

UNIX® I LINUX®

PRZEWODNIK ADMINISTRATORA SYSTEMÓW

WYDANIE IV



EVI NEMETH • GARTH SNYDER • TRENT R. HEIN • BEN WHALEY

Terry Morreale, Ned McClain, Ron Jachim, David Schweikert, Tobi Oetiker

» Idź do

- Spis treści
- Przykładowy rozdział
- Skorowidz

» Katalog książek

- Katalog online
- Zamów drukowany katalog

» Twój koszyk

- Dodaj do koszyka

» Cennik i informacje

- Zamów informacje o nowościach
- Zamów cennik

» Czytelnia

- Fragmenty książek online

» Kontakt

Helion SA
ul. Kościuszki 1c
44-100 Gliwice
tel. 32 230 98 63
e-mail: helion@helion.pl
© Helion 1991–2011

Unix i Linux. Przewodnik administratora systemów. Wydanie IV

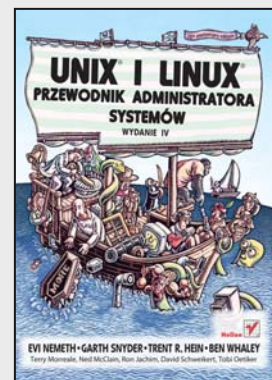
Autorzy: Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley

Tłumaczenie: Marek Pętlicki, Leszek Sagalara

ISBN: 978-83-246-2968-8

Tytuł oryginału: [UNIX and Linux System Administration Handbook \(4th Edition\)](#)

Format: 172×245, stron: 1552



Najobszerniejszy przewodnik po świecie systemów Unix i Linux!

- Jak obowiązkowo ciążą na administratorze?
- Jak zarządzać użytkownikami?
- Jak poprawić wydajność systemu?

Systemy Unix i Linux wykorzystywane są wszędzie tam, gdzie wymagana jest najwyższa niezawodność, wydajność i elastyczność. Ich potencjał, możliwości oraz odporność na niesprzyjające otoczenie sprawiły, że są dominującymi systemami operacyjnymi w zastosowaniach sieciowych. Jeżeli jednak systemy te kojarzą Ci się wyłącznie z czarnym ekranem konsoli oraz trybem tekstowym, jesteś w błędzie. Już od dawna systematycznie zwiększają one swój udział w zastosowaniach domowych. Co w sobie kryją? Jak nimi administrować i jak zwiększać ich wydajność?

Na te i setki innych pytań odpowiada ten obszerny przewodnik. Autorzy rozłożyli na czynniki pierwsze i omówili każde zagadnienie, z którym możesz mieć styczność w codziennej pracy. Po lekturze tej książki będziesz posiadał obszerną wiedzę w tej materii. Instalacja systemu, skrypty powłoki, kontrolowanie procesów, konfiguracja uprawnień to zadania, które nie będą Ci sprawiały żadnych problemów. Ponadto dowiesz się, jak zarządzać użytkownikami, przestrzenią dyskową, zadaniami okresowymi oraz backupami. Dużą uwagę poświęciłeś rozdziałom omawiającym zagadnienia sieciowe. Jest pewne, że serwer, który trafi w Twoje ręce, będzie oferował wiele usług dostępnych przez sieć. Protokoły routingu, usługa DNS, firewall, serwer plików to elementy, które niejednokrotnie będziesz musiał konfigurować.

Nie znajdziesz na rynku obszerniejszej książki poświęconej systemom Unix i Linux. Jeżeli jesteś z nimi związany w pracy zawodowej, interesujesz się systemami operacyjnymi lub korzystasz z nich w domu, ta książka obowiązkowo musi znaleźć się na Twojej półce!

Ta książka to obowiązkowa pozycja dla wszystkich administratorów!

SPIS TREŚCI

Słowo wstępne	45
Wstęp	47
Podziękowania	51

I PODSTAWY ADMINISTROWANIA

1	Od czego zacząć?	55
1.1.	Podstawowe obowiązki administratora	56
	Dodawanie i usuwanie kont użytkowników	57
	Podłączanie i odłączanie sprzętu	57
	Wykonywanie kopii zapasowych	57
	Instalacja i aktualizowanie oprogramowania	58
	Monitorowanie systemu	58
	Rozwiązywanie problemów	58
	Zarządzanie lokalną dokumentacją	58
	Uważne monitorowanie stanu zabezpieczeń	59
	Udzielanie pomocy użytkownikom	59

1.2.	Podstawowe narzędzia administratora	59
1.3.	Tarcia między Uniksem a Linuksem	61
1.4.	Dystrybucje systemu Linux	62
1.5.	Przykładowe systemy używane w tej książce	64
	Przykładowe dystrybucje systemu Linux	65
1.6.	Narzędzia administracyjne specyficzne dla określonych systemów	67
1.7.	Notacja i konwencje typograficzne	68
1.8.	Jednostki	69
1.9.	Strony podręcznika systemowego i inne rodzaje dokumentacji	70
	Organizacja podręcznika systemowego	70
	man: czytanie stron podręcznika systemowego	71
	Miejsce przechowywania stron podręcznika	72
	GNU Texinfo	73
1.10.	Inna dokumentacja autorytatywna	73
	Przewodniki dotyczące określonych systemów	73
	Dokumentacja dotycząca określonych pakietów	74
	Książki	75
	RFC i inne dokumenty internetowe	75
	Linux Documentation Project	75
1.11.	Inne źródła informacji	76
1.12.	Sposoby wyszukiwania i instalacji oprogramowania	77
	Jak sprawdzić, czy oprogramowanie zostało już zainstalowane?	78
	Instalowanie nowego oprogramowania	79
	Instalacja oprogramowania ze źródeł	81
1.13.	Administrowanie systemem pod przymusem	82
1.14.	Zalecana literatura	83
	Administracja systemu	83
	Niezbędne narzędzia	83
1.15.	Ćwiczenia	84

2 Pisanie skryptów i powłoka

87

- 2.1. Podstawy powłoki 88
 - Edycja poleceń 89
 - Potoki i przekierowania 89
 - Zmienne i oznakowanie 91
 - Popularne polecenia filtrujące 92
- 2.2. Skrypty w powłoce bash 96
 - Od poleceń do skryptów 97
 - Wejście i wyjście 99
 - Argumenty wiersza poleceń i funkcje 100
 - Zasięg zmiennej 102
 - Przepływ sterowania 103
 - Pętle 105
 - Tablice i działania arytmetyczne 107
- 2.3. Wyrażenia regularne 109
 - Proces dopasowywania 110
 - Znaki dosłowne 110
 - Znaki specjalne 110
 - Przykłady wyrażeń regularnych 112
 - Przechwytywanie 113
 - Zachłanność, lenistwo i katastrofalne wycofania 114
- 2.4. Programowanie w języku Perl 115
 - Zmienne i tablice 116
 - Tablice i literały łańcuchowe 117
 - Wywołania funkcji 118
 - Konwertowanie typów w wyrażeniach 119
 - Rozwijanie i ujednolicanie zmiennych w łańcuchach 119
 - Hasze 119
 - Odwołania i automatyczne tworzenie anonimowych referencji 121
 - Wyrażenia regularne w Perlu 122
 - Wejście i wyjście 123
 - Przepływ sterowania 123
 - Przyjmowanie i sprawdzanie poprawności wejścia 126
 - Perl jako filtr 127
 - Dodatkowe moduły dla języka Perl 128

- 2.5. Skrypty w języku Python 129
 - Python: szybki start 130
 - Obiekty, łańcuchy, liczby, listy, słowniki, krotki i pliki 132
 - Przykład sprawdzania poprawności wejścia 134
 - Pętle 135
- 2.6. Reguły poprawnego pisanie skryptów 136
- 2.7. Zalecana literatura 138
 - Podstawy powłoki i tworzenie skryptów w powłoce bash 138
 - Wyrażenia regularne 139
 - Skrypty w języku Perl 139
 - Skrypty w języku Python 139
- 2.8. Ćwiczenia 139

3 Uruchamianie i zamykanie systemu

141

- 3.1. Ładowanie systemu 142
 - Awaryjne uruchamianie do powłoki 142
 - Etapy procesu rozruchowego 143
 - Inicjalizacja jądra 143
 - Konfigurowanie sprzętu 144
 - Tworzenie procesów jądra 144
 - Interwencja operatora (tylko w trybie odzyskiwania) 145
 - Wykonywanie skryptów startowych 146
 - Zakończenie procesu rozruchowego 146
- 3.2. Rozruch komputera 147
- 3.3. GRUB 148
 - Opcje jądra 149
 - Konfiguracja wielosystemowa 150
- 3.4. Rozruch w trybie pojedynczego użytkownika 151
 - Tryb pojedynczego użytkownika w programie GRUB 151
 - Tryb pojedynczego użytkownika w systemach z procesorami SPARC 152
 - Tryb pojedynczego użytkownika w systemie HP-UX 152
 - Tryb pojedynczego użytkownika w systemie AIX 153

- 3.5. Skrypty startowe 153
 - Init i jego poziomy uruchomieniowe 154
 - Przegląd skryptów startowych 156
 - Skrypty startowe w systemie Red Hat 158
 - Skrypty startowe w systemie SUSE 160
 - Skrypty startowe w systemie Ubuntu i demon Upstart 161
 - Skrypty startowe w systemie HP-UX 162
 - Uruchamianie systemu AIX 164
- 3.6. Rozruch systemu Solaris 164
 - SMF (Service Management Facility) w systemie Solaris 165
 - Nowy, wspaniały świat — rozruch z SMF 167
- 3.7. Ponowne uruchamianie i zamykanie systemu 168
 - shutdown — elegancki sposób zatrzymywania systemu 169
 - halt i reboot — prostsze sposoby wyłączenia systemu 170
- 3.8. Ćwiczenia 170

4 Kontrola dostępu

i uprawnienia administratora

173

- 4.1. Tradycyjna kontrola dostępu w systemie Unix 174
 - Kontrola dostępu w systemie plików 175
 - Prawa własności do procesów 176
 - Konto użytkownika root 176
 - Setuid i setgid 177
- 4.2. Nowoczesne mechanizmy kontroli dostępu 177
 - Kontrola dostępu oparta na rolach 179
 - SELinux 180
 - Uprawnienia w standardzie POSIX 180
 - PAM 181
 - Kerberos — niezależne uwierzytelnianie kryptograficzne 181
 - Listy kontroli dostępu 182
- 4.3. Kontrola dostępu w praktyce 182
 - Wybór hasła użytkownika root 183
 - Logowanie na konto użytkownika root 184
 - su — zmiana tożsamości użytkownika 185

- sudo — su z ograniczeniami 186
- Skrytki i depozyty na hasła 189
- 4.4. Inni pseudoużytkownicy 191
- 4.5. Ćwiczenia 192

5 Kontrolowanie procesów

193

- 5.1. Elementy składowe procesu 194
 - PID — numer identyfikacyjny procesu 195
 - PPID — identyfikator procesu macierzystego 195
 - UID i EUID — rzeczywisty i efektywny identyfikator użytkownika 195
 - GID i EGID: rzeczywisty i efektywny identyfikator grupy 196
 - Uprzejmość 196
 - Terminal sterujący 197
- 5.2. Cykl życia procesu 197
- 5.3. Sygnały 198
- 5.4. Polecenie kill — wysłanie sygnałów 201
- 5.5. Stany procesów 202
- 5.6. Polecenia nice i renice — zmiana priorytetów przełączania 203
- 5.7. Polecenie ps — monitorowanie procesów 205
- 5.8. Dynamiczne monitorowanie procesów
 - polecenia top, prstat i topas 209
- 5.9. System plików /proc 210
- 5.10. Śledzenie sygnałów i funkcji systemowych
 - polecenia strace, truss i tusc 211
- 5.11. Procesy niekontrolowane 213
- 5.12. Zalecana literatura 215
- 5.13. Ćwiczenia 215

6 System plików

217

- 6.1. Ścieżki dostępu 219
 - Ścieżki względne i bezwzględne 219
 - Spacje w nazwach plików 220

6.2.	Montowanie i odmontowywanie systemów plików	221
6.3.	Organizacja drzewa plików	224
6.4.	Typy plików	226
	Zwykłe pliki	228
	Katalogi	228
	Pliki urządzeń znakowych i blokowych	229
	Gniazda lokalne	230
	Nazwane potoki	231
	Dowiązania symboliczne	231
6.5.	Atrybuty plików	232
	Bity uprawnień	232
	Bity setuid i setgid	233
	Bit lepkości	234
	Polecenie ls — wyświetlanie listy i sprawdzanie plików	234
	Polecenie chmod — zmiana uprawnień	236
	Polecenia chown i chgrp — zmiana właściciela i grupy	238
	Polecenie umask — ustawianie uprawnień domyślnych	238
	Dodatkowe opcje w systemie Linux	239
6.6.	Listy kontroli dostępu (ACL)	240
	Krótka i brutalna historia list kontroli dostępu w systemie Unix	241
	Implementacje ACL	242
	Obsługa ACL w różnych systemach operacyjnych	243
	Listy ACL w stylu POSIX	244
	Listy ACL w stylu NFSv4	248
6.7.	Ćwiczenia	255

7 Dodawanie nowych użytkowników

257

7.1.	Plik etc/passwd	259
	Nazwa użytkownika	260
	Zaszyfrowane hasło	263
	Numer UID (identyfikator użytkownika)	264
	Domyślne numery GID	265
	Pole GECOS	266
	Katalog domowy	267
	Powłoka logowania	267

- 7.2. Pliki /etc/shadow i /etc/security/passwd 268
- 7.3. Plik /etc/group 271
- 7.4. Dodawanie użytkowników — podstawy 273
 - Edycja plików passwd i group 274
 - Ustawianie hasła 274
 - Tworzenie katalogu domowego i instalowanie plików startowych 275
 - Ustawianie uprawnień i praw własności 276
 - Ustawienie miejsca odbioru poczty 277
 - Konfigurowanie ról i uprawnień administracyjnych 277
 - Końcowe kroki 277
- 7.5. Dodawanie użytkowników za pomocą useradd 278
 - Polecenie useradd w systemie Ubuntu 278
 - Polecenie useradd w SUSE 280
 - Polecenie useradd w systemie Red Hat 280
 - Polecenie useradd w systemie Solaris 281
 - Polecenie useradd w systemie HP-UX 282
 - Polecenie useradd w systemie AIX 282
 - Przykłady użycia polecenia useradd 285
- 7.6. Hurtowe dodawanie użytkowników za pomocą newusers (Linux) 285
- 7.7. Usuwanie użytkowników 286
- 7.8. Wyłączanie kont 288
- 7.9. Zarządzanie użytkownikami za pomocą narzędzi systemowych 289
- 7.10. Minimalizowanie ryzyka za pomocą PAM 290
- 7.11. Scentralizowane zarządzanie kontami 290
 - LDAP a Active Directory 290
 - Systemy pojedynczego logowania 291
 - Systemy zarządzania tożsamością 292
- 7.12. Zalecana literatura 293
- 7.13. Ćwiczenia 294

8 Pamięć masowa

295

- 8.1. Chcę tylko dodać dysk! 296
 - Linux 296
 - Solaris 297

HP-UX	298
AIX	298
8.2. Urządzenia pamięci masowej	299
Dyski twarde	300
Dyski SSD	302
8.3. Interfejsy urządzeń pamięci masowej	304
Interfejs PATA	305
Interfejs SATA	306
Interfejs równoległy SCSI	307
Interfejs szeregowy SCSI	310
Co jest lepsze: SCSI czy SATA?	310
8.4. Obieranie cebuli, czyli programowa strona pamięci masowej	311
8.5. Podłączanie i niskopoziomowa obsługa dysków	314
Weryfikacja instalacji na poziomie sprzętowym	315
Pliki urządzeń dyskowych	315
Formatowanie i zarządzanie uszkodzonymi blokami	318
Bezpieczne wymazywanie dysków ATA	320
hdparm — ustawianie parametrów dysku i interfejsu (Linux)	321
Monitorowanie dysku twardego za pomocą SMART	323
8.6. Partycjonowanie dysków	324
Tradycyjne partycjonowanie	326
Partycjonowanie w stylu Windows	328
GPT — tablica partycji GUID	329
Partycjonowanie w systemie Linux	329
Partycjonowanie w systemie Solaris	330
Partycjonowanie w systemie HP-UX	330
8.7. RAID — nadmiarowa macierz niedrogich dysków	331
RAID programowy a sprzętowy	331
Poziomy RAID	332
Przywracanie dysku po awarii	335
Wady RAID 5	336
mdadm — programowy RAID w systemie Linux	337
8.8. Zarządzanie woluminami logicznymi	340
Implementacje LVM	341
Zarządzanie woluminami logicznymi w systemie Linux	342
Zarządzanie woluminami logicznymi w systemie HP-UX	347
Zarządzanie woluminami logicznymi w systemie AIX	349

- 8.9. Systemy plików 350
 - Systemy plików w Linuksie: rodzina ext 351
 - VxFS i HFS — systemy plików w HP-UX 352
 - JFS2 w systemie AIX 353
 - Terminologia systemu plików 353
 - Polimorfizm systemu plików 354
 - mkfs — formatowanie systemu plików 355
 - fsck — sprawdzanie i naprawa systemu plików 355
 - Montowanie systemu plików 356
 - Ustawianie automatycznego montowania 357
 - Montowanie napędów USB 360
 - Włączanie obszaru wymiany 361
- 8.10. ZFS — rozwiązanie wszystkich problemów z pamięcią masową 362
 - Architektura ZFS 362
 - Przykład: dodawanie dysków w systemie Solaris 363
 - Systemy plików i ich właściwości 364
 - Dziedziczenie właściwości 366
 - Osobne systemy plików dla każdego użytkownika 367
 - Kopie migawkowe i klony 367
 - Surowe woluminy 369
 - Współdzielenie systemów plików przez NFS, CIFS i iSCSI 370
 - Zarządzanie pulą pamięci masowej 370
- 8.11. Sieci pamięci masowej 373
 - Sieci SAN 374
 - iSCSI — SCSI przez IP 375
 - Rozruch z woluminu iSCSI 376
 - Inicjatory iSCSI różnych producentów 377
- 8.12. Ćwiczenia 380

9 Procesy okresowe

383

- 9.1. cron — harmonogram poleceń 384
- 9.2. Format plików crontab 385
- 9.3. Zarządzanie plikami crontab 387
- 9.4. Linux i rozszerzenia Vixie-cron 388

- 9.5. Niektóre zastosowania programu cron 389
 - Proste przypomnienia 390
 - Porządkowanie systemu plików 390
 - Sieciowa dystrybucja plików konfiguracyjnych 392
 - Rotacja plików dziennika 392
- 9.6. Ćwiczenia 392

10 Kopie zapasowe

395

- 10.1. Kilka podstawowych kwestii 396
 - Wszystkie kopie zapasowe wykonuj z jednej, centralnej lokalizacji 396
 - Oznaczaj swoje nośniki 397
 - Wybierz rozsądny przedział między kolejnymi kopiami 397
 - Starannie wybieraj systemy plików 398
 - Postaraj się, aby dzienna kopia mieściła się na jednym nośniku 398
 - Przechowuj nośniki poza ośrodkiem 399
 - Chroń swoje kopie 399
 - Ogranicz aktywność podczas wykonywania kopii 400
 - Sprawdzaj swoje nośniki 401
 - Opracuj cykl życia nośników 402
 - Przygotuj dane do archiwizacji 402
 - Przygotuj się na najgorsze 403
- 10.2. Urządzenia i nośniki do archiwizacji 404
 - Nośniki optyczne: CD-R/RW, DVD±R/RW, DVD-RAM i Blu-ray 404
 - Przenośne i wymienne dyski twarde 405
 - Ogólnie o taśmach magnetycznych 406
 - Małe napędy z taśmą 8 mm i DDS (DAT) 406
 - DLT i S-DLT 406
 - AIT i SAIT 407
 - VXA i VXA-X 407
 - LTO 408
 - Zmieniarki automatyczne, układarki i biblioteki taśm 408
 - Dyski twarde 408
 - Internet i chmurowe usługi archiwizacyjne 409
 - Podsumowanie typów nośników 409
 - Co kupić? 410

- 10.3. Oszczędność miejsca i czasu dzięki kopiom przyrostowym 411
 - Prosty harmonogram 412
 - Harmonogram umiarkowany 413
- 10.4. Konfiguracja kopii z wykorzystaniem polecenia dump 413
 - Archiwizacja systemów plików 414
 - Przywracanie danych z kopii przy użyciu restore 417
 - Odtwarzanie całego systemu plików 420
 - Odtwarzanie danych na nowym sprzęcie 421
- 10.5. Archiwizowanie i odtwarzanie przy aktualizacjach 422
- 10.6. Inne programy do archiwizacji 422
 - Program tar — pakowanie plików 422
 - Program dd — przrzucanie bitów 424
 - Kopie ZFS 424
- 10.7. Korzystanie z wielu plików na jednej taśmie 425
- 10.8. Bacula 426
 - Model systemu Bacula 427
 - Konfigurowanie systemu Bacula 429
 - Instalacja bazy danych i demonów systemu Bacula 429
 - Konfigurowanie demonów systemu Bacula 430
 - Wspólne sekcje konfiguracyjne 431
 - bacula-dir.conf — konfiguracja zarządcy 433
 - bacula-sd.conf — konfiguracja demona magazynowania 436
 - bconsole.conf — konfiguracja konsoli 438
 - Instalacja i konfiguracja demona plików klienta 438
 - Uruchamianie demonów systemu Bacula 439
 - Dodawanie nośników do puli 439
 - Ręczne uruchamianie archiwizacji 439
 - Uruchamianie zadania przywracania 440
 - Archiwizacja klientów Windows 443
 - Monitorowanie konfiguracji systemu Bacula 444
 - Kruczki i sztuczki 444
 - Inne narzędzia archiwizujące 445
- 10.9. Komercyjne narzędzia do archiwizacji 446
 - ADSM (TSM) 446
 - Veritas NetBackup 447
 - EMC NetWorker 447
 - Inne rozwiązania 447

10.10. Zalecana literatura 448

10.11. Ćwiczenia 448

11 Syslog i pliki dzienników 451

11.1. Wyszukiwanie plików z dziennikami 453

Specjalne pliki dzienników 455

Lokalizacje dzienników w różnych systemach 456

11.2. Syslog — rejestrator zdarzeń systemowych 457

Architektura systemu syslog 457

Konfigurowanie demona syslogd 458

Przykłady pliku konfiguracyjnego 462

Diagnostyka systemu syslog 465

Zamienniki dla systemu syslog 465

Rejestrowanie komunikatów jądra i uruchamiania systemu 466

11.3. Rejestrowanie i obsługa błędów w systemie AIX 468

Konfiguracja systemu syslog w AIX 469

11.4. Program logrotate — zarządzanie plikami dzienników 471

11.5. Pozyskiwanie użytecznych informacji z plików dziennika 472

11.6. Strategie rejestrowania 474

11.7. Ćwiczenia 476

12 Oprogramowanie — instalacja i zarządzanie 477

12.1. Instalacja systemów Linux i OpenSolaris 478

Rozruch komputera z wykorzystaniem sieci 479

Konfigurowanie PXE w systemie Linux 479

Rozruch sieciowy komputerów o architekturze innej niż x86 480

Kickstart — zautomatyzowany instalator

systemu Red Hat Enterprise Linux 480

AutoYaST — zautomatyzowana instalacja systemu SUSE 483

Automatyczna instalacja przy użyciu instalatora Ubuntu 484

- 12.2. Instalacja systemu Solaris 486
 - Instalacje sieciowe przy użyciu JumpStart 487
 - Instalacje sieciowe przy użyciu Automated Installer 492
- 12.3. Instalacja systemu HP-UX 493
 - Automatyzacja instalacji przez Ignite-UX 496
- 12.4. Instalacja systemu AIX przy użyciu Network Installation Manager 496
- 12.5. Zarządzanie pakietami 498
- 12.6. Zarządzanie pakietami w systemie Linux 499
 - rpm — zarządzanie pakietami RPM 499
 - dpkg — zarządzanie pakietami .deb w systemie Ubuntu 501
- 12.7. Korzystanie z wysokopoziomowych systemów zarządzania pakietami w systemie Linux 502
 - Repozytoria z pakietami 503
 - RHN — Red Hat Network 504
 - APT — Advanced Package Tool 505
 - Konfigurowanie apt-get 506
 - Przykład pliku /etc/apt/sources.list 507
 - Własny serwer lustrzany jako lokalne repozytorium 508
 - Automatyzacja programu apt-get 509
 - yum — zarządzanie wydaniem opartym na formacie RPM 510
 - Zypper — zarządzanie pakietami w SUSE 511
- 12.8. Zarządzanie pakietami w systemach uniksowych 512
 - Pakiety w systemie Solaris 512
 - Pakiety w systemie HP-UX 513
 - Zarządzanie oprogramowaniem w systemie AIX 516
- 12.9. Kontrola wersji 516
 - Tworzenie kopii zapasowych plików 516
 - Formalne systemy kontroli wersji 517
 - Subversion 518
 - Git 520
- 12.10. Lokalizowanie i konfigurowanie oprogramowania 524
 - Organizacja procesu lokalizowania 525
 - Testowanie 526
 - Lokalne kompilowanie 527
 - Rozproszone lokalizowanie 528

- 12.11. Korzystanie z narzędzi do zarządzania konfiguracją 529
 - cfengine — układ odpornościowy komputera 529
 - LCFG — system konfiguracji na dużą skalę 530
 - Template Tree 2 — pomocnik cfengine 530
 - DMTF i CIM — model wspólnych informacji 531
- 12.12. Udostępnianie oprogramowania przez NFS 531
 - Przestrzenie nazw pakietów 532
 - Zarządzanie zależnościami 533
 - Skrypty osłonowe 534
- 12.13. Zalecana literatura 534
- 12.14. Ćwiczenia 535

13 Sterowniki i jądro

537

- 13.1. Dostosowywanie jądra 538
- 13.2. Sterowniki i pliki urządzeń 539
 - Pliki urządzeń i numery urządzeń 540
 - Tworzenie plików urządzeń 541
 - Konwencje nazewnicze dla urządzeń 542
 - Własne jądro kontra moduły ładowalne 543
- 13.3. Konfigurowanie jądra w systemie Linux 544
 - Dostrajanie parametrów jądra systemu Linux 544
 - Budowanie jądra w systemie Linux 545
 - Jeśli się nie popsuło, nie naprawiaj 545
 - Konfigurowanie opcji jądra 547
 - Budowanie plików binarnych jądra 548
 - Dodawanie sterownika urządzenia w systemie Linux 549
- 13.4. Konfigurowanie jądra w systemie Solaris 551
 - Obszar jądra systemu Solaris 551
 - Konfigurowanie jądra za pomocą pliku etc/system 552
 - Dodawanie sterownika urządzenia w systemie Solaris 554
 - Diagnostyka konfiguracji systemu Solaris 554
- 13.5. Konfigurowanie jądra w systemie HP-UX 555
- 13.6. Zarządzanie jądrem systemu AIX 556
 - Object Data Manager 557
 - Dostrajanie jądra 558

- 13.7. Ładowalne moduły jądra 559
 - Ładowalne moduły jądra w systemie Linux 560
 - Ładowalne moduły jądra w systemie Solaris 561
- 13.8. Udev w systemie Linux, czyli przyjemne z pożytecznym 562
 - Sysfs w Linuksie — zwierciadło duszy urządzeń 563
 - Testowanie urządzeń za pomocą udevadm 564
 - Tworzenie reguł i trwałych nazw 565
- 13.9. Zalecana literatura 568
- 13.10. Ćwiczenia 569

II SIECI

14 Sieci TCP/IP

573

- 14.1. TCP/IP i jego związek z internetem 574
 - Kto zarządza internetem? 574
 - Standardy sieciowe i dokumentacja 575
- 14.2. Przewodnik po sieci 577
 - IPv4 i IPv6 578
 - Pakiety i enkapsulacja 579
 - Ramkowanie w sieciach Ethernet 579
 - Maksymalna jednostka transmisji (MTU) 580
- 14.3. Adresowanie pakietów 581
 - Adresowanie sprzętowe (MAC) 581
 - Adresowanie IP 582
 - „Adresowanie” za pomocą nazw 583
 - Porty 583
 - Rodzaje adresów 584
- 14.4. Adresy IP — szczegółowe informacje 584
 - Klasy adresów IPv4 585
 - Podział na podsieci 586
 - Sztuczki i narzędzia do wyliczania podsieci 587
 - CIDR — bezklasowe trasowanie międzydomenowe 588
 - Przydzielanie adresów 589

Adresy prywatne i NAT	590
Adresowanie IPv6	592
14.5. Wyznaczanie tras	594
Tablice tras	594
Przekierowania ICMP	596
14.6. ARP — protokół translacji adresów	597
14.7. DHCP — protokół dynamicznej konfiguracji hostów	598
Oprogramowanie DHCP	599
Jak działa DHCP?	599
Oprogramowanie DHCP w wersji ISC	600
14.8. Kwestie bezpieczeństwa	602
Przekazywanie pakietów IP	602
Przekierowania ICMP	602
Wybór trasy przez nadawcę	603
Pakiety ping na adres rozgłoszeniowy i inne formy ukierunkowanego rozgłaszania	603
Fałszowanie adresów IP	603
Zapory sieciowe oparte na serwerze	604
Wirtualne sieci prywatne	605
14.9. PPP — protokół punkt-punkt	606
14.10. Podstawowa konfiguracja sieciowa	607
Przypisywanie nazwy komputera i adresu IP	608
ifconfig — konfigurowanie interfejsów sieciowych	609
Opcje sprzętu sieciowego	612
route — konfigurowanie tras statycznych	612
Konfigurowanie DNS	614
14.11. Konfigurowanie sieci w różnych systemach	615
14.12. Sieci w systemie Linux	616
NetworkManager	616
Konfigurowanie sieci w Ubuntu	617
Konfigurowanie sieci w SUSE	618
Konfiguracja sieci w systemie Red Hat	619
Opcje sprzętu sieciowego w systemie Linux	621
Opcje TCP/IP w systemie Linux	622
Zmienne jądra związane z bezpieczeństwem	625
NAT i filtrowanie pakietów w systemie Linux	625

- 14.13. Sieci w systemie Solaris 626
 - Podstawowa konfiguracja sieci w systemie Solaris 626
 - Przykłady konfiguracji w systemie Solaris 629
 - Konfiguracja DHCP w systemie Solaris 629
 - ndd — dostrajanie protokołu TCP/IP i interfejsu w systemie Solaris 631
 - Bezpieczeństwo w systemie Solaris 632
 - Zapory sieciowe i filtrowanie pakietów w systemie Solaris 632
 - NAT w systemie Solaris 633
 - Dziwactwa sieciowe systemu Solaris 634
- 14.14. Sieci w HP-UX 634
 - Podstawowa konfiguracja sieci w HP-UX 634
 - Przykłady konfiguracji w systemie HP-UX 636
 - Konfiguracja DHCP w systemie HP-UX 638
 - Dynamiczna rekonfiguracja i dostrajanie systemu HP-UX 638
 - Bezpieczeństwo, zapory sieciowe, filtrowanie pakietów i NAT w systemie HP-UX 639
- 14.15. Sieci w systemie AIX 640
 - no — zarządzanie parametrami dostrajania sieci w systemie AIX 642
- 14.16. Zalecana literatura 642
- 14.17. Ćwiczenia 644

15 Wyznaczanie tras

647

- 15.1. Przesyłanie pakietów — szczegóły 648
- 15.2. Demony i protokoły wyznaczania tras 652
 - Protokoły wektora odległości 652
 - Protokoły stanu łączy 653
 - Miary kosztu 654
 - Protokoły wewnętrzne i zewnętrzne 654
- 15.3. Prezentacja protokołów 655
 - RIP i RIPng — protokół informowania o trasach 655
 - OSPF — najpierw najkrótsza ścieżka 656
 - EIGRP — rozszerzony protokół trasowania bramy wewnętrznej 657
 - IS-IS — „standard” ISO 657

- Protokoły IRDP i ND 658
- BGP — protokół bramy brzegowej 658
- 15.4. Kryteria wyboru strategii wyznaczania tras 658
- 15.5. Demony trasujące 660
 - routed — przestarzała implementacja RIP 660
 - gated — wieloprotokołowy demon trasujący pierwszej generacji 661
 - Quagga — dominujący demon trasujący 661
 - rand — wieloprotokołowy system trasowania dla HP-UX 662
 - XORP — router w komputerze 663
 - Specyfika różnych producentów 663
- 15.6. Routery Cisco 664
- 15.7. Zalecana literatura 667
- 15.8. Ćwiczenia 667

