

Unix i Linux : przewodnik administratora systemów / Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley, Dan Mackin, James Garnett, Fabrizio Branca, Adrian Mouat. – Wydanie V. – Gliwice, copyright © 2018

Spis treści

Pamięci Evi	35
Wstęp	37
Słowo wstępne	39
Podziękowania	41
I. PODSTAWY ADMINISTROWANIA	
1 Od czego zacząć?	45
1.1. Podstawowe obowiązki administratora	46
Kontrola dostępu	46
Podłączanie sprzętu	46
Automatyzacja zadań	47
Nadzorowanie kopii zapasowych	47
Instalacja i aktualizowanie oprogramowania	47
Monitorowanie	48
Rozwiązywanie problemów	48
Zarządzanie lokalną dokumentacją	48
Uważne monitorowanie stanu zabezpieczeń	48
Dostosowywanie wydajności	49
Opracowanie polityki serwera	49
Współpraca z dostawcami	49
Udzielanie pomocy użytkownikom	49
1.2. Podstawowe narzędzia administratora	50
1.3. Dystrybucje systemu Linux	51
1.4. Przykładowe systemy używane w tej książce	52
Przykładowe dystrybucje systemu Linux	53
Przykładowa dystrybucja systemu Unix	54
1.5. Notacja i konwencje typograficzne	54
1.6. Jednostki	56
1.7. Strony podręcznika systemowego i inne rodzaje dokumentacji	57
Organizacja podręcznika systemowego	57
man — czytanie stron podręcznika systemowego	58
Miejsce przechowywania stron podręcznika	58
1.8. Inna dokumentacja autorytatywna	59

Przewodniki dotyczące określonych systemów	59
Dokumentacja dotycząca określonych pakietów	59
Książki	60
RFC i inne dokumenty internetowe	60
1.9. Inne źródła informacji	60
Bądź na bieżąco	61
Dokumenty HOWTO i witryny informacyjne	61
Konferencje	62
1.10. Sposoby wyszukiwania i instalacji oprogramowania	62
Jak sprawdzić, czy oprogramowanie jest już zainstalowane?	63
Instalowanie nowego oprogramowania	64
Instalacja oprogramowania ze źródeł	66
Instalacja ze skryptu WWW	67
1.11. Gdzie hostować?	68
1.12. Specjalizacje i dyscypliny pokrewne	69
DevOps	69
Inżynierowie ds. niezawodności	69
Inżynierowie ds. bezpieczeństwa	69
Administratorzy sieci	69
Administratorzy baz danych	70
Inżynierowie sieciowych centrów operacyjnych	70
Technicy centrów danych	70
Architekci	70
1.13. Zalecana literatura	70
Administracja systemu i DevOps	71
Niezbędne narzędzia	71
2 Rozruch i demony zarządzania systemem	73
2.1. Przegląd procesu rozruchowego	74
2.2. Oprogramowanie sprzętowe systemu	75
BIOS a UEFI	75
BIOS	76
UEFI	76
2.3. Programy rozruchowe	78
2.4. GRUB	78
Konfiguracja programu GRUB	79
Wiersz poleceń programu GRUB	80
Opcje jądra systemu Linux	80
2.5. Rozruch systemu FREEBSD	81
Ścieżka BIOS-u — BOOT()	81
Ścieżka UEFI	82
Konfiguracja programu loader	83
Polecenia programu loader	83
2.6. Demony zarządzania systemem	83
Zadania procesu init	84

Implementacje procesu init	85
Tradycyjny init	85
systemd kontra reszta świata	86
init osądzony i przykładowie ukarany	86
2.7. systemd w szczegółach	87
Jednostki i pliki jednostek	87
systemctl — zarządzanie systemd	88
Statusy jednostek	89
Jednostki celu	91
Zależności pomiędzy jednostkami	93
Kolejność wykonywania	94
Przykład bardziej złożonego pliku jednostki	94
Usługi lokalne i dostosowywanie	95
Zastrzeżenia związane z usługami i kontrolą rozruchu	96
Rejestrowanie zdarzeń w systemd	98
2.8. init i skrypty startowe w systemie FreeBSD	99
2.9. Procedury ponownego uruchamiania i zamykania systemu	101
Wyłączanie fizycznych systemów	101
Wyłączanie systemów chmurowych	101
2.10. Strategie postępowania w przypadku problemów z rozruchem	102
Tryb pojedynczego użytkownika	102
Tryb pojedynczego użytkownika w systemie FreeBSD	104
Tryb pojedynczego użytkownika z programem GRUB	104
Odzyskiwanie systemów chmurowych	104
3 Kontrola dostępu i uprawnienia administratora	107
3.1. Standardowa kontrola dostępu w systemie Unix	108
Kontrola dostępu w systemie plików	109
Prawa własności do procesów	109
Konto użytkownika root	110
setuid i setgid	111
3.2. Zarządzanie kontem użytkownika Root	111
Logowanie na konto użytkownika root	111
su — zmiana tożsamości użytkownika	112
sudo — su z ograniczeniami	113
Wyłączanie konta użytkownika root	120
Konta systemowe inne niż root	121
3.3. Rozszerzenia standardowego modelu kontroli dostępu	122
Wady modelu standardowego	122
PAM	123
Kerberos — sieciowe uwierzytelnianie kryptograficzne	124
Listy kontroli dostępu do systemu plików	124
Możliwości systemu Linux	124
Przestrzenie nazw w systemie Linux	125
3.4. Nowoczesne mechanizmy kontroli dostępu	125

Oddzielne ekosystemy	126
Obowiązkowa kontrola dostępu (MAC)	126
Kontrola dostępu oparta na rolach	127
Security-enhanced Linux (SELinux)	128
AppArmor	129
3.5. Zalecana literatura	131
4 Kontrolowanie procesów	133
4.1. Elementy składowe procesu	134
PID — numer identyfikacyjny procesu	134
PPID — identyfikator procesu macierzystego	135
UID i EUID — rzeczywisty i efektywny identyfikator użytkownika	135
GID i EGID — rzeczywisty i efektywny identyfikator grupy	136
Uprzejmość	136
Terminal sterujący	136
4.2. Cykl życia procesu	137
Sygnały	137
Polecenie kill — wysłanie sygnałów	140
Stany procesów i wątków	141
4.3. Polecenie ps — monitorowanie procesów	142
4.4. Interaktywne monitorowanie procesów — polecenie top	144
4.5. Polecenia nice i renice — zmiana priorytetów przełączania	146
4.6. System plików /proc	147
4.7. Siedzenie sygnałów i funkcji systemowych — polecenia strace i truss	148
4.8. Procesy niekontrolowane	150
4.9. Procesy okresowe	152
cron — harmonogram poleceń	152
Powszechne zastosowania zaplanowanych zadań	160
5 System plików	163
5.1. Ścieżki dostępu	165
5.2. Montowanie i odmontowywanie systemów plików	166
5.3. Organizacja drzewa plików	168
5.4. Typy plików	171
Zwykłe pliki	172
Katalogi	172
Dowiązania twarde	173
Pliki urządzeń znakowych i blokowych	173
Gniazda lokalne	174
Nazwane potoki	175
Dowiązania symboliczne	175
5.5. Atrybuty plików	176
Bity uprawnień	176
Bity setuid i setgid	177

