejących plików plikami, które mają starszy czas modyfikacji wskaźnika
`-E` *limit*	Ogranicza ilość powtórzeń próby odczytu lub zapisu po wystąpieniu błędu
`-G` *grupa*	Wybiera pliki w oparciu o nazwę grupy lub identyfikator GID. Aby wybrać identyfikator GID, umieść znak # przed numerem grupy

Tabela 13.9. *Opcje polecenia pax — ciąg dalszy*

Opcje polecenia pax	Opis
`-H`	Podąża tylko za symbolicznymi łączami wiersza poleceń podczas przemieszczania się między fizycznymi systemami plików
`-L`	Podąża za łączami symbolicznymi, przemieszczając się wewnątrz struktury katalogów
`-P`	Ustawienie domyślne. Nie podąża za łączami symbolicznymi
`-T` *`czas`*	Wybiera pliki w oparciu o datę modyfikacji. Więcej informacji na temat składni tego parametru znajdziesz w instrukcji obsługi polecenia `pax`
`-U` *`użytkownik`*	Wybiera pliki w oparciu o nazwę właściciela lub identyfikator UID, jeśli nazwa jest poprzedzona znakiem #
`-X`	Nie przechodzi do katalogów znajdujących się na innym urządzeniu
`-Y`	Opcja odpowiadająca opcji `-D` z wyjątkiem tego, że sprawdzany jest czas modyfikacji wskaźnika za pomocą nazwy ścieżki utworzonej po zakończeniu modyfikacji wszystkich plików
`-Z`	Opcja odpowiadająca opcji `-u` z wyjątkiem tego, że sprawdzany jest czas modyfikacji wskaźnika za pomocą nazwy ścieżki utworzonej po zakończeniu modyfikacji wszystkich plików

Jak widać, polecenie `pax` to elastyczne i użyteczne narzędzie archiwizacji. Może być szczególnie przydatne przy migracji danych ze starszych typów systemów Linux do nowej wersji. Jeśli staniesz przed koniecznością odtworzenia zarchiwizowanych danych ze starszego lub niedziałającego systemu Unix, obsługa różnych formatów plików narzędzia `pax` może okazać się zbawienna.

Podsumowanie

Miejmy nadzieję, że nigdy nie przydarzy Ci się poważna awaria dysku, ale jeśli tak się stanie, wysiłek włożony w tworzenie kopii bezpieczeństwa zwróci się z nawiązką. Na rynku mamy do dyspozycji wiele rodzajów urządzeń pozwalających na tworzenie kopii bezpieczeństwa. Tradycyjny napęd taśm jest doskonałym rozwiązaniem tworzenia kopii bezpieczeństwa dużych ilości danych. Jeśli w grę wchodzi długoterminowe przechowywanie danych archiwalnych, nagrywalne dyski CD-ROM i DVD będą dobrym rozwiązaniem. Jeśli natomiast najbardziej zależy Ci na zminimalizowaniu czasu, w którym system będzie niedostępny, najlepszym rozwiązaniem jest wykorzystanie kopii lustrzanych dysków. Gdy mówimy o narzędziach służących do wykonywania kopii bezpieczeństwa, należy zwrócić szczególną uwagę na polecenia `dump` i `restore`, dostępne od czasów wczesnych systemów Unix (chociaż obecnie polecenia są w pewnym stopniu uważane za niestabilne). Narzędzie *Amanda* to doskonałe rozwiązanie do wykonywania sieciowych kopii bezpieczeństwa. Jeśli masz do czynienia z kopiami bezpieczeństwa w wielu różnych formatach, przyda Ci się polecenie `pax`.