16 Sprzęt sieciowy

669

- 16.1. Ethernet — sieć uniwersalna 670
 - Jak działa Ethernet? 672
 - Topologia Ethernetu 672
 - Skръtka nieekranowana 673
 - Włókna światłowodowe 675
 - Łączenie i rozszerzanie sieci Ethernet 676
- 16.2. Sieci bezprzewodowe — internet dla nomadów 681
- 16.3. DSL i modemy kablowe — ostatnia mila 684
- 16.4. Testowanie i diagnostyka sieci 685
- 16.5. Układanie okablowania 686
 - Możliwości okablowania skръtką 686
 - Połączenia do biur 686
 - Standardy okablowania 687
- 16.6. Kwestie związane z projektowaniem sieci 687
 - Architektura sieci a architektura budynku 688
 - Rozbudowa 689
 - Przeciążenie 689
 - Konserwacja i dokumentacja 690

- 16.7. Kwestie związane z zarządzaniem 690
- 16.8. Zalecana literatura 691
- 16.9. Ćwiczenia 691

17 DNS — system nazw domenowych 693

- 17.1. Kto potrzebuje DNS? 695
 - Zarządzanie własnym systemem DNS 695
- 17.2. Jak działa DNS? 696
 - Rekordy zasobów 696
 - Delegowania 697
 - Buforowanie i efektywność 698
 - Odpowiedzi wielokrotne 699
- 17.3. DNS dla niecierpliwych 699
 - Dodawanie nowego komputera do systemu DNS 700
 - Konfigurowanie klienta DNS 703
- 17.4. Serwery nazw 705
 - Serwery autorytatywne i buforujące 706
 - Serwery rekurencyjne i nierekurencyjne 708
- 17.5. Przestrzeń nazw DNS 709
 - Rejestracja nazwy domeny drugiego poziomu 710
 - Tworzenie własnych poddomen 710
- 17.6. Projektowanie własnego środowiska DNS 711
 - Zarządzanie przestrzenią nazw 711
 - Serwery autorytatywne 712
 - Serwery buforujące 713
 - Wymagania sprzętowe 714
 - Bezpieczeństwo 715
 - Podsumowanie 715
- 17.7. Co nowego w DNS? 716
- 17.8. Baza danych DNS 719
 - Polecenia w plikach strefowych 719
 - Rekordy zasobów 720
 - Rekord SOA 724

Rekordy NS	727
Rekordy A	728
Rekordy PTR	728
Rekordy MX	729
Rekordy CNAME	731
Sztuczka z CNAME	732
Rekordy SRV	734
Rekordy TXT	735
Rekordy zasobów IPv6	736
Rekordy SPF	737
Rekordy DKIM i ADSP	739
Rekordy zasobów SSHFP	743
Rekordy zasobów DNSSEC	744
Rekordy sklejające: połączenia między strefami	744
17.9. Oprogramowanie BIND	746
Ustalenie numeru wersji	746
Komponenty BIND	748
Pliki konfiguracyjne	749
Instrukcja include	751
Instrukcja options	751
Instrukcja acl	759
Instrukcja key (TSIG)	760
Instrukcja trusted-keys	760
Instrukcja server	761
Instrukcja masters	762
Instrukcja logging	763
Instrukcja statistics-channels	763
Instrukcja zone	763
Instrukcja controls dla rndc	767
Rozdzielony DNS i instrukcja view	768
17.10. Przykłady konfiguracji BIND	770
Strefa localhost	770
Mała firma zajmująca się sprawami bezpieczeństwa	772
Internet Systems Consortium (isc.org)	775
17.11. Oprogramowanie NSD-Unbound	776
Instalacja i konfigurowanie NSD	777
Uruchamianie nsd	785
Instalacja i konfigurowanie Unbound	786

17.12. Aktualizowanie plików strefowych	793
Przesyłanie informacji strefowych	794
Automatyczne aktualizacje w BIND	795
17.13. Kwestie związane z bezpieczeństwem	798
Nowe spojrzenie na listy kontroli dostępu w BIND	798
Otwarty resolver	800
Uruchamianie w środowisku chroot	801
Bezpieczna komunikacja między serwerami za pomocą TSIG i TKEY	801
Konfigurowanie TSIG dla BIND	802
TSIG w NSD	805
DNSSEC	805
Strategia dotycząca DNSSEC	809
Rekordy zasobów DNSSEC	810
Włączanie DNSSEC	812
Generowanie par kluczy	813
Podpisywanie stref	815
Łańcuch zaufania DNSSEC	818
DLV	819
Wymiana kluczy DNSSEC	821
Narzędzia DNSSEC	822
Usuwanie błędów w DNSSEC	824
17.14. Microsoft i DNS	826
17.15. Diagnostyka i usuwanie błędów	827
Rejestrowanie w BIND	827
Rejestrowanie w NSD-Unbound	833
Programy sterujące serwerami nazw	834
Statystyki serwera nazw	837
Diagnostyka przy użyciu dig	838
Niepoprawne delegowania	839
Narzędzia sprawdzające poprawność działania DNS	840
Kwestie związane z wydajnością	842
17.16. Kwestie specyficzne dla różnych producentów	843
Specyfika systemu Linux	843
Specyfika systemu Solaris	846
Specyfika systemu HP-UX	847
Specyfika systemu AIX	847

- 17.17. Zalecana literatura 849
 - Listy i grupy dyskusyjne 849
 - Książki i inna dokumentacja 850
 - Zasoby sieciowe 850
 - Dokumenty RFC 851
- 17.18. Ćwiczenia 851

18 NFS

853

- 18.1. Wprowadzenie do sieciowych systemów plików 854
 - Kontrola stanu 854
 - Problemy wydajności 855
 - Bezpieczeństwo 855
- 18.2. NFS 855
 - Wersje protokołu 856
 - Protokoły transportowe 857
 - Stan 857
 - Eksporty systemu plików 857
 - Blokowanie plików 858
 - Bezpieczeństwo 859
 - Odwzorowanie tożsamości w wersji 4. 861
 - Dostęp z uprawnieniami root i konto nobody 862
 - Wydajność w wersji 4. 863
 - Limity dyskowe 863
- 18.3. Serwery NFS 864
 - Polecenie share i plik dfstab (Solaris, HP-UX) 866
 - Polecenie exportfs i plik exports (Linux, AIX) 867
 - Plik exports w AIX 867
 - Plik exports w Linuksie 869
 - Demon nfsd 871
- 18.4. NFS po stronie klienta 872
 - Montowanie zdalnych systemów plików podczas rozruchu systemu 875
 - Ograniczanie eksportów do uprzywilejowanych portów 876
- 18.5. Odwzorowanie tożsamości w NFSv4 876
- 18.6. Statystyki połączeń NFS: nfsstat 877
- 18.7. Dedykowane serwery plików NFS 878

- 18.8. Montowanie automatyczne 879
 - Odwzorowania pośrednie 881
 - Odwzorowania bezpośrednie 881
 - Odwzorowania główne 882
 - Odwzorowania wykonywalne 882
 - Widoczność zasobów montowanych automatycznie 883
 - Automount i replikowane systemy plików 884
 - Automatyczne użycie mechanizmu automount
(wersja 3., wszystkie systemy oprócz Linuksa) 885
 - Specyfika Linuksa 885
- 18.9. Zalecana literatura 886
- 18.10. Ćwiczenia 886

19 Współdzielenie plików systemowych 889

- 19.1. Które pliki współdzielić? 890
- 19.2. Kopiowanie plików 891
 - Użycie NFS 892
 - Systemy typu „push” a systemy typu „pull” 893
 - rdist: wypychanie plików 893
 - rsync: bezpieczniejszy transfer plików 896
 - Pobieranie plików 899
- 19.3. LDAP: Lightweight Directory Access Protocol 899
 - Struktura danych w katalogu LDAP 900
 - Znaczenie usługi LDAP 901
 - Dokumentacja i specyfikacje LDAP 903
 - OpenLDAP: tradycyjna implementacja serwera LDAP
na licencji open source 903
 - 389 Directory Server: alternatywna implementacja serwera LDAP
na licencji open source 905
 - Użycie LDAP w miejsce /etc/passwd i /etc/group 906
 - Zapytania LDAP 907
 - LDAP a bezpieczeństwo 908
- 19.4. NIS: Network Information Service 908
 - Model danych NIS 909
 - Zasada działania NIS 910
 - Bezpieczeństwo NIS 912

- 19.5. Definiowanie priorytetów dla źródeł informacji administracyjnej 912
 - Program nscd: buforowanie wyników wyszukiwania 913
- 19.6. Zalecana literatura 914
- 19.7. Ćwiczenia 914

20 Poczta elektroniczna

917

- 20.1. Systemy obsługi poczty elektronicznej 919
 - Klienci poczty 920
 - System przyjmujący 921
 - System transportowy 922
 - System dostarczania lokalnego 922
 - Skrzynki pocztowe 923
 - Systemy dostępne 923
 - Tak dużo elementów, tak mało czasu 924
- 20.2. Anatomia wiadomości pocztowej 924
 - Nagłówki wiadomości 925
- 20.3. Protokół SMTP 927
 - Wysłałeś mi EHLO 928
 - Kody błędów SMTP 929
 - Uwierzytelnianie SMTP 929
- 20.4. Projekt systemu pocztowego 930
 - Użycie serwerów poczty 931
- 20.5. Aliasy pocztowe 935
 - Odczyt aliasów z plików 937
 - Wysyłanie wiadomości do plików 938
 - Wysyłanie wiadomości do programów 939
 - Aliasy na przykładach 939
 - Budowanie bazy aliasów 940
 - Wykorzystanie list pocztowych i oprogramowania do zarządzania listami 940
 - Oprogramowanie do obsługi list pocztowych 941
- 20.6. Skanowanie treści: mechanizmy antyspamowe i antywirusowe 941
 - Spam 942
 - Oszustwa 943

Prywatność	944
Filtrowanie antyspamowe	944
Zasady filtrowania	945
Szare listy i DCC	946
SpamAssassin	946
Czarne listy	947
Białe listy	947
Miltering: filtrowanie poczty	948
SPF i Sender ID	949
DomainKeys, DKIM, and ADSP	950
Funkcje antyspamowe specyficzne dla serwerów MTA	950
MailScanner	951
amavisd-new	952
Testowanie efektywności skanera	956
20.7. Konfiguracja serwera poczty	956
20.8. Sendmail	958
Plik switch	959
Uruchamianie serwera sendmail	959
Kolejki pocztowe	961
20.9. Konfiguracja serwera sendmail	962
Preprocesor m4	963
Elementy konfiguracji serwera sendmail	964
Plik konfiguracyjny zbudowany z przykładowego pliku .mc	965
20.10. Elementy konfiguracji serwera sendmail	966
Tabele i bazy danych	966
Makra i funkcje ogólnego zastosowania	967
Konfiguracja klienta	974
Opcje konfiguracyjne	975
Mechanizmy antyspamowe serwera sendmail	977
Konfiguracja milterów w serwerze sendmail	981
Serwer sendmail i amavisd	982
20.11. Serwer sendmail i bezpieczeństwo	983
Własność plików	984
Uprawnienia	985
Bezpieczniejsze przysyłanie wiadomości do plików i programów	986
Opcje prywatności	987
Uruchamianie serwera sendmail w środowisku chroot	988
Ataki blokady usług	989

SASL: Simple Authentication and Security Layer	989
TLS: Transport Layer Security	990
20.12. Wydajność serwera sendmail	991
Tryby dostarczania	991
Grupy kolejek i dzielenie koperty	991
Procesy obsługi kolejki	991
Kontrola obciążenia	992
Niedostarczalne wiadomości w kolejce	992
Dostrajanie jądra	994
20.13. Testowanie i diagnostyka serwera sendmail	995
Monitorowanie kolejki	996
Pliki dziennika	996
20.14. Exim	998
Instalacja serwera Exim	999
Uruchamianie serwera Exim	1001
Narzędzia serwera Exim	1001
Język konfiguracji serwera Exim	1002
Plik konfiguracyjny serwera Exim	1003
Opcje globalne	1004
ACL (ang. access control lists)	1006
Skanowanie treści na etapie ACL	1010
Mechanizmy uwierzytelniające	1012
Routery	1013
Transporty	1017
Konfiguracja ponowień	1018
Konfiguracja przepisywania	1018
Lokalna funkcja skanująca	1019
Połączenie serwera Exim z demonem amavisd	1019
Zapisywanie dzienników	1020
Diagnostyka	1021
20.15. Postfix	1021
Architektura serwera Postfix	1022
Bezpieczeństwo	1024
Polecenia i dokumentacja serwera Postfix	1024
Konfiguracja serwera Postfix	1025
Domeny wirtualne	1030
Kontrola dostępu	1032
Zwalczanie spamu i wirusów	1035

Filtrowanie treści za pomocą amavisd	1038
Diagnostyka	1040
20.16. Konfiguracja mechanizmu DKIM	1042
DKIM: DomainKeys Identified Mail	1042
DKIM-milter	1043
Konfiguracja DKIM w amavisd-new	1045
DKIM w serwerze sendmail	1047
DKIM w serwerze Exim	1047
DKIM w serwerze Postfix	1050
20.17. Zintegrowane rozwiązania pocztowe	1051
20.18. Zalecana literatura	1052
Literatura na temat spamu	1052
Literatura na temat serwera sendmail	1052
Literatura na temat serwera Exim	1053
Literatura na temat serwera Postfix	1053
Dokumenty RFC	1053
20.19. Ćwiczenia	1053
Ćwiczenia dotyczące serwera sendmail	1055
Ćwiczenia dotyczące serwera Exim	1056
Ćwiczenia dotyczące serwera Postfix	1056

21 Zarządzanie siecią

1059

21.1. Rozwiązywanie problemów z siecią	1060
21.2. Polecenie ping: sprawdzenie, czy host jest dostępny	1062
21.3. Polecenie smokeping: gromadzenie statystyk polecenia ping	1065
21.4. Polecenie traceroute: śledzenie pakietów IP	1066
21.5. Polecenie netstat: śledzenie statystyk sieciowych	1069
Weryfikacja konfiguracji interfejsu sieciowego	1069
Monitoring stanu połączeń sieciowych	1071
Identyfikacja nasłuchujących usług sieciowych	1072
Kontrola tablic routingu	1073
Przeglądanie statystyk działania protokołów sieciowych	1074
21.6. Analiza aktywności interfejsu sieciowego	1075

- 21.7. Podsluchiwanie pakietów 1076
 - Program tcpdump:
 - przemysłowy standard podsluchiwania pakietów 1078
 - Programy Wireshark i TShark: tcpdump z dopalaczami 1079
- 21.8. Program Netalyzr utworzony przez ICSI 1081
- 21.9. Protokoły zarządzania sieciowego 1081
- 21.10. SNMP 1083
 - Konstrukcja SNMP 1084
 - Operacje obsługiwane przez protokół SNMP 1085
 - RMON: MIB do zdalnego monitoringu 1086
- 21.11. Agent NET-SNMP 1086
- 21.12. Aplikacje do zarządzania siecią 1088
 - Narzędzia pakietu NET-SNMP 1088
 - Gromadzenie danych SNMP i tworzenie wykresów 1089
 - Nagios: monitorowanie zdarzeń związanych z usługami 1090
 - Idealne narzędzie do monitoringu sieci: nadal szukamy 1091
 - Komercyjne platformy do zarządzania siecią 1092
- 21.13. Monitorowanie połączeń: NetFlow 1093
 - Monitorowanie danych NetFlow za pomocą nfdump i NfSen 1094
 - Konfiguracja NetFlow na routerze Cisco 1096
- 21.14. Zalecana literatura 1096
- 21.15. Ćwiczenia 1097

22 Bezpieczeństwo

1099

- 22.1. Czy Unix jest bezpieczny? 1100
- 22.2. Drogi do naruszenia bezpieczeństwa 1102
 - Socjotechnika 1102
 - Podatności oprogramowania 1103
 - Błędy konfiguracji 1104
- 22.3. Filozofia bezpieczeństwa 1105
 - Poprawki bezpieczeństwa 1105
 - Zbędne usługi 1106
 - Zdalne logowanie zdarzeń 1107
 - Kopie zapasowe 1107

Wirusy i robaki	1107
Konie trojańskie	1108
Rootkity	1109
Filtrowanie pakietów	1109
Hasła	1109
Czułość	1110
Ogólna filozofia	1110
22.4. Hasła i konta użytkowników	1111
Okres ważności haseł	1111
Konta współużytkowane	1112
Programy powłoki	1112
Użytkownicy typu root	1113
22.5. PAM: uniwersalny mechanizm uwierzytelniania	1113
Obsługa mechanizmu PAM	1114
Konfiguracja mechanizmu PAM	1114
Szczegółowy przykład konfiguracji Linuksa	1117
22.6. Programy z atrybutem setuid	1118
22.7. Efektywne użycie mechanizmu chroot	1119
22.8. Narzędzia bezpieczeństwa	1120
Skaner portów sieciowych nmap	1120
Nessus: skaner sieciowy następnej generacji	1122
Wyszukiwanie słabych haseł: John the Ripper	1123
Plik hosts_access: kontrola dostępu hostów	1124
Programowalny system wykrywania włamań sieciowych: Bro	1125
Popularny system wykrywania włamań: Snort	1126
Wykrywanie włamań na poziomie hosta: OSSEC	1126
22.9. Mandatory Access Control (MAC)	1130
Security-enhanced Linux (SELinux)	1130
22.10. Narzędzia kryptograficzne	1132
Kerberos: zunifikowane podejście do bezpieczeństwa sieciowego	1133
PGP: Pretty Good Privacy	1133
Bezpieczna zdalna powłoka SSH	1134
Stunnel	1139
22.11. Zapory sieciowe	1141
Zapory filtrujące pakiety	1141
Sposoby filtrowania usług	1142

Zapory z kontrolą stanu	1143
Poziom bezpieczeństwa oferowany przez zapory sieciowe	1144
22.12. Funkcje zapór sieciowych Linuksa	1145
Reguły, łańcuchy i tablice	1145
Cele reguł	1146
Konfiguracja zapory iptables	1146
Kompletny przykład	1147
22.13. Zapora IPFilter dla systemów Unix	1150
22.14. VPN (ang. Virtual Private Network)	1153
Tunelowanie IPsec	1154
Czy sam VPN wystarczy?	1154
22.15. Certyfikacja i standardy	1154
Certyfikacja	1155
Standardy bezpieczeństwa	1156
22.16. Źródła informacji o bezpieczeństwie	1159
CERT: organizacja Uniwersytetu Carnegie Mellon	1159
SecurityFocus.com i lista e-mailowa BugTraq	1159
Schneier on Security	1160
SANS: System Administration, Networking, and Security Institute	1160
Źródła związane z dostawcami rozwiązań	1160
Inne listy e-mailowe i strony WWW	1161
22.17. Reakcja na atak	1162
22.18. Zalecana literatura	1164
22.19. Ćwiczenia	1165

23 Hosting WWW

1169

23.1. Podstawy hostingu WWW	1170
Lokalizowanie zasobów w sieci	1170
Adresy URL	1171
Jak działa HTTP?	1171
Dynamiczne generowanie treści	1172
Serwery aplikacji	1174
Równoważenie obciążenia	1175

23.2.	Instalacja serwera HTTP	1177
	Wybór serwera	1177
	Instalacja serwera Apache	1178
	Konfiguracja serwera Apache	1180
	Uruchamianie serwera Apache	1181
	Analiza dzienników systemowych	1181
	Optymalizacja pod kątem wydajnego serwowania treści statycznych	1182
23.3.	Interfejsy wirtualne	1182
	Wykorzystanie nazwanych hostów wirtualnych	1183
	Konfiguracja interfejsów wirtualnych	1183
	Konfiguracja interfejsów wirtualnych w serwerze Apache	1186
23.4.	SSL	1187
	Generowanie pliku żądania podpisania certyfikatu (CSR)	1187
	Konfiguracja SSL w serwerze Apache	1189
23.5.	Serwery buforujące i pośredniczące	1190
	Wykorzystanie serwera buforująco-pośredniczącego Squid	1190
	Konfiguracja serwera Squid	1191
	Odwrotny serwer pośredniczący w Apache	1192
23.6.	Skalowanie bez ograniczeń	1193
	Przetwarzanie w chmurach	1194
	Hosting kolokacyjny	1194
	Sieci dystrybucji treści (CDN)	1195
23.7.	Ćwiczenia	1195

III RÓŻNOŚCI

24 Wirtualizacja

1199

24.1.	Terminologia wirtualizacji	1201
	Pełna wirtualizacja	1201
	Parawirtualizacja	1202
	Wirtualizacja na poziomie systemu operacyjnego	1203
	Natywna wirtualizacja	1203
	Przetwarzanie w chmurze	1204

Migracja w locie	1205
Porównanie technologii wirtualizacyjnych	1205
24.2. Zalety wirtualizacji	1205
24.3. Zastosowania praktyczne	1207
24.4. Wirtualizacja w Linuksie	1208
Wprowadzenie do Xen	1209
Podstawy Xen	1210
Instalacja gości w Xen: virt-install	1211
Migracja w locie w Xen	1212
KVM	1214
Instalacja i wykorzystanie KVM	1214
24.5. Strefy i kontenery w Solarisie	1216
24.6. Partycje robocze w AIX	1220
24.7. Integrity Virtual Machines w HP-UX	1222
Tworzenie i instalacja maszyn wirtualnych	1223
24.8. VMware: wirtualizujący system operacyjny	1224
24.9. Amazon Web Services	1225
24.10. Zalecana literatura	1230
24.11. Ćwiczenia	1230

25 X Window System

1231

25.1. Menadżer logowania	1234
25.2. Procedura działania aplikacji w środowisku X	1235
Zmienna środowiska DISPLAY	1236
Uwierzytelnianie klienta	1237
Przekazywanie połączeń X za pomocą SSH	1238
25.3. Konfiguracja serwera X	1240
Sekcja Device	1242
Sekcja Monitor	1242
Sekcja Screen	1243
Sekcja InputDevice	1244
Sekcja ServerLayout	1245
Nowoczesny konfigurator serwera X: xrandr	1246
Ustawienia trybu jądra	1247

- 25.4. Rozwiązywanie problemów z serwerem X 1248
 - Specjalne kombinacje klawiszy 1248
 - Gdy serwer X odmawia współpracy 1249
- 25.5. Środowiska graficzne 1251
 - KDE 1251
 - GNOME 1252
 - Które jest lepsze: GNOME czy KDE? 1252
- 25.6. Zalecana literatura 1253
- 25.7. Ćwiczenia 1253

26 Drukowanie

1255

- 26.1. Architektura podsystemu drukowania 1256
 - Najważniejsze podsystemy drukowania 1257
 - Program obsługi kolejki wydruku 1257
- 26.2. CUPS 1258
 - Interfejsy podsystemu drukowania 1258
 - Kolejka drukowania 1259
 - Wiele drukarek i kolejek 1260
 - Instancje drukarek 1260
 - Drukowanie sieciowe 1260
 - Filtry 1261
 - Administracja serwerem CUPS 1263
 - Konfiguracja sieciowego serwera wydruków 1263
 - Automatyczna konfiguracja drukarki 1264
 - Konfiguracja drukarki sieciowej 1264
 - Przykłady konfiguracji drukarek 1265
 - Konfiguracja klasy drukarki 1266
 - Wyłączenie usługi 1266
 - Inne zadania konfiguracyjne 1267
- 26.3. Drukowanie w środowisku graficznym 1267
 - kprinter: print documents 1269
 - Drukowanie w przeglądarce Konqueror 1270
- 26.4. System V 1270
 - Informacje ogólne 1271
 - Cele i klasy 1271

Krótkie wprowadzenie do polecenia lp	1272
Polecenia lpsched i lpshut: uruchamianie i zatrzymywanie drukowania	1272
Konfiguracja środowiska drukowania: polecenie lpadmin	1273
Przykłady użycia polecenia lpadmin	1276
Odczyt stanu drukowania: polecenie lpstat	1276
Usuwanie wydruków: polecenie cancel	1276
Kontrola kolejki: accept i reject	1277
Kontrola drukowania: polecenia enable i disable	1278
Przenoszenie wydruków: polecenie lpmove	1278
Programy interfejsów	1278
26.5. Drukowanie w systemach BSD i AIX	1280
Podstawy architektury systemu wydruku BSD	1281
Kontrola środowiska wydruku	1282
Obsługa kolejek wydruku: demon lpd	1282
Wysyłanie zadań wydruku: polecenie lpr	1283
Sprawdzanie kolejki wydruku: polecenie lpq	1283
Usuwanie zadań wydruku: polecenie lprm	1283
Modyfikacja ustawień systemu wydruku: polecenie lpc	1284
Plik /etc/printcap	1286
Zmienne pliku printcap	1288
26.6. Niełatwa historia drukowania w Uniksie	1293
Historia drukowania i powstanie podsystemów drukowania	1293
Różnorodność drukarek	1294
26.7. Popularne oprogramowanie drukujące	1295
26.8. Języki wydruku	1296
PostScript	1297
PCL	1297
PDF	1298
XPS	1299
PJL	1299
Sterowniki drukarek i obsługa języków definicji strony	1299
26.9. Pliki PPD	1301
26.10. Rozmiary papieru	1302
26.11. Zagadnienia praktyczne	1304
Wybór drukarki	1304
Drukarki GDI	1305
Drukowanie dwustronne	1305

Akcesoria do drukarek	1306
Porty szeregowo i równoległe	1306
Drukarki sieciowe	1307
Porady związane z drukowaniem	1307
26.12. Rozwiązywanie problemów	1312
Ponowne uruchamianie demona wydruku	1312
Dzienniki systemowe	1312
Problemy z drukowaniem bezpośrednim	1313
Problemy z drukowaniem sieciowym	1313
Problemy specyficzne dla dystrybucji	1314
26.13. Zalecana literatura	1314
26.14. Ćwiczenia	1315

27 Podstawy centrów danych

1317

27.1. Poziomy niezawodności centrów danych	1318
27.2. Chłodzenie	1320
Sprzęt elektroniczny	1321
Instalacja oświetleniowa	1321
Obsługa	1321
Całkowite obciążenie cieplne	1322
Gorące i zimne korytarze	1322
Wilgotność	1324
Monitorowanie środowiska	1324
27.3. Zasilanie	1324
Wymagania zasilania szaf	1325
Zdalne sterowanie	1327
27.4. Szafy	1328
27.5. Narzędzia	1328
27.6. Zalecana literatura	1328
27.7. Ćwiczenia	1329

28 Informatyka a ekologia

1331

- 28.1. Pierwsze kroki w ekologicznej informatyce 1332
- 28.2. Piramida informatyki proekologicznej 1334
- 28.3. Proekologiczne strategie w informatyce: centra danych 1335
 - Konsolidacja aplikacji 1335
 - Konsolidacja serwerów 1337
 - Sieci pamięci masowej SAN 1338
 - Wirtualizacja serwerów 1338
 - Serwery na żądanie 1339
 - Szczegółowe planowanie pojemności 1339
 - Konfiguracja serwera zoptymalizowana pod kątem zużycia energii 1340
 - Przetwarzanie w chmurze 1341
 - Tanie chłodzenie 1342
 - Efektywne chłodzenie centrum danych 1342
 - Obniżenie wydajności w czasie awarii zasilania 1342
 - Wydłużenie żywotności 1343
 - Dopuszczanie wyższych temperatur w serwerowniach 1344
 - Urządzenia z obniżonym poborem mocy 1344
- 28.4. Proekologiczne strategie w informatyce: przestrzeń robocza użytkownika 1344
- 28.5. Firmy wspierające ekologię w IT 1347
- 28.6. Ćwiczenia 1347

29 Wydajność

1349

- 29.1. Metody poprawy wydajności 1351
- 29.2. Czynniki wpływające na wydajność 1353
- 29.3. Metody analizy problemów z wydajnością 1355
- 29.4. Kontrola wydajności systemu 1356
 - Inwentaryzacja sprzętu 1356
 - Gromadzenie danych o wydajności 1359
 - Analiza użycia procesora 1359
 - Zarządzanie pamięcią przez system 1362
 - Analiza użycia pamięci 1364

- Analiza obciążenia wejścia-wyjścia 1366
- Analiza wydajności podsystemu dyskowego: program xdd 1369
- Gromadzenie statystyk w czasie i budowanie raportów:
 - program sar 1369
- Monitorowanie systemu AIX: nmon i nmon_analyser 1370
- Wybór planisty operacji wejścia-wyjścia w Linuksie 1370
- Szczegółowe profilowanie systemu Linux: program oprofile 1371
- 29.5. Pomocy! Mój system nagle bardzo zwolnił! 1371
- 29.6. Zalecana literatura 1374
- 29.7. Ćwiczenia 1374

30 Współpraca z Windows

1377

- 30.1. Logowanie z Windows do systemów Unix 1378
- 30.2. Zdalne pulpity 1378
 - Serwer X uruchomiony w Windows 1379
 - VNC: Virtual Network Computing 1380
 - Windows RDP: Remote Desktop Protocol 1381
- 30.3. Uruchamianie Windows i aplikacji dla tego systemu 1382
 - Dual boot, czyli dlaczego nie należy tego robić 1383
 - Alternatywy Microsoft Office 1383
- 30.4. Używanie w Windows narzędzi obsługiwanych z wiersza poleceń 1384
- 30.5. Kompatybilność standardów e-mail i WWW w systemie Windows 1384
- 30.6. Współdzielenie plików z Smbą i CIFS 1385
 - Samba: serwer CIFS dla systemów Unix 1386
 - Instalacja serwera Samba 1387
 - Kodowanie nazw plików 1388
 - Uwierzytelnianie użytkowników 1389
 - Podstawy współdzielenia plików 1389
 - Zasoby grupowe 1390
 - Automatyczne przekierowanie MS DFS 1391
 - Prosty klient CIFS: smbclient 1392
 - Klient CIFS w Linuksie 1392
- 30.7. Współdzielenie drukarek w systemie Samba 1394
 - Instalacja sterownika drukarki z systemu Windows 1395
 - Instalacja sterownika drukarki z wiersza poleceń 1396

- 30.8. Usuwanie problemów z systemem Samba 1397
- 30.9. Uwierzytelnianie Active Directory 1399
 - Przygotowanie do integracji z Active Directory 1401
 - Integracja mechanizmu Kerberos z Active Directory 1401
 - Samba jako uczestnik domeny Active Directory 1403
 - Konfiguracja PAM 1405
 - Zamienniki dla winbind 1406
- 30.10. Zalecana literatura 1406
- 30.11. Ćwiczenia 1407

31 Urządzenia i terminale szeregowo 1409

- 31.1. Standard RS-232C 1410
- 31.2. Inne standardy złączy 1413
 - DB-9 1413
 - RJ-45 1414
- 31.3. Twardy i miękki sygnał wykrycia nośnej 1415
- 31.4. Sprzętowa kontrola przepływu 1416
- 31.5. Pliki urządzeń portów szeregowych 1417
- 31.6. Konfiguracja parametrów portu szeregowego w Linuksie: setserial 1418
- 31.7. Pseudoterminale 1419
- 31.8. Konfiguracja terminali 1419
 - Proces logowania 1420
 - Plik /etc/ttytype 1421
 - Plik /etc/gettytab 1422
 - Plik /etc/gettydefs 1422
 - Plik /etc/inittab 1423
 - Konfiguracja getty w Linuksie 1425
 - Ubuntu Upstart 1426
 - Solaris i sacadm 1426
- 31.9. Znaki specjalne i sterownik terminala 1427
- 31.10. Ustawienie opcji terminala: polecenie stty 1428

- 31.11. Automatyczne ustawianie opcji: polecenie tset 1429
- 31.12. Oczyszczanie terminala 1430
- 31.13. Diagnostowanie połączenia szeregowego 1430
- 31.14. Połączenie z konsolami na porcie szeregowym 1431
- 31.15. Ćwiczenia 1432

32 Zarządzanie i reguły w IT

1435

- 32.1. Cel istnienia IT 1436
 - Budżetowanie i wydatki 1437
 - Reguły w IT 1437
 - Definiowanie poziomu usług (SLA) 1438
- 32.2. Struktura organizacji IT 1443
 - Fundament: rejestracja zgłoszeń i system zarządzania zgłoszeniami 1444
 - Funkcje systemów zgłoszeniowych 1444
 - Przydzielanie zgłoszeń 1445
 - Akceptacja systemów zgłoszeniowych przez użytkowników 1446
 - Przykłady systemów zgłoszeniowych 1447
 - Przydzielanie zgłoszeń 1448
 - Kompetencje IT 1449
 - Zarządzanie czasem 1450
- 32.3. Help desk 1450
 - Zakres usług 1451
 - Dostępność help desku 1451
 - Uzależnienie od help desku 1451
- 32.4. Architekci korporacji 1451
 - Procesy muszą być powtarzalne 1452
 - Zostawianie śladów z okruszków 1452
 - Uznanie istotności dokumentacji 1453
 - Przystosowywanie i pisanie kodu 1453
 - Utrzymanie porządku w systemie 1453
- 32.5. Zespół utrzymaniowy 1454
 - Minimalizacja przestojów 1454
 - Dokumentacja zależności 1455
 - Zmiana przeznaczenia lub wycofywanie starego sprzętu 1455

Utrzymanie lokalnej dokumentacji	1456
Utrzymanie niezależnych środowisk	1460
Automatyzacja	1461
32.6. Zarządzanie	1462
Przywództwo	1463
Zarządzanie personelem	1463
Zatrudnianie	1464
Zwalnianie	1465
Mechanika zarządzania personelem	1465
Kontrola jakości	1466
Zarządzanie bez ingerowania	1467
Związki społeczne	1467
Kontakty ze zwierzchnikami	1468
Zakupy	1469
Rozstrzyganie konfliktów	1471
32.7. Reguły i procedury	1473
Różnice między regułami i procedurami	1473
Najlepsze praktyki tworzenia reguł	1474
Procedury	1475
32.8. Przywracanie systemu po katastrofie	1476
Ocena ryzyka	1476
Zarządzanie katastrofą	1477
Zespół do zwalczania skutków katastrof	1479
Zasilanie i wentylacja	1479
Nadmiarowe łącza internetowe	1481
Incydenty bezpieczeństwa	1481
32.9. Zgodność: regulacje i standardy	1482
ITIL: Information Technology Infrastructure Library	1484
NIST: National Institute for Standards and Technology	1485
32.10. Zagadnienia prawne	1486
Ochrona prywatności	1486
Wymuszanie stosowania reguł	1487
Kontrola = odpowiedzialność	1488
Licencje na oprogramowanie	1489
32.11. Organizacje, konferencje i inne zasoby	1489
32.12. Zalecana literatura	1491
32.13. Ćwiczenia	1492

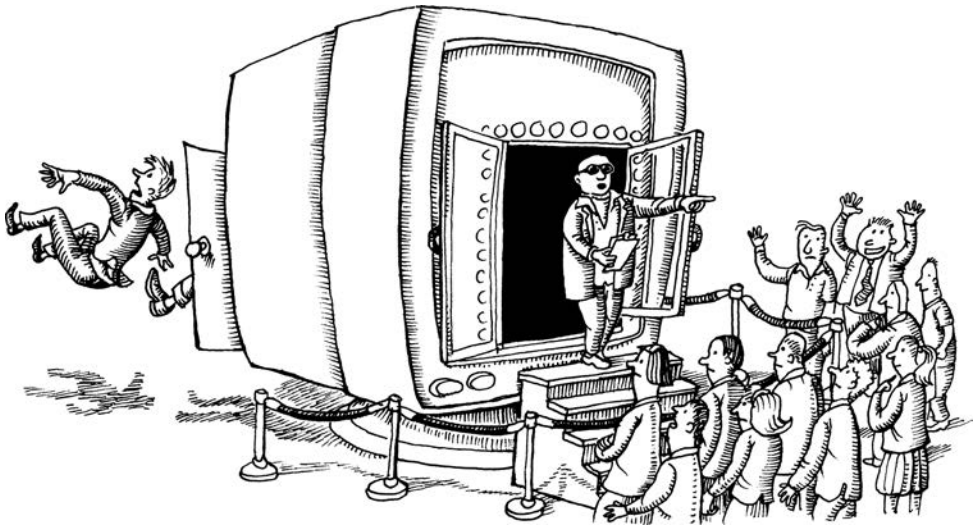
A	Krótką historia	
	administracji systemami	1497

B	W obronie systemu AIX	1509
----------	------------------------------	-------------

Kolofon	1513
O współpracownikach	1515
O autorach	1517
Skorowidz	1519

7

DODAWANIE NOWYCH UŻYTKOWNIKÓW



W większości systemów jednym z rutynowych obowiązków jest dodawanie i usuwanie nowych użytkowników. Są to zadania proste, ale i nużące, dlatego większość administratorów, aby zautomatyzować ten proces, wprowadza do narzędzi dostarczanych wraz z systemem operacyjnym pewne ulepszenia, a następnie przekazuje właściwą pracę asystentowi lub operatorowi.

Oprócz rozproszonych serwerów, na których jest jedynie dwóch użytkowników, obserwujemy obecnie ponowny wzrost liczby serwerów scentralizowanych, zawierających setki kont. Administratorzy muszą posiadać gruntowną znajomość systemu kont

użytkowników, aby zarządzać usługami sieciowymi i konfigurować konta w sposób właściwy dla lokalnego środowiska komputerowego. Zarządzanie kontami na serwerach to często jedynie jeden z wielu elementów obsługi kont dla całego przedsiębiorstwa.

Współczesne środowiska produkcyjne wymagają nie tylko narzędzi do dodawania użytkowników do określonych komputerów, ale i takich, które umożliwią zarządzanie użytkownikami i ich niezliczonymi kontami oraz hasłami w całym środowisku komputerowym, czyli potrzebują systemu zarządzania tożsamością. Usługi katalogowe, takie jak Active Directory firmy Microsoft, OpenLDAP czy Fedora Directory Server, są w powszechnym użyciu, dlatego omówimy tu dokładniej wpływ tego rodzaju systemów na zadania związane z zarządzaniem kontami (jak zwykle, krótkowzroczny Microsoft nie współpracuje zbyt dobrze z innymi, chyba że przekażesz zarządzanie Active Directory).

Potrzeby niektórych ośrodków mogą przekraczać możliwości nawet takich systemów. Nie będziemy tu omawiać komercyjnych systemów zarządzania tożsamością, ale wskażemy kilku kandydatów. Prawdopodobnie systemy te będą odpowiednim rozwiązaniem dla bardzo dużych ośrodków, zwłaszcza takich, w których wymagane jest przestrzeganie regulacji prawnych, takich jak ustawa HIPAA (ang. *Health Insurance Portability and Accountability Act*) lub ustawa Sarbanesa-Oxleya (w przypadku USA); patrz strona 292.

Higiena obsługi kont jest kluczowym warunkiem bezpieczeństwa systemu. Rzadko używane konta są głównym celem ataków, podobnie jak konta z łatwymi do odgadnięcia hasłami. Jeśli nawet do dodawania i usuwania użytkowników wykorzystujesz zautomatyzowane narzędzia dostępne w Twoim systemie, ważne jest, abyś rozumiał, jakie zmiany wprowadzają te narzędzia. Dlatego też temat zarządzania kontami zaczniemy od omówienia zwykłych plików, które należy zmodyfikować, aby dodać użytkowników do pojedynczego komputera.

Następnie zajmiemy się zautomatyzowanymi narzędziami występującymi w każdym z naszych przykładowych systemów operacyjnych oraz plikami konfiguracyjnymi, które sterują ich zachowaniem. Co dziwne (a może raczej dezorientujące), we wszystkich naszych przykładowych systemach narzędzia do zarządzania kontami noszą nazwy `useradd`, `userdel` i `usermod`, choć niekoniecznie są to dokładnie takie same programy (poza tym w systemie AIX ta zgodność nazewnicza została uzyskana przez zastosowanie skryptów osłonowych dla rodzimych narzędzi `mkuser`, `rmuser` i `chuser`).

Domyślne narzędzie `useradd` jest całkiem dobre i powinno wystarczyć do obsługi większości ośrodków. Niestety, narzędzie `userdel` nie zawsze jest tak dokładne, jak byśmy sobie tego życzyli.

Większość systemów zawiera również proste narzędzia graficzne umożliwiające dodawanie i usuwanie użytkowników, choć zazwyczaj nie oferują one trybu wsadowego ani zaawansowanych ustawień lokalizacyjnych. Są na tyle proste, że nie warto tu szczegółowo omawiać ich działania, wskażemy jednak, gdzie można uzyskać dokumentację producenta dla każdego z tych narzędzi.

W tym rozdziale skupimy się głównie na dodawaniu i usuwaniu użytkowników. Wiele kwestii związanych z zarządzaniem użytkownikami omawiamy w innych rozdziałach, a tutaj będziemy się jedynie do nich odwoływać, np.:

- mechanizm PAM (ang. *Pluggable Authentication Modules*) odpowiadający za szyfrowanie uwierzytelniania i wymuszający stosowanie silnych haseł, omawiany jest w rozdziale 22., „Bezpieczeństwo” (od strony 1113),
- skrytki i depozyty ułatwiające zarządzanie hasłami opisane są w rozdziale 4., „Kontrola dostępu i uprawnienia administratora” (patrz strona 189),
- usługi katalogowe, takie jak NIS i OpenLDAP, przedstawione zostały w rozdziale 19., „Współdzielenie plików systemowych”, od strony 899; kilka komentarzy na temat Active Directory można też znaleźć w rozdziale 30., „Współpraca z Windows”, na stronie 1399,
- kwestie proceduralne i prawne są głównym tematem rozdziału 32., „Zarządzanie i reguły w IT”.

W trzech następnych podrozdziałach przyjrzymy się podstawowym plikom, które odgrywają dużą rolę w zarządzaniu użytkownikami.

7.1. PLIK ETC/PASSWD

Plik */etc/passwd* zawiera listę użytkowników rozpoznawanych przez system. Może on zostać rozszerzony lub zastąpiony przez usługę katalogową, stanowi więc kompletne i autorytatywne rozwiązanie tylko w samodzielnych systemach.

Podczas logowania system odwołuje się do pliku */etc/passwd*, aby określić m.in. identyfikator użytkownika (UID) i jego katalog domowy. Każdy wiersz w tym pliku reprezentuje jednego użytkownika i zawiera siedem pól rozdzielonych dwukropkami. Oto te pola:

- nazwa użytkownika,
- symbol zastępujący zaszyfrowane hasło (patrz strona 263),
- numer UID (identyfikator użytkownika),
- domyślny numer GID (identyfikator grupy),
- informacje „GECOS”: pełna nazwa, numer pokoju, telefon wewnętrzny, telefon domowy,
- katalog domowy,
- domyślna powłoka.

Przykładowo poniższe wiersze są prawidłowymi wpisami pliku */etc/passwd*:

```
root:x:0:0:The System,,x6096,:/bin/sh
jl:l:100:0:Jim Lane,ECOT8-3,,:/staff/jl:/bin/sh
dotty:x:101:20:~/home/dotty:/bin/tcsh
```

Zaszyfrowane hasła umieszczane były w drugim polu, ale nie jest to już bezpieczne rozwiązanie; przy wykorzystaniu szybkiego sprzętu ich złamanie (odszyfrowanie) jest kwestią minut. Obecnie wszystkie wersje systemów Unix i Linux ukrywają zaszyfrowane hasła i umieszczają je w oddzielnym pliku, który nie jest przeznaczony do odczytu dla innych. W systemach Linux, Solaris i HP-UX plik *passwd* w polu przeznaczonym na zaszyfrowane hasło zawiera znak x, a w systemie AIX jest to ! lub * (w przypadku AIX znak * jest symbolem zastępczym, który wyłącza konto).

W rzeczywistości zaszyfrowane hasło w systemach Linux, Solaris i HP-UX przechowywane jest w pliku */etc/shadow*, a w systemie AIX w pliku */etc/security/passwd*. Mają one różne formaty.

Jeśli konta użytkowników są współdzielone za pośrednictwem usługi katalogowej, np. NIS lub LDAP, w pliku *passwd* mogą znajdować się specjalne wpisy rozpoczynające się znakiem + lub -. Wpisy te informują system o tym, w jaki sposób dane usługi katalogowej mają być zintegrowane z zawartością pliku */etc/passwd*. Sposób integracji można również ustawić w pliku */etc/nsswitch.conf* (lub */etc/nscontrol.conf* w systemie AIX).

➤ *Więcej informacji na temat pliku nsswitch.conf można znaleźć na stronie 912.*

W następnych punktach omówimy szczegółowo plik */etc/passwd*.

Nazwa użytkownika

Nazwy użytkowników muszą być unikatowe i — w zależności od systemu operacyjnego — muszą przestrzegać ograniczeń dotyczących długości i zestawu znaków. W tabeli 7.1 przedstawione zostały zasady obowiązujące w naszych przykładowych systemach. Nazwy użytkowników nie mogą nigdy zawierać dwukropków ani znaków nowego wiersza, ponieważ znaki te są używane odpowiednio jako separatory pól i separatory wpisów. Jeśli korzystasz z NIS lub NIS+, nazwy użytkowników mogą zawierać maksymalnie osiem znaków, niezależnie od stosowanego systemu operacyjnego.

➤ *Więcej informacji na temat NIS można znaleźć na stronie 908.*

Pierwotnie systemy Unix dopuszczały stosowanie wyłącznie znaków alfanumerycznych i ograniczały długość nazwy użytkownika do ośmiu znaków. Każdy system ma nieco inne reguły, dlatego musisz przyjąć najbardziej restrykcyjne ograniczenia, aby zapobiec ewentualnym konfliktom. Taki konserwatyzm zagwarantuje, że użytkownicy będą mogli posługiwać się tą samą nazwą użytkownika na każdym komputerze. Najbardziej uniwersalnym rozwiązaniem jest stosowanie nazw składających się z ośmiu (lub mniej) znaków i zawierających wyłącznie małe litery, cyfry i znaki podkreślenia.

Tabela 7.1. Reguły tworzenia nazw użytkowników

System	Liczba znaków	Zestaw znaków	Pierwszy znak	Dodatkowe wymogi
Linux	32 ^a	a-z0-9 _ -	a-z _	niektóre dystrybucje są bardziej pobłażliwe
Solaris	8 ^b	A-Za-z0-9+.-_	A-Za-z	co najmniej jedna mała litera
HP-UX	8	A-Za-z0-9 _	A-Za-z	
AIX	8 ^c	POSIX; bez spacji, cudzysłowów i znaków #, =, /, ? \	inny niż -@~	niedozwolone same duże litery niedozwolone są nazwy „default” i „ALL”

^a Choć Linux dopuszcza 32 znaki, tradycyjne programy (np. `top` lub `rsh`) oczekują 8 lub mniej znaków.

^b To ograniczenie zostało zwiększone.

^c W systemie AIX w wersji 5.3 lub wyższej można to zmienić, patrz następna strona.

W nazwach użytkowników uwzględnia się wielkość znaków. Dokument RFC 822 nakazuje jednak, aby w adresach e-mail wielkość znaków była ignorowana. Nic nam nie wiadomo o jakichkolwiek problemach związanych z łączeniem dużych znaków z małymi w nazwach użytkowników, ale tradycyjnie stosuje się nazwy zawierające małe znaki, poza tym są one łatwiejsze do wpisywania. Jeśli nazwy użytkowników *jan* i *Jan* przypisane będą różnym osobom, mogą wystąpić problemy związane z pocztą.

Nazwy użytkowników powinny być łatwe do zapamiętania, dlatego przypadkowa sekwencja znaków nie jest dobrą nazwą. Unikaj stosowania przezwisk nawet wtedy, kiedy w Twojej organizacji panują nieformalne stosunki. Nazwy w rodzaju *DarkLord* lub *FajnaLaska* pasują bardziej do *@hotmail.com*. Jeśli Twój użytkownicy nie mają żadnego szacunku dla siebie, weź pod uwagę choćby ogólną wiarygodność Twojej organizacji.

Ponieważ nazwy użytkowników są często używane w adresach e-mail, warto ustalić standardowy sposób ich tworzenia. Użytkownicy powinni samodzielnie odgadnąć nazwy pozostałych użytkowników. Rozsądny schemat nazewniczy musi raczej zakładać użycie imion, nazwisk, inicjałów lub kombinacji tych elementów.

Bez względu na przyjęty schemat wyboru nazw użytkowników i tak w końcu dojdzie do sytuacji, w której wystąpią zduplikowane lub zbyt długie nazwy, dlatego czasami trzeba robić wyjątki. Określ standardowy sposób postępowania w przypadku konfliktów, np. dodanie numeru na końcu nazwy. Przy zbyt długich nazwach możesz wykorzystać funkcję nazw zastępczych swojego systemu pocztowego, aby utożsamić dwie wersje nazwy, co przynajmniej rozwiązuje problem z pocztą.

W dużych organizacjach często stosuje się adresy e-mail zawierające pełne imię i nazwisko (np. *Jan.Kowalski@mojawitryna.com*), dzięki czemu właściwe nazwy użytkowników pozostaną nieznane dla osób postronnych. To dobry pomysł, ale nie zwalnia od obowiązku stosowania przedstawionych wyżej wskazówek. Najlepiej, aby nazwy użytkowników miały ścisły oraz przewidywalny związek z ich faktycznymi imionami i nazwiskami, choćby dla samego ułatwienia administrowania, jeśli nie ma innych powodów.

Nazwy użytkowników powinny być unikatowe z dwóch powodów. Po pierwsze, użytkownik powinien na każdym komputerze logować się za pomocą tej samej nazwy. Ta zasada służy głównie dla wygody zarówno Twojej, jak i użytkownika.

Po drugie, określona nazwa użytkownika powinna zawsze odnosić się do tej samej osoby. Niektóre polecenia (np. `ssh`) mogą być skonfigurowane w taki sposób, że zdalni użytkownicy będą weryfikowani na podstawie ich nazw. Jeśli `scott@boulder.colorado.edu` i `scott@refuge.colorado.edu` to dwie różne osoby, przy niewłaściwie skonfigurowanych kontaktach jeden użytkownik `scott` mógłby zalogować się na konto drugiego użytkownika o tej samej nazwie bez podawania hasła.

Z doświadczenia wynika, że zduplikowane nazwy prowadzą do pomyłek w dostarczaniu poczty. System pocztowy może doskonale odróżniać obu użytkowników o nazwie `scott`, ale często inni użytkownicy będą wysyłali pocztę pod zły adres.

Jeśli w Twojej organizacji istnieje globalny plik nazw zastępczych (aliasów), nowe nazwy użytkowników nie mogą się pokrywać z żadną z nazw określonych w tym pliku. W przeciwnym razie poczta zostanie dostarczona użytkownikowi, do którego należy dana nazwa zastępcza, a nie nowemu użytkownikowi.

➤ *Więcej informacji na temat stosowania nazw zastępczych w adresach pocztowych można znaleźć na stronie 935.*



W systemie AIX można zmienić maksymalną długość nazwy użytkownika za pomocą polecenia `chdev`. Odpowiednie urządzenie nosi nazwę `sys0`. Polecenie `lsattr -D -l sys0` wyświetli listę domyślnych atrybutów urządzenia. Jednym z nich jest atrybut `max_logname`, który odpowiada za maksymalną długość nazwy użytkownika. Poniższe polecenie wyświetli tylko ten konkretny atrybut:

```
aix$ lsattr -El sys0 -a max_logname
max_logname 9 Maximum login name length at boot time True
```

Aby zmienić to ograniczenie, użyj poniższego polecenia. Zmiana zostanie wprowadzona przy następnym uruchomieniu systemu¹.

```
aix$ sudo su -
aix# chdev -l sys0 -a max_logname=16
```

System podaje, że domyślna długość nazwy to dziewięć znaków, ale specyfikacja długości w systemie AIX to rozmiar bufora, a w nim mieści się jeszcze znak null, który przerywa łańcuch. Dlatego też faktyczny domyślny limit to tylko osiem znaków, a nasze polecenie `chdev` ustawia limit na piętnaście znaków.

¹ Na początku nam się to nie udawało, ponieważ korzystaliśmy z `sudo` (patrz strona 186), a zmienne środowiskowe ustawione przez polecenie `sudo` zazwyczaj są inne niż wtedy, gdy najpierw wydajemy polecenie `sudo su -`, a dopiero potem właściwe polecenie. Polecenie `chdev` zwraca na to uwagę. Nowe wersje polecenia `sudo` (1.70 lub wersje późniejsze) mają opcję `-i`, którą można zastosować w takich sytuacjach.

AIX obsługuje znaki wielobajtowe (np. dla języków azjatyckich), ale nie zaleca się ich używania. Sugerowanym rozwiązaniem jest stosowanie znaków dopuszczalnych w nazwach plików zgodnie ze standardem POSIX.

Zaszyfrowane hasło

Nowoczesne systemy nie przechowują hasła w pliku `/etc/passwd`, a przy pierwszym logowaniu proszą użytkownika o podanie prawdziwego hasła. Ponadto, oprócz standardowego algorytmu `crypt` systemu Unix, obsługują również kilka innych metod szyfrowania. Zaszyfrowane hasło jest oznaczane w celu identyfikacji sposobu szyfrowania użytego do jego wygenerowania. Nasze przykładowe systemy obsługują wiele różnych algorytmów szyfrowania: tradycyjny `crypt` (oparty na DES), MD5, Blowfish oraz iteratywną wersję MD5 zapożyczoną z projektu serwera WWW Apache.

Kolejną ważną kwestią jest długość hasła często określana przez algorytm wykorzystany do szyfrowania. W tabeli 7.2 przedstawione zostały maksymalne i minimalne długości haseł oraz algorytmy szyfrowania dostępne w naszych przykładowych systemach. Niektóre systemy umożliwiają wpisanie dowolnie długiego hasła, ale „po cichu” przycinają je zgodnie z limitem podanym w tabeli.

Tabela 7.2. Algorytmy szyfrowania i ograniczenia długości hasła

System	Minimum	Maksimum	Algorytmy	Miejsce ustawienia
Linux	5	8	crypt, MD5, Blowfish ^a , SHA256, SHA 512	<code>/etc/login.defs</code>
Solaris	6	8 ^b	crypt, MD5, Blowfish, SHA256, SHA 512	<code>/etc/security/policy.conf</code> <code>/etc/security/crypt.conf</code>
HP-UX	6 ^c	8	crypt	<code>/usr/include/limits.h^d</code>
AIX	0	8	crypt, MD5 (BSD), Apache	argument polecenia <code>passwd</code>

^a W systemach SUSE i openSUSE domyślnym algorytmem jest Blowfish; większość pozostałych używa MD5.

^b Maksymalna długość zależy od wybranego algorytmu.

^c Administrator (*root*) może ustawić nazwę użytkownika o dowolnej długości.

^d Ten plik zawiera bardzo dużo konstrukcji `#if def`, dlatego jest dość trudny do odczytania i zrozumienia.

Jeśli pominiessz systemowe narzędzia do dodawania użytkowników i zdecydujesz się utworzyć nowe konto przez ręczną edycję pliku `/etc/passwd` (oczywiście, za pomocą `vi` `pw`; patrz strona 274), w polu przeznaczonym na zaszyfrowane hasło wpisz znak gwiazdki lub `x`. Zapobiegnie to możliwości nieautoryzowanego użycia konta przed ustawieniem właściwego hasła przez Ciebie lub użytkownika. Nigdy, w żadnym przypadku nie pozostawiaj tego pola pustego, bo możesz doprowadzić do ogromnej luki w bezpieczeństwie systemu, ponieważ wtedy dostęp do tego konta nie wymaga podania żadnego hasła.

Algorytm MD5 pod względem kryptograficznym jest nieco lepszy niż poprzedni standard DES używany przez `crypt`, poza tym mechanizm MD5 umożliwia stosowanie haseł o dowolnej długości. Dłuższe hasła są bezpieczniejsze — pod warunkiem, że z nich

korzystasz. W algorytmie MD5 odkryto pewne niedoskonałości, ale na standard DES udało się przeprowadzić skuteczne ataki typu brute-force. Algorytmy SHA256 i Blowfish to prawdziwi siłacze w dziedzinie szyfrowania. Na stronie 1111 podane zostały wskazówki dotyczące wyboru hasła.

Zaszyfrowane hasła mają stałą długość (trzydzieści cztery znaki dla MD5, trzynaście dla DES), bez względu na długość niezaszyfrowanego hasła. Hasła są szyfrowane w połączeniu z wartościami losowymi (ang. *salt*), aby dane hasło mogło przyjmować wiele zaszyfrowanych form. Jeśli dwóch użytkowników wybierze to samo hasło, nie można będzie odkryć tego faktu przez porównanie zaszyfrowanych hasła. Hasła MD5 są łatwe do zauważenia, ponieważ zawsze rozpoczynają się od \$1\$ lub \$md5\$². Hasła zaszyfrowane algorytmem Blowfish rozpoczynają się od \$2a\$, a hasła SHA256 — od \$5\$.



Dla nowych hasła system SUSE stosuje domyślnie algorytm Blowfish, co jest bardzo rozsądnym rozwiązaniem. Szukaj prefiksu \$2a\$.



Obecnie w OpenSolaris domyślnym algorytmem jest SHA256 (prefiks \$5\$), choć wcześniejsze wersje używały domyślnie MD5.

Numer UID (identyfikator użytkownika)

Numer UID identyfikuje użytkownika w systemie. Nazwy użytkowników służą tylko ich wygodzie, bo oprogramowanie i system plików posługują się wewnątrz numerami UID. Identyfikatory UID to zwykle 32-bitowe liczby całkowite bez znaku.

Użytkownik *root* z definicji ma identyfikator UID o numerze 0. Większość systemów definiuje również pseudoużytkowników, takich jak *bin* i *daemon*, którzy są właścicielami plików konfiguracyjnych. Tradycyjnie tacy sztuczni użytkownicy umieszczani są na początku pliku */etc/passwd* i mają przyznane niskie numery UID oraz fałszywą powłokę (np. */bin/false*), żeby nikt nie mógł się zalogować na ich konta. Aby pozostawić dużo miejsca dla takich pseudoużytkowników, których mógłbyś dodawać w przyszłości, zalecamy, aby identyfikatory UID prawdziwych użytkowników rozpoczynały się od numeru 500 lub wyższego (pożądany zakres dla nowych identyfikatorów można określić w plikach konfiguracyjnych dla polecenia *useradd*).

➡ Opis konta *root* można znaleźć na stronie 176.

Inny specjalny identyfikator UID należy do użytkownika o nazwie *nobody*; ma on zwykle przypisaną wartość -1 lub -2 , co odpowiada najwyższemu i drugiemu w kolejności identyfikatorowi spośród wszystkich możliwych numerów UID. Nazwa *nobody* używana jest wtedy, gdy na jednym z komputerów użytkownik *root* próbuje uzyskać przez NFS dostęp do plików innego komputera, który nie ufa temu pierwszemu.

² \$1\$ to oznaczenie algorytmu MD5 w BSD; Sun stosuje własny wariant MD5 i oznacza go \$md5\$.

➤ *Więcej informacji na temat konta nobody można znaleźć na stronie 862.*

Posiadanie wielu kont o identyfikatorze UID równym 0 to zły pomysł. Możliwość logowania się z uprawnieniami administratora na różne powłoki lub przy użyciu różnych haseł może wydawać się udogodnieniem, jednak takie ustawienie powoduje tylko większe zagrożenie dla bezpieczeństwa i konieczność zabezpieczenia wielu kont. Jeśli użytkownicy muszą mieć więcej sposobów logowania się z uprawnieniami użytkownika *root*, lepiej będzie, jeśli skorzystają z programów typu *sudo*.

Unikaj powtórnego wykorzystywania numerów UID nawet wtedy, kiedy użytkownicy opuścili już organizację, a ich konta zostały usunięte. Dzięki podjęciu takich środków ostrożności unikniesz zamieszania w sytuacji, gdyby kiedyś zaszła konieczność odtworzenia plików z kopii zapasowej, gdzie użytkownicy są identyfikowani za pomocą numerów UID, a nie nazw.

Numery UID muszą być unikatowe w całej organizacji. Oznacza to, że określony numer UID powinien odnosić się do tej samej nazwy użytkownika i tej samej osoby na wszystkich komputerach, do korzystania z których jest uprawniona. Nieprzestrzeganie zasady niepowtarzalności numerów UID może zwiększyć zagrożenie dla bezpieczeństwa w takich systemach jak NFS, a także wprowadzać zamęt w sytuacji, gdy użytkownik zmieni swoją grupę roboczą.

Jeśli grupy komputerów są zarządzane przez różne osoby lub organizacje, utrzymanie unikatowych numerów UID może być trudne. Wiązą się z tym zarówno problemy natury technicznej, jak i politycznej. Najlepszym rozwiązaniem jest posiadanie centralnej bazy danych lub serwera katalogowego, który zawiera wpisy każdego użytkownika i wymusza niepowtarzalność. Prostszy schemat polega na przypisaniu określonego zakresu numerów UID każdej grupie w organizacji i pozwolenie jej na samodzielne zarządzanie swoimi zestawami. Takie rozwiązanie pozwala utrzymać odrębne przestrzenie numerów UID, ale nie rozwiązuje występujących równolegle problemów z unikatowymi nazwami użytkowników.

W zarządzaniu numerami UID i informacjami o kontach użytkowników dużą popularność zdobywa LDAP. Temat ten zostanie przedstawiony pobieżnie w tym rozdziale, od strony 290, a bardziej dokładnie omówimy go w rozdziale 19., „Współdzielenie plików systemowych”, od strony 899.

Domyślne numery GID

Podobnie jak UID, numery identyfikacyjne grup również są 32-bitowymi liczbami całkowitymi. GID o numerze 0 jest zarezerwowany dla grupy o nazwie *root* lub *system*. Tak samo jak w przypadku identyfikatorów UID, system dla własnych potrzeb administracyjnych korzysta z kilku predefiniowanych grup. Niestety, producenci nie zachowują tu żadnej konsekwencji. Przykładowo w systemach Red Hat i SUSE grupa *bin* ma identyfikator GID 1, a w systemach Ubuntu, Solaris, HP-UX i AIX grupa ta ma identyfikator o numerze 2.

W dawnych czasach, gdy moc obliczeniowa była droga, grupy służyły do celów rozliczeniowych. Chodziło o to, aby opłaty za wykorzystanie sekund czasu procesora, minut czasu zalogowania i kilobajtów zajętego miejsca na dysku zostały naliczone właściwemu wydziałowi. Obecnie grupy służą głównie do współdzielenia dostępu do plików.

Plik `/etc/group` definiuje grupy; korzysta przy tym z pola GID w pliku `/etc/passwd`, przyznając domyślny (lub „efektywny”) numer GID podczas logowania. Przy określaniu praw dostępu domyślny numer GID nie jest traktowany w jakiś szczególny sposób, ma znaczenie jedynie podczas tworzenia nowych plików i katalogów. Standardowo właścicielem nowych plików jest Twoja efektywna grupa, jeśli jednak chcesz udostępnić pliki innym użytkownikom w ramach jakiegoś projektu zespołowego, musisz pamiętać o tym, aby ręcznie zmienić właściciela grupowego tych plików.

➞ Więcej informacji na temat ustawiania bitu `setgid` dla katalogów można znaleźć na stronie 233.

Aby ułatwić współpracę, możesz ustawić dla katalogu bit `setgid` (02000) lub zamontować system plików z opcją `grp1d`. Oba te rozwiązania sprawią, że nowo tworzone pliki będą domyślnie należeć do tej samej grupy, co ich katalog nadrzędny.

Pole GECOS

Pole GECOS używane jest czasem do zapisywania informacji osobistych o każdym użytkowniku. Nie ma ściśle zdefiniowanej składni. Choć możesz tu przyjąć dowolną konwencję formatowania, polecenie `finger` interpretuje wpisy GECOS rozdzielone przecinakami w następującej kolejności:

- imię i nazwisko (często jest to jedyne używane pole),
- numer budynku i pokoju,
- wewnętrzny numer telefonu,
- domowy numer telefonu.

Polecenie `chfn` umożliwia użytkownikom zmianę swoich informacji GECOS³. Polecenie jest przydatne do zapisywania aktualnych informacji o użytkowniku, takich jak numer telefonu, ale może również zostać wykorzystane niewłaściwie. Użytkownik może np. wprowadzić tam niewłaściwe informacje lub treści obsceniczne. W niektórych systemach można ograniczyć pola, które mogą być modyfikowane za pomocą polecenia `chfn`; wiele ośrodków akademickich wyłącza je całkowicie. W większości systemów polecenie `chfn` może operować tylko na pliku `/etc/passwd`, jeśli więc do przechowywania informacji o użytkownikach wykorzystujesz LDAP lub inną usługę katalogową, `chfn` może w ogóle nie działać.

³ Wyjątkiem jest system Solaris, w którym nie ma polecenia `chfn`. Superużytkownik może zmienić informacje GECOS użytkownika za pomocą polecenia `passwd -g`.

➤ Więcej informacji na temat LDAP można znaleźć na stronie 899.



W systemie AIX polecenie `chfn` akceptuje opcję `-R moduł`, która wczytuje podany *moduł* w celu przeprowadzenia właściwej aktualizacji. Dostępne moduły znajdują się z katalogu `/usr/lib/security`, a jeden z nich może korzystać z LDAP.

Katalog domowy

Katalog domowy użytkownika jest podczas logowania katalogiem domyślnym. Musisz zdawać sobie sprawę z tego, że katalogi domowe zamontowane na sieciowym systemie plików mogą być niedostępne w przypadku problemów z serwerem lub siecią. Jeśli w czasie logowania katalog domowy użytkownika jest niedostępny, system wyświetli komunikat informujący o braku katalogu domowego⁴ i przeniesie użytkownika do katalogu `/`. System Linux nie pozwoli się załogować, jeśli w pliku `/etc/login.defs` w wierszu `DEFAULT_HOME` wpisana będzie wartość `no`.

Powłoka logowania

Powłoka logowania to zazwyczaj interpreter poleceń, np. powłoka Bourne'a lub C (`/bin/sh` lub `/bin/csh`), ale może to być dowolny program. W systemie Unix tradycyjnie powłoką domyślną jest `sh`, a w systemach Linux i Solaris jest nią `bash` (ang. „*Bourne again*” shell⁵). W systemie AIX powłoką domyślną jest `ksh`, powłoka Korn; `tcsh` to rozszerzona powłoka C z możliwością edycji poleceń. W systemach linuksowych `sh` i `csh` są w rzeczywistości po prostu dowiązaniem odpowiednio do powłok `bash` i `tcsh`.

Niektóre systemy umożliwiają użytkownikom zmianę swoich powłok za pomocą polecenia `chsh`, ale podobnie jak w przypadku `chfn`, polecenie to może nie działać, jeśli do zarządzania informacjami o użytkownikach wykorzystujesz LDAP lub inną usługę katalogową. Gdy używasz pliku `/etc/passwd`, administrator zawsze może zmienić powłokę użytkownika, edytując plik `passwd` za pomocą polecenia `vipw`.



Linux obsługuje polecenie `chsh` i ogranicza możliwość zmian do powłok wymienionych w pliku `/etc/shells`. SUSE również narzuca wybór z pliku `/etc/shells`, ale system Red Hat w przypadku wybrania powłoki spoza listy tylko ostrzega. Dodając nowe wpisy do pliku `shells`, pamiętaj o konieczności podania ścieżek bezwzględnych, ponieważ oczekują tego `chsh` i inne programy.

⁴ Taki komunikat pojawi się tylko przy logowaniu na konsoli lub przez terminal, ale nie podczas logowania za pośrednictwem graficznych menadżerów logowania, takich jak `xdm`, `gdm` lub `kdm`. Wtedy nie tylko nie zobaczysz żadnego komunikatu, ale zostaniesz natychmiast wylogowany, ponieważ menadżer wyświetlania nie będzie miał możliwości zapisu do właściwego katalogu (np. `~/gnome`).

⁵ Gra słów; w języku angielskim brzmi to jak *born again shell*, czyli odrodzona powłoka — przyp. tłum.



W systemie AIX użytkownik może zmienić swoją powłokę za pomocą polecenia `chsh` i wybrać inną z obszernej listy. Autorytatywna lista sprawdzonych powłok znajduje się w pliku `/etc/security/login.cfg`⁶. Plik `/etc/shells` zawiera jedynie ich podzbiór i używany jest tylko przez demona FTP, in. `ftpd`. Wiele powłok z tej długiej listy to po prostu dowiązania twarde do pojedynczego pliku binarnego. Przykładowo `sh`, `ksh`, `rksh`, `psh` i `tsh` (zarówno w `/bin`, jak i w `/usr/bin`) są tym samym programem, który zmienia swoje zachowanie w zależności od tego, pod jaką nazwą został wywołany. Podobnie jak `chfn`, polecenie `chsh` przyjmuje opcję `-R moduł` w celu obsługi LDAP i innych systemów usług katalogowych.



W systemie Solaris tylko superużytkownik może zmienić powłokę użytkownika (używając polecenia `passwd -e`). Plik `/etc/shells` (którego domyślnie nie ma, choć istnieje jego strona podręcznika systemowego) zawiera listę dozwolonych powłok.

7.2. PLIKI /ETC/SHADOW I /ETC/SECURITY/PASSWD

Plik *shadow* (zwany też plikiem przesłaniania haseł lub plikiem cieni) może być odczytany tylko przez superużytkownika. W pliku przechowywane są zaszyfrowane hasła, chronione przed wścibskimi oczami i programami do łamania haseł. Mieszczą się w nim również pewne dodatkowe informacje o kontach, które nie były uwzględnione w pierwotnym formacie `/etc/passwd`. Obecnie przesłanianie haseł jest domyślnie włączone niemal we wszystkich systemach.

W systemie AIX plik przechowujący zaszyfrowane hasła nosi nazwę `/etc/security/passwd`, podczas gdy we wszystkich pozostałych systemach jest to `/etc/shadow`. Oczywiście, ich formaty i zawartość są różne. Najpierw przyjrzymy się plikowi `/etc/shadow`.

Plik *shadow* nie jest nadzbiorem pliku *passwd*, a plik *passwd* nie jest generowany na jego podstawie. Musisz utrzymywać oba te pliki lub skorzystać z takich narzędzi jak `useradd`, które będą to robić za Ciebie. Podobnie jak `/etc/passwd`, plik `/etc/shadow` zawiera jeden wiersz dla każdego użytkownika. Każdy wiersz to dziewięć pól rozdzielonych dwukropkami, a przeznaczonych na:

- nazwę użytkownika,
- zaszyfrowane hasło,
- datę ostatniej zmiany hasła,
- minimalną liczbę dni między zmianami hasła,
- maksymalną liczbę dni między zmianami hasła,

⁶ Do wprowadzania zmian w plikach z katalogu `/etc/security` użyj polecenia `chsec`, zamiast edytować je bezpośrednio.

- liczbę dni określającą wyprzedzenie, z jakim należy ostrzegać użytkowników o wygaśnięciu hasła,
- liczbę dni od wygaśnięcia hasła, po upływie których konto zostanie wyłączone (Linux) lub liczbę dni, po których konto automatycznie wygaśnie (Solaris),
- datę ważności konta,
- pole zarezerwowane, które obecnie jest zawsze puste, z wyjątkiem systemu Solaris.

Jedyne wymagane wartości to nazwa użytkownika i hasło. W pliku */etc/shadow* pola z datami bezwzględny podawane są jako liczba dni (**nie** sekund), jakie upłynęły od 1 stycznia 1970 roku, co nie jest standardowym sposobem odliczania czasu w systemach Unix i Linux. Możesz jednak zamienić sekundy na dni, jakie upłynęły od początku ery Uniksa, stosując polecenie:

```
solaris$ expr `date +%s` / 864007
```

Typowy wpis w pliku *shadow* wygląda tak:

```
millert:$md5$em5J8hL$a$iQ3pXe0sakdRaRFyy7Ppj.:14469:0:180:14:::
```

Oto bardziej szczegółowe opisy tych pól.

- Nazwa użytkownika jest taka sama jak w pliku */etc/passwd*. Pole łączy wpisy użytkownika w plikach *passwd* i *shadow*.
- Zaszyfrowane hasło jest identyczne w koncepcji i wykonaniu z tym, które kiedyś przechowywane było w pliku */etc/passwd*; tutaj przedstawione zostało fikcyjne hasło MD5 z systemu Solaris.
- W polu ostatniej zmiany zapisany jest czas, w którym hasło użytkownika było ostatnio zmieniane. Pole to jest wypełniane przez polecenie *passwd*.
- Czwarte pole określa liczbę dni, które muszą upłynąć między zmianami hasła. Chodziło o to, aby zmusić użytkownika do autentycznej zmiany hasła, uniemożliwiając mu natychmiastowe przywrócenie poprzedniego hasła po wymuszonej zmianie. Uważamy jednak, że funkcja ta może być nieco niebezpieczna w razie naruszenia bezpieczeństwa. Zalecamy ustawienie w tym polu wartości 0.
- Piąte pole określa maksymalną liczbę dozwolonych dni między zmianami hasła. Dzięki temu administrator może wymusić zmiany hasel; więcej informacji na ten temat można znaleźć na stronie 1111. W systemie Linux rzeczywista maksymalna liczba dni jest sumą wartości tego pola oraz wartości z pola siódmego (tzw. okres łaski).
- Szóste pole określa liczbę dni przed wygaśnięciem hasła, kiedy program *login* powinien ostrzec użytkownika o nieuchronnie zbliżającym się terminie.

⁷ Dzień ma 86 400 sekund: 60*60*24.

- W systemach Solaris i HP-UX siódme pole interpretowane jest inaczej niż w systemie Linux. W Linuksie siódme pole określa, ile dni po przekroczeniu maksymalnego terminu ważności hasła należy odczekać, zanim konto zostanie zablokowane.

W systemach Solaris i HP-UX działanie tego pola wygląda następująco: jeśli użytkownik nie zaloguje się w czasie wyznaczonym przez liczbę dni podaną w siódmym polu, konto zostanie wyłączone. Nieużywane konta są ulubionym celem hakerów, a ta funkcja daje możliwość pozbycia się takich kont. Działa to jednak tylko wtedy, gdy użytkownik jest wymieniony w pliku `/var/adm/lastlog`, więc konta użytkowników, którzy nigdy się nie zalogowali, nie będą automatycznie wyłączane. A zatem funkcja ta nie sprawdzi się w środowisku sieciowym, ponieważ każdy komputer ma własny plik `lastlog`.

- Ósme pole określa dzień (liczony od 1 stycznia 1970 roku) wygaśnięcia konta użytkownika. Po tej dacie użytkownik nie będzie mógł się zalogować, chyba że administrator ponownie wprowadzi tu jakąś wartość. Jeśli pole pozostanie puste, konto nigdy nie wygaśnie.

W systemie Linux można ustawić datę wygaśnięcia za pomocą polecenia `usermod`, które przyjmuje daty w formacie `rrrr-mm-dd`. W systemie Solaris polecenie `usermod` potrafi również obliczać dni, jakie upłynęły od początku ery Uniksa. Akceptuje ono daty w ok. trzydziestu formatach określonych w pliku `/etc/datemsk`, niestety, nie ma wśród formatu `rrrr-mm-dd` używanego w systemie Linux.

- Dziewiąte pole jest zarezerwowane do wykorzystania w przyszłości. Jest to uznawane przez systemy Linux i HP-UX, ale Solaris wykorzystuje ostatnie cztery bity do odliczania nieudanych prób zalogowania.

Popatrzmy ponownie na nasz przykładowy wiersz z pliku `shadow`:

```
millert:$md5$em5J8hL$a$iQ3pXe0sakdRaRfyy7Ppj.:14469:0:180:14:::
```

W tym przykładzie użytkownik `millert` po raz ostatni zmieniał swoje hasło 13 sierpnia 2009 roku. Hasło musi zostać zmienione ponownie w ciągu 180 dni, a przez ostatnie dwa tygodnie przed tym terminem użytkownik `millert` będzie otrzymywał ostrzeżenia o konieczności zmiany hasła. Konto nie ma ustawionej daty wygaśnięcia.

W systemach Solaris, HP-UX i Linux możesz użyć narzędzia `pwconv`, aby uzgodnić zawartość pliku `shadow` z plikiem `passwd` przez dodanie nowych użytkowników i usunięcie tych, których nie ma już w pliku `passwd`. W systemie Linux program `pwconv` wypełnia większość wpisów w pliku `shadow` wartościami domyślnymi podanymi w pliku `/etc/login.defs`.



W systemie Solaris użytkownik `root` za pomocą polecenia `passwd -f nazwa_użytkownika` może wymusić na użytkowniku zmianę hasła przy następnym logowaniu. Jest to przydatne w sytuacji, gdy regularnie uruchamiasz programy do łamania zabezpieczeń w celu wykrycia źle wybranych (słabo zabezpieczonych) haseł (w systemie Linux ta sama opcja `-f` umożliwia użytkownikowi zmianę informacji na swój temat).



W systemie AIX nie używa się terminu przesłaniania haseł, ale koncepcja jest taka sama. Zasyfrowane hasła przechowywane są w pliku */etc/security/passwd*, w całkowicie innym formacie niż ten, który występuje w pliku */etc/passwd*. Oto przykład pochodzący z czystej instalacji systemu AIX, gdzie domyślnym algorytmem szyfrowania haseł jest crypt⁸:

```
trent:
  password = u10.0aYxRx4qI
  lastupdate = 1224876639
  flags = ADMCHG
```

```
evi:
  password = Pi1r2q0PabZ.Q
  lastupdate = 1235785246
  flags =
```

Ten format nie wymaga dokładniejszych wyjaśnień. Poszczególne wpisy oddzielone są jedną lub kilkoma pustymi wierszami. Taki sam format stosowany jest w większości plików konfiguracyjnych w katalogu */etc/security*, gdzie nazwa użytkownika wyznacza dowolny kontrolowany lub rejestrowany obiekt.

System AIX dostarcza niezliczoną liczbę ustawień kontrolujących wszystkie aspekty logowania i haseł. Niektóre opcje dotyczą użytkowników, a inne portów (aby kontrolować porty TTY, na których dany użytkownik może się zalogować). Szczegółowe informacje znajdują się komentarzach zawartych w plikach *etc/security/login.cfg* i *etc/security/user*. Przydatnym poleceniem jest *pwdadm*, które umożliwia wymuszenie na użytkowniku zmiany hasła przy następnym logowaniu.

7.3. PLIK /ETC/GROUP

Plik */etc/group* zawiera nazwy grup w systemie Unix oraz listę członków każdej grupy. Oto fragment pliku *group* z systemu AIX:

```
system:!0:root,pconsole,esaadmin
staff:!1:ipsec,esaadmin,trent,ben,garth,evi
bin:!2:root,bin
sys:!3:root,bin,sys
adm:!4:bin,adm
nobody:!4294967294:nobody,lpd
```

Każdy wiersz odpowiada jednej grupie i zawiera cztery pola:

- nazwę grupy,
- zasyfrowane hasło lub znak zastępczy,

⁸ Wybranie silniejszego algorytmu szyfrowania powinno być jedną z pierwszych czynności do wykonania po zainstalowaniu systemu AIX.

- numer GID,
- listę członków grupy, rozdzielonych przecinkami (uważaj, aby nie wpisywać spacji).

Podobnie jak w przypadku pliku */etc/passwd*, poszczególne pola rozdzielane są dwukropkami. Dla zachowania zgodności nazwy grup powinny być ograniczone do ośmiu znaków, choć wiele systemów tego nie wymaga. Możliwe jest ustawienie hasła dla grupy, dzięki czemu użytkownicy niebędący jej członkami mogą ją wybrać za pomocą polecenia *newgrp*, ale rzadko się z tego korzysta. Tylko Linux w pełni obsługuje hasła grup⁹. Hasło można ustawić za pomocą polecenia *gpasswd*; będzie ono przechowywane w zaszyfrowanej formie w pliku */etc/gshadow*. Zazwyczaj nie stosuje się haseł dla grup, występują one bardzo rzadko.

Podobnie jak nazwy użytkowników i numery UID, nazwy grup i numery GID powinny być jednakowe na wszystkich komputerach, które współdzielą pliki za pośrednictwem sieciowego plików. Może to być trudne do uzyskania w środowisku heterogenicznym, ponieważ odmienne systemy operacyjne używają różnych numerów GID dla grup o tych samych nazwach.

Odkryliśmy, że najlepszym sposobem poradenia sobie z tym problemem jest unikanie używania grupy systemowej jako domyślnej grupy logowania użytkownika. Niektóre systemy kontrolują wykonywanie poleceń przy użyciu własności grupy w połączeniu z bitami uprawnień. Niejednolite numery GID na różnych systemach powodują zamieszanie przy instalowaniu i aktualizacji oprogramowania w ramach całej organizacji.

Jeśli użytkownik ma przypisaną domyślną grupę w pliku */etc/passwd*, ale nie jest wymieniony jako członek tej grupy w pliku */etc/group*, ostatnie słowo należy do */etc/passwd*. Członkostwo grupy przydzielane podczas logowania jest połączeniem tego, co znajduje się w plikach *passwd* i *group*.

Niektóre systemy ograniczają liczbę grup, do których użytkownik może należeć. Najczęściej spotykany limit to 8 grup, ale w systemie Solaris wynosi on 16, w HP-UX — 20, a w systemach AIX i Linux liczba grup jest pozornie nieograniczona.

Aby zminimalizować potencjalne konflikty z numerami GID przydzielanymi domyślnie przez producentów, zalecamy rozpoczęcie numerowania lokalnych grup od 500 lub wyższych wartości.

Pierwotnie w systemie Unix nowym użytkownikom przydzielana była grupa reprezentująca ich ogólną kategorię, np. „studenci” lub „finanse”. Taka konwencja zwiększała jednak prawdopodobieństwo, że przez niedbałe ustawienia dostępu użytkownicy będą mogli czytać nawzajem swoje pliki, nawet jeśli nie było to intencją właściciela. Aby uniknąć tego problemu, należy tworzyć unikatową grupę dla każdego użytkownika. Grupa może nosić tę samą nazwę co użytkownik. Możesz też przydzielić im ten sam numer GID i UID.

⁹ Aby ustawić hasło dla grupy w systemie Solaris, trzeba posłużyć się plikiem *shadow* i ręcznie skopiować oraz wkleić łańcuch z hasłem do pliku */etc/group*. Nie ma tu pliku */etc/gshadow* ani jego odpowiednika.

We wszystkich dystrybucjach Linuksa, z wyjątkiem SUSE, narzędzie `useradd` domyślnie tworzy dla użytkownika prywatną grupę. Systemy Unix domyślnie umieszczają wszystkich nowych użytkowników w tej samej grupie, ale program `useradd` można w nich skonfigurować w taki sposób, aby obsługiwał również prywatne grupy.

Użytkownik powinien być jedynym członkiem swojej prywatnej grupy. Jeśli chcesz umożliwić użytkownikom współdzielenie plików z wykorzystaniem mechanizmu grup, utwórz w tym celu osobne grupy. Koncepcja grupy prywatnej nie miała na celu zniechęcenia do korzystania z grup jako takich — chodziło po prostu o wprowadzenie bardziej restrykcyjnej grupy **domyślnej** dla każdego użytkownika, aby nie dochodziło do nieza mierzonego udostępniania plików. Możesz również osiągnąć ten cel za pośrednictwem polecenia `umask` (patrz strona 238).

Systemy Linux, Solaris i HP-UX zawierają polecenia służące do tworzenia, modyfikowania i usuwania grup: `groupadd`, `groupmod` i `groupdel`. System AIX wymaga ręcznej modyfikacji pliku `/etc/group` za pomocą edytora tekstu. Zawiera on jednak polecenie `grpck` służące do sprawdzania składni tego pliku.

7.4. DODAWANIE UŻYTKOWNIKÓW — PODSTAWY

Zanim utworzysz konto dla nowego użytkownika w firmie, urzędzie lub instytucji naukowej, musisz pamiętać o tym, aby użytkownik podpisał i opatrzył datą umowę użytkownika i regulamin korzystania z kont. (Co?! Nie masz umowy użytkownika i regulaminu? Zajrzyj na stronę 1473, gdzie dowiesz się, dlaczego ich potrzebujesz i co powinny zawierać).

Użytkownicy nie mają żadnego określonego powodu, aby podpisywać regulamin, więc zdobądź ich podpisy, póki jeszcze możesz to wymusić. Stwierdziliśmy, że zdobycie podpisu pod regulaminem wymaga znacznie więcej wysiłku, gdy konto zostało już założone. Jeśli tylko procedura to dopuszcza, wykonaj całą papierkową robotę przed utworzeniem konta.

Proces dodawania nowego użytkownika składa się z kilku kroków wymaganych przez system, dwóch kroków mających na celu skonfigurowanie wygodnego środowiska pracy dla nowego użytkownika oraz kilku dodatkowych kroków dla wygody administratora.

Działania wymagane to:

- podpisanie regulaminu przez użytkownika,
- zmodyfikowanie plików `passwd` i `shadow` w celu zdefiniowania konta użytkownika,
- dodanie użytkownika do pliku `/etc/group` (nie jest to konieczne, ale warto to zrobić),
- ustawienie początkowego hasła,
- utworzenie katalogu domowego użytkownika i ustawienie jego własności i praw dostępu (polecenia `chown` i `chmod`),
- skonfigurowanie ról i uprawnień (jeśli korzystasz z RBAC, zajrzyj na stronę 277).

Dla użytkownika:

- skopiowanie domyślnych plików startowych do katalogu domowego użytkownika,
- skonfigurowanie skrzynki pocztowej użytkownika i ustawienie aliasów pocztowych.

Dla administratora:

- sprawdzenie, czy konto jest poprawnie skonfigurowane,
- wprowadzenie informacji kontaktowych o użytkowniku i statusu konta do bazy danych.

Ta lista aż prosi się o skrypt lub inne narzędzie, na szczęście, każdy z naszych przykładowych systemów zawiera coś takiego w postaci polecenia `useradd`.

Aby dodawać użytkowników, musisz być użytkownikiem `root`, a w systemie AIX musisz mieć uprawnienie `UserAdmin`. To doskonała okazja do skorzystania z `sudo`; patrz strona 186.

Edycja plików `passwd` i `group`

Jeśli musisz ręcznie dodać użytkownika, do modyfikowania plików `passwd` i `shadow` używaj polecenia `vi`. Wbrew nazwie nie wymaga ono korzystania z `vi`, możesz użyć swojego ulubionego edytora zdefiniowanego w zmiennej środowiskowej `EDITOR`. Co ważniejsze, powoduje ono zablokowanie pliku, dzięki czemu Twoje modyfikacje i operacje zmiany hasła przez użytkowników nie będą ze sobą kolidować.

W systemach Solaris i Red Hat po zmodyfikowaniu pliku `passwd` polecenie `vi` automatycznie spyta, czy chcesz dokonać edycji pliku `shadow`. W systemach SUSE i Ubuntu funkcję tę spełnia polecenie `vi` `-s`.

W systemach HP-UX i AIX nie zaleca się ręcznej edycji pliku `passwd`, bez względu na to, czy miałyby się to odbywać za pomocą polecenia `vi`, czy bez niego (w systemie AIX w ogóle nie ma tego polecenia). Zamiast tego należy skorzystać odpowiednio z polecenia `useradd` lub wielozadaniowych narzędzi administracyjnych `smh` i `SMIT`. Polecenie `useradd` zostanie omówione szczegółowo, początek na stronie 278.

Jeśli nowy użytkownik ma należeć do kilku innych grup, oprócz grupy domyślnej określonej w pliku `passwd`, musisz zmodyfikować plik `/etc/group` i dopisać nazwę użytkownika do każdej z dodatkowych grup.

Ustawianie hasła

Nigdy nie pozostawiaj nowego konta — ani żadnego innego konta, które ma dostęp do powłoki — bez ustawionego hasła. Złożoność hasła można wymusić za pomocą plików konfiguracyjnych; pod koniec tego rozdziału podamy listę plików i zmiennych używanych w poszczególnych systemach operacyjnych. Hasło dla nowego użytkownika możesz ustawić przy użyciu polecenia:

\$ `sudo passwd nazwa_nowego_użytkownika`

☞ *Zasady wyboru dobrego hasła znajdziesz na stronie 183.*

Zostaniesz poproszony o podanie rzeczywistego hasła. Niektóre zautomatyzowane systemy dodawania nowych użytkowników nie wymagają podawania początkowego hasła. W zamian użytkownik zmuszony jest ustawić hasło podczas pierwszego logowania. Jest to wprawdzie wygodne, ale stanowi olbrzymie zagrożenie: każdy, kto odgadnie nazwę nowego użytkownika (lub odszuka ją w pliku */etc/passwd*), może się zacząć i przejąć konto, zanim uprawniony użytkownik będzie miał sposobność się zalogować.

Tworzenie katalogu domowego i instalowanie plików startowych

Katalog domowy dla nowego użytkownika możesz utworzyć zwykłym poleceniem `mkdir`. Musisz również ustawić odpowiednie prawa własności i uprawnienia do katalogu, ale najlepiej zrobić to dopiero po zainstalowaniu lokalnych plików startowych.

Tradycyjnie nazwy plików startowych rozpoczynają się kropką i kończą literami *rc*, co jest skrótem od „run command” (uruchom polecenie), pozostałości po systemie operacyjnym CTSS. Początkowa kropka powoduje, że polecenie `ls` ukrywa te „interesujące” pliki z listy zawartości katalogu, chyba że użyta zostanie opcja `-a`.

Zalecamy, aby dostarczyć użytkownikom domyślne pliki startowe dla każdej powłoki występującej w Twoich systemach, aby nadal mieli sensowne środowisko domyślne, jeśli zdecydują się zmienić powłokę. W tabeli 7.3 zamieściliśmy listę typowych plików startowych.

Przykładowe pliki startowe tradycyjnie przechowywane są w katalogu */etc/skel* (Linux, Solaris, HP-UX) lub */etc* (wszystkie systemy). W systemie AIX, gdzie zawsze wszystko jest trochę inne, są one ukryte w katalogu */etc/security*). Jeśli modyfikujesz przykładowe pliki startowe dostarczone przez producenta systemu, warto ich zmodyfikowane kopie umieścić w katalogu */usr/local/etc/skel*. Linux część plików startowych przechowuje w katalogu */etc/profile.d*, gdzie powłoka szuka informacji dotyczących kolorowania wyjścia polecenia `ls`, aby było czytelne na ciemnym tle, lub ścieżki dostępu do plików binarnych Kerberos.

W zależności od powłoki użytkownika, katalog */etc* może zawierać ogólnosystemowe pliki startowe, które są przetwarzane przed plikami startowymi użytkownika. Przykładowo powłoki `bash` i `sh` wczytują najpierw plik */etc/profile*, a dopiero potem przystępują do przetwarzania plików *~/.profile* i *~/.bash_profile*. Pliki te są dobrym miejscem na wprowadzenie ogólnosystemowych ustawień domyślnych, należy jednak pamiętać o tym, że użytkownik może nadpisać te ustawienia własnymi plikami startowymi. Szczegóły dotyczące innych powłok znajdziesz na stronach podręcznika systemowego.

Pamiętaj o tym, aby ustawić sensowne wartości domyślne dla `umask`; zalecamy tu 077, 027 lub 002, w zależności od poziomu zaufania i rozmiaru organizacji. Jeśli nie używasz indywidualnych grup, zalecamy maskę 077, ponieważ daje pełne prawa dostępu

Tabela 7.3. Pliki startowe i ich zastosowanie

Polecenie	Nazwa pliku	Typowe zastosowanie
sh	<i>.profile</i>	ustawienie ścieżki wyszukiwania, typu terminala i środowiska
bash ^a	<i>.bashrc</i> <i>.bash_profile</i>	ustawienie typu terminala (jeśli jest to konieczne) ustawienie opcji <code>bi</code> <code>ff</code> i <code>mesg</code> ustawienie zmiennych środowiskowych ustawienie nazw zastępczych (aliasów) dla poleceń ustawienie ścieżki wyszukiwania ustawienie wartości <code>umask</code> w celu ustalenia uprawnień ustawienie zmiennej <code>CDPATH</code> do wyszukiwania plików ustawienie zmiennych <code>PS1</code> (znak zachęty) i <code>HISTCONTROL</code>
csh (tcsh)	<i>.login</i> <i>.cshrc</i>	podobne do <i>.bashrc</i> dla csh podobne do <i>.login</i> dla csh
vi (vim)	<i>.exrc</i> (<i>.vimrc</i>)	ustawienie opcji edytora vi (vim)
emacs	<i>.emacs</i>	ustawienie opcji i przypisań klawiszy edytora emacs
mail (mailx)	<i>.mailrc</i>	definicje prywatnych aliasów pocztowych ustawienie opcji czytnika poczty (oryginalnego klienta poczty systemu UNIX)
GNOME	<i>.gconf</i> <i>.gconfpath</i>	środowisko GNOME: konfiguracja użytkownika wprowadzona przez <code>gconf</code> ścieżka dodatkowej konfiguracji użytkownika przez <code>gconf</code>
KDE	<i>.kde/</i>	środowisko KDE: katalog z plikami konfiguracyjnymi

^a W trybie emulacji sh bash wczytuje również plik *.profile* lub */etc/profile*.

właścicielowi, odbierając dostęp grupie i pozostałym użytkownikom. Szczegółowe informacje na temat `umask` znajdują się na stronie 238.

Pliki startowe i katalogi z ustawieniami dla środowisk GNOME i KDE to tylko wierzchołek góry lodowej; `gconf` to narzędzie przechowujące ustawienia aplikacji dla programów działających pod GNOME, co przypomina nieco rejestr w systemie Windows.

Ustawianie uprawnień i praw własności

Po skonfigurowaniu katalogu domowego przekaz go użytkownikowi i upewnij się, że ma on odpowiednie uprawnienia. Można to wykonać za pomocą polecenia:

```
$ sudo chown -R nowy_użytkownik:nowa_grupa ~nowy_użytkownik
```

Zauważ, że nie możesz użyć polecenia:

```
$ sudo chown nowy_użytkownik:nowa_grupa ~nowy_użytkownik/.*
```

aby ustawić właściciela plików rozpoczynających się znakiem kropki, ponieważ `nowy_użytkownik` nabędzie prawa własności nie tylko do własnych plików, ale również do katalogu nadrzędnego (np. */home*). To bardzo częsta i niebezpieczna pomyłka.

Ustawienie miejsca odbioru poczty

Rozwiązaniem wygodnym dla użytkowników jest odbieranie poczty tylko na jednym komputerze. Często jest to realizowane za pomocą wpisu w globalnym pliku aliasów `/etc/mail/aliases` lub opcji `userDB` programu `sendmail` na głównym serwerze pocztowym. Ogólne informacje na temat poczty znajdują się w rozdziale 20.

Konfigurowanie ról i uprawnień administracyjnych

Kontrola dostępu oparta na rolach (RBAC) umożliwia rozdzielanie uprawnień systemowych na poszczególnych użytkownikach i jest dostępna na wielu naszych przykładowych systemach. Mechanizm RBAC nie jest tradycyjną częścią systemu Unix ani modelu kontroli dostępu w Linuksie, ale jeśli stosuje się go w Twojej organizacji, konfigurowanie ról musi być częścią procesu dodawania użytkowników. RBAC został szczegółowo omówiony od strony 179 w rozdziale 4., „Kontrola dostępu i uprawnienia administratora”.

Regulacje prawne, takie jak ustawa Sarbanesa-Oxleya (SOX) i ustawa Gramma-Leacha-Bliley (GLBA) w Stanach Zjednoczonych, skomplikowały wiele aspektów administracji systemem w przedsiębiorstwach, w tym również zarządzanie użytkownikami. Może się okazać, że role są jedynym realnym rozwiązaniem, które będzie w stanie zapewnić zgodność z wymogami prawnymi.

➞ Więcej informacji na temat ustaw SOX i GLBA można znaleźć w rozdziale 32.

Końcowe kroki

Aby sprawdzić, czy nowe konto zostało poprawnie utworzone, najpierw musisz się wylogować, a następnie zalogować ponownie jako nowy użytkownik i wykonać poniższe polecenia:

```
$ pwd          /* Aby zweryfikować katalog domowy */  
$ ls -la       /* Aby sprawdzić własność i grupę plików startowych */
```

Musisz podać nowym użytkownikom ich nazwy i początkowe hasła. Często informacje te przesyłane są pocztą elektroniczną, ale ze względu na bezpieczeństwo zazwyczaj nie jest to dobry pomysł. Zrób to osobiście lub telefonicznie, chyba że stworzysz 500 kont na komputerach CS-1 dla nowych studentów w miasteczku uniwersyteckim. Wtedy przerzucić problem na ich wykładowców! Jest to również dobry moment na przekazanie użytkownikom dodatkowej dokumentacji omawiającej lokalne zwyczaje, jeśli ją opracowałeś.

Jeśli Twoja organizacja wymaga od użytkowników podpisania regulaminu lub zasad właściwego korzystania z konta, upewnij się, że zostało to zrobione przed aktywacją. Pozwoli to zapobiec niedopatrzeniom i da podstawę do ewentualnych sankcji, które być może trzeba będzie w przyszłości zastosować.

➤ Więcej informacji na temat podpisywania umowy użytkownika można znaleźć na stronie 1487.

Przypomnij nowym użytkownikom o konieczności natychmiastowej zmiany hasła. Jeśli chcesz, możesz to wymusić, ustawiając szybkie wygaśnięcie hasła. Innym rozwiązaniem jest użycie skryptu, który przetestuje konta nowych użytkowników i sprawdzi, czy ich zaszyfrowane hasła w pliku *shadow* zostały zmienione¹⁰.

W środowisku, w którym osobiście znasz użytkowników, możesz stosunkowo łatwo śledzić, kto i dlaczego korzysta z systemu. Jeśli jednak zarządzasz dużą i dynamicznie zmieniającą się bazą użytkowników, musisz znaleźć bardziej sformalizowany sposób śledzenia aktywności kont. Jeśli kiedyś fakt utworzenia konta zatrze się w Twojej pamięci, utrzymywanie bazy danych zawierającej informacje kontaktowe i statusy kont pozwoli Ci łatwo sprawdzić, kim jest dany użytkownik i dlaczego ma założone konto.

7.5. DODAWANIE UŻYTKOWNIKÓW ZA POMOCĄ USERADD

W każdym systemie program *useradd* realizuje tę samą opisaną wcześniej prostą procedurę. Jest on jednak konfigurowalny i zapewne warto dostosować go do swojego środowiska. Ponieważ każdy system ma własną koncepcję na temat tego, co powinno być dostosowane, gdzie należy wyprowadzić zmiany i jakie powinno być domyślne zachowanie, omówmy te szczegóły osobno.

W tabeli 7.4 zawarliśmy podręczny spis poleceń i plików konfiguracyjnych związanych z zarządzaniem użytkownikami. Każdy z naszych przykładowych systemów ma pakiet poleceń służących do działań na użytkownikach, zwykle zawiera on co najmniej *useradd*, *usermod* i *userdel*. Ponieważ wszystkie te polecenia są konfigurowane w podobny sposób, zaprezentujemy je tu na przykładzie polecenia *useradd*, uzupełniając jego wpisy o inne polecenia specyficzne dla danego systemu.

Warto zauważyć, że choć w każdym systemie polecenia te noszą nazwy *useradd* itd., same narzędzia różnią się w zależności od systemu.

Polecenie *useradd* w systemie Ubuntu



Ubuntu umożliwia dodawanie użytkowników na dwa sposoby: za pomocą *adduser* i *useradd*. Polecenie *adduser* to napisany w Perlu skrypt osłonowy dla polecenia *useradd*, który jest nieco bardziej pomocny (tworzy katalogi domowe, kopiuje pliki startowe itd.).

Polecenie *adduser* jest konfigurowane w pliku */etc/adduser.conf*, który zawiera m.in. następujące opcje:

¹⁰ Ponieważ to samo hasło może mieć wiele zaszyfrowanych form, ta metoda sprawdza tylko, czy użytkownik zresetował hasło, a nie to, czy rzeczywiście zmienił je na inne.

Tabela 7.4. Polecenia i pliki konfiguracyjne służące do zarządzania użytkownikami

System	Polecenia	Pliki konfiguracyjne	Uwagi
Ubuntu	useradd	/etc/login.defs /etc/default/useradd	bardziej przyjazna wersja Perla
	adduser	/etc/adduser.conf	
SUSE	useradd	/etc/login.defs	dla dostosowań lokalnych dla dostosowań lokalnych dla dostosowań lokalnych dla dostosowań lokalnych
		/etc/default/useradd	
		/etc/default/passwd	
		/usr/sbin/useradd.local	
		/usr/sbin/userdel.local	
		/usr/sbin/userdel-pre.local /usr/sbin/userdel-post.local	
Red Hat	useradd	/etc/login.defs /etc/default/useradd	
Solaris	useradd	/etc/default/{login,passwd} /etc/security/policy.conf	
HP-UX	useradd	/etc/default/useradd /etc/default/security	narzędzie GUI, zwane również sam
	smh		
AIX	useradd	/etc/security/user /etc/security/login.cfg /etc/security/mkuser.default ^a	wywoływane przez useradd wywoływane przez usermod wywoływane przez userdel narzędzie GUI
	mkuser		
	chuser		
	rmuser		
	SMIT		

^a W starszych systemach AIX plik ten znajduje się w katalogu `/usr/lib/security`.

- reguły lokalizacji katalogów domowych: pod względem grup, nazw użytkowników itd.,
- ustawienia uprawnień dla nowych katalogów domowych,
- zakresy numerów UID i GID dla użytkowników systemowych i ogólnych,
- opcję tworzenia indywidualnej grupy dla każdego użytkownika,
- udziały dyskowe (niestety, tylko jako wartość logiczną),
- dopasowanie nazw użytkowników i grup na podstawie wyrażeń regularnych.

Inne typowe parametry polecenia `useradd`, takie jak reguły dotyczące haseł, ustawiane są jako parametry modułu PAM odpowiedzialnego za regularne uwierzytelnianie

hasel (omówienie PAM, czyli dołączalnych modułów uwierzytelniania, znajduje się na stronie 1113). Polecenie `adduser` ma bliźniacze polecenie `addgroup` oraz pokrewne `deluser` i `delgroup`.

Polecenie `useradd` w SUSE



Polecenie `useradd` w systemie SUSE domyślnie nie tworzy katalogu domowego dla nowego użytkownika ani nie kopiuje plików startowych. Musisz zażądać tych udogodnień, podając opcję `-m` (pliki startowe pobierane są z katalogu `/etc/skel`); `useradd` nie tworzy też plików poczty dla nowych użytkowników.

Polecenie `useradd` w SUSE również nie powoduje powstania indywidualnych grup dla użytkowników; domyślny numer GID w pliku `passwd` ustawiany jest na podstawie zmiennej `GROUP` w pliku `/etc/default/useradd`. Ponadto nowi użytkownicy dodawani są do grup określonych przez zmienną `GROUPS`. Domyślnie są to grupy `video` i `dialout`, które umożliwiają dostęp do bufora ramek i oprogramowania `pppd` do obsługi połączeń dodzwanianych.

Aby zrekompensować te różnice, polecenie `useradd` w systemie SUSE wywołuje `/usr/sbin/useradd.local`, skrypt powłoki `bash`, który możesz dostosować do swoich potrzeb.

Plik `/etc/login.defs` w systemie SUSE reguluje następujące kwestie:

- pozwolenie na zalogowanie, jeśli katalog domowy użytkownika nie istnieje,
- stopień tolerancji (zwłoka i blokada) przy nieudanych próbach zalogowania,
- położenie plików „wiadomości dnia” i *ttytype* (typy terminali),
- ograniczenie dotyczące korzystania z poleceń `chsh` i `chfn`,
- wygasanie hasel,
- zakresy numerów UID i GID dla systemu i użytkowników,
- reguły tworzenia właściwych nazw użytkowników i grup,
- maski użytkowników (domyślnie 022),
- lokalne skrypty korzystające z poleceń `useradd` i `userdel`.

Zarówno strona podręcznika systemowego dla pliku `login.defs`, jak i komentarze w samym pliku zawierają cenne informacje opisujące różne parametry i ich znaczenie.

Polecenie `useradd` w systemie Red Hat



W systemie Red Hat Linux Enterprise polecenie `useradd` pobiera swoje parametry konfiguracyjne z pliku `/etc/login.defs`, który odpowiada za takie kwestie jak wygasanie hasel, algorytmy szyfrowania, pliki poczty oraz zakresy numerów UID i GID. Poszczególne parametry wyjaśnione są w komentarzach zawartych w tym pliku.

Polecenie `useradd -D` wyświetla parametry domyślne, które będą zastosowane dla nowych użytkowników. Są one zapisane w pliku `/etc/default/useradd`. W systemie Red Hat nowi użytkownicy umieszczani są w swoich indywidualnych grupach. We wpisach w pliku `passwd` użyto znaku „x” jako symbolu zastępczego dla hasła, a w pliku `shadow` użyto kodu „!!”, który wyłącza logowanie i wymaga, aby administrator systemu ustawił hasło dla nowego użytkownika. Domyślnym algorytmem szyfrowania jest MD5. W katalogu nowego użytkownika umieszczane są pliki startowe z katalogu `/etc/skel`.

Polecenie `useradd` w systemie Solaris

 W systemie Solaris niektóre domyślne parametry dotyczące logowania i haseł przechowywane są w plikach `/etc/default/login` i `/etc/default/passwd`; pozostałe zostały wbudowane w program `useradd`. Polecenie `useradd -D` wyświetli domyślne wartości dla kilku parametrów. Za pomocą dodatkowych opcji można je wykorzystać do przywrócenia niektórych ustawień domyślnych.

Formaty plików `default/login` i `default/passwd` są podobne do formatu pliku `login.defs` w systemie Linux. Puste wiersze i wiersze rozpoczynające się znakiem `#` są ignorowane, a każdy wiersz niebędący komentarzem stanowi przypisanie wartości lub zmiennej. Składnia wygląda jednak tak:

```
NAZWA=wartość
```

a nie tak:

```
NAZWA <puste znaki> wartość
```

Plik `/etc/default/passwd` kontroluje następujące elementy:

- minimalną długość hasła,
- wygaśnięcie hasła,
- wymagany stopień złożoności hasła,
- sprawdzenie możliwości złamania hasła.

Plik `/etc/default/login` odpowiada za takie kwestie jak:

- strefa czasowa,
- ograniczenie wielkości plików, jakie użytkownik może tworzyć,
- możliwość logowania się użytkownika `root` tylko na konsoli,
- wymagalność hasła dla każdego użytkownika,
- obsługa nieudanych prób zalogowania,
- początkowa ścieżka wyszukiwania danego użytkownika,
- domyślna maska użytkownika (domyślnie 022),
- opcje programu `syslog`: czy ma rejestrować logowania użytkownika `root` i nieudane próby zalogowania.

Pliki */etc/security/policy.conf* i */etc/security/crypt.conf* określają algorytmy szyfrowania, które mogą być używane dla haseł.

Polecenie **useradd** w systemie HP-UX



Domyślnie polecenie **useradd** w systemie HP-UX nie tworzy katalogów domowych ani nie umieszcza użytkownika w jego indywidualnej grupie. Opcja *-m* spowoduje jednak, że **useradd** utworzy katalogi domowe i umieści w nich pliki startowe z katalogu */etc/skel*.

Parametry konfiguracyjne polecenia **useradd** ustawione są w plikach */etc/default/useradd* i */etc/default/security*, przy czym plik *useradd* przyjmuje format w stylu Linuksa, czyli NAZWA <puste znaki> wartość, a plik *security* używa formatu Solarisa, tj. NAZWA=wartość. HP potrafi niezłe namieszać! Składnię można wywnioskować z innych wpisów w pliku, jeśli jednak użyjesz złej składni, wartość, którą spróbujesz ustawić, zostanie po cichu zignorowana. Nie pojawi się żaden komunikat o błędzie.

Plik */etc/default/useradd* kontroluje takie opcje jak:

- domyślna grupa i powłoka,
- główny poziom drzewa katalogu domowego,
- wygasanie konta,
- tworzenie katalogów domowych,
- pozwalanie na duplikowanie numerów UID.

Plik */etc/default/security* zawiera dodatkowe parametry konfiguracyjne, z których część dotyczy zarządzania użytkownikami, czyli:

- pozwolenia na logowanie w przypadku braku katalogu domowego,
- dopuszczania pustych haseł,
- minimalnej długość hasła,
- obsługi nieudanych prób logowania,
- obsługi nieaktywnych kont,
- domyślnej maski dla nowych użytkowników (domyślnie 027).

Nazwy zmiennych w tym pliku są długie i trafne, dzięki czemu dokładnie określają, za co odpowiada każda zmienna.

Polecenie **useradd** w systemie AIX



W systemie AIX polecenie **useradd** to w rzeczywistości skrypt osłonowy powłoki ksh dla **mkuser**, rodzimego odpowiednika **useradd** w AIX. Podobnie polecenie **usermod** wywołuje **chuser**, a **userdel** wywołuje **rmuser**. Strony podręcznika systemowego

dla tych poleceń można wywołać, odwołując się zarówno do ich oryginalnych nazw, jak i tych, pod jakimi występują w pozostałych systemach.

Pliki konfiguracyjne kontrolujące wiele różnych aspektów logowania i haseł znajdują się w katalogu `/etc/security`. Są tam trzy istotne pliki: `login.cfg`, `user` i `mkuser.default`. Pierwsze dwa używają znaku `*` dla oznaczania komentarzy; trzeci nie zawiera komentarzy. Pliki te podzielone są na sekcje w następującej postaci:

```
etykieta:
    atrybut = wartość
    następny-atomyt = wartość
```

```
następna-etykieta:
    atrybut = wartość
```

Przykładowo w pliku `/etc/security/user` etykietami są nazwy użytkowników (lub słowo `default`); możliwe atrybuty podane są w tabeli 7.5 na następnej stronie.

Całkiem spora lista! Komentarze w pliku często podają wartości domyślne, które są dość sensowne dla instalacji o niskim poziomie bezpieczeństwa. Zalecamy wprowadzenie kilku zmian:

- zmianę wartości `umask` z 022 na 077,
- zmianę wartości `loginretries` z 0 (brak ograniczeń) na małą liczbę całkowitą, np. 5,
- zmianę wartości `minlen` z 0 (dopuszczalny brak hasła) na co najmniej 6 lub 7,
- zmianę wartości `expires` z 0 (nigdy) na rok (tylko jeśli dysponujesz narzędziem umożliwiającym okresowe odświeżanie dat wygaśnięcia dla prawowitych użytkowników).

Niestety, to tylko jeden z plików konfiguracyjnych kontrolujących logowanie nowych użytkowników. Plik `/etc/security/login.cfg` zawiera parametry kontrolujące nieudane próby logowania (opóźnienie między wyświetleniem znaków zachęty do podania loginu i hasła, liczbę dozwolonych prób zalogowania przed wyłączeniem konta, czas trwania blokady konta, czas jego przywrócenia itd.), przedziały czasowe, w których można się zalogować, znak zachęty wyświetlany podczas prośby o podanie hasła, listę dozwolonych powłok, maksymalną dopuszczalną liczbę jednoczesnych logowań, czas oczekiwania na wprowadzenie hasła, rodzaj używanego uwierzytelniania (jeśli korzystasz z PAM¹¹, musisz to podać właśnie w tym pliku) oraz algorytmy szyfrowania haseł (domyślnie jest to `crypt`). Możliwości konfiguracji są niesamowicie rozbudowane, aż do przesady. Jeszcze większy zamęt powoduje to, że niektóre parametry pojawiają się w obu plikach, przy czym czasem występują pod tą samą nazwą (np. `logintimes`), a czasem nazywają się inaczej (np. `loginretries` i `logindisable`). Krótko mówiąc, jeden wielki bałagan i mętlik.

¹¹ Mechanizm PAM pojawił się w AIX stosunkowo niedawno; pełną funkcjonalność powinien mieć w wersji 5.3 lub późniejszych.

Tabela 7.5. Opcje konta użytkownika w pliku `/etc/security/user` (AIX)

Opcja	Wartość	Znaczenie
account_locked	logiczna	wartość true blokuje możliwość logowania
admin	logiczna	wartość true nadaje uprawnienia administratora
auth1	lista metod	główna metoda uwierzytelniania
auth2	lista metod	drugorzędna metoda uwierzytelniania
dictionlist	nazwy plików	słowniki, w których nie może występować hasło
expires	data	data wygaśnięcia konta użytkownika
histexpire	tygodnie	okres, przez jaki użytkownik nie może ponownie użyć wykorzystanego hasła
histsize	numer	liczba poprzednich haseł, które nie mogą zostać użyte ponownie
login	logiczna	czy pozwolić na zalogowanie (przdatne dla kont typu bin)
loginretries	numer	liczba prób zalogowania przed zablokowaniem konta
logintimes	przedział czasu	ograniczenie czasu, w którym użytkownik może się zalogować
maxexpired	tygodnie	okres łaski dla haseł, które wygasły
maxrepeats	numer	liczba dopuszczalnych powtórzeń znaku w hasle
minage, maxage	tygodnie	minimalny i maksymalny okres ważności hasła
minalpha	numer	minimalna liczba liter w hasle
mindiff	znaki	liczba znaków starego hasła, które mogą wystąpić w nowym hasle
minlen	numer	minimalna długość hasła (nie ustawiaj tu wartości 0)
minother	numer	minimalna liczba znaków nieliterowych w hasle
pwdchecks	nazwy plików	funkcje wywoływane w celu sprawdzenia bezpieczeństwa haseł
pwdwarntime	dni	okres łaski ostrzegający użytkownika o konieczności zmiany hasła
rlogin	logiczna	określa, czy użytkownik może się zalogować na to konto przez rlogin lub telnet
su	logiczna	określa, czy inni użytkownicy mogą zalogować się na to konto przez su
ttys	lista urządzeń	terminale, na których użytkownik może się logować
umask	ósemkowa	domyślne prawa dostępu do plików tworzonych przez użytkownika

➔ Więcej informacji na temat PAM można znaleźć na stronie 1113.

W AIX polecenie `useradd` nie ma opcji `-D`, która pokazywałaby domyślne wartości dla nowych użytkowników. Polecenie `useradd` umieszcza nowych użytkowników w pojedynczej grupie i nie tworzy ich katalogów domowych, chyba że zostanie wywołane z opcją `-m` (w tym przypadku skopiuje ono również plik `.profile` z katalogu `/etc/security`).

Przykłady użycia polecenia `useradd`

Aby utworzyć nowego użytkownika „*hilbert*”, używając systemowych wartości domyślnych w Linuksie, wystarczy po prostu wydać polecenie:

```
$ sudo useradd hilbert
```

Polecenie to powinno utworzyć w pliku */etc/passwd* następujący wpis:

```
hilbert:x:1005:20::/home/hilbert:/bin/sh
```

Polecenie `useradd` wyłączyło konto, wstawiając znak `x` w polu przeznaczonym na hasło. Aby można było korzystać z konta, musisz mu przypisać prawdziwe hasło.

Poniżej przedstawiamy bardziej realistyczny przykład. Określimy, że podstawową grupą użytkownika *hilbert* ma być „*faculty*” i powinien on również zostać dodany do grupy „*famous*”. Zmienimy też domyślne położenie katalogu domowego oraz powłokę i poprosimy `useradd` o utworzenie katalogu domowego, jeśli jeszcze nie istnieje:

```
$ sudo useradd -c "David Hilbert" -d /home/math/hilbert -g faculty -G famous -m -s  
↪/bin/tcsh hilbert
```

Polecenie to utworzy następujący wpis w pliku *passwd*:

```
hilbert:x:1005:30:David Hilbert:/home/math/hilbert:/bin/tcsh
```

Przypisany numer UID jest większy niż najwyższy UID w systemie, a odpowiedni wpis w pliku *shadow* to:

```
hilbert!:14322:0:99999:7:0::
```

Znaki zastępcze dla hasła w plikach *passwd* i *shadow* mogą różnić się w zależności od systemu operacyjnego. Do czasu nadania hasła dla konta znak zastępczy w pliku *shadow* blokuje możliwość zalogowania. Ponadto polecenie `useradd` doda użytkownika *hilbert* do odpowiednich grup w pliku */etc/group*, utworzy katalog */home/math/hilbert* i skopiuje do niego pliki z katalogu */etc/skel*.

7.6. HURTOWE DODAWANIE UŻYTKOWNIKÓW ZA POMOCĄ `NEWUSERS` (LINUX)



W systemie Linux istnieje polecenie `newusers`, za pomocą którego jednocześnie utworzysz wiele kont na podstawie zawartości pliku tekstowego. Jest ono dość ułomne, ale może okazać się przydatne, gdy musisz dodać większą liczbę użytkowników naraz, np. przy tworzeniu kont dla całego rocznika studentów. Polecenie `newusers` oczekuje pliku wejściowego zawierającego takie same wiersze jak plik */etc/passwd*, z tym, że pole z hasłem musi zawierać hasło początkowe zapisane jawnym tekstem, dlatego dobrze pilnuj tego pliku.

Polecenie `newusers` uznaje parametr wygasania haseł ustawiony w pliku `/etc/login.defs`, ale w odróżnieniu od `useradd` nie kopiuje domyślnych plików startowych. Jednym plikiem startowym, jaki zapewnia, jest `.xauth`.

Dla uniwersytetu potrzebny jest skrypt wsadowy `adduser`, który na podstawie listy studentów pobranej z danych rekrutacyjnych lub rejestracyjnych wygeneruje plik wejściowy dla `newusers`, w którym użytkownicy będą mieli przypisane niepowtarzalne i zgodne z lokalnie przyjętymi regułami nazwy kont, silne, losowo wygenerowane hasła oraz numery UID i GID przyporządkowane rosnąco dla każdego użytkownika. Prawdopodobnie lepiej będzie napisać własny skrypt osłonowy dla `useradd` w języku Perl lub Python, niż zmusić do działania polecenie `newusers`, aby robiło dokładnie to, czego oczekujesz.

7.7. USUWANIE UŻYTKOWNIKÓW

Gdy użytkownik opuszcza organizację, jego konto i pliki powinny zostać usunięte z systemu. Procedura ta wymaga usunięcia wszystkich odwołań do nazwy użytkownika, które były dodane przez Ciebie lub przez program `useradd`. Jeśli usuwasz użytkownika ręcznie, możesz posłużyć się poniższą listą czynności do wykonania:

- usunąć użytkownika ze wszystkich spisów telefonów i lokalnych baz danych o użytkownikach,
- usunąć użytkownika z pliku *aliases* lub dodać adres do przekazywania poczty,
- usunąć plik `crontab` użytkownika i wszystkie jego zadania `at` lub kolejki wydruku,
- zabić wszystkie działające procesy użytkownika,
- usunąć użytkownika z plików *passwd*, *shadow*¹², *group* i *gshadow*,
- usunąć katalog domowy użytkownika,
- usunąć skrzynkę pocztową użytkownika,
- usunąć jego wpisy z kalendarzy grupowych, systemów rezerwacji pomieszczeń itd.,
- usunąć lub przekazać uprawnienia do list dyskusyjnych prowadzonych przez usuniętego użytkownika.

Zanim usuniesz czyjś katalog domowy, pamiętaj o tym, aby przenieść w inne miejsce wszelkie pliki, które mogą być potrzebne innym użytkownikom. Zazwyczaj trudno określić, o jakie pliki może chodzić, dlatego przed ich usunięciem zawsze warto wykonać dodatkową kopię zapasową katalogu domowego użytkownika i skrzynki pocztowej.

Po usunięciu użytkownika możesz sprawdzić, czy jego stary numer UID nie jest właścicielem plików w systemie. Aby wyszukać takie osierocone pliki, możesz użyć polecenia

¹² `/etc/security/{passwd,group}` w systemie AIX.

find z argumentem `-nouser`. Ponieważ polecenie `find` potrafi „uciec” na serwery sieciowe, jeśli nie zachowasz ostrożności, zwykle najbezpieczniej sprawdzać osobno poszczególne systemy plików za pomocą opcji `-xdev`:

```
$ sudo find system_plików -xdev -nouser
```

Zabicie działających procesów usuniętego użytkownika może być nieco utrudnione w środowiskach rozproszonych. W kalendarzach grupowych i systemach rezerwacji pomieszczeń mogą istnieć aktywne wpisy wprowadzone przez nieistniejącego już użytkownika i należy je stamtąd usunąć. Prawdopodobnie w swoim środowisku znajdziesz więcej tego rodzaju miejsc, z których trzeba usunąć ślady po użytkowniku — zrób własną listę, np. w formie skryptu czyszczącego.

Jeśli w Twojej organizacji przydziela się użytkownikom własne stacje robocze, na ogół najprostszym i najbardziej wydajnym rozwiązaniem jest powtórne odtworzenie całego systemu z głównego obrazu przed przekazaniem go nowemu użytkownikowi. Przed przeprowadzeniem nowej instalacji warto jednak wykonać kopię lokalnych plików znajdujących się na dysku twardym na wypadek, gdyby były potrzebne w przyszłości.

W każdym z naszych przykładowych systemów występuje polecenie `userdel`, które automatyzuje proces usuwania użytkownika. Najprawdopodobniej nie przeprowadzi ono tego zdania tak dokładnie, jak byś sobie tego życzył, chyba że skrupulatnie wprowadzisz do niego nowe funkcje, rozszerzające liczbę miejsc, w których przechowywane są informacje związane z użytkownikiem.



W systemie Ubuntu `deluser` to skrypt Perla, który wywołuje tradycyjne polecenie `userdel`; cofa on wszystkie operacje wykonane przez `adduser`. Aby ułatwić lokalizację ustawień, wywołuje skrypt `deluser.local`, jeśli taki istnieje. Plik konfiguracyjny `/etc/deluser.conf` umożliwia ustawienie następujących opcji.

- Czy usunąć katalog domowy i skrzynkę pocztową użytkownika?
- Czy wykonać kopię plików użytkownika i gdzie je umieścić?
- Czy usunąć wszystkie pliki należące do użytkownika?
- Czy usunąć grupę, jeśli nie ma już żadnych członków?



SUSE obsługuje zestaw skryptów do wykonywania zadań wstępnych i końcowych, a także skrypt `userdel.local`, który wspomaga polecenie `userdel`, informując domyślne narzędzie o lokalnych ustawieniach. Możesz je skonfigurować w pliku `/etc/login.defs`.



W systemie Red Hat istnieje skrypt `userdel.local`, ale nie ma żadnych skryptów do wykonywania zadań wstępnych i końcowych, które automatyzowałyby takie rzeczy jak wykonywanie kopii plików użytkownika przeznaczonego do usunięcia.



Systemy Solaris i AIX mają kilka dodatkowych miejsc, w których przechowywane są informacje o użytkownikach, przede wszystkim chodzi

tu o pliki kontrolujące role i klasy autoryzacji. Dlatego też polecenia `userdel` w tych systemach mają nieco więcej pracy do wykonania przy czyszczeniu wszystkich odwołań do usuniętego użytkownika.

Przykładowo, oprócz `/etc/passwd` i `/etc/group`, polecenie `userdel` w systemie Solaris aktualizuje również pliki `/etc/shadow`, `/etc/project` i `/etc/user_attr`. W systemie AIX polecenie `userdel` modyfikuje w katalogu `/etc/security` następujące pliki: `user`, `user.roles`, `lastlog`, `environ`, `audit/config`, `limits`, `passwd` i `group`. Solaris nie jest tak skrupulatny, jak można by oczekiwać: jego polecenie `userdel` pozostawiło testowy login z profilem skonfigurowanym w pliku `user_attr`, który powinien zostać wyczyszczony.



W systemie HP-UX polecenie `userdel` to banalny, prosty skrypt, który usuwa zmiany wprowadzone przez `useradd`. Modyfikuje tylko pliki `passwd`, `shadow` i `group`.

7.8. WYŁĄCZANIE KONT

Czasami zdarza się, że konto użytkownika musi zostać tymczasowo wyłączone. Najprostszym sposobem jest dopisanie gwiazdki lub innego znaku na początku zaszyfrowanego hasła użytkownika w plikach `/etc/security/passwd` (AIX) lub `/etc/shadow`. Uniemożliwi to większość prób dostępu na hasło, ponieważ tak zmodyfikowanego hasła nie da się sensownie odszyfrować. Jednak takie polecenia jak `ssh`, które niekoniecznie muszą sprawdzać hasła systemowe, mogą nadal funkcjonować.



We wszystkich dystrybucjach Linuksa polecenia `usermod -L użytkownik` i `usermod -U użytkownik` umożliwiają łatwe zablokowanie i odblokowanie hasła. Jest to po prostu szybszy sposób wykonania na hasła opisanych powyżej operacji: opcja `-L` umieszcza znak `!` na początku zaszyfrowanego hasła w pliku `/etc/shadow`, a opcja `-U` go usuwa.



W systemie Solaris użytkownik `root` może zablokować konto za pomocą polecenia `passwd -l nazwa_użytkownika`, zmusić użytkownika do zmiany hasła za pomocą opcji `-f` lub odblokować konto za pomocą opcji `-u`. Zablokowanie konta powoduje wstawienie znaków `*LK*` do pola z hasłem w pliku `/etc/shadow`. Jest to również wartość ustawiana dla użytkowników przez polecenie `useradd`.



System HP-UX obsługuje tylko hasła zaszyfrowane algorytmem `crypt`. Znak `*` nigdy nie występuje w polu hasła wygenerowanym przez `crypt`, dlatego dopisanie go do zaszyfrowanego hasła uniemożliwi zalogowanie się użytkownika.



W systemie AIX konto jest zablokowane, jeśli plik `/etc/passwd` zamiast znaku `!` zawiera `*`. Za pomocą polecenia `pwdadm` można wymusić na użytkowniku zmianę hasła lub zablokować jego konto, tak aby tylko administrator mógł zmienić hasło.

Niestety, zmodyfikowanie hasła użytkownika po prostu uniemożliwi logowanie. Użytkownik nie zostanie powiadomiony o zawieszeniu konta ani poinformowany o powodach,

dla których konto nie działa. Innym sposobem wyłączenia konta jest zastąpienie powłoki użytkownika programem, który wyświetli komunikat z wyjaśnieniem i wytłumaczy, co należy zrobić w takiej sytuacji. Następnie program zakończy działanie, zamykając sesję logowania.

Takie podejście ma zarówno zalety, jak i wady. Nie zostaną wyłączone te formy dostępu, które sprawdzają hasło, ale nie zwracają uwagi na powłokę. Aby ułatwić przeprowadzenie sztuczki z wyłączeniem powłoki, wiele demonów zapewniających dostęp bez logowania do systemu (np. `ftpd`) sprawdza, czy powłoka logowania użytkownika jest wymieniona w pliku `/etc/shells`; jeśli jej tam nie ma, następuje odmowa dostępu. O takie zachowanie nam chodzi. Niestety, nie jest ono powszechne, jeśli więc zdecydujesz się na wyłączanie kont przez modyfikowanie powłoki, będziesz musiał przeprowadzić dość wyczerpujące testy.

Kolejny problem polega na tym, że jeśli użytkownik spróbuje się zalogować przez system X Window lub za pośrednictwem emulatora terminala, który nie pozostawia widocznego wyjścia po wylogowaniu, może nigdy nie zobaczyć Twojego starannie napisanego wyjaśnienia powodów zawieszenia konta.

Domyślnie program `sendmail` nie dostarczy poczty użytkownikowi, którego powłoka nie występuje w pliku `/etc/shell`. Zakłócanie przepływu poczty to zły pomysł, nawet jeśli odbiorca i tak nie może jej natychmiast przeczytać. Możesz obejść to domyślne zachowanie programu `sendmail`, dodając do pliku `/etc/shells` fałszywą powłokę o nazwie `/SENDMAIL/ANY/SHELL/`.

7.9. ZARZĄDZANIE UŻYTKOWNIKAMI ZA POMOCĄ NARZĘDZI SYSTEMOWYCH

Systemy HP-UX i AIX wyposażono we wszechstronne narzędzia do administracji systemem, które potrafią zarządzać użytkownikami, przynajmniej w podstawowym zakresie. W systemie AIX jest to SMIT (ang. *System Management Interface Tool*), a w HP-UX nosi ono obecnie nazwę `smh` (ang. *System Management Homepage*)¹³. Każde z tych narzędzi zawiera ekrany przeznaczone do dodawania użytkowników i zarządzania nimi, przy wykorzystaniu interfejsu graficznego lub w formie terminala z menu opartym na bibliotece `curses`. Jeśli jesteś zupełnie początkującym administratorem lub wcześniej pracowałeś w całkiem innym systemie operacyjnym, narzędzia te będą sensownym punktem wyjścia dla wielu często wykonywanych zadań administracyjnych.

Program SMIT z systemu AIX ma przydatną opcję: jeśli naciśniesz klawisz *F6*, wyświetlone zostaną polecenia i argumenty zaplanowane do wykonania. Ponadto rejestruje on całą interakcję i przechowuje plik skryptowy zawierający polecenia, które zostały wykonane w Twoim imieniu. Może to być dobre narzędzie do nauki w miarę zapoznawania

¹³ We wcześniejszych wersjach systemu HP-UX miało ono nazwę `sam` (ang. *System Administration Manager*).

się z zawiłościami systemu AIX. Oparty na bibliotece `curses` program `smh` z systemu HP-UX oferuje przydatne, jednoznakowe skróty. Są one widoczne na każdej stronie menu i umożliwiają szybkie przejście do potrzebnego polecenia.

7.10. MINIMALIZOWANIE RYZYKA ZA POMOCĄ PAM

Dołączalne moduły uwierzytelniania (PAM, ang. *Pluggable Authentication Module*) omawiane są w rozdziale 22., „Bezpieczeństwo”, na stronie 1113. Umożliwiają one centralne zarządzanie systemowymi funkcjami uwierzytelniania za pośrednictwem standardowych procedur bibliotecznych, dzięki czemu takie programy jak `login`, `sudo`, `passwd` i `su` nie muszą dostarczać własnego kodu uwierzytelniającego. Mechanizm PAM zmniejsza ryzyko związane z pisanem bezpiecznego oprogramowania, umożliwia administratorom określanie zasad bezpieczeństwa w ramach całego ośrodka i definiuje łatwy sposób dodawania do systemu nowych metod uwierzytelniania.

Dodawanie i usuwanie użytkowników nie wiąże się z modyfikowaniem konfiguracji PAM, ale narzędzia biorące w tym udział działają zgodnie z regułami i ograniczeniami PAM. Poza tym wiele parametrów konfiguracyjnych PAM przypomina te, które są używane przez `useradd` lub `usermod`. Jeśli zmienisz parametry w sposób przedstawiony w tym rozdziale, a `useradd` nie będzie na nie zwracał uwagi, sprawdź, czy konfiguracja PAM w systemie nie nadpisuje Twoich nowych wartości.

7.11. SCENTRALIZOWANE ZARZĄDZANIE KONTAMI

Pewne formy scentralizowanego zarządzania kontami są niezbędne w średnich i dużych organizacjach, niezależnie od tego, czy będą to przedsiębiorstwa, uczelnie, czy urzędy państwowe. W całej organizacji użytkownicy potrzebują wygody i bezpieczeństwa przy stosowaniu tej samej nazwy użytkownika, numeru UID i hasła. Administratorzy muszą dysponować scentralizowanym system umożliwiającym natychmiastowe rozpropagowanie zmian (takich jak unieważnienie konta) do każdego miejsca.

Takie scentralizowanie można osiągnąć na wiele sposobów, z których większość (włącznie z systemem Active Directory firmy Microsoft) wymaga zastosowania LDAP (ang. *Lightweight Directory Access Protocol*), przynajmniej w pewnym zakresie. Istnieje wiele dostępnych rozwiązań: od schematycznych instalacji LDAP opartych na oprogramowaniu open source, po wyrafinowane komercyjne systemy zarządzania tożsamością, które kosztują masę pieniędzy.

LDAP a Active Directory

LDAP to uniwersalne repozytorium bazodanowe, które może przechowywać nie tylko dane związane z zarządzaniem użytkownikami, ale i inne typy danych. Używa się w nim hierarchicznego modelu klient-serwer, który może obsługiwać wiele serwerów i jedno-

czesnych klientów. Jedną z wielkich zalet LDAP jako repozytorium dla danych logowania w ramach całego ośrodka jest to, że może ono wymusić unikatowe numery UID i GID we wszystkich systemach. Poza tym dobrze współpracuje z systemem Windows, choć w drugą stronę tylko w niewielkim stopniu.

☞ *Więcej informacji na temat LDAP i jego implementacji można znaleźć w podrozdziale rozpoczynającym się na stronie 899.*

Usługa Active Directory firmy Microsoft korzysta z protokołów LDAP oraz Kerberos i może zarządzać wieloma rodzajami danych włącznie z informacjami o użytkownikach. Jest nieco egotyczna i w interakcji z repozytoriami LDAP systemu Unix i Linux chce pełnić funkcję nadrzędną. Jeśli potrzebujesz pojedynczego systemu uwierzytelniania dla całego ośrodka, w którym oprócz systemów Unix i Linux są również komputery z systemem Windows, prawdopodobnie najprościej będzie przekazać kontrolę Active Directory, a uniksowe i linuksowe bazy danych LDAP wykorzystywać jako serwery drugorzędne.

Aby zaimplementować taką konfigurację, będziesz potrzebować Active Directory i Services for Unix firmy Microsoft lub komercyjnej platformy integracyjnej Active Directory, takiej jak Quest Authentication Services (dawniej Vintela Authorization Services). Virtual Directory firmy Sun może pomóc Ci w integracji różnych systemów autoryzujących (uwierzytelniających).

Każdy z naszych czterech przykładowych systemów ma wbudowaną obsługę LDAP, choć czasem tylko po stronie klienta (np. HP-UX). LDAP często występuje w parze z PAM w celu przeprowadzania uwierzytelnienia.

LDAP jest bazą danych, dlatego przechowywane tu informacje muszą przestrzegać ściśle określonego schematu. Schematy wyrażane są w postaci plików XML, z polami nazw pochodzących z odpowiednich dokumentów RFC; jeśli chodzi o zarządzanie użytkownikami, jest to głównie RFC 2307. Dokładniejsze informacje na ten temat znajdziesz w rozdziale 19., „Współdzielenie plików systemowych”.

Systemy pojedynczego logowania

Systemy pojedynczego logowania (SSO, ang. *single sign-on*) zachowują równowagę między wygodą użytkownika a względami bezpieczeństwa. Idea polega na tym, aby użytkownik mógł się uwierzytelnić po jednorazowym zalogowaniu (po znaku zachęty, na stronie WWW lub w oknie systemu Windows). Użytkownik uzyskuje wtedy potwierdzenie tożsamości (zazwyczaj niezauważalnie, więc nie jest tu wymagane aktywne zarządzanie), które może później wykorzystać do uzyskania dostępu do innych komputerów i aplikacji. Użytkownik musi zapamiętać tylko jeden login i hasło zamiast wielu.

Taki schemat dopuszcza stosowanie bardziej złożonych poświadczeń (ponieważ użytkownik nie musi o nich pamiętać ani nawet się nimi zajmować), co teoretycznie zwiększa poziom bezpieczeństwa. Jednak nieuprawnione przejęcie konta może spowodować większe szkody, ponieważ jeden login zapewni napastnikowi dostęp do wielu komputerów i aplikacji. Systemy SSO stanowią duże zagrożenie w sytuacji, gdy użytkownik

odejście od komputera, a wciąż będzie zalogowany. Poza tym serwery uwierzytelniające stają się krytycznym wąskim gardłem. Ich awaria może sparaliżować pracę całego przedsiębiorstwa.

Systemy SSO to stosunkowo prosta idea, jednak wdrożenie jej wiąże się z wieloma komplikacjami, ponieważ poszczególne aplikacje i komputery, z których użytkownik może chcieć korzystać, muszą rozumieć proces uwierzytelniania i znać poświadczenia SSO. W niektórych systemach SSO poświadczeniami użytkowników zarządza Kerberos; zostało to omówione dokładniej w rozdziale 22., „Bezpieczeństwo”, od strony 1133.

Istnieje kilka systemów SSO na licencji open source:

- JOSSO, serwer SSO na licencji open source napisany w języku Java,
- CAS (ang. *Central Authentication Service*), opracowany na uniwersytecie Yale (również w języku Java),
- Likewise Open, narzędzie integracyjne, które sprawia, że Active Directory dobrze współpracuje z systemami Linux i Unix.

Dostępnych jest również mnóstwo systemów komercyjnych. Większość z nich jest zintegrowana z pakietami zarządzania tożsamością, które zostaną omówione w następnym punkcie.

Systemy zarządzania tożsamością

„Zarządzanie tożsamością” to najnowsze modne hasło w dziedzinie zarządzania użytkownikami. Mówiąc po ludzku, oznacza to identyfikowanie użytkowników Twojego systemu, poświadczanie ich tożsamości i przyznawanie uprawnień na podstawie tych uwierzytelnionych tożsamości. Działania standaryzacyjne w tej dziedzinie prowadzone są przez World Wide Web Consortium i The Open Group.

Komercyjne systemy zarządzania tożsamością łączą kilka kluczowych pojęć systemu Unix w jeden miły dla oka graficzny interfejs użytkownika wypełniony marketingowym żargonem. Podstawą wszystkich tego rodzaju systemów jest baza danych zawierająca uwierzytelnienia użytkowników i dane autoryzacyjne, często zapisana w formacie LDAP. Kontrolę zapewniają takie pojęcia jak grupy systemu Unix, a ograniczone uprawnienia administracyjne wymuszane są za pośrednictwem narzędzi w rodzaju sudo. Większość tego rodzaju systemów została zaprojektowana zgodnie z wymogami prawnymi dotyczącymi odpowiedzialności, monitorowania i dzienników kontroli.

Istnieje wiele takich systemów komercyjnych: Identity Management firmy Oracle, Sun Identity Management Suite¹⁴, Courion, Avatier Identity Management Suite (AIMS) i BMC Identity Management Suite, by wymienić tylko kilka z nich. Dokonując oceny systemów zarządzania tożsamością, zwróć uwagę na następujące cechy:

¹⁴ Teraz, gdy firma Sun została przejęta przez Oracle, nie jest pewne, czy system ten będzie nadal oferowany jako osobny produkt.

- generowanie globalnie unikatowych identyfikatorów użytkownika,
- możliwość tworzenia, zmiany i usuwania kont użytkowników w całej organizacji, niezależnie od sprzętu i systemu operacyjnego,
- bezpieczny interfejs WWW do zarządzania z możliwością dostępu z zewnątrz,
- możliwość łatwego wyświetlania wszystkich użytkowników, którzy mają określony zestaw uprawnień,
- prosty sposób podglądu wszystkich uprawnień przydzielonych określonemu użytkownikowi,
- możliwość pozwolenia użytkownikowi na zmianę (i zresetowanie) własnych haseł, z wymuszeniem reguł wyboru silnych haseł,
- możliwość globalnej zmiany swoich haseł przez użytkowników za pomocą jednej operacji,
- mechanizm obiegu organizacji pracy, np. warstwowy system zatwierdzeń przed przyznaniem użytkownikowi określonych uprawnień,
- możliwość koordynacji z bazą danych działu kadr w celu automatycznego zablokowania dostępu pracownikom, którzy złożyli wypowiedzenie lub zostali zwolnieni,
- konfigurowalne rejestrowanie wszystkich zmian i działań administracyjnych,
- konfigurowalne raporty tworzone na podstawie zarejestrowanych danych (z podziałem na użytkowników, daty itd.),
- kontrola dostępu oparta na rolach, w tym obsługa kont użytkowników za pomocą ról,
- interfejs, za pomocą którego osoba odpowiedzialna za rekrutację może poprosić o skonfigurowanie kont zgodnie z określoną rolą,
- wyjątki w działaniach opartych na rolach, łącznie z obiegiem określającym proces zatwierdzania wyjątków.

Weź również pod uwagę sposób wdrożenia systemu w miejscach, gdzie odbywa się właściwa autoryzacja i uwierzytelnianie. Czy system wymaga zainstalowania wszędzie własnego agenta, czy dopasowuje się do podległych mu systemów?

7.12. ZALECANA LITERATURA

„The Complete Buyer’s Guide for Identity Management”, dokumentacja firmy Sun Microsystems, 2008 r., sun.systemnews.com/articles/129/4/sec/20930.

7.13. ĆWICZENIA

Ćwiczenie 7.1. W jaki sposób ustalana jest domyślna grupa użytkownika? Jak można ją zmienić?

Ćwiczenie 7.2. Wyjaśnij różnice między następującymi wartościami `umask`: 077, 027, 022 i 755. W jaki sposób ustawiłbyś jedną z tych wartości jako domyślną maskę dla nowych użytkowników w ramach całej organizacji? Czy możesz wymusić na swoich użytkownikach używanie standardowej wartości `umask`?

Ćwiczenie 7.3. Do czego służy plik przesłaniania haseł (*shadow*)?

★ Ćwiczenie 7.4. Określ system uwierzytelniania używany przez program `login` w Twoim systemie. Jeśli korzysta z PAM, ustal, jakie inne programy w systemie również z niego korzystają.

★ Ćwiczenie 7.5. Wymień czynności wymagane w celu dodania użytkownika do systemu bez użycia programu `useradd`. Jakie dodatkowe czynności są wymagane w Twoim lokalnym środowisku?

★ Ćwiczenie 7.6. Ustal konwencję nazewnictwa dla nowych użytkowników w Twojej organizacji. Jakie rządzą nią reguły? W jaki sposób zapewniana jest niepowtarzalność nazw? Czy możesz wskazać jakieś wady? Jak są usuwani użytkownicy?

★★ Ćwiczenie 7.7. Znajdź listę nazwisk (np. z lokalnego spisu telefonów dostępnego on-line) i wykorzystaj je jako dane wejściowe dla skryptu tworzącego nazwy użytkowników zgodnie z konwencją nazewnictwa przyjętą w Twojej organizacji. Ilu użytkowników udało Ci się dodać przed wystąpieniem kolizji? Ile kolizji było ogółem? Wykorzystaj te dane do oceny konwencji nazewnictwa w Twojej organizacji i zaproponuj usprawnienia.

★★ Ćwiczenie 7.8. Napisz skrypt pomocny w monitorowaniu poprawności pliku `/etc/passwd` (punkty b i e wymagają dostępu do konta użytkownika *root*, chyba że jesteś zdolny):

- a) znajdź wszystkie wpisy z identyfikatorem UID równym 0,
- b) znajdź wszystkie wpisy bez hasła (wymaga dostępu do pliku `/etc/shadow`),
- c) znajdź wszystkie zestawy wpisów o zduplikowanych identyfikatorach UID,
- d) znajdź wszystkie wpisy ze zduplikowanymi nazwami użytkownika,
- e) znajdź wszystkie wpisy bez daty wygaśnięcia (wymaga dostępu do pliku `/etc/shadow`).

★★★★★ Ćwiczenie 7.9. Napisz moduł PAM, który przeprowadza uwierzytelnianie za pomocą losowo generowanego kodu PIN, wysyłając go na telefon komórkowy użytkownika jako wiadomość SMS, a następnie prosi o wpisanie tego kodu w celu weryfikacji. Zainstaluj swój moduł i skonfiguruj go w stosie logowania PAM, aby uzyskać dwustopniowe uwierzytelnianie.

SKOROWIDZ

389 Directory Server, 900, 905

A

AA, 919, 922

Abell Vic, 223

access agent, *Patrz* AA

access control entry,

Patrz kontrola dostępu wpis

Access Control List,

Patrz kontrola dostępu lista

access points, *Patrz* WAP

ACE, 240, *Patrz* kontrola dostępu wpis

ACL, *Patrz* kontrola dostępu lista

Acrobat Reader, 1298

Active Directory, 258, 290, 291, 615, 826, 890,
900, 903, 905, 906, 907, 1133, 1386, 1389,
1399, 1400, 1401, 1402, 1403, 1404, 1405,
1406

Adaptive Security Appliance, 605

Address Resolution Protocol, *Patrz* ARP

Adobe, 1296

Adobe Systems, 1297

adres

część hosta, 584

część sieciowa, 584

Ethernet, 582

grupowy, 584

IP, 582, 583, 584, 587, 589, 599, 603, 608,
613, 617, 619, 627, 638, 694, 696, 700,
703, 709, 721, 729, 747, 750, 754, 755,
762, 764, 774, 779, 782, 785, 791, 801,
839, 844, 926, 1067

Ipv4, 585

Ipv6, 585, 592, 593

jednostkowy, 584

MAC, 581

rozgłoszeniowy, 584, 587, 588, 603, 610,
611, 624, 625, 627, 632, 639, 642, 672

sprzętowy, 581, 582

swobodny, 584

Token Ring, 582

adresowanie, 581

bloków logicznych, 305

ADSM, *Patrz* TSM

ADSP, 944, 950, 951, 1043, 1044

Advanced Package Tool, *Patrz* APT

Advanced Technology Attachment, *Patrz* ATA

AirPort Express, 682

AIT, 407

AIX, 64, 66, 67, 77, 153, 155, 164, 180, 188,
202, 205, 206, 207, 208, 209, 211, 212, 221,
244, 262, 271, 282, 289, 298, 318, 335, 349,
353, 355, 377, 380, 414, 469, 496, 539, 542,
556, 640, 664, 847, 867, 875, 995, 1064,
1075, 1130, 1186, 1220, 1232, 1241,
1257, 1280, 1359, 1370, 1509, 1510
obsługa błędów, 468

algorytm
Blowfish, *Patrz* hasło algorytm Blowfish
dynamiczny, 196
kontrola przeciążenia, 616
MD5, 183, 486
NSEC3RSASHA1, 816
RSA-SHA-1, 813
wymiany kluczy Diffiego-Hellmana, 804

aliasy, 928, 935, 936, 937, 938, 939, 940, 966,
968, 969, 971, 972, 984, 985, 987, 991,
1015, 1016, 1024, 1025, 1026, 1027, 1028,
1029, 1030, 1031, 1032, 1186

Alpine, 920

Amanda, 427, 445

amavisd, 919, 925, 926, 933, 934, 944, 952, 953,
954, 955, 977, 982, 1019, 1038, 1039, 1042,
1043, 1045, 1046, 1047

Amazon Web Services, 1194, 1225, 1226, 1341

AME, 407

analizator okablowania, 685

Anderson Paul, 530

Anvin H. Peter, 479

AP, *Patrz* WAP

Apache, *Patrz* serwer Apache

Apple, 682, 1294, 1380

APT, 502, 505

Arch, 518

architektura, 504, 688
x86, *Patrz* x86

archiwum
CPAN, 128, 253
tar, 78, 81

ARP, 577, 583

ARPANET, 574

Artifex, 1299

ASHRAE, 1320

Assmann Claus, 990

ATA, 304, 305, 319, 323

ATA Packet Interface, *Patrz* ATAPI

atak
blokady usług, 989, 1372
odmowy usług, 603, 800
smerfów, 603
zatrucia DNS, 790

ATAPI, 305

Atkins Stephen, 1370

Atkins Todd, 473

atrybut wykonywalności, 96

AUTH_SYS, 860

Automated Installer, 487

automatyczne ożywianie, 122

automatyczne tworzenie anonimowych
referencji, 122

autouzgadnianie, 612, 631, 679

autovivification, *Patrz* automatyczne ożywianie

AutoYaST, *Patrz* YaST2

AXFR, 785, 794, 795

B

Bacula, 426, 427, 431, 438, 441, 442
konfigurowanie, 429, 430, 433, 434, 435,
438
raporty, 444

barewords, *Patrz* gołe słowa

Basic Input/Output System, *Patrz* BIOS

Bazaar-NG, 518

BCP, 576

Berkeley Software Distribution, *Patrz* BSD

bezklasowe trasowanie międzydomenowe,
588

bezpieczeństwo, 602, 625, 632, 639, 683,
695, 708, 715, 729, 747, 748, 755, 772,
784, 796, 798-803, 810, 812, 813, 834,
855, 859, 860, 861, 865, 867, 868, 870,
874, 876, 891, 892, 893, 896, 908, 909,
912, 913, 918, 923, 975, 983, 1024, 1035,
1072, 1099, 1100, 1110, 1118, 1120, 1123,
1130, 1144, 1154, 1174, 1190, 1225, 1238,
1295, 1379, 1387, 1436, 1481

bezpieczne wymazywanie, 320, 321

beziprzewodowy punkt dostępu, *Patrz* WAP

BGP, 653, 658, 659, 662

biała lista, *Patrz* lista biała

biblioteka
 aktywna, 533
 elementów kontrolnych, 1233, 1251, 1252
 ldns, 777
 modułów, 116
 PCRE, 109
 rozszerzeń językowych, 116
 taśm, 408
 uwierzytelniania, 181
 współdzielona, 533
 BIND, 194, 694, 695, 698, 699, 700, 702, 706,
 708, 713, 714, 715, 717, 718, 719, 722,
 726, 729, 733, 745-749, 752, 753, 755,
 760, 762-772, 775, 776, 777, 778, 779,
 782, 787, 792-805, 812-834, 837, 838,
 840-848, 1120, 1384
 BIOS, 147, 315
 bit
 lepkości, 234, 235
 setgid, 233, 234, 235
 setuid, 233, 235
 trybu tradycyjnego, 246
 uprawnień, 234, 253
 wykonywalności, 235, 237
 BlackBerry, 1051
 Bluetooth, 1293
 błąd, 1006
 BIND, 827
 DNSSEC, 824
 informacja administracyjna, 912
 konfiguracji, 685, 1104
 NSD, 827
 protokołu, 685
 przepełnienie bufora, 1103
 SMTP, 929
 unbound, 827
 walidacji danych wejściowych, 1103
 zaokrąglenia, 1250
 boot loader, *Patrz* program rozruchowy
 BOOTP, 493, 496, 497, 599
 brama, 649, 650, 651, 652, 653, 655, 659, 660,
 1066, 1067, 1068, 1073, 1141, 1143
 Bro, 1110, 1125, 1126, 1144
 Brocade, 1352
 Bryant Bill, 1133

BSD, 62, 1256, 1257, 1258, 1273, 1279, 1280,
 1282, 1283, 1285, 1286, 1288, 1294, 1295,
 1302, 1307, 1512
 buforowanie, 698
 negatywne, 699
 Burgess Mark, 529

C

Cacti, 1088, 1089, 1090
 Carrier Sense, *Patrz* wykrywanie stanu
 kanału, CSMA/CD
 CDN, 1195
 centrum danych, 1317, 1321, 1324, 1325,
 1326, 1328, 1335
 chłodzenie, 1320, 1322, 1342, 1344
 koszty, 1332, 1335
 monitoring, 1324
 niezawodność, 1318, 1324, 1325, 1327,
 1342
 wilgotność, 1324
 zasilanie, 1324, 1325, 1327, 1332
 centrum przetwarzania danych,
 Patrz centrum danych
 certyfikacja, 1155, 1188
 Chacon Scott, 518
 CHAP, 376
 Chatsworth Products, 1328
 Check Point, 605
 Christiansen Tom, 138
 chroot, 784, 787, 789, 801, 987, 988, 989,
 1024, 1028, 1119, 1120, 1140
 ciasteczka, 1237, 1238, 1239, 1240
 CIDR, 588, 591, 592, 614
 CIFS, 218, 370, 373, 1385, 1386, 1387, 1390,
 1392, 1393, *Patrz* system plików
 CIM, 531
 Cisco, 531, 605, 662, 683, 1093, 1352
 ClamAV, 1108
 Classless Inter-Domain Routing, *Patrz* CIDR
 CodeWeavers, 1382
 Collision Detection, *Patrz* wykrywanie
 kolizji, CSMA/CD
 Common Criteria for Information Technology
 Security Evaluation, 1158
 Common Information Model, *Patrz* CIM

Common UNIX Printing System, *Patrz* CUPS
 Communicate Pro, 1051
 Comprehensive Perl Archive Network, *Patrz*
 archiwum CPAN
 content distribution network, *Patrz* CDN
 cookie, *Patrz* ciasteczka
 Cooper Mendel, 109
 CRC, *Patrz* suma kontrolna
 CSMA/CD, 672
 CUPS, 1255-1268, 1270, 1274, 1279, 1293,
 1294, 1296, 1300-1307, 1309, 1311-1313
 Cyber-Ark, 190
 cyfrowa linia abonencka, *Patrz* DSL
 Cygwin, 1232, 1378, 1380, 1384
 czarna lista, *Patrz* lista czarna
 czas
 bezwzględny, 816
 rzeczywisty, 197
 systemowy, 213
 względny, 816
 ważności, *Patrz* TTL

D

DA, 919, 922, 927
 dane
 archiwizacja, 426, 1442
 centrum, *Patrz* centrum danych
 hasz, 116, 119, 133, 908, 1388
 jednostka bazowa, 579
 odtworzenie, 401
 przechowywanie, 409
 sekwencyjne przesyłanie, 299
 skalarne, 116
 zarządzanie, 1442
 Darik's Boot and Nuke, 321
 DCC, 946
 DCE, 1411, 1412
 DDS, 406
 deduplikacja, 411
 definicja poziomu usług, *Patrz* SLA
 delegowanie, 697, 839, 841
 delivery agent, *Patrz* DA
 demilitarized zone, *Patrz* DMZ
 demon, 178, 197, 203, 427
 amavisd, *Patrz* amavisd
 automount, 879, 880, 882, 883, 884

cron, 79, 88, 384, 509, 524
 crond, 389
 cupsd, 1260, 1263, 1264, 1312
 devfsadm, 542
 DHCP, 796
 dhcpcd, 600
 dhcrelay, 601
 gated, 661, 663, 664
 init, 154
 klogd, 466
 kontroli bezpieczeństwa, 1037
 lpd, 1257, 1281, 1282, 1286, 1289, 1290,
 1313
 lpsched, 1257, 1272, 1273, 1274, 1278
 magazynowania, 427, 436
 mountd, 885
 named, 793, 804, 835
 ndpd-router, 664
 nfsd, 871, 872
 nmbd, 1386
 nsd, 913, 914
 nwmad, 627
 odwzorowujący tożsamości, 861
 pkg.depotd, 512
 plików, 438
 ramd, 663
 RIP, 656
 ripngd, 663
 routed, 660, 664
 serwera ISC, *Patrz* demon dhcpcd
 slurpd, 903
 smbd, 1386
 sshd, 1135
 stunnel, 1139
 svnserve, 518
 swagentd, 513
 synchronizacji czasu, 205
 syslog, 186
 syslogd, 452, 458, 459, 461
 systemowy, 145, 146
 śledzenie, 213
 trasujący, 652, 660
 udevd, 230, 542, 564
 vantaged, 824
 wydruku, *Patrz* program obsługi kolejki
 wydruku

- ypbind, 911
- zebra, 662
- Deraison Renaud, 1122
- Deutsch L. Peter, 1296
- DHCP, 479, 480, 483, 485, 487, 493, 496, 497, 598, 599, 602, 607, 611, 615, 629, 638, 700, 703, 711, 727, 764, 774, 794, 795, 796
- Digital Subscriber Line, *Patrz* DSL
- Dihu Habeeb, 946
- directory service, *Patrz* usługa katalogowa
- Distributed Checksum Clearinghouses, *Patrz* DCC
- Distributed Management Task Force, *Patrz* DMTF
- DKIM, 919, 921, 933, 942, 944, 950, 951, 981, 998, 1008, 1009, 1042, 1043, 1044, 1045, 1046, 1047, 1048, 1050
- DLP, 933
- DLT, 406
- DLV, 791, 807, 810, 816, 818, 819, 820, 821
- DMA, 305, 322
- DMTF, 531, 1083
- DMZ, 1143, 1144, 1192
- DNS, 583, 608, 614, 693-700, 703, 705-749, 752, 755-764, 766, 768, 769, 770, 772-778, 786, 789-810, 814, 818, 819, 822, 823, 824, 826, 830, 833, 835, 838-850, 901, 912, 931, 932, 944, 947, 948, 949, 950, 966, 971, 973, 974, 977, 979, 983, 991, 993, 1021, 1027, 1036, 1042, 1043, 1046, 1048, 1060, 1062, 1063, 1065, 1066, 1067, 1068, 1072, 1078, 1080, 1081, 1337, 1400
- DNSKEY, 806, 807, 808, 810, 811, 814, 815, 816, 818, 820, 822, 824
- DNS-OARC, 809
- DNSSEC, 777, 779, 781, 786, 790, 791, 798, 801, 805, 806, 807, 808, 809, 810, 812, 813, 814, 817, 818, 819, 820, 821, 822, 823, 824, 825, 830, 834, 835, 838, 839, 841, 842
- Doering Gert, 1420
- dokumentacja, 73, 1438, 1455-1462
 - BCP, *Patrz* BCP
 - FYI, *Patrz* FYI
 - RFC, *Patrz* RFC
- SLA, *Patrz* SLA
- STD, *Patrz* STD
- uzupełniająca, 74
- w internecie, 76
- Domain Name System, *Patrz* DNS
- DomainKeys, *Patrz* DKIM
- domena, *Patrz* DNS
 - rozgłoszeniowa, 672
 - wirtualna, 1030
 - wirtualnej skrzynki pocztowej, 1031
- donuts, 823
- dopasowanie, 110, 113, 885
- Dovecot, 924
- dowiązanie
 - symboliczne, 227, 228, 231
 - twarde, 228, 229, 235
- drukarka, 1257, 1261, 1264, 1274, 1277, 1280, 1288, 1293, 1294, 1304
- akcesoria, 1306
- GDI, 1305
- klasa, 1266, 1272
- sieciowa, 1264, 1265, 1295, 1307, 1311, 1313
- współdzielenie, 1394
- drukowanie, 1256, 1263, 1271, 1272, 1293, 1295, 1299, 1302
- dwustronne, *Patrz* duplex
- podgląd wydruku, 1308
- strona nagłówekowa, 1307
- drzewo plików, 221
- DSL, 606, 670, 684, 685
- DTE, 1411, 1412
- Dynamic Host Configuration Protocol, *Patrz* DHCP
- dysk
 - ATA, *Patrz* ATA
 - dodawanie, 296
 - formatowanie, 318, 319
 - nazwa, 316, 317, 318
 - PATA, *Patrz* PATA
 - SATA, *Patrz* SATA
 - SCSI, *Patrz* SCSI
 - SSD, 295, 299, 300, 302
 - klaster, 303
 - test wydajności, 323

dysk

twardy, 295, 300, 302, 405, 408

awarie, 301, 335

błędy, 323, 324

wydajność, 1366, 1368, 1369

wirtualny, 375

dystrybucja, 63

CentOS, 66

Debian, 61

Red Hat, 62, 65, 77, 148, 158, 159, 191,

280, 324, 389, 413, 478, 480, 486, 588,

599, 617, 619, 622, 662, 843, 846,

1131, 1184, 1208, 1419

SUSE, 62, 65, 77, 148, 160, 264, 280, 324,

478, 483, 503, 511, 599, 616, 617, 618,

619, 622, 845, 975, 1132, 1184, 1418

sygnałów, 197

Ubuntu, 63, 65, 148, 161, 278, 287, 324,

359, 478, 486, 588, 599, 617, 622, 843,

844, 1132, 1184, 1208, 1418, 1420,

1421, 1425, 1426

dziennik, 474, 567, 780, 783, 784, 787, 788,

796, 804, 810, 815, 825, 829, 830, 833,

839, 841, 997, 1020, 1040, 1249, 1312,

1510

alarmów, 1020

błędów, 1181

dostępu, 1181

odrzuć, 1020

E

ECN, 616

edytor, 518

ed, 95

emacs, 59, 89

gedit, 59

nano, 60

tekstu, 59

vi, 59

EGID, 196

EIGRP, 652, 653, 657, 659, 660

ekologia IT, 1332, 1333, 1335, 1344, 1345,

1347

e-mailowa książka adresowa, 899

EMC, 447

Enhanced Interior Gateway Routing

Protocol, *Patrz* EIGRP

enkapsulacja, 579

eSATA, 307, 405, *Patrz też* SATA

ESMTP, 922, 927, 928, 929, 930, 988, 1022

Ethernet, 163, 374, 375, 579, 580, 583, 612,

670, 671, 672, 673, 676, 677, 678, 679, 680,

681, 684, 685, 1061, 1064, 1071, 1077,

1237, 1293, 1338, 1339, 1411, 1429

przepustowość, 670

topologia, 672

etykieta, 105

EUID, 195

Evince, 1296, 1298, 1308

Exabyte, 407

Exim, 919, 922, 930, 948, 956, 957, 998, 999,

1000, 1001, 1002, 1003, 1004, 1005, 1006,

1007, 1008, 1010, 1011, 1012, 1013, 1015,

1016, 1017, 1018, 1019, 1020, 1021, 1022,

1042, 1047, 1048

diagnostyka, 1021

Explicit Congestion Notification, *Patrz* ECNext2-4, *Patrz* system plików

eXtensible Open Router Platform,

Patrz XORP**F**

FastCGI, 1173

FAT, 219

fault management resource identifier,

Patrz FMRI

FC-AL, 305

Fedora, 65, 258, 900

Ferraiol David, 179

FHS, 528

Fibre Channel, 304, 305, 374, 375

Patrz też FC-AL

Field Julian, 951

Filesystem Hierarchy Standard, *Patrz* FHS,*Patrz* system plików hierarchia

filtr, 92

antyspamowy, 925, 932, 933, 942, 944, 945,

946, 948, 949, 977, 998, 1019, 1036

antywirusowy, 932, 933, 942, 945, 949,

977, 998, 1010, 1019, 1038, 1108

pakietów, 1109

filtrowanie, 604, 633, 639, 679, 1016, 1141,
1142, 1145, 1261, 1281
FireWire, 305
firmware, *Patrz* oprogramowanie sprzętowe
FlowScan, 1094
FMRI, 165, 166
format papieru, 1302
Foster Dan, 1509, 1510
FQDN, 709, 710
fragmentacja, 581
Frame Relay, 684
frazja kodująca, *Patrz* hasło fraza
Frazao Jorge, 841
FreeBSD, 62, 426
FSUID, 196
FTP, 479, 1106, 1110, 1142, 1143, 1144
funkcja, 102
 exec, 197
 fork, 197
 join, 118
 kill, 174
 print, 118
 printf, 118
 settimeofday, 174
 skryptowa, 97
 time, 213
 wait, 198
 write, 213
 zestaw, 530
FUSD, 539
FUSE, 539
FYI, 576

G

GECOS, 266
Gelato, 539
Ghostscript, 1296, 1297, 1299, 1305
Ghostview, 1296, 1298, 1306, 1308
gibi-, 69
GID, 175, 176, 177, 196, 244, 259, 265, 861,
863
Gimp, 1384
Git, 518, 520
global server load balancing, *Patrz* GSLB

główny rekord rozruchowy, *Patrz* MBR
Gmail, *Patrz* Google Gmail
gniazdo
 lokalne, 227
 RJ-45, *Patrz* RJ-45
gniazdo lokalne, 230
GNOME, 547, 1233, 1234, 1251, 1252
Google, 76, 79, 109, 669
Google Gmail, 918, 920, 925, 926, 1043, 1383
Goyvaerts Jan, 115
GRand Unified Bootloader, *Patrz* GRUB
greediness, *Patrz* zachłanność
GRUB, 148, 149, 151, *Patrz też* program
 rozruchowy
GSLB, 698
GUID, *Patrz* partycja tablica GPT

H

Hamilton Bruce, 76
hash, *Patrz* dane hasz
hasło, 183, 190, 191, 263, 268, 274, 481, 898,
1109, 1111, 1113, 1115, 1117, 1118, 1123,
1124, 1135, 1141, 1388, 1389, 1392, 1395,
1402
algorytm Blowfish, 183
algorytm MD5, 183
DES, 183
długość, 263
frazja, 184, 190
MD5, 486
menadżera rozruchu, 1104
odzew, 190
skrytka, 190
hasz, *Patrz* dane hasz
Hazel Philip, 109, 998
help desk, 1450, 1451
Hewlett-Packard, 66, 408, , 480, 493, 1297
HFS, *Patrz* system plików HFS
HIDS, 1126
High-performance File System, *Patrz* system
 plików HFS
host, 584, 585, 586, 588, 593, 595, 602, 610
host-based intrusion detection system,
 Patrz HIDS

hosting

kolokacyjny, 1194

w chmurze, 1194

Hotmail, *Patrz* MSN Hotmail

HP, *Patrz* Hewlett-Packard

HP-UX, 64, 66, 77, 152, 162, 179, 202, 208,
212, 221, 234, 243, 244, 270, 282, 289,
298, 317, 330, 335, 347, 352, 379, 457,
493, 513, 539, 542, 555, 631, 634, 635,
662, 704, 847, 864, 866, 876, 884, 897,
994, 1064, 1075, 1130, 1185, 1270, 1274,
1278, 1358

HP-UX Porting and Archiving Centre, 78

HTTP, 479, 483, 487, 1061, 1172, 1258

hub, *Patrz* koncentrator

I

IANA, 578

IBM, 67, 218, 408, 446, 480, 516, 556, 1509,
1510, 1511, 1512

ICANN, 574, 578, 589

ICMP, 577, 581, 633, 1062, 1063, 1064, 1066,
1067, 1068, 1069, 1073, 1074, 1076, 1085

IDE, 304, 305, 321

identyfikacja biometryczna, 181

IEC, 69

IEEE1394, *Patrz* FireWire

IGF, 575

IGMP, 584

Ignite-UX, 493

IGRP, 657

IMAP, 919, 920, 923, 931, 966, 978, 1012,
1017, 1024, 1139

IMAPS, 923, 1072

instalacja, 478, 483, 492, 999, 1177, 1178,
1191, 1211, 1215, 1223, 1383, 1387, 1396
nienadzorowana, 481
sieciowa, 479
zautomatyzowana, 483

instalacja oprogramowania, 77

instancja drukarek, 1260

instrukcja

case, 105

exec, 106

for-in, 105, 106, 135

if-then, 103

if-then-else, 103

open, 123

print, 131

read, 107

server, 779

special, 895

split, 120

while, 106, 107, 120, 135

zone, 779

Integrated Drive Electronics, *Patrz* IDE

Integrity Virtual Machines, *Patrz* IVM

Intel, 479

interfejs, 304

API, 794

ATA, *Patrz* ATA

drukarki, 1278, 1279

Fibre Channel, *Patrz* Fibre Channel

graficzny, 607, 615, 618, 619, 620, 1051,
1236, 1247, 1380

IDE, *Patrz* IDE

PATA, *Patrz* PATA

SATA, *Patrz* SATA

SCSI, *Patrz* SCSI

sieciowy, 1069, 1075, 1077, 1078

szeregowy, 304, 1410, 1430, 1431

użytkownika, 1233

wirtualny, 1182, 1185, 1186

International Electrotechnical Commission,
Patrz IEC

International Organization for
Standardization, *Patrz* ISO

internet, 574

Internet Assigned Numbers Authority,
Patrz IANA

Internet Control Message Protocol,
Patrz ICMP

Internet Corporation for Assigned Names
and Numbers, *Patrz* ICANN

Internet Governance Forum, *Patrz* IGF

Internet Group Management Protocol,
Patrz IGMP

Internet Message Access Protocol,
Patrz IMAP

Internet Protocol, *Patrz* IP
 Internet Protocol security, *Patrz* IPsec
 internet service providers, *Patrz* ISP
 Internet Society, *Patrz* ISOC
 Internet Systems Consortium, *Patrz* ISC
 interpreter, 97
 IOS, 662, 664
 IP, 305, 375, 482, 577
 IPFilter, 632, 639, 1141, 1150, 1151, 1152, 1153
 iPhone, 1051
 IPP, 1294
 IPS, 512
 IPsec, 605, 1154
 IPv4, 578, 649, 656, 779, 782, 787, 1009, 1154
 IPv6, 578, 581, 583, 584, 589, 592, 599, 614, 649, 653, 655, 656, 657, 658, 662, 663, 664, 779, 782, 787, 838, 1009, 1154
 IRDP, 658
 ISC, 599, 807
 iSCSI, 370, 375, 376
 cel, 377, 378, 379
 inicjator, 377, 378, 379, 380
 ISDN, 684
 IS-IS, 654, 657, 662
 iSNS, 375
 ISO, 674
 ISO 17799, 1157
 ISO/IEC 27002, 1157
 ISOC, 574, 1170
 ISP, 574
 IVM, 1222
 IXFR, 794, 795

J

Jacobson Van, 1066, 1078
 JailKit, 1120
 jądro, 89, 96, 142, 143, 149, 174, 177, 193, 197, 466, 537, 543, 1247
 dane, 194
 dostrajanie, 558, 994
 inicjalizacja, 143
 kompilacja, 539, 545
 komunikat wyjściowy, 315
 konfigurowanie, 544, 548, 551, 552, 555, 556, 558, 559, 560, 561

 moduły ładowalne, 559, 560, 561
 monolityczne, 538, 555
 statystyki, 210
 wątek, 207
 jednoczesny dostęp, 672
 jednostki, 69
 język
 definicji strony, 1300
 expect, 60
 opisu dokumentu, 1298
 opisu strony, 1296, 1297, 1299
 Perl, 60, 88, 96, 109, 481, 1384
 programowanie, 115
 typy danych, 116
 Python, 60, 79, 88, 96, 129, 1384
 Ruby, 60, 129
 JFS, *Patrz* system plików
 Jodies Krischan, 588
 John the Ripper, 1110, 1123, 1124, 1136
 JumpStart, 487, 489, 492
 Justman Ian, 946

K

kabel
 koncentryczny, 673
 miedziany dwuosiowy, 305
 UTP, *Patrz* UTP
 kanał
 komunikacyjny, 89
 plikowy, 828
 syslog, 828
 karta graficzna, 1242, 1243, 1244, 1245, 1248, 1250
 katalog, 224, 227, 228
 domowy, 259, 267, 275, 325, 367, 398, 518, 1389, 1399
 kolejki, 1276, 1281, 1288
 KDE, 547, 1232, 1233, 1234, 1251, 1252, 1258, 1263, 1264, 1267, 1268, 1269, 1296, 1312
 KDEPrint, 1267, 1268, 1269, 1270
 KeePass, 190
 Kerberos, 181, 291, 826, 860, 891, 1133, 1155, 1337, 1389, 1400, 1401, 1402, 1403
 Kerio MailServer, 1051
 kernel mode setting, *Patrz* KMS
 Kernel-based Virtual Machine, *Patrz* KVM

- kibi-, 69
- Kickstart, 480, 483, 484
- klasa
 - czasu rzeczywistego, 197
 - drukarek, *Patrz* drukarka klasa
 - planowania, 197
- klasteryzacja, 352
- kławiatura, 1244, 1248
- klient
- konfigurowanie, 703
 - poczty, 920, 921, 922, 924, 925, 927, 968, 1008, 1035
- klon, 369
- klucz, 93, 779, 780, 781, 785, 792, 797, 802-824, 837, 909, 1027, 1042, 1049, 1112, 1132, 1134, 1135
- KMS, 1240, 1247
- Knowles Brad, 841
- kod
 - rozruchowy, 142
 - zakończenia, 198
- Kojm Tomasz, 1108
- kolejka
 - poczty, 961, 991, 992, 993, 996, 1040
 - wiadomości oczekujących, 1023
 - wydruków, 1256, 1259, 1261, 1266, 1272, 1277, 1282, 1283
- kolejkowanie poleceń, *Patrz* NCQ
- kolizja, 672
- kolokacja, *Patrz* hosting kolokacyjny
- kolumna ogranicznik, 92
- komentarz, 703
- kompilowanie, 527, 539
- komponent, 503, 504, 530
 - universe, 508
- komunikat
 - ICMP, 594, 658
 - kategoria, 829
- koncentrator, 677, 683
- konfiguracja wielosystemowa,
 - Patrz* wielosystemowość
- konfigurowanie, 478, 524, 525, 528, 529, 530, 614, 615, 617, 619, 626, 629, 634, 640, 703, 777, 1025, 1129, 1180, 1183, 1191, 1240, 1263, 1264, 1265, 1280, 1396, 1401, 1421
- Konqueror, 1269, 1270
- konsolidacja
 - aplikacji, 1335
 - serwerów, 1337
- kontrola dostępu, 173, 177, 180, 232, 240, 388, 1032, 1033, 1041, 1124, 1130
- lista, 182, 232, 240, 241, 242, 243, 244, 245, 247, 248, 249, 253, 370, 798, 800, 801, 948, 998, 999, 1003, 1006, 1007, 1008, 1010, 1011, 1012, 1019, 1021, 1048, 1390
- PAM, *Patrz* PAM
- przepływu, 1416
- role, 179, 182, 186, 189, 277
- wady, 178
- wpis, 240, 251
- kontrola przeciążenia, 616
- koń trojański, 1108
- kopia
 - internetowa, 409
 - lustrzana, 508
 - macierzy RAID, 399
 - migawkowa, 313, 367, 368, 399, 400, 424
 - odwzorowań, 909
 - przyrostowa, 411
 - referencyjna danych domeny, 696
 - zapasowa, 395, 404, 412, 413, 516, 529, 1107, 1442
 - szyfrowanie, 399
- kotwica, 806
- kpdf, 1298
- krotki, 132
- kryptografia, 181, 944, 983, 990, 1034, 1042, 1048, 1051, 1110, 1132, 1134, 1160
- książka telefoniczna, 899, 908
- Kuhn Rick, 179
- KVM, 1208, 1209, 1214, 1215, 1216

L

- LAN, 673, 674, 682, 685, 688, 857
- LBA, 305
- LCFG, 530
- LDAP, 265, 290, 583, 608, 826, 890, 891, 899-908, 912, 932, 933, 935, 966, 968, 970-973, 976, 1000, 1013, 1022, 1389, 1400, 1404, 1512

LDAP Data Interchange Format, *Patrz* LDIF
 LDIF, 901
 ldns, 777, 781, 786, 805, 813, 814, 815, 816,
 817, 818, 822, 823
 LeftHand Networks, 879
 Leres Craig, 841
 Lightweight Directory Access Protocol,
 Patrz LDAP
 Lightweight Wireless Access Point Protocol,
 Patrz LWAPP
 limit zużycia zasobów, 176
 Linux, 173, 176, 178, 182, 191, 196, 197, 202,
 206, 207, 208, 211, 212, 215, 222, 223,
 230, 237, 238, 239, 243, 267, 270, 285,
 296, 311, 316, 321, 329, 334, 337, 342,
 353, 387, 413, 426, 456, 461, 479, 499,
 539, 542, 544, 560, 596, 599, 613, 616,
 663, 682, 843, 867, 880, 897, 994, 1072,
 1076, 1112, 1117, 1130, 1145, 1183, 1208,
 1210, 1225, 1247, 1263, 1356, 1363, 1370,
 1382, 1392, 1420, 1425
 Linux Documentation Project, 75
 lista, 117, 132, 1005, *Patrz też* tablica
 ACL, *Patrz* kontrola dostępu lista
 biała, 947, 948, 1009
 czarna, 947, 979, 1009, 1036
 kontrola dostępu, *Patrz* kontrola dostępu
 lista
 kontrolna, 479
 pocztowa, 933, 935, 940, 941, 946, 1051
 szara, 946
 live, 478, 486
 Local Area Network, *Patrz* LAN
 logical unit number, *Patrz* numer urządzenia
 logicznego
 logical volume manager, *Patrz* LVM
 lokalizowanie, *Patrz* konfigurowanie
 LTO, 408
 LUN, *Patrz* numer urządzenia logicznego
 LVM, 313, 314, 334, 341, 342
 LWAPP, 683

Ł

łańcuch, 117

M

MAC, 1130, 1132
 macierz RAID, *Patrz* RAID
 Mackerras Paul, 896
 magistrala systemowa, 144
 mail submission agent, *Patrz* MSA
 mail transport agent, *Patrz* MTA
 Maildir, 923, 1017, 1029, 1031
 Maildrop, 922
 MailScanner, 951
 makro, 958, 963, 965, 966, 967, 968, 969, 971,
 972, 973, 974, 978, 981, 995, 1004, 1006
 maksymalna jednostka transmisji, *Patrz* MTU
 maksymalny dopuszczalny rozmiar
 datagramu, *Patrz* MTU
 Mandatory Access Control, *Patrz* MAC
 maska sieci, 246, 250, 586, 587, 589, 598, 613,
 617, 618, 619, 638, 649
 master boot record, *Patrz* MBR
 matryca przełączająca, 678
 maximum transfer unit, *Patrz* MTU
 mbox, 923, 1017, 1029
 MBR, 327, 328, 330
 mebi-, 69
 menadżer
 logowania, 1232, 1234, 1237, 1248
 woluminów logicznych, *Patrz* LVM,
 wolumin logiczny
 Mercurial, 518
 message store, *Patrz* skrzynka pocztowa
 metadane, 347
 metaznak, 112
 Metcalfe Robert, 670
 miara kosztu, 654
 MIB, 1084, 1086
 Microsoft Outlook, 920, 1385
 Międzynarodowa Komisja Elektrotechniczna,
 Patrz IEC
 Międzynarodowa Organizacja Normalizacyjna,
 Patrz ISO
 migawka, *Patrz* kopia migawkowa
 migracja w locie, 1205, 1206, 1212, 1216
 mikrojądro, 538
 Miller Todd, 186
 militer, 948, 949, 951, 952, 977, 981, 982,
 1038, 1042, 1043, 1044, 1045, 1047, 1050

MIME, 920, 944, 976, 1011, 1261, 1262
 MKS Toolkit, 1384
 model wspólnych informacji, *Patrz* CIM
 Mondo Rescue, 445
 monitor, 1243, 1245, 1248, 1250, 1345
 Moore'a prawo, *Patrz* prawo Moore'a
 Mozilla Thunderbird, 1134
 MPLS, 579, 684
 MRTG, 1089
 MSA, 919, 921, 922, 932, 933, 960, 961, 962, 975
 MSN Hotmail, 918, 920
 MTA, 919, 921, 922, 927, 932, 933, 935, 941, 943, 946-962, 973, 974, 977, 1043, 1045
 MTU, 581, 807, 808, 809, 824
 Multiple Access, *Patrz* jednoczesny dostęp, CSMA/CD
 Multipurpose Internet Mail Extensions, *Patrz* MIME
 MySQL, 428, 429
 mysz, 1244, 1245, 1248

N

Nagios, 1088, 1090, 1091
 nagłówki, 579
 wiadomości, wiadomość e-mail nagłówek
 narzędzia wiersza poleceń, 59, 497, 588
 NAT, 591, 625, 633, 639
 National Security Agency, *Patrz* NSA
 Native Command Queuing, *Patrz* NCQ
 Nautilus, 228
 Nawias klamrowy, *Patrz* symbol []
 nazwa
 ścieżki dostępu, *Patrz* plik nazwa
 użytkownika, *Patrz* użytkownik nazwa
 NCQ, 306
 ND, 658, 664
 Neighbor Discovery, *Patrz* ND
 Nessus, 1122, 1123, 1144
 Netalyzer, 1081
 NetBackup, *Patrz* Veritas NetBackup
 NetBIOS, 1385
 NetBSD, 62
 Netfilter, 1145, 1149
 NetFlow, 1093, 1094, 1095, 1096
 Netscape, 900, 905, 1000

NET-SNMP, *Patrz* SNMP
 Network Address Translation, *Patrz* NAT
 Network Appliance, 878
 Network Auto-Magic, *Patrz* tryb NWAM
 Network Information Service, *Patrz* NIS
 Network Installation Manager, *Patrz* NIM
 NetWorker, *Patrz* EMC NetWorker
 NetworkManager, 616
 NFS, 191, 203, 218, 242, 243, 265, 370, 373, 479, 483, 487, 497, 531, 853, 855, 862, 864, 872, 892, *Patrz* też system plików dedykowane, 878
 wersje, 856
 NFSv3, 390
 NFSv4, 242, 243, 244, 248, 249, 250, 251, 252, 254, 857
 nice value, *Patrz* uprzejmość
 niceness, *Patrz* uprzejmość
 NIM, 496
 NIS, 908, 909, 935, 966, 1022, 1027, 1028
 NIST 800, 1158
 Nortel, 1352
 Novell, 65
 NSA, 180
 NSD, 694, 695, 701, 702, 705, 706, 708, 713, 715, 717, 718, 726, 745, 746, 747, 776, 777, 778, 779, 780, 781, 782, 784, 785, 786, 793, 794, 795, 798, 799, 802, 805, 812, 813, 814, 815, 817, 818, 820, 822, 825, 833, 836, 837, 840, 842, 843
 NSEC, 797, 810, 811, 814, 815, 816, 817, 822, 823
 NTFS, 219
 NTP, 1337, 1400
 numer
 jednostki, 540
 seryjny, 702, 724, 725, 726, 771, 772, 793, 794, 804, 815, 816, 817
 urządzenia, 540
 urządzenia logicznego, 309
 WWN, *Patrz* WWN

O

Object Data Manager, 67, *Patrz* ODM
 OBP, *Patrz* OpenBoot
 obszar wymiany, 361

obudowa, 307
 ODM, 556, 557, 558, 1510, 1511
 odwrotna notacja polska, 1003
 odwzorowanie, 696, 700, 705, 709
 bezpośrednie, 881, 882
 główne, 882
 odwrotne, 709
 pośrednie, 881, 882
 wykonywalne, 882
 Oetiker Tobias, 1065, 1089
 okablowanie, 686, 687
 Open Shortest Path First, *Patrz* OSPF
 OpenBoot, 487
 OpenBSD, 62
 Open-iSCSI, 377
 OpenLDAP, 258, 900, 901, 903, 904, 905,
 907, 1000
 OpenOffice, 1298, 1299, 1383
 OpenSolaris, 478, *Patrz* Solaris
 OpenXPS, *Patrz* XPS
 operator
 arytmetyczny, 108
 formatowania łańcuchów, 133
 leniwy, 115
 logiczny, 108
 postinkrementacji, 107
 relacyjny, 108
 wieloznaczny, 115
 zachłanny, 114, 115
 oprogramowanie
 filtrujące, *Patrz* filtrowanie
 sprzętowe, 147
 zarządzanie, 516
 Oracle, 66, 408
 OSPF, 656, 657, 659, 662
 OSSEC, 1109, 1110, 1126, 1127, 1128
 OWASP, 1159

P

paczkowanie operacji, 855
 Padl Software, 906
 pakiet, 77, 78, 498, 499, 504, 532, 579, 677,
 871, 1067
 Debian, 501, 505
 filtrowanie, 625, 1109, 1141, 1142, 1143
 findutils, 79

grupowy, 499, 672, 673
 IP, 579, 602, 603, 647, 648
 IPFilter, *Patrz* IPFilter
 jądra, 509
 jednostkowy, 673
 LAMP, 1170
 nagłówek, 579
 ping, 603, 611
 pkgutil, 79
 podsłuchiwanie, 1076, 1077, 1078, 1079
 pojedynczy, 672
 przekierowania ICMP, 596
 rozgłoszeniowy, 672
 rozmiar, 580
 RPM, 499, 500, 502
 UDP, 579
 palindrom, 109
 PAM, 179, 181, 259, 290, 1112, 1113, 1114,
 1115, 1116, 1117, 1118, 1399, 1400,
 1405, 1406
 pamięć, 1362, 1364
 dysk twardy, *Patrz* dysk twardy
 EEPROM, 407
 fizyczna, 194
 flash, 299, 302
 masowa, 295, 310, 312, 370, 373, 437,
 474, 1338
 nośnik optyczny, *Patrz* nośnik optyczny
 pula, 370, 372
 RAM, 144
 taśma magnetyczna, *Patrz* taśma
 magnetyczna
 wirtualna, 194, 214, 537, 1354
 wydajność, 1362, 1364
 zrzut, 199
 Parallel ATA, *Patrz* PATA
 parametr sieciowy, 598
 parawirtualizacja, 1201, 1202, 1209
 parsowanie, 1511
 partycja, 296, 303, 312, 318, 324, 326, 329, 361
 aktywna, 328
 główna, 325
 logiczna, 328
 rozszerzona, 328
 systemowa, 422
 tablica, 326, 330

- partycja
 - tablica GPT, 297, 329, 330
 - tablica GUID, *Patrz* partycja tablica GPT
 - użytkownika, 422
 - WPAR, 1220, 1221
- PAT, 625
- PATA, 304, 305, 306, 320
- PCI DSS, 1157
- PCL, 1259, 1290, 1296, 1297, 1298, 1299, 1301
- PDF, 1262, 1264, 1270, 1296, 1298, 1299,
1300, 1305, 1308
- PDL, *Patrz* język opisu strony
- peering points, *Patrz* punkt połączeń
- Pennock Phil, 1049
- Perl-compatible regular expression,
Patrz biblioteka PCRE
- pętla, *Patrz* instrukcja
- pętla FC-AL, *Patrz* FC-AL
- PGP, 1133, *Patrz* kryptografia
- phishing, 951, 1102
- PID, 195, 197, 204, 206, 222
- Pilgrim Mark, 130
- PJL, 1299, 1300
- Plain Old Telephone Service, *Patrz* POTS
- plik
 - administracyjny, 519
 - atrybuty, 232
 - blokowanie, 858
 - crontab, 384, 385, 389
 - deskryptor, 211
 - dfstab, 866
 - dziennika, 95, 225, 315, 325, 351, 355,
384, 392, 452, 453, 455, 456, 474, 996,
997, 1020, 1040, 1351, *Patrz też* dziennik
 - exports, 867, 869
 - FIFO, 231
 - hasel użytkowników, 898
 - historia modyfikacji, 517
 - kluczy SSH, 191
 - kodowanie nazw, 1388
 - konfiguracyjny, 97, 143, 160, 163, 224,
384, 392, 431, 480, 483, 484, 494, 511,
531, 555, 625, 626, 700, 701, 749, 781,
801, 819, 834, 843, 865, 880, 1003,
1018, 1025, 1114, 1234, 1263, 1511
 - kopia, 498
 - synchronizacja, 890
 - kopiowanie, 891
 - licznik dowiązań, 235
 - manifestu, 492
 - nazwa, 220, 228, 231, 387
 - odmowy, 388
 - odwzorowań, 910
 - passwd, 274
 - PPD, 1301
 - przełączania usług, 959
 - reguł, 565
 - shadow, 268, 269, 274
 - startowy, 275
 - strefowy, 698, 701, 702, 719, 737, 771,
774, 778, 783, 784, 785, 796, 801, 816,
817, 823, 835, 844, 845, 846
 - sysidcfg, 490
 - systemowy, 224
 - tekstowy, 1510
 - typ, 226, 232, 1261, 1262
 - urządzenia, 176, 218, 227, 229, 540, 541,
543, 562
 - urządzenia portu szeregowego, 1417
 - właściciel, 175, 232, 238
 - współdzielenie, 891, 1389
 - wykonywalny, 1118
 - zezwoleń, 387
- Plonka Dave, 1094
- plug and play, 305
- Pluggable Authentication Modules, *Patrz* PAM
- poczta elektroniczna, 918, 924, 930, 1385
- podpis transakcji, 798, 801, 802, 804, 805
- podpowłoka, 99
- podręcznik systemowy, 70
- PoE, 680
- Point-to-Point Protocol, *Patrz* PPP
- polecenie, 102, 178
 - add_drv, 562
 - adduser, 278
 - apt-get, 505, 506, 508, 509, 510
 - arp, 598
 - ATA TRIM, 320
 - backup, 414
 - bash, 60
 - cancel, 1276
 - cat, 210
 - catman, 72
 - cd, 220, 418

- cfdisk, 297
- cfgmgr, 360, 558
- ch*, 1511
- chdev, 262, 557
- chfn, 266
- chgrp, 238
- chkconfig, 161
- chmod, 232, 236, 237, 247, 254, 273
- chname, 705
- chown, 238, 273
- chroot, 176, *Patrz* chroot
- chsh, 267, 268
- configure, 81, 778
- cpan, 128
- crfs, 350, 355
- crontab, 384, 387
- cut, 90, 92
- date, 213
- dd, 356
- DDT, 841
- df, 357
- diff, 517, 1301
- dig, 698, 700, 702, 705, 713, 721, 723, 728, 739, 740, 746, 748, 752, 766, 777, 785, 786, 788, 798, 800, 804, 809, 820, 826, 838, 839, 840, 841
- diskpart, 328
- dladm, 610
- dnssec-signzone, 815, 816, 817, 820
- doc, 777, 779, 780, 833, 839, 841, 842, 843, 845, 846
- dpkg, 501
- drill, 698, 700, 702, 777, 785, 786, 798, 818, 822, 825, 826, 838, 839
- drvconfig, 562
- dump, 413, 414, 415, 416
- echo, 99
- enable, 662
- enscript, 1296
- ethtool, 621
- export, 92
- exportfs, 192, 867
- extendvg, 350
- fc, 99
- fdisk, 297, 328, 329, 330, 378
- filtrujące, *Patrz* filtr
- find, 90, 220, 221, 391
- finger, 266
- format, 330, 363
- fsck, 222, 354, 355
- ftp, 803
- fuser, 222, 223
- gated, 635
- getfacl, 246
- git, 522
- gparted, 297, 330
- grep, 90, 95
- halt, 170
- hdparm, 321, 322, 323
- head, 95
- host, 838
- hostname, 609, 666
- idisk, 331
- ifconfig, 581, 609, 610, 611, 612, 613, 630, 635
- ifdown interfejs, 616
- ifup, 618
- info, 73
- initlog, 467
- insf, 542
- install, 894
- installadm, 492
- installp, 516
- ioscan, 298
- ipnat, 633
- iptables, 626
- iscsi, 378
- iscsiadm, 378
- iscsiutil, 380
- kill, 201
- killall, 202
- label, 439
- lamers, 841
- lanscan, 635
- last, 456
- ldns-keygen, 781
- less, 73, 95
- list media, 439
- ln, 231, 232
- locate, 78
- logger, 465
- lp, 1256, 1271, 1272, 1275, 1276

polecenie

- lpc, 1284
- lpq, 1283
- lpr, 91, 1259, 1269, 1281, 1283, 1296
- lprm, 1283
- lpstat, 1276
- ls, 175, 221, 227, 229, 234, 235, 236, 247, 252, 253
- ls*, 1511
- lsattr, 557
- lsconn, 557
- lsdev, 298, 557
- lspp, 516
- lvchange, 346
- lvlnboot, 349
- LVM, 342
- lvresize, 346
- make, 81, 547, 549, 1000
- make install, 81
- make_depots, 494
- makewhatis, 72
- man, 70, 72
- manage_index, 494
- mandb, 72
- manpath, 72
- mdadm, 337
- mk*, 1511
- mkboot, 347
- mkdev, 557
- mkdir, 228, 275
- mkfs, 350, 354, 355
- mkiv, 350
- mknamsv, 705
- mknod, 230, 231, 542
- mkps, 361
- mkstf, 542
- mkswap, 361
- mktcpip, 558, 640
- mkvg, 341, 350
- mmencode, 803
- modify discovery, 379
- modload, 562
- modprobe, 560
- modunload, 562
- more, 210
- mount, 221, 354, 358, 391, 874
- mt, 421, 425
- named-check, 804
- namerslv, 705
- ndd, 557, 596, 631, 638, 994
- netstat, 594, 1060, 1069, 1070, 1071, 1072, 1073, 1074, 1075, 1076
- newaliases, 392
- newusers, 285
- nfsstat, 877
- nice, 204, 205
- nim_master_setup, 497
- no, 597, 642, 995
- nroff, 73
- nsdc, 836
- nsdc rebuild, 793
- nslookup, 838
- odmadd, 557
- odmdrop, 557
- odmshow, 557
- parted, 297, 330
- passwd, 177, 268, 270
- perl, 128
- pfexec, 186
- pgrep, 202
- ping, 1062, 1064
- pkg, 512
- pkill, 202
- powłoki, 1510
- powłoki systemowej, 60
- pr, 1296
- printf, 99
- procsig, 211
- programu Zyper, 511
- prtconf, 554
- ps, 90, 144, 203, 205, 206, 207, 208, 210, 214, 222
- psig, 211
- pstops, 1262
- pvcree, 341
- rdist, 893, 894, 895, 896
- read, 100
- reboot, 170
- renice, 204
- resize2fs, 346
- restore, 413, 414, 417, 418, 419, 420
- rm, 227, 231, 320, 378

- rm*, 1511
- rmdev, 557
- rmdir, 228
- rmmmod, 560
- rmnamsv, 705
- rncd, 836
- rncd freeze, 796
- rncd reload, 793, 804, 835
- rncd thaw, 796, 836
- rodzina, 1510, 1511
- route, 595, 612, 613, 614, 619
- routed, 628
- rozruchowe SUN, 152
- rpm, 499
- rsync, 896, 897, 898, 899
- run, 439
- SD, 514
- sendmail, *Patrz* sendmail
- setfacl, 246
- sfdisk, 297
- sh, 60
- share, 865, 866, 867, 868
- shutdown, 143, 169
- smit easy_install, 516
- smit install_software, 516
- snoop, 1079
- sort, 93
- strace, 212
- su, 185, 186
- sudo, 182, 186, 188, 189, 296, 297, 817, 1000
- svcad, 166
- svcs, 165, 166
- svn update, 520
- swapon, 361
- swinstall, 80, 494, 513
- sysctl, 545, 624
- sysdef, 555
- tail, 95
- tcpdump, 1078
- tee, 94
- telinit, 143
- telnet, 803, 1106, 1134, 1136, 1139, 1140, 1141, 1143, 1171
- test, 104
- top, 209, 210, 214
- topas, 209
- truss, 212
- udevadm, 564, 567
- ufsdump, 414
- ufsrestore, 414
- umask, 238, 273
- umount, 222
- unbound-control, 837
- uniq, 94
- unmount, 358
- updatedb, 79
- update-rc.d, 162
- uptime, 214
- useradd, 273, 274, 278, 280, 281, 282, 284, 285
- userdel, 278, 287
- usermod, 278, 288
- vgextend, 347
- vipw, 274
- visudo, 188
- vmstat, 210
- wc, 94
- wget, 79, 899
- whereis, 78
- which, 78
- wireshark, 1079
- xargs, 220, 221
- xdpyinfo, 1250
- ypmake, 910
- yppush, 910
- ypxfr, 910
- zfs get, 366, 368, 369
- zpool, 371
- POP, 919, 920, 923, 931, 966, 978, 1139
- port, 583
 - przełącznika, 673
 - sieciowy uprzywilejowany, 177
 - szeregowy, 1417, 1418
 - szeregowy RS-232C, *Patrz* RS-232
- port sieciowy
 - uprzywilejowany, 177
- Portable Document Format, *Patrz* PDF
- POSIX, 180, 182, 241, 243, 244, 251
- Post Office Protocol, *Patrz* POP
- Postfix, 919, 922, 925, 926, 928, 930, 948, 956, 957, 1021-1042, 1050
- PostgreSQL, 428

- PostScript, 1259, 1262, 1276, 1279, 1290,
 - 1291, 1292, 1296, 1297, 1298, 1299, 1300,
 - 1301, 1302, 1304, 1305, 1308
- PostScript Printer Description, *Patrz* plik PPD
- potok, 90, 92, 99, 211, 227, 231, 538, 1281
 - polecieć, 94
- POTS, 684
- Power over Ethernet, *Patrz* PoE
- powłoka, 88, 96
 - awaryjne uruchamianie, 142
 - bash, 60, 88, 92, 96, 97, 102, 104, 105,
 - 115, 185, 204, 267, 1236, 1378
 - Bourne'a, 88, 104, 267
 - C, 267, *Patrz* powłoka csh
 - csh, 88, 204, 841
 - domyślna, 88, 259
 - funkcje, 88
 - interaktywna, 203
 - Korna, 88, 267
 - ksh, 88, 267
 - logowania, 97, 267, 386
 - polecenie, 482
 - root, 145
 - sh, 88, 267, 384, 386
 - składnia, 88
 - smrsh, 986
 - tcsh, 88
 - tryb logowania, 185
 - użytkownika, 145
- poziom uruchomieniowy, 1423
- PPID, 195
- Pratt Ian, 1209
- prawo Moore'a, 299
- Preboot eXecution Environment, *Patrz* PXE
- predictive self-healing, *Patrz* restarter
- prepublikacja, 821
- Printer Control Language, *Patrz* PCL
- Printer Job Language, *Patrz* PJL
- priorytet, 196, 203, 204, 206, 1436, 1441
 - procesu, 176
- proces, 193, 197, 537 *Patrz też* program
 - errdemon, 468, 469
 - init, 144, 145, 147, 154, 155, 158, 160, 163,
 - 164, 197, 198, 1420, 1424, 1425, 1426
 - poziomy, 154
 - jądra, 144
 - macierzysty, *Patrz* PPID
 - mudd, 1073
 - niekontrolowany, 213, 214
 - ntpd, 205
 - numer identyfikacyjny, *Patrz* PID
 - obsługi pamięci, 144
 - osierocony, 198
 - potomny, 195, 197
 - śledzenie, 213
 - samorzutny, 144
 - telinit, 155
 - uśpiony, 203
 - właściciel, 176
 - zachłanny, 1371
 - zajętość pamięci, 214
 - zatrzymany, 203
 - zniszczenie, 198, 287
 - zombie, 203, 206
- procesor
 - przeciążenie, 1372
 - SPARC, 152
 - wydajność, 1359
- procmail, 922
- program *Patrz też* proces, demon
 - amavisd, *Patrz* amavisd
 - cfengine, 529, 530
 - chage, 1112
 - dd, 422, 424
 - dhcpcagent, 630
 - dump, 397, 412, *Patrz też* polecenie dump
 - emacs, 228
 - filtrujący, 127
 - gzip, 72, 215
 - iptables, 1145
 - Kickstart, *Patrz* Kickstart
 - lmt, 1024
 - logcheck, 473
 - login, 177
 - logrotate, 471, 472
 - lsuf, 223
 - m4, 963
 - nmap, 1120, 1122
 - nroff, 72
 - nsupdate, 796
 - obsługi kolejki wydruku, 1257
 - pipe, 1024
 - powłoki, 1112
 - rozruchowy, 143, 148, 150

- rsync, 528
 - savelog, 472
 - SEC, 473
 - smtp, 1024
 - Splunk, 473
 - star, 445
 - swatch, 473
 - sync, 445
 - tar, 415, 422
 - traceroute, 1064, 1066, 1067, 1068
 - YaST, 161
 - yum, 510, 511
 - zonec, 777
 - programowanie obiektowe, 60
 - protokół, 577
 - ATAPI, *Patrz* ATAPI
 - bezstanowy, 1171
 - bramy brzegowej, *Patrz* BGP
 - CHAP, 376
 - DHCP, 599
 - EIGRP, *Patrz* EIGRP
 - enkapsulacyjny, 606
 - HTTP, *Patrz* HTTP
 - IGMP, *Patrz* IGMP
 - IPsec, *Patrz* IPsec
 - IS-IS, *Patrz* IS-IS
 - iSNS, 375
 - kapsułkowy, 606
 - kontroli transmisji, 605
 - LWAPP, *Patrz* LWAPP
 - ND, *Patrz* ND
 - NetFlow, *Patrz* NetFlow
 - numer portu, 574
 - OSPF, *Patrz* OSPF
 - PPP, *Patrz* PPP
 - punkt-punkt, *Patrz* PPP
 - SMTP, 927
 - stanu łączy, 653
 - TCP/IP, *Patrz* TCP/IP
 - tekstowy, 928
 - trasowania, 652, 654, 655
 - wektora odległości, 652, 653, 654, 655, 657
 - WEP, *Patrz* WEP
 - wewnętrzny, 655
 - własnościowy, 657
 - wykrywania routerów, *Patrz* IRDP
 - wyznaczania tras, *Patrz* trasowanie
 - zarządzania sieciowego, 1082
 - zewnętrzny, 655
 - przeglądy projektowe, 88
 - przekierowanie, 1391
 - przekierowanie ICMP, 596, 602
 - przełączanie, *Patrz* uprzejmość
 - przełącznik, 672, 673, 676, 677, 678, 680, 681, 683, 686, 689, 690, 1060, 1083
 - beprzewodowy, 683
 - przerwanie, 198
 - przestrzeń adresowa, 194
 - przetwarzanie w chmurze, 1204, 1225, 1341
 - pseudosieć, 649
 - pseudoterminale, 1419
 - pseudourządzenie, 541
 - pull, 893, 899, 910
 - punkt
 - montowania, 221
 - połączeń, 574
 - zaufania, *Patrz* kotwica
 - push, 893, 910
 - PuTTY, 1378, 1380
 - PXE, 147, 479, 483, 487
- ## Q
- Quagga, 656, 660, 661, 662, 663, 664
 - Quantum, 408
- ## R
- RAID, 296, 307, 312, 314, 327, 331, 334, 399, 1369
 - poziomy, 332, 333, 334
 - programowy, 337
 - wady, 336
 - ramka, 579, 677
 - Jumbo, 681
 - RANCID, 666
 - randomizacja czasu, 509
 - RBAC, *Patrz* kontrola dostępu role
 - RDP, 1381
 - Red Hat, *Patrz* dystrybucja Red Hat
 - Red Hat Enterprise Linux, *Patrz* dystrybucja Red Hat
 - Red Hat Network, 502, 504
 - redundant array of inexpensive/independent disks, *Patrz* RAID

Reed Darren, 632, 639, 1150
 reflektometria, 685
 reguła, 565, 566, 567, 568
 domyślna, 565
 lokalna, 565
 ReiserFS, *Patrz* system plików
 rekord
 DNS ADSP, 950
 DNS MX, 934, 995
 DNS TXT, 1044
 DS, 810, 814, 818, 819, 821, 822
 rozruchowy, *Patrz* MBR
 zasobów, 696
 relacyjna baza danych, 428
 Remote Desktop Protocol, *Patrz* RDP
 repeater, *Patrz* koncentrator
 replikacja, 1190
 request coalescing, *Patrz* paczkowanie
 Request for Comments, *Patrz* RFC
 resolver, 695, 703, 704, 713, 800, 801, 830
 otwarty, 800, 801
 restarter, 167, 168
 RFC, 75, 575, 576, 694
 RHEL, *Patrz* dystrybucja Red Hat
 RHN, *Patrz* Red Hat Network
 RIP, 653, 655, 656, 657, 658, 659, 660, 662
 RIPE, 808, 819, 822, 824
 RIPng, 653, 655, 656, 660, 662, 664
 RJ-45, 673, 675, 1413, 1414
 RMON MIB, 1086
 roaming, 683
 robak Morrisa, 1100
 role, *Patrz* kontrola dostępu role
 Role Based Access Control, *Patrz* kontrola
 dostępu role
 Romao Artur, 841
 rootkit, 1109, 1126
 Route Administration Manager Daemon, 663
 router, 580, 584, 596, 659, 663, 678, 679, 681,
 998, 1013, 1014, 1015, 1017, 1019, 1060,
 1083, 1294
 brzegowy, 590
 Cisco, 664, 665
 modularny, 679
 o ustalonej konfiguracji, 679
 routing, *Patrz* trasowanie

Routing Information Protocol, *Patrz* RIP
 Rowland Craig, 473
 rozgałęźnik, 94
 równoważenie obciążenia, *Patrz* GSLB
 RPM, 512, 516
 RPO, 403
 RRDtool, 1089, 1090, 1092
 RRSIG, 797, 806, 810, 811, 815, 816, 817, 822
 RS-232, 1410, 1411, 1413
 Rsyslog, 466
 RTO, 403

S

SAIT, 407
 Samba, 1386-1401
 SAN, 296, 373, 374, 400, 879, 1200, 1338,
 1369
 SANS, 1160
 SAS, 310, 311, 321
 SASL, 983, 989, 990, 1000, 1035
 SATA, 304, 305, 306, 307, 310, 320, 321, 323
 Satellite Server, 502
 Schneier Bruce, 1160
 SCSI, 304, 305, 309, 310, 314, 319, 375
 adres, 309
 numer jednostki, *Patrz* numer urządzenia
 logicznego
 równoległy, 307
 szeregowy, *Patrz* SAS
 terminacja, *Patrz* terminacja
 złącza, 308
 SD, 515
 SDH, 684
 S-DLT, 406
 SDSC Secure Syslog, 466
 SecSpider, 809, 819, 820, 825
 Security-enhanced Linux, *Patrz* SELinux
 segment, 326, 579, *Patrz też* partycja
 bezwzrostowy, 673
 fizyczny, 673
 logiczny, 673
 SELinux, 180, 182, 186, 1130, 1131, 1132
 semafor, 537
 Sender ID, 926, 949, 1035
 sendmail, 922, 926, 930, 948, 956-1001, 1021-
 1025, 1028, 1040, 1042, 1043, 1045, 1047

- Senft Andrew, 1294
 Sensaphone, 1324
 separator, 579
 Serial ATA, *Patrz* SATA
 Serial Attached SCSI, *Patrz* SAS
 Service Management Facility, *Patrz* SMF
 serwer
 Apache, 62, 194, 518, 1120, 1177, 1178,
 1181, 1183, 1186, 1187, 1189, 1192,
 1263, 1385
 autorytatywny, 694, 706, 708, 753, 758,
 763, 792, 840
 bezstanowy, 854, 857
 buforujący, 694, 706, 708, 713, 749, 763,
 771, 1191
 DHCP, *Patrz* DHCP
 DNS, 146, 695, 696, *Patrz też* serwer
 nazw, demon systemowy
 dystrybucyjny, 706
 główny, 700, 701, 706, 909
 HTTP, 1177, *Patrz* HTTP
 IMAP, 924
 LDAP, 175
 lokalny, 698
 lustrzany, 508
 master, 700
 na żądanie, 1339
 nazw, 694, 695, 697, 698, 699, 700,
 703-710, 714, 727, 767, 801, 831,
 834, 837-840
 NFS, *Patrz* NFS
 NIS, 175
 nsd, 779, 784
 odwrotny pośredniczący, 1192
 poczty, 918, 923, 947, 948, 956, 959, 960,
 962, 964, 966, 974, 975, 977, 982,
 1026, 1042, 1045
 podległy, 696, 706, 707, 784, 785, 793,
 794, 795, 799, 823, 831, 838
 POP, 924
 pośredniczący, 1190
 proxy, 479
 rekurencyjny, 698, 706, 708, 793
 SMTP, 146, *Patrz też* demon systemowy
 sshd, 896
 wirtualny, 1200
 wydruku, *Patrz* program obsługi kolejki
 wydruku
 Xorg, *Patrz* Xorg
 z kontrolą stanu, 854
 Shapiro Greg, 990
 shebang, 96
 Shimpie Anand, 304
 Shuttleworth Mark, 65
 sieciowy system plików, *Patrz* NFS
 sieć
 autonomiczna, 659
 bezprowadowa, 681, 683
 diagnostyka, 685
 dokumentacja, 690
 dystrybucji treści, *Patrz* CDN
 konfigurowanie, 607, 609, 615, 616, 617,
 619, 626, 629, 634, 640
 LAN, *Patrz* LAN
 OSI, 657
 projektowanie, 687, 688, 689
 SAN, *Patrz* SAN
 wirtualna, 581
 wirtualna lokalna, *Patrz* VLAN
 sieć WAN, *Patrz* WAN
 SIG(0), 805
 Simple Authentication and Security Layer,
 Patrz SASL
 Simple Event Correlator, *Patrz* program SEC
 Simple Mail Transport Protocol, *Patrz* SMTP
 skalar, 117
 skaner, *Patrz* filtr
 skanowanie, 933, 941, 944, 953, 954, 977,
 982, 998, 1019, 1038, 1122
 portów sieciowych, 1120
 skrętka
 nieekranowana, *Patrz* UTP
 skrypt, 60, 87, 96, 99, 153, 383, 498, 509
 init, 142
 powłoki, *Patrz* skrypt init
 sh, 88
 startowy, 146, 153, 154, 156, 158, 160,
 163, 164, 620, 626, 627, 1232, 1234
 wywołanie, 100
 skrzynka pocztowa, 923
 Skype, 669

- SLA, 1436, 1438, 1439, 1440, 1441, 1442,
1443, 1451, 1462
- słowo kluczowe, 490, 933
- esac, 105
 - network_interface, 490
- Small Computer Systems Interface, *Patrz* SCSI
- SMART, 323
- SMF, 164, 165, 166
- SMH, 636
- SMI, 330
- SMIT, 289, 349, 558, 640, 1510, 1511, 1512
- SMTP, 921, 922, 926-930, 934, 941, 942, 943,
945, 946, 950, 953, 954, 956, 974, 976,
980, 981, 982, 983, 984, 987, 989, 990,
992, 1000-1017, 1021, 1022, 1024, 1032,
1035, 1037, 1038, 1041, 1048, 1385
- SNMP, 1082, 1083, 1084, 1085, 1086, 1087,
1088, 1089, 1090, 1093
- Snort, 1110, 1126, 1144
- Software Assistant, 514
- Software Distributor, *Patrz* SD
- Solaris, 64, 66, 71, 72, 77, 148, 152, 164,
167, 179, 186, 191, 202, 205, 208, 209,
211, 212, 213, 230, 234, 237, 238, 243, 244,
248, 252, 254, 264, 270, 281, 297, 316, 324,
330, 334, 341, 357, 359, 378, 388, 414, 426,
456, 462, 486, 487, 492, 512, 530, 539, 540,
542, 551, 554, 560, 561, 610, 614, 626, 635,
662, 846, 864, 866, 875, 884, 985, 994, 1000,
1064, 1075, 1079, 1113, 1130, 1153, 1185,
1200, 1225, 1232, 1248, 1270, 1272, 1274,
1358, 1426
- sondowanie, 635
- sortowanie, 93, 94
- spam, 921, 924, 926-934, 936, 938, 941, 942,
943, 944, 945-954, 973-977, 981, 1011,
1015, 1019, 1020, 1035, 1038
- odbity, 945
- SpamAssassin, 944, 946, 947, 951, 952, 981,
998, 1011, 1012, 1037
- Sparta, 807, 822, 823, 824
- Spectra Logic, 408
- SPF, 921, 926, 927, 942, 944, 949, 950, 1035
- spooler, *Patrz* program obsługi kolejki
- wydruku
- sprawdzanie drogi powrotnej, *Patrz* uRPF
- SQLite, 428, 429
- Squid, 1190
- SSD, 320, 374
- SSH, 1072, 1106, 1109, 1112, 1124, 1134,
1135, 1137, 1138, 1139, 1143, 1148, 1153,
1238, 1378, 1379, 1380
- SSL, 605, 923, 976, 983, 1013, 1051, 1187
- SSO, *Patrz* system pojedynczego logowania
- standard POSIX, 61
- Standard Hierarchii Systemu Plików, *Patrz* FHS
- statystyki systemu NFS, *Patrz* polecenie
- nfsstat
- STD, 576
- sterownik, 229, 296, 538, 539, 541, 549, 559,
998, 1017, 1242
- drukarki, 1394, 1395, 1396, 1397
 - terminala, 1427, 1428, 1429
 - urządzenia, 144
 - widmowy, 541
- sticky bit, *Patrz* bity lepkości
- Storage Area Network, *Patrz* SAN
- Storage Technology, 408
- Stowarzyszenie Przemysłu
- Telekomunikacyjnego, *Patrz* TIA
- strefa, 696, 700, 701, 702, 705, 707, 709, 724,
726, 727, 744, 745, 761, 764, 771-785,
791-797, 804-824, 826, 830, 831, 835-842,
845, 846
- Subversion, 518
- suma kontrolna, 579
- Sun Microsystems, 66, 152, 164, 218, 486,
632, 853, 880, 908, 1200, 1383, 1416, 1511
- Sun Yellow Pages, 908
- superużytkownik, *Patrz* UID 0
- SUSE, *Patrz* dystrybucja SUSE
- Sweet Michael, 1294
- switch, *Patrz* przełącznik
- sygnał, 176, 198, 200, 537, *Patrz też* przerwanie
- blokowanie, 199
 - CTS, 1416
 - DCD, 1415
 - ignorowanie, 199
 - nazwa, 199
 - przechwytywanie, 199
 - RTS, 1416
- sygnał wykrycia nośnej, *Patrz* sygnał DCD
- Symantec, 447, 531

- symbol
 - ' , 92
 - " , 91, 92
 - " , 91, 121
 - # , 96, 116, 131
 - \$, 91, 112
 - \$, 117
 - % , 117, 119
 - && , 91
 - () , 112
 - * , 112
 - ., 131
 - ., 91, 116
 - ;; , 105
 - @ , 1005
 - @ , 117
 - [] , 104, 132, 144
 - [] , 116
 - ^ , 112
 - ` , 92
 - { } , 91, 119
 - || , 91
 - = , 91
 - a , 151
 - e , 151
 - i , 158
 - tabulacji , 93
- sysfs , 563
- syslog , 452, 457, 462, 468, 469, 780, 783, 784, 787, 788, 789, 801, 827, 828, 829, 833, 845, 996, 1107, 1125, 1131, 1511
- system
 - aktualizacja , 1105
 - autonomiczny , 654
 - detekcji włamań , 1109, 1125, 1126
 - dostarczający , *Patrz* DA
 - dostępowy , *Patrz* AA
 - jądro , *Patrz* jądro
 - klienta poczty , 919
 - kompresji , 521
 - kontroli wersji , 516, 517, 520, 525, 1453
 - lokalizowania , 525, 528, 529
 - ładowanie , 142, 197
 - obsługi poczty , 919
 - operacyjny , 1295
 - aktualizacja , 422
 - plików , 214, 217, 218, 219, 221, 224, 228, 239, 243, 297, 311, 313, 350, 351, 352, 353, 361, 367, 369, 373, 395, 415, 537, 544, 853, 854, 855, 858, 860, 869, 871, 872, 873, 874, 875, 879, 880, 881, 882, 883, 884, 885, 1108, 1220
 - archiwizacja , 414
 - charakterystyka , 353
 - formatowanie , 355
 - HFS , 243
 - hierarchia , 226
 - JFS2 , 244
 - księgowanie , 240, 352, 353
 - montowanie , 356, 357
 - naprawa , 355
 - odtwarzanie , 420
 - polimorfizm , 354
 - porządkowanie , 390
 - terminologia , 353
 - wirtualny , *Patrz* sysfs
 - zmiana rozmiaru , 345
 - plików Btrfs , 218, 314, 362
 - plików ZFS , 218, 254, 297, 314, 324, 330, 334, 337, 357, 362, 363, 364, 367, 370, 371, 414, 424, 425
 - pocztowy , 930, 931
 - podstawiania tożsamości , *Patrz* UID, GID
 - pojedynczego logowania , 291
 - syslog , *Patrz* syslog
 - system zarządzania urządzeniami , *Patrz* udev
 - transportowy , *Patrz* MTA
 - trasowania , 662
 - Voice-over-IP , 579
 - wejścia-wyjścia , 538
 - wydajność , 1366
 - wydruku , 1300, 1307
 - zamykanie , 168
 - zarządzania pakietami , 502, 503, 504, 505, 512, 513, 532
 - zgłoszeniowy , 1444, 1451, 1453
- System Management Interface Tool , *Patrz* SMIT
- system operacyjny IOS , *Patrz* IOS
- system transportowy , *Patrz* MTA
- System V , 1257, 1258, 1270, 1271, 1274, 1275, 1279, 1294, 1295, 1302, 1307
- szara lista , *Patrz* lista szara

szperacz sieciowy, 685
 szyfrowanie, *Patrz* kryptografia

Ś

ścieżka dostępu, 219, *Patrz* plik nazwa
 ślad magnetyczny, 320
 śledzenie błędów, 88
 światłowod, 305, 673, 676, 689
 jednomodowy, 676
 wielomodowy, 676

T

tablica, 107, 116, 119, 121, 132
 asocjacyjna, *Patrz* dane hasz
 dostępu, 1028
 odwzorowań, 1027
 przeglądowa, 1027
 routingu, 1073
 tras, 594, 648, 652, 653, 658
 Tandberg, 407
 target number, *Patrz* SCSI adres
 taśma magnetyczna, 299
 TCP, 577, 581, 583, 605, 874
 TCP/IP, 573, 574, 577, 578, 579, 583, 594,
 603, 612, 622, 631, 640, 642, 1060, 1061,
 1082
 Telecommunications Industry Association,
 Patrz TIA
 telnet, 664
 Template Tree 2, 530
 terminacja, 308, 314, 319
 terminal, 1428, 1430
 ASCII, 1419
 CRT, 1419
 konfigurowanie, 1421
 sterujący, 197, 206
 Texinfo, 73
 TFTP, 479, 497
 Thunderbird, 920
 TIA, 674
 time to live, *Patrz* TTL
 Tivoli Storage Manager, *Patrz* TSM
 TLS, 605, 837, 983, 990, 1000, 1004,
 1013, 1051

token ring, 579, 582
 TortoiseSVN, 520
 Torvalds Linus, 1208
 Transmission Control Protocol, *Patrz* TCP
 transport, 998, 1017
 Transport Layer Security, *Patrz* SASL
 trasa pseudosieci, 649
 trasowanie, 589, 594, 604, 613, 648, 654, 659
 dynamiczne, 596, 658, 659
 grupowe, 648
 jednostkowe, 648
 lokalne, 658
 statyczne, 595, 612, 652, 658, 659
 szkieletowe, 658
 źródłowe, 648
 Tridgell Andrew, 896, 1386
 Troan Erik, 471
 Trojnara Michał, 1139
 tryb
 automatycznego uzgadniania, 612
 DMA, *Patrz* DMA
 dostarczania poczty, 991
 dupleksowy, 612
 graficzny, 481
 konserwacyjny, *Patrz* tryb odzyskiwania
 master, 306
 nadrzędny, *Patrz* tryb master
 NWAM, 627
 odzyskiwania, 143, 145, 146, 151, 152
 podległy, *Patrz* tryb slave
 pojedynczego użytkownika, *Patrz* tryb
 odzyskiwania
 półdupleksowy, 612
 slave, 306
 transportowy, 1154
 tunelowy, 1154
 zdegradowany, 400
 TSIG, 779, 780, 781, 797, 801, 802, 804, 805,
 812, 822, 826, 834
 TSM, 446
 TTL, 698, 821, 822, 831, 842, 1066, 1067,
 1068
 tunelowanie, 581, 593
 tuples, *Patrz* krotki
 twinaxial, *Patrz* kabel miedziany dwuosiowy

U

Ubuntu, *Patrz* dystrybucja Ubuntu
 udev, 563
 UDP, 577, 579, 581, 583, 857, 874, 1068,
 1071, 1072, 1073, 1074
 UFS, 414, *Patrz* system plików
 UID, 175, 176, 177, 195, 196, 206, 244, 247,
 259, 264, 265, 861, 863, 1399, *Patrz też*
 EUID
 0, 176, 191, 204, 238
 -1, 191
 -2, 191
 UIO, 539
 Unbound, 694, 695, 699, 705, 706, 708, 713,
 717, 718, 746, 776, 777, 786, 798, 799,
 820, 822, 825, 833, 838, 840, 842, 843
 unicast reverse path forwarding, *Patrz* uRPF
 Uniform Resource Identifier, *Patrz* URI
 Uniform Resource Locator, *Patrz* URL
 Uniform Resource Names, *Patrz* URN
 Universal Serial Bus, *Patrz* USB
 Unshielded Twisted Pair, *Patrz* UTP
 uprawnienia, 229, 232, 234, 235, 236, 238, 247,
 249, 985, *Patrz też* użytkownik
 uprawnienia
 uprzejmość, 196, 197, 203
 wartość, 203
 Upstart, 161
 Uptime Institute, 1319, 1320
 URI, 1170, 1171
 URL, 1170, 1171, 1179, 1180, 1181, 1187,
 1192, 1193
 URN, 1170
 uRPF, 604
 urządzenie, 567
 blokowe, 541, 543, 549
 sieciowe, 549
 szeregowe, 543, 1409
 testowanie, 564
 TTY, *Patrz* urządzenie szeregowie
 zarządzanie, 565
 znakowe, 541, 543, 549
 USB, 305, 311, 360, 405, 1409, 1411
 User Datagram Protocol, *Patrz* UDP

usługa

automatycznego montowania
 systemów plików, 166
 chmurowa, 409
 DLV, *Patrz* DLV
 katalogowa, 900
 kryptograficzna, 166
 pocztowa zewnętrzna, 918
 sieciowa nasłuchująca, 1072
 ssh, 165, 166
 zakres, *Patrz* SLA
 zbędna, 1106
 UTP, 673, 674
 uwierzytelnianie, 1012, 1013
 użytkownik, 175
 bin, 191
 daemon, 191
 dodawanie, 258, 273, 285
 nazwa, 260, 262, 387
 nobody, 191, 192, 264, 862
 numer identyfikacyjny, *Patrz* UID, GID
 root, 176, 177, 178, 182, 184, 186, 191,
 201, 264, 455, 481, 521, 634, 784, 786,
 801, 844, 862, 1108, 1113, 1136
 sys, 191
 tożsamość, 185, 195
 uprawnienia, 176-182, 185, 186, 187, 191,
 195, 196, 240, 276
 usuwanie, 286
 uwierzytelnianie, 1035, 1114, 1115, 1117,
 1118, 1133, 1134, 1135, 1232, 1237,
 1389
 wyłączanie, 288
 zarządzanie tożsamością, 258, 292

V

van Rossum Guido, 130
 Vantages, 819, 822, 824, 825
 VeriSign, 805, 845, 990, 1155
 Veritas, 218, 243, 352, 447
 Version Control with Subversion, 74
 Virtual Local Area Networks, *Patrz* VLAN
 Virtual Network Computing, *Patrz* VNC
 Virtual Partitions, 1222

Virtual Private Network, *Patrz* VPN
 Vixie Paul, 388
 Vixie-cron, *Patrz* demon cron
 VLAN, 678
 VMware, 1200, 1202, 1224, 1225
 VMware Server, 1382
 VNC, 1380, 1381
 Voice over IP, *Patrz* VoIP
 VoIP, 680
 VPN, 605, 1153, 1154
 VXA, 407
 VXA-X, 407
 VxFS, *Patrz* system plików,

W

walidacja, 1511
 Wall Larry, 115
 WAN, 1086
 WAP, 681, 682
 Ward Grady, 183
 warstwa
 IP, 579, 580, 584, 613
 łącza, 579, 580, 583, 584, 634, 685
 TCP, 579
 wartość
 łańcuchowa, 107
 skalarna, 119, 121
 wątek, 194
 Weiner Sam, 807
 WEP, 683
 wiadomość do plików, 938, 986, 987
 wiadomość do programów, 939
 wiadomość e-mail, 924, 943
 ciało, 925
 koperta, 924, 991
 nagłówki, 924, 925, 926, 977
 wideokonferencja, 584
 wielosystemowość, 150, 376
 Wi-Fi, 1293
 Wi-Fi Protected Access, *Patrz* WPA
 Windows, 150, 241, 248, 250, 311, 427, 438,
 518, 604, 786, 826, 1232, 1305, 1377, 1382
 Wine, 1382
 Wired Equivalent Privacy, *Patrz* WEP
 wireless access points, *Patrz* WAP
 Wireshark, 686, 1079
 wirtualizacja, 1200, 1201, 1204, 1205, 1207,
 1208, 1220, 1222, 1224, 1333, 1338, 1342,
 1345
 na poziomie systemu operacyjnego, 1201,
 1203
 natywna, 1203
 pełna, 1201, 1214
 sprzętowa, 1203
 zalety, 1205
 wirtualna sieć prywatna, *Patrz* VPN
 wirus, 919, 920, 924, 926, 927, 930, 931, 933,
 941, 942, 948, 949, 951, 955, 956, 973,
 974, 977, 1015, 1035, 1038, 1054, 1107
 właściciel
 pliku, 175
 procesu, 176
 uprawnienia, 246
 wolumin
 fizyczny, 341
 logiczny, 296, 313, 324, 327, 340, 342,
 347, 349, 361, *Patrz też* LVM
 World Wide Name, *Patrz* WWN
 WPA, 683
 Wtyczka Molex, 305
 WWN, 310
 WWW, 1383, 1384, 1385
 wybór trasy przez nadawcę, 603
 wycofywanie, 114, 115
 wydajność, 1349, 1351, 1353
 analiza, 1355, 1356, 1359, 1362, 1364,
 1366, 1369, 1370, 1371
 operacji dyskowych, 1354
 pamięci, 1354
 procesora, 1354
 wydanie, 503
 wykrywanie
 kolizji, 672
 stanu kanału, 672
 wyrażenie regularne, 95, 109, 110, 114, 115,
 122, 135, 1038
 typ argumentów, 119
 wyznaczanie tras, *Patrz* trasowanie
 wzmacniak, *Patrz* koncentrator
 wzorzec, 95, 106, 113

X

X, 1231-1239, 1241, 1243, 1245-1251,
1378-1384
X Window System, *Patrz* X
X11, *Patrz* X
x86, 147
Xen, 1200, 1202, 1208-1216, 1222, 1225
XFree86, 1232
XML Paper Specification, *Patrz* XPS
Xorg, 1232, 1233, 1240, 1241, 1244, 1245,
1247, 1248, 1249
XORP, 663
xpdf, 1298
XPS, 1299

Y

Yahoo! Mail, 918
YaST, 617
YaST2, 483
Yellowdog Updater Modified,
Patrz program yum
Ylönen Tatu, 1134

Z

zachłanność, 114
zamykanie systemu, 177
zaporą
sieciowa, 604, 632, 639, 1124, 1130, 1137,
1141, 1143, 1144, 1154, 1190
z kontrolą stanu, 1143

zarządzanie, 1435, 1462, 1463, 1465, 1467,
1471, 1473
energią, 1340, 1341
pamięcią, 1362
siecią, 1060, 1081, 1088, 1092
sprzętem, 1511
urządzeniami, 565
zarządzanie oprogramowaniem,
Patrz oprogramowanie zarządzanie
Zebra, 661, 662
zegar, 804
zegar systemowy, 176
Zimbra, 920, 924, 1051
Zimmermann Phil, 944, 1133
złącze
DB-25, 1411, 1413, 1414
DB-9, 1413
RJ-45, *Patrz* RJ-45
zmienna, 91, 100
globalna, 103
MANPATH, 72
powłoki bash, 92
skalarna, 117
środowiska DISPLAY, 1236, 1237
środowiskowa, 92, 97, 188, 274
znak, *Patrz* symbol
specjalny, 110
Zypper, 503, 511

Ta książka to obowiązkowa pozycja dla wszystkich administratorów!

Systemy Unix i Linux wykorzystywane są wszędzie tam, gdzie wymagana jest najwyższa niezawodność, wydajność i elastyczność. Ich potencjał, możliwości oraz odporność na niesprzyjające otoczenie sprawiły, że są dominującymi systemami operacyjnymi w zastosowaniach sieciowych. Jeżeli jednak systemy te kojarzą Ci się wyłącznie z czarnym ekranem konsoli oraz trybem tekstowym, jesteś w błędzie. Już od dawna systematycznie zwiększają one swój udział w zastosowaniach domowych. Co w sobie kryją? Jak nimi administrować i jak zwiększać ich wydajność?

Na te i setki innych pytań odpowiada ten obszerny przewodnik. Autorzy rozbili go na czynniki pierwsze i omówili każde zagadnienie, z którym możesz mieć styczność w codziennej pracy. Po lekturze tej książki będziesz posiadał obszerną wiedzę w tej materii. Instalacja systemu, skrypty powłoki, kontrolowanie procesów, konfiguracja uprawnień to zadania, które nie będą Ci sprawiały żadnych problemów. Ponadto dowiesz się, jak zarządzać użytkownikami, przestrzenią dyskową, zadaniami okresowymi oraz backupami. Dużą uwagę poświęcili również rozdziałom omawiającym zagadnienia sieciowe. Jest pewne, że serwer, który trafi w Twoje ręce, będzie oferował wiele usług dostępnych przez sieć. Protokoły routingu, usługi DNS, firewall, serwer plików to elementy, które niejednokrotnie będziesz musiał konfigurować.

Nie znajdziesz na rynku obszerniejszej książki poświęconej systemom Unix i Linux. Jeżeli jesteś z nimi związany w pracy zawodowej, interesujesz się systemami operacyjnymi lub korzystasz z nich w domu, ta książka obowiązkowo musi znaleźć się na Twojej półce!

- Skrypty powłoki
- Uruchamianie i zamykanie systemu
- Kontrola dostępu, uprawnienia administratora
- Nadzór nad procesami
- System plików
- Zarządzanie użytkownikami
- Wykorzystanie zasobów dyskowych
- Zadanie okresowe — cron
- Tworzenie kopii zapasowych i odtwarzanie z nich
- Logi systemowe
- Instalacja oprogramowania i zarządzanie nim
- Sterowniki i jądro systemu
- Konfiguracja dostępu do sieci
- Wyznaczanie tras — routing
- Sprzęt sieciowy
- Rozwiązywanie nazw — DNS
- Sieciowe systemy plików
- Poczta elektroniczna
- Zarządzanie siecią, protokół SNMP
- Hosting WWW
- Graficzny interfejs użytkownika — X Window System
- Podstawy centrów danych



Na katalogowy 6662



Księgarnia internetowa:
http://helion.pl



Zamówienia telefoniczne:
0 801 339900
0 601 339900

helion.pl
Internetowa Księgarnia

Sprawdź najnowsze promocje:
• <http://helion.pl/promocje>
Kupując wyznaczony czasami:
• <http://helion.pl/promocje>
Zamów informacje o nowościach:
• <http://helion.pl/glosnosc>



Helion

Helion Sp. z o.o.
ul. Akademicka 14, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
<http://helion.pl>



PREMIUM HALL



KOD KREZYDŁO

Cena 199,00 zł

ISBN 978-83-246-2968-8



9 788324 629688

Informatyka w najlepszym wydaniu