Bit lepkości	177
Polecenie ls — wyświetlanie listy i sprawdzanie plików	177
Polecenie chmod — zmiana uprawnień	179
Polecenia chown i chgrp — zmiana właściciela i grupy	181
Polecenie umask — ustawianie uprawnień domyślnych	181
Dodatkowe opcje w systemie Linux	182
5.6. Listy kontroli dostępu (ACL)	183
Mała uwaga	184
Rodzaje ACL	184
Implementacje ACL	185
Obsługa ACL w systemie Linux	186
Obsługa ACL w systemie FreeBSD	186
Listy ACL w stylu POSIX	186
Listy ACL w stylu NFSv4	190
6 Oprogramowanie — instalacja i zarządzanie	195
6.1. Instalacja systemów operacyjnych	196
Instalacja przez sieć	196
Konfigurowanie PXE	198
Kickstart — zautomatyzowany instalator systemów Red Hat i CentOS	198
Automatyczna instalacja przy użyciu instalatora Ubuntu	201
Rozruch sieciowy przy użyciu narzędzia Cobbler, linuksowego serwera uruchomieniowego typu open source	203
Automatyzacja instalacji FreeBSD	203
6.2. Zarządzanie pakietami	204
6.3. Systemy zarządzania pakietami w Linuksie	206
rpm — zarządzanie pakietami RPM	206
dpkg — zarządzanie pakietami .deb	207
6.4. Wysokopoziomowe systemy zarządzania pakietami w systemie Linux	208
Repozytoria z pakietami	209
RHN — Red Hat Network	210
APT — Advanced Package Tool	210
Konfigurowanie repozytorium	212
Przykład pliku /etc/apt/sources.list	212
Własny serwer lustrzany jako lokalne repozytorium	213
Automatyzacja APT	214
yum — zarządzanie wydaniem opartym na formacie RPM	215
6.5. Zarządzanie oprogramowaniem w systemie FreeBSD	215
System bazowy	216
pkg — menedżer pakietów FreeBSD	217
Kolekcja portów	218
6.6. Lokalizowanie i konfigurowanie oprogramowania	219
Organizacja procesu lokalizowania	219
Strukturyzacja aktualizacji	220

Ograniczanie pola gry	220
Testowanie	221
6.7. Zalecana literatura	221
7 Pisanie skryptów i powłoka	223
7.1. Filozofia pisania skryptów	224
Pisz mikroskrypty	224
Poznaj dobrze kilka narzędzi	225
Automatyzuj wszystko	226
Nie optymalizuj przedwcześnie	226
Wybierz właściwy język skryptowy	227
Reguły poprawnego pisania skryptów	228
7.2. Podstawy powłoki	230
Edycja poleceń	231
Potoki i przekierowania	231
Zmienne i oznakowanie	233
Zmienne środowiskowe	234
Popularne polecenia filtrujące	235
7.3. Skrypty w powłoce sh	238
Wykonywanie poleceń	239
Od poleceń do skryptów	240
Wejście i wyjście	242
Spacje w nazwach plików	243
Argumenty wiersza poleceń i funkcje	243
Przeptyw sterowania	245
Pętle	247
Działania arytmetyczne	249
7.4. Wyrażenia regularne	249
Proces dopasowywania	250
Znaki dosłowne	250
Znaki specjalne	250
Przykłady wyrażeń regularnych	252
Przechwytywanie	253
Zachłanność, lenistwo i katastrofalne wycofania	254
7.5. Programowanie w języku Python	255
Python 3	255
Python 2 czy Python 3?	256
Python — szybki start	256
Obiekty, łańcuchy, liczby, listy, słowniki, krotki i pliki	258
Przykład sprawdzania poprawności wejścia	260
Pętle	261
7.6. Programowanie w języku Ruby	262
Instalacja	263
Ruby — szybki start	263
Bloki	265

Symbole i hasze opcji	266
Wyrażenia regularne w języku Ruby	267
Ruby jako filtr	268
7.7. Zarządzanie bibliotekami i środowiskiem języków Python i Ruby	269
Wyszukiwanie i instalowanie pakietów	269
Tworzenie odtwarzalnych środowisk 270 Wiele środowisk	271
7.8. Kontrola wersji przy użyciu Git	274
Przykład prostego repozytorium Git	276
Zastrzeżenia dotyczące Git	278
Społecznościowe tworzenie kodu z systemem Git	278
7.9. Zalecana literatura	279
Powłoki i tworzenie skryptów	279
Wyrażenia regularne	280
Python	280
Ruby	281
8 Zarządzanie użytkownikami	283
8.1. Mechanika konta	284
8.2. Plik etc/passwd	285
Nazwa użytkownika	285
Zaszyfrowane hasło	286
Numer UID (identyfikator użytkownika)	288
Domyślne numery GID	289
Pole GECOS	289
Katalog domowy	290
Powłoka logowania	290
8.3. Plik /etc/shadow w systemie Linux	290
8.4. Pliki /etc/master.passwd i /etc/login.conf w systemie FreeBSD	292
Plik /etc/master.passwd 292 Plik /etc/login.conf	293
8.5. Plik/etc/group	294
8.6. Ręczne dodawanie użytkowników	296
Edycja plików passwd i group	296
Ustawianie hasła	297
Tworzenie katalogu domowego i instalowanie plików startowych	298
Ustawianie uprawnień i praw własności do katalogu domowego	300
Konfigurowanie ról i uprawnień administracyjnych	300
Finalizacja	300
8.7. Skrypty do dodawania użytkowników: useradd, ad duser i newusers	301
Polecenie useradd w systemie Linux	301
Polecenie useradd w systemach Debian i Ubuntu	302
Polecenie useradd w systemie FreeBSD	303
Polecenie newusers w systemie Linux — hurtowe dodawanie użytkowników	304
8.8. Bezpieczne usuwanie kont i plików użytkowników	304

8.9. Blokowanie kont użytkowników	305
8.10. Minimalizowanie ryzyka za pomocą PAM	306
8.11. Scentralizowane zarządzanie kontami	307
LDAP a Active Directory	307
Systemy pojedynczego logowania na poziomie aplikacji	307
Systemy zarządzania tożsamością	308
9 Chmura obliczeniowa	311
9.1. Chmura w kontekście	312
9.2. Platformy chmur obliczeniowych	314
Chmury publiczne, prywatne i hybrydowe	314
Amazon Web Services	315
Google Cloud Platform	316
DigitalOcean	316
9.3. Podstawy usługi chmurowej	317
Dostęp do chmury	318
Regiony i strefy dostępności	319
Wirtualne serwery prywatne	320
Sieci	321
Pamięć masowa	321
Tożsamość i autoryzacja	322
Automatyzacja	323
Funkcje bezserwerowe	323
9.4. Wirtualne serwery prywatne — szybki start	324
Amazon Web Services	324
Google Cloud Platform	328
DigitalOcean	329
9.5. Kontrola kosztów	331
9.6. Zalecana literatura	333
10 Rejestrowanie zdarzeń	335
10.1. Położenie plików z dziennikami	338
Specjalne pliki dzienników	338
Przeglądanie dzienników w rejestratorze systemd	340
10.2. Rejestrator systemd	340
Konfiguracja rejestratora systemd	341
Dodatkowe opcje filtrujące rejestratora	342
Współistnienie z programem syslog	343
10.3. syslog	344
Czytanie komunikatów systemu syslog	344
Architektura systemu rsyslog	345
Wersje systemu rsyslog	346
Konfiguracja systemu rsyslog	346
Przykłady pliku konfiguracyjnego	355
Bezpieczeństwo komunikatów systemu syslog	357

Diagnostyka konfiguracji systemu syslog	359
10.4. Rejestrowanie komunikatów jądra i uruchamiania systemu	359
10.5. Pliki dzienników — zarządzanie i ratowanie	360
logrotate — międzyplatformowe zarządzanie dziennikami	360
newsyslog — zarządzanie dziennikami w systemie FreeBSD	362
10.6. Zarządzanie dziennikami na dużą skalę	362
Zestaw narzędzi ELK	362
Graylog	363
Rejestrowanie zdarzeń jako usługa	363
10.7. Strategie rejestrowania	364
11 Sterowniki i jądro	367
11.1. Obowiązki administratora systemu związane z jądrem	368
11.2. Numerowanie wersji jądra	369
Wersje jądra w systemie Linux	369
Wersje jądra w systemie FreeBSD	370
11.3. Urządzenia i ich sterowniki	370
Pliki urządzeń i numery urządzeń	371
Wyzwania związane z zarządzaniem plikami urządzeń	372
Ręczne tworzenie plików urządzeń	372
Nowoczesne zarządzanie plikami urządzeń	373
Zarządzanie urządzeniami w systemie Linux	373
Zarządzanie urządzeniami w systemie FreeBSD	378
11.4. Konfigurowanie jądra w systemie Linux	380
Dostrajanie parametrów jądra systemu Linux	380
Budowanie własnego jądra	381
Dodawanie sterownika urządzenia w systemie Linux	385
11.5. Konfiguracja jądra w systemie FreeBSD	385
Dostrajanie parametrów jądra FreeBSD	385
Budowanie jądra w systemie FreeBSD	386
11.6. Ładowalne moduły jądra	387
Ładowalne moduły jądra w systemie Linux	387
Ładowalne moduły jądra w systemie FreeBSD	389
11.7. Rozruch	389
Komunikaty rozruchowe systemu Linux	390
Komunikaty rozruchowe systemu FreeBSD	394
11.8. Uruchamianie niestandardowych jąder w chmurze	395
11.9. Błędy jądra	396
Błędy jądra w systemie Linux	397
Panika jądra w systemie FreeBSD	399
11.10. Zalecana literatura	400
12 Drukowanie	401
12.1. CUPS	402
Interfejsy podsystemu drukowania	403

Kolejka drukowania	403
Wiele drukarek i kolejek	404
Instancje drukarek	404
Przeglądanie drukarek sieciowych	404
Filtry	405
12.2. Administracja serwerem CUPS	406
Konfiguracja sieciowego serwera wydruków	407
Automatyczna konfiguracja drukarki	407
Konfiguracja drukarki sieciowej	407
Przykłady konfiguracji drukarek	408
Wyłączenie usługi	408
Inne zadania konfiguracyjne	409
12.3. Rozwiązywanie problemów	409
Ponowne uruchamianie demona wydruku	409
Pliki dzienników	410
Połączenia w drukowaniu bezpośrednim	411
Problemy z drukowaniem sieciowym	411
12.4. Zalecana literatura	412

II. SIECI

13 Sieci TCP/IP	415
13.1. TCP/IP i jego związek z internetem	416
Kto zarządza internetem?	416
Standardy sieciowe i dokumentacja	417
13.2. Podstawy sieci	418
IPv4 i IPv6	419
Pakiety i enkapsulacja	421
Ramkowanie w sieciach Ethernet	422
Maksymalna jednostka transmisji (MTU)	422
13.3. Adresowanie pakietów	423
Adresowanie sprzętowe (MAC)	423
Adresowanie IP	424
„Adresowanie” za pomocą nazw	425
Porty	425
Rodzaje adresów	426
13.4. Adresy IP — szczegółowe informacje	426
Klasy adresów IPv4	427
Podział na podsieci w IPv4	428
Sztuczki i narzędzia do wyliczania podsieci	429
CIDR — bezklasowe trasowanie międzypdomenowe	430
Przydzielanie adresów	431
Adresy prywatne i NAT	431
Adresowanie IPv6	433
13.5. Wyznaczanie tras	437

Tablice tras	438
Przekierowania ICMP	439
13.6. Protokoły ARP (IPv4) i ND (IPv6)	440
13.7. DHCP — protokół dynamicznej konfiguracji hostów	441
Oprogramowanie DHCP	441
Sposób działania DHCP	442
Oprogramowanie DHCP w wersji ISC	443
13.8. Kwestie bezpieczeństwa	444
Przekazywanie pakietów IP	444
Przekierowania ICMP	445
Wybór trasy przez nadawcę	445
Pakiety ping na adres rozgłoszeniowy i inne formy ukierunkowanego rozgłaszania	445
Fałszowanie adresów IP	446
Zapory sieciowe oparte na serwerze	446
Wirtualne sieci prywatne	447
13.9. Podstawowa konfiguracja sieciowa	448
Przypisywanie nazwy komputera i adresu IP	448
Interfejs sieciowy i konfiguracja IP	449
Konfigurowanie tras	451
Konfigurowanie DNS	452
Konfigurowanie sieci w różnych systemach	453
13.10. Sieci w systemie Linux	454
NetworkManager	454
ip — ręczne konfigurowanie sieci	455
Konfigurowanie sieci w systemach Debian i Ubuntu	456
Konfiguracja sieci w systemach Red Hat i CentOS	456
Opcje sprzętu sieciowego w systemie Linux	458
Opcje TCP/IP w systemie Linux	459
Zmienne jądra związane z bezpieczeństwem	461
13.11. Sieci w systemie FreeBSD	461
ifconfig — konfigurowanie interfejsów sieciowych	462
Konfigurowanie sprzętu sieciowego w systemie FreeBSD	462
Konfiguracja sieci w systemie FreeBSD w czasie rozruchu	463
Konfiguracja TCP/IP w systemie FreeBSD	463
13.12. Rozwiązywanie problemów z siecią	464
Polecenie ping — sprawdzenie, czy host jest dostępny	465
Polecenie traceroute — śledzenie pakietów IP	467
Podśluchiwanie pakietów	470
13.13. Monitoring sieci	473
Polecenie smokeping — gromadzenie statystyk polecenia ping	473
iPerf — śledzenie wydajności sieci	474
Cacti — gromadzenie danych i tworzenie wykresów	475
13.14. Zapory sieciowe i NAT	476
iptables w systemie Linux — reguły, łańcuchy i tablice	476

Zapora IPFilter dla systemów Unix	481
13.15. Sieci w chmurze	484
Wirtualna chmura prywatna (VPC) w AWS	484
Sieci w GCP	490
Sieci w DigitalOcean	492
13.16. Zalecana literatura	493
Historia	493
Pozycje klasyczne i biblie	493
Protokoły	493
14 Sprzęt sieciowy	495
14.1. Ethernet — sieć uniwersalna	496
Przesyłanie sygnałów w sieci Ethernet	496
Topologia Ethernetu	498
Skrętka nieekranowana	498
Włókna światłowodowe	500
Łączenie i rozszerzanie sieci Ethernet	501
Autouzgadnianie	503
Power over Ethernet	504
Ramki Jumbo	504
14.2. Sieci bezprzewodowe — internet dla nomadów	505
Standardy bezprzewodowe	505
Klient bezprzewodowy	506
Infrastruktura bezprzewodowa i punkty dostępu	506
Bezpieczeństwo sieci bezprzewodowych	509
14.3. SDN — programowalna sieć komputerowa	509
14.4. Testowanie i diagnostyka sieci	510
14.5. Układanie okablowania	510
Możliwości okablowania skrętką	511
Połączenia do biur	511
Standardy okablowania	511
14.6. Kwestie związane z projektowaniem sieci	512
Architektura sieci a architektura budynku	513
Rozbudowa	513
Przeciążenie	513
Konserwacja i dokumentacja	514
14.7. Kwestie związane z zarządzaniem	514
14.8. Zalecana literatura	515
15 Wyznaczanie tras	517
15.1. Przesyłanie pakietów — szczegóły	518
15.2. Demony i protokoły wyznaczania tras	521
Protokoły wektora odległości	522
Protokoły stanu łączy	523
Miary kosztu	523

Protokoły wewnętrzne i zewnętrzne	524
15.3. Prezentacja protokołów	524
RIP i RIPng — protokół informowania o trasach	524
OSPF — najpierw najkrótsza ścieżka	526
EIGRP — rozszerzony protokół trasowania bramy wewnętrznej	526
BGP — protokół bramy brzegowej	526
15.4. Grupowa koordynacja protokołów wyznaczania tras	527
15.5. Kryteria wyboru strategii wyznaczania tras	527
15.6. Demony trasujące	528
routed — przestarzała implementacja RIP	529
Quagga — dominujący demon trasujący	529
XORP — router w komputerze	530
15.7. Routery Cisco	530
15.8. Zalecana literatura	533
16 DNS — system nazw domenowych	535
16.1. Architektura DNS	536
Zapytania i odpowiedzi	536
Dostawcy usług DNS	537
16.2. Wyszukiwania w DNS	538
resolv.conf — konfigurowanie resolvera klienta	538
nsswitch.conf — kogo zapytać o nazwę?	538
16.3. Przestrzeń nazw DNS	539
Rejestracja nazwy domeny	540
Tworzenie własnych poddomen	540
16.4. Jak działa DNS	541
Serwery nazw	541
Serwery autorytatywne i buforujące	542
Serwery rekurencyjne i nierekurencyjne	542
Rekordy zasobów	543
Delegowania	543
Buforowanie i efektywność	545
Odpowiedzi wielokrotne i równoważenie obciążenia DNS metodą	
Round Robin	545
Diagnostyka przy użyciu narzędzi do odpytywania	546
16.5. Baza danych DNS	549
Polecenia dla analizatora w plikach strefowych	549
Rekordy zasobów	550
Rekord SOA	553
Rekordy NS	555
Rekordy A	556
Rekordy AAAA	556
Rekordy PTR	557
Rekordy MX	558
Rekordy CNAME	559

Rekordy SRV	560
Rekordy TXT	561
Rekordy SPF, DKIM i DMARC	562
Rekordy DNSSEC	562
16.6. Oprogramowanie BIND	562
Komponenty BIND	563
Pliki konfiguracyjne	563
Instrukcja include	565
Instrukcja options	565
Instrukcja acl	571
Instrukcja key (TSIG)	571
Instrukcja server	572
Instrukcja masters	573
Instrukcja logging	573
Instrukcja statistics-channels	573
Instrukcja zone	574
Instrukcja controls dla rndc	577
16.7. Rozdzielony DNS i instrukcja view	578
16.8. Przykłady konfiguracji BIND	580
Strefa localhost	580
Mała firma zajmująca się sprawami bezpieczeństwa	581
16.9. Aktualizowanie plików strefowych	584
Przesyłanie informacji strefowych	584
Automatyczne aktualizacje	585
16.10. Kwestie związane z bezpieczeństwem DNS	587
Nowe spojrzenie na listy kontroli dostępu w BIND	588
Otwarty resolver	589
Uruchamianie w środowisku chroot	590
Bezpieczna komunikacja między serwerami za pomocą TSIG i TKEY	590
Konfigurowanie TSIG dla BIND	591
DNSSEC	593
Strategia dotycząca DNSSEC	594
Rekordy zasobów DNSSEC	594
Włączanie DNSSEC	596
Generowanie par kluczy	596
Podpisywanie stref	598
Łańcuch zaufania DNSSEC	600
Wymiana kluczy DNSSEC	600
Narzędzia DNSSEC	601
Usuwanie błędów w DNSSEC	603
16.11. Diagnostyka systemu BIND	604
Rejestrowanie w BIND	604
Sterowanie serwerem nazw za pomocą rndc	610
Wyszukiwanie niepoprawnych delegowań z poziomu wiersza poleceń	611
16.12. Zalecana literatura	613

Książki i inna dokumentacja	613
Zasoby sieciowe	613
Dokumenty RFC	613
17 Systemy pojedynczego logowania	615
17.1. Podstawowe elementy SSO	616
17.2. LDAP — „lekkie” usługi katalogowe	617
Zastosowania LDAP	618
Struktura danych w katalogu LDAP	618
OpenLDAP — tradycyjna implementacja serwera LDAP na licencji open source	620
389 Directory Server — alternatywna implementacja serwera LDAP na licencji open source	620
Zapytania LDAP	621
Konwertowanie plików passwd i group do LDAP	622
17.3. Wykorzystanie usług katalogowych do logowania	623
Kerberos	623
Demon sssd	626
Plik nsswitch.conf	627
PAM — uniwersalny mechanizm uwierzytelniania	627
Przykład konfiguracji PAM	629
17.4. Rozwiązania alternatywne	630
NIS — Network Information Service	630
rsync — bezpieczniejszy transfer plików	631
17.5. Zalecana literatura	631
18 Poczta elektroniczna	633
18.1. Architektura systemów obsługi poczty elektronicznej	634
Klienci poczty	635
System przyjmujący	635
System transportowy	636
System dostarczania lokalnego	636
Skrzynki pocztowe	637
Systemy dostępne	637
18.2. Anatomia wiadomości pocztowej	637
18.3. Protokół SMTP	640
Wysłałeś mi EHLO	640
Kody błędów SMTP	641
Uwierzytelnianie SMTP	642
18.4. Mechanizmy antyspamowe i antywirusowe	643
Oszustwa	643
SPF i Sender ID	644
DKIM	644
18.5. Prywatność i szyfrowanie	645
18.6. Aliasy pocztowe	646

Odczyt aliasów z plików	648
Wysyłanie wiadomości do plików	648
Wysyłanie wiadomości do programów	649
Budowanie bazy aliasów	649
18.7. Konfiguracja serwera poczty	649
18.8. Sendmail	651
Plik switch	652
Uruchamianie serwera sendmail	652
Kolejki pocztowe	654
Konfiguracja serwera sendmail	655
Preprocesor m4	655
Elementy konfiguracji serwera sendmail	656
Plik konfiguracyjny zbudowany z przykładowego pliku .mc	657
Elementy konfiguracji	658
Tabele i bazy danych	658
Makra i funkcje ogólnego zastosowania	659
Konfiguracja klienta	664
Opcje konfiguracyjne m4	665
Mechanizmy antyspamowe serwera sendmail	667
Serwer sendmail i bezpieczeństwo	670
Testowanie i diagnostyka serwera sendmail	676
18.9. Exim	678
Instalacja serwera Exim	679
Uruchamianie serwera Exim	681
Narzędzia serwera Exim	681
Język konfiguracji serwera Exim	682
Plik konfiguracyjny serwera Exim	683
Opcje globalne	684
ACL (ang. access control lists)	686
Skanowanie treści na etapie ACL	689
Mechanizmy uwierzytelniające	689
Routery	690
Transporty	693
Konfiguracja ponowień	694
Konfiguracja przepisywania	695
Lokalna funkcja skanująca	695
Zapisywanie dzienników	695
Diagnostyka	696
18.10. Postfix	697
Architektura serwera Postfix	697
Bezpieczeństwo	699
Polecenia i dokumentacja serwera Postfix	699
Konfiguracja serwera Postfix	700
Domeny wirtualne	704
Kontrola dostępu	706

Diagnostyka	709
18.11. Zalecana literatura	710
Literatura na temat serwera sendmail	710
Literatura na temat serwera Exim	711
Literatura na temat serwera Postfix	711
Dokumenty RFC	711
19 Hosting WWW	713
19.1. Protokół HTTP	714
URL — jednolity lokalizator zasobu	715
Struktura transakcji HTTP	716
curl — HTTP z wiersza poleceń	718
Ponowne użycie połączenia TCP	719
HTTP przez TLS	720
Wirtualne hosty	720
19.2. Podstawy oprogramowania WWW	721
Serwery WWW i oprogramowanie pośredniczące w ruchu HTTP	722
Balansery obciążenia	723
Pamięć podręczna	725
Sieci dostarczania treści (CDN)	728
Języki sieci WWW	729
Interfejsy programowania aplikacji (API)	731
19.3. Hosting WWW w chmurze	733
Budowa kontra zakup	733
Platforma jako usługa	734
Hosting treści statycznych	735
Bezserwerowe aplikacje WWW	735
19.4. Apache httpd	736
httpd w praktyce	736
Ustawienia konfiguracyjne httpd	737
Konfigurowanie hostów wirtualnych	739
Rejestrowanie zdarzeń	742
19.5. NGINX	743
Instalacja i uruchamianie serwera NGINX	743
Konfigurowanie serwera NGINX	744
Konfigurowanie TLS dla serwera NGINX	747
Równoważenie obciążenia z serwerem NGINX	747
19.6. HAProxy	748
Kontrolowanie stanu serwera	749
Statystyki serwera	750
Lepkie sesje	750
Terminacja TLS	751
19.7. Zalecana literatura	752

III. PAMIĘĆ MASOWA

20 Pamięć masowa	755
20.1. Chcę tylko dodać dysk!	756
Linux	757
FreeBSD	758
20.2. Urządzenia pamięci masowej	759
Dyski twarde	760
Dyski SSD	763
Dyski hybrydowe	766
Technologia Advanced Format i 4-kilobajtowe bloki	767
20.3. Interfejsy urządzeń pamięci masowej	768
Interfejs SATA	768
Interfejs PCI Express	768
Interfejs SAS	769
USB	770
20.4. Podłączanie i niskopoziomowa obsługa dysków	771
Weryfikacja instalacji na poziomie sprzętowym	771
Pliki urządzeń dyskowych	772
Formatowanie i zarządzanie uszkodzonymi blokami	773
Bezpieczne wymazywanie dysków ATA	774
hdparm i camcontrol — ustawianie parametrów dysku i interfejsu	775
Monitorowanie dysku twardego za pomocą SMART	776
20.5. Obieranie cebuli, czyli programowa strona pamięci masowej	777
Elementy systemu pamięci masowej	777
Mapper urządzeń w systemie Linux	779
20.6. Partycjonowanie dysków	780
Tradycyjne partycjonowanie	781
Partycje MBR	782
GPT — tablica partycji GUID	783
Partycjonowanie w systemie Linux	784
Partycjonowanie w systemie FreeBSD	784
20.7. Zarządzanie woluminami logicznymi	784
Zarządzanie woluminami logicznymi w systemie Linux	785
Zarządzanie woluminami logicznymi w systemie FreeBSD	790
20.8. RAID — nadmiarowa macierz niedrogich dysków	790
RAID programowy a sprzętowy	790
Poziomy RAID	791
Przywracanie dysku po awarii	794
Wady RAID 5	794
mdadm — programowy RAID w systemie Linux	795
20.9. Systemy plików	799
20.10. Tradycyjne systemy plików — UFS, ext4 i XFS	800
Terminologia systemu plików	801
Polimorfizm systemu plików	802
Formatowanie systemu plików	802

fsck — sprawdzanie i naprawa systemu plików	802
Montowanie systemu plików	804
Ustawianie automatycznego montowania	804
Montowanie napędów USB	807
Zalecenia dotyczące obszaru wymiany	807
20.11. Systemy plików następnej generacji: ZFS i Btrfs	808
Kopiowanie przy zapisie	808
Wykrywanie błędów	809
Wydajność	809
20.12. ZFS — rozwiązanie wszystkich problemów z pamięcią masową	810
ZFS w systemie Linux	810
Architektura ZFS	811
Przykład: dodawanie dysków	812
Systemy plików i ich właściwości	812
Dziedziczenie właściwości	814
Osobne systemy plików dla każdego użytkownika	815
Kopie migawkowe i klony	815
Surowe woluminy	816
Zarządzanie pulą pamięci masowej	817
20.13. Btrfs — ograniczona wersja ZFS dla systemu Linux	819
Btrfs kontra ZFS	819
Konfigurowanie i konwertowanie pamięci masowej	820
Woluminy i podwoluminy	822
Migawki woluminów	823
Płytkie kopie	823
20.14. Strategia tworzenia kopii zapasowych	824
20.15. Zalecana literatura	825
21 NFS	827
21.1. Sieciowe systemy plików	828
Współzawodnictwo	828
Kontrola stanu	829
Problemy wydajności	829
Bezpieczeństwo	830
21.2. NFS	830
Wersje protokołu	831
Zdalne wywoływanie procedur	832
Protokoły transportowe	832
Stan	832
Eksporty systemu plików	833
Blokowanie plików	834
Bezpieczeństwo	834
Odwzorowanie tożsamości w wersji 4.	836
Dostęp z uprawnieniami root i konto nobody	837
Wydajność w wersji 4.	838

21.3. Serwery NFS	838
Plik exports w Linuksie	839
Plik exports w systemie FreeBSD	841
Demon nfsd	842
21.4. NFS po stronie klienta	844
Montowanie zdalnych systemów plików podczas rozruchu systemu	846
Ograniczanie eksportów do uprzywilejowanych portów	847
21.5. Odwzorowanie tożsamości w NFSv4	847
21.6. Statystyki połączeń NFS — nfsstat	848
21.7. Dedykowane serwery plików NFS	848
21.8. Montowanie automatyczne	849
Odwzorowania pośrednie	851
Odwzorowania bezpośrednie	851
Odwzorowania główne	851
Odwzorowania wykonywalne	852
Widoczność zasobów montowanych automatycznie	852
Automount i replikowane systemy plików	853
Automatyczne użycie mechanizmu automount (wersja 3., wszystkie systemy oprócz Linuksa)	854
Specyfika Linuksa	854
21.9. Zalecana literatura	855
22 SMB	857
22.1. Samba — serwer SMB dla systemów Unix	858
22.2. Instalacja i konfigurowanie serwera Samba	859
Współdzielenie plików z uwierzytelnianiem lokalnym	860
Współdzielenie plików za pomocą kont uwierzytelnianych przez Active Directory	861
Konfigurowanie udziałów	861
22.3. Montowanie plików udostępnionych przez SMB	863
22.4. Przeglądanie plików udostępnionych przez SMB	864
22.5. Zapewnienie bezpieczeństwa Samby	865
22.6. Usuwanie problemów z systemem Samba	865
Sprawdzanie stanu Samby za pomocą smbstatus	865
Konfigurowanie rejestrowania zdarzeń w Sambie	866
Zarządzanie zestawami znaków	867
22.7. Zalecana literatura	868
IV. OPERACJE	
23 Zarządzanie konfiguracją	871
23.1. Zarządzanie konfiguracją w pigułce	872
23.2. Niebezpieczeństwa związane z zarządzaniem konfiguracją	873
23.3. Elementy zarządzania konfiguracją	873
Operacje i parametry	874

Zmienne	875
Fakty	876
Obsługa zmian	876
Powiązania	876
Paczki i repozytoria paczek	877
Środowiska	877
Ewidencjonowanie i rejestracja klientów	878
23.4. Porównanie popularnych systemów CM	879
Terminologia	880
Modele biznesowe	880
Opcje architekuralne	880
Opcje językowe	883
Opcje zarządzania zależnościami	884
Ogólne uwagi na temat systemu Chef	886
Ogólne uwagi na temat systemu Puppet	886
Ogólne uwagi na temat systemów Ansible i Salt	887
YAML	887
23.5. Wprowadzenie do systemu Ansible	889
Ansible na przykładzie	890
Ustawienia klienta	892
Grupy klientów	894
Przypisywanie zmiennych	895
Grupy dynamiczne i obliczane	895
Listy zadań	896
Parametry state	898
Iteracja	898
Interakcja z Jinja	899
Generowanie szablonów	899
Powiązania — akcje i scenariusze	900
Role	902
Zalecenia dotyczące ustrukturyzowania bazy konfiguracyjnej	903
Opcje dostępu Ansible	904
23.6. Wprowadzenie do systemu Salt	906
Ustawianie sługi	908
Powiązania wartości zmiennych dla sług	909
Dopasowywanie sług	910
Stany w systemie Salt	912
Salt i Jinja	913
Identyfikatory stanów i zależności	914
Funkcje stanowe i wykonawcze	916
Parametry i nazwy	917
Powiązania stanów ze sługami	919
Wysokie stany	920
Formuły Salt	921
Środowiska	921

Mapa drogowa dokumentacji	925
23.7. Porównanie systemów Ansible i Salt	926
Elastyczność i skalowalność procesu wdrażania	926
Wbudowane moduły i rozszerzalność	927
Bezpieczeństwo	927
Różności	928
23.8. Wzorce postępowania	929
23.9. Zalecana literatura	931
24 Wirtualizacja	933
24.1. Terminologia wirtualizacji	934
Hipernadzorcy	934
Migracja w locie	937
Obrazy maszyn wirtualnych	937
Konteneryzacja	938
24.2. Wirtualizacja w Linuksie	939
Xen	939
Instalacja gości w Xen	940
KVM	942
Instalacja gości w KVM	942
24.3. Bhyve w systemie FreeBSD	943
24.4. VMware	943
24.5. VirtualBox	944
24.6. Packer	944
24.7. Vagrant	946
24.8. Zalecana literatura	947
25 Kontenery	949
25.1. Pojęcia ogólne i podstawowe	950
Obsługa przez jądro	951
Obrazy	951
Sieć	952
25.2. Docker — silnik kontenerowy typu open source	953
Podstawowa architektura	953
Instalacja	955
Konfigurowanie klienta	955
Praca z kontenerem	956
Woluminy	959
Kontenery danych	960
Sieci w Dockerze	961
Sterowniki pamięci masowej	963
Opcje dockerd	964
Budowanie obrazów	966
Repozytoria	969
25.3. Kontenery w praktyce	971

Rejestrowanie zdarzeń	972
Porady dotyczące bezpieczeństwa	972
Rozwiązywanie problemów i usuwanie błędów	975
25.4. Grupowanie kontenerów i zarządzanie nimi	976
Krótki przegląd oprogramowania do zarządzania kontenerami	977
Kubernetes	977
Mesos i Marathon	978
Docker Swarm	979
ECS — obsługa kontenerów EC2 w AWS	980
25.5. Zalecana literatura	981
26 Ciągła integracja i ciągłe dostarczanie	983
26.1. Podstawy CI/CD	985
Zasady i praktyki	985
Środowiska	988
Przełączniki funkcji	989
26.2. Potoki	990
Proces budowania	990
Testowanie	991
Wdrażanie	993
Techniki wdrażania bez przestojów	994
26.3. Jenkins — serwer automatyzacji typu open source	995
Podstawowe pojęcia związane z Jenkinsem	995
Rozproszone procesy budowania	997
Potok jako kod	997
26.4. CI/CD w praktyce	998
UlsahGo, trywialna aplikacja internetowa	999
Testowanie jednostkowe UlsahGo	1000
Pierwsze kroki z potokiem Jenkinsa	1001
Budowanie obrazu DigitalOcean	1003
Zapewnienie pojedynczego systemu do testowania	1005
Testowanie kropli	1008
Wdrażanie UlsahGo do pary kropli i balansera obciążenia	1008
Zamknięcie potoku demonstracyjnego	1010
26.5. Kontenery a CI/CD	1010
Kontenery jako środowisko budowania	1011
Obrazy kontenerów jako artefakty budowania	1011
26.6. Zalecana literatura	1012
27 Bezpieczeństwo	1013
27.1. Elementy bezpieczeństwa	1015
27.2. Drogi do naruszenia bezpieczeństwa	1015
Socjotechnika	1015
Podatności oprogramowania	1016
Rozproszona odmowa usługi (DDoS)	1017

Nadużycia wewnętrzne	1018
Błędy konfiguracji sieci, systemu lub aplikacji	1018
27.3. Podstawowe środki bezpieczeństwa	1019
Aktualizacje oprogramowania	1019
Zbędne usługi	1020
Zdalne logowanie zdarzeń	1021
Kopie zapasowe	1021
Wirusy i robaki	1021
Rootkity	1022
Filtrowanie pakietów	1022
Hasła i uwierzytelnianie wieloskładnikowe	1023
Czułość	1023
Testy penetracyjne aplikacji	1024
27.4. Hasła i konta użytkowników	1024
Zmiany haseł	1025
Menedżery haseł	1025
Okres ważności haseł	1027
Konta współużytkowane	1027
Programy powłoki	1028
Użytkownicy typu root	1028
27.5. Narzędzia bezpieczeństwa	1028
Skaner portów sieciowych nmap	1028
Nessus — skaner sieciowy następnej generacji	1030
Metasploit — oprogramowanie do testów penetracyjnych	1031
Lynis — podręczny audyt bezpieczeństwa	1031
Wyszukiwanie słabych haseł — John the Ripper	1031
Programowalny system wykrywania włamań sieciowych — Bro	1032
Popularny system wykrywania włamań — Snort	1033
Wykrywanie włamań na poziomie hosta — OSSEC	1033
Fail2Ban — system reagowania na ataki brute-force	1036
27.6. Narzędzia kryptograficzne	1036
Kryptografia klucza symetrycznego	1037
Kryptografia klucza publicznego	1037
Infrastruktura klucza publicznego	1038
TLS	1040
Kryptograficzne funkcje skrótu	1040
Generowanie liczb losowych	1042
Wybór oprogramowania kryptograficznego	1043
Polecenie openssl	1043
PGP — Pretty Good Privacy	1045
Kerberos — zunifikowane podejście do bezpieczeństwa sieciowego	1046
27.7. Bezpieczna zdalna powłoka SSH	1046
Podstawowe elementy OpenSSH	1047
Klient ssh	1048
Uwierzytelnianie za pomocą klucza publicznego	1050

ssh-agent	1051
Aliasy hostów w pliku ~/.ssh/config	1052
Multipleksacja połączeń	1053
Przekierowywanie portów	1054
sshd — serwer OpenSSH	1055
Weryfikacja klucza hosta za pomocą SSHFP	1056
Przesyłanie plików	1057
Inne metody bezpiecznego logowania	1057
27.8. Zapory sieciowe	1058
Zapory filtrujące pakiety	1058
Filtrowanie usług	1058
Zapory z kontrolą stanu	1059
Poziom bezpieczeństwa oferowany przez zapory sieciowe	1059
27.9. VPN (ang. Virtual Private Network)	1060
Tunelowanie IPsec	1060
Czy sam VPN wystarczy?	1061
27.10. Certyfikacja i standardy	1061
Certyfikacja	1061
Standardy bezpieczeństwa	1062
27.11. Źródła informacji o bezpieczeństwie	1064
SecurityFocus.com oraz listy dyskusyjne BugTraq i OSS	1065
Schneier on Security	1065
Raport firmy Verizon z dochodzeń w sprawach dotyczących naruszenia danych	1065
Instytut SANS	1065
Źródła związane z poszczególnymi dystrybucjami	1066
Inne listy e-mailowe i strony WWW	1066
27.12. Reakcja na atak	1066
27.13. Zalecana literatura	1068
28 Monitoring	1069
28.1. Przegląd monitoringu	1070
Instrumentacja	1071
Rodzaje danych	1071
Pobieranie i przetwarzanie	1072
Powiadomienia	1072
Panele i interfejsy użytkownika	1073
28.2. Kultura monitoringu	1073
28.3. Platformy monitorujące	1074
Platformy czasu rzeczywistego typu open source	1075
Platformy szeregów czasowych typu open source	1076
Platformy open source do tworzenia wykresów	1078
Komercyjne platformy monitorujące	1079
Hostowane platformy monitorujące	1079
28.4. Zbieranie danych	1080

StatsD — ogólny protokół przesyłania danych	1080
Pozyskiwanie danych z wyjścia poleceń	1082
28.5. Monitorowanie sieci	1083
28.6. Monitorowanie systemów	1084
Polecenia dla systemów monitorowania	1085
collectd — pozyskiwanie ogólnych danych systemowych	1086
sysdig i dtrace — śledzenie działań w systemie	1086
28.7. Monitorowanie aplikacji	1087
Monitorowanie dzienników	1087
Supervisor + Munin — proste rozwiązanie dla ograniczonych zastosowań	1088
Komercyjne narzędzia do monitorowania aplikacji	1088
28.8. Monitorowanie bezpieczeństwa	1089
Weryfikowanie integralności systemu	1089
Monitorowanie wykrywania włamań	1090
28.9. Protokół SNMP	1091
Organizacja SNMP	1092
Operacje protokołu SNMP	1093
Net-SNMP — narzędzia dla serwerów	1093
28.10. Kruczki i sztuczki	1095
28.11. Zalecana literatura	1096
29 Wydajność	1097
29.1. Filozofia dostrajania wydajności	1098
29.2. Metody poprawy wydajności	1099
29.3. Czynniki wpływające na wydajność	1101
29.4. Zabieranie cykli procesora	1102
29.5. Analizowanie problemów z wydajnością	1102
29.6. Kontrola wydajności systemu	1103
Inwentaryzacja sprzętu	1103
Gromadzenie danych o wydajności	1105
Analiza użycia procesora	1106
Zarządzanie pamięcią przez system	1108
Analiza użycia pamięci	1109
Analiza obciążenia wejścia-wyjścia	1111
Testowanie wydajności podsystemu dyskowego — program fio	1112
Gromadzenie statystyk w czasie i budowanie raportów — program sar	1113
Wybór planisty operacji wejścia-wyjścia w Linuksie	1113
Szczegółowe profilowanie systemu Linux — program perf	1114
29.7. Pomocy! Mój system nagle bardzo zwolnił!	1115
29.8. Zalecana literatura	1117
30 Podstawy centrów danych	1119
30.1. Szafy	1120
30.2. Zasilanie	1121

Wymagania zasilania szaf	1122
Jednostki mocy — kVA a kW	1123
Wydajność energetyczna	1123
Pomiary	1124
Koszt	1124
Zdalne sterowanie	1124
30.3. Chłodzenie i środowisko	1124
Szacowanie zapotrzebowania na chłodzenie	1125
Gorące i zimne korytarze	1126
Wilgotność	1128
Monitorowanie środowiska	1128
30.4. Poziomy niezawodności centrów danych	1129
30.5. Bezpieczeństwo centrów danych	1129
Lokalizacja	1130
Ogrodzenie	1130
Dostęp do obiektu	1130
Dostęp do szaf	1130
30.6. Narzędzia	1131
30.7. Zalecana literatura	1132
31 Metodologia i reguły w IT	1133
31.1. Teoria wielkiej unifikacji — DevOps	1134
Zasady DevOps	1135
Administracja systemem w świecie DevOps	1138
31.2. Rejestracja zgłoszeń i system zarządzania zgłoszeniami	1139
Funkcje systemów zgłoszeniowych	1140
Przydzielanie zgłoszeń	1140
Akceptacja systemów zgłoszeniowych przez użytkowników	1141
Przykłady systemów zgłoszeniowych	1142
Przydzielanie zgłoszeń	1143
31.3. Utrzymanie lokalnej dokumentacji	1143
Infrastruktura jako kod	1144
Standaryzacja dokumentacji	1144
31.4. Utrzymanie niezależnych środowisk	1146
31.5. Przywracanie systemu po katastrofie	1147
Ocena ryzyka	1147
Plan naprawy	1148
Zespół do zwalczania skutków katastrof	1149
Incydenty bezpieczeństwa	1150
31.6. Reguły i procedury	1151
Różnice między regułami i procedurami	1151
Najlepsze praktyki tworzenia reguł	1152
Procedury	1152
31.7. Definiowanie poziomu usług (SLA)	1153
Zakresy i opisy usług	1154

Reguły ustalania priorytetów zadań	1155
31.8. Zgodność — regulacje i standardy	1156
31.9. Zagadnienia prawne	1159
Ochrona prywatności	1159
Wymuszanie stosowania reguł	1160
Kontrola = odpowiedzialność	1160
Licencje na oprogramowanie	1161
31.10. Organizacje, konferencje i inne zasoby	1162
31.11. Zalecana literatura	1163
Krótką historia administracji systemami	1165
Kolofon	1175
O współpracownikach	1177
O autorach	1179
Skorowidz	1181

oprac. BPK