

Spis treści

Przedmowa	9
Czego się można dowiedzieć z tej książki?	10
Jaki jest układ tej książki?	11
Dedykacja	12
Podziękowania	13
Kontakt z Czytelnikami	14
Usługi dla Czytelników	14
Część I. Instalacja i konfiguracja serwera SUSE	15
Rozdział 1. Instalacja SUSE LINUX Enterprise Server	17
Omówienie metod instalacji	18
Instalacja z CD-ROM-u	19
Instalacja za pomocą programu VNC	20
Instalacja sieciowa	22
Instalacja za pomocą programu AutoYaST	23
Plany przedinstalacyjne	23
Instalacja systemu SLES 9 w 10 łatwych krokach	30
Wybór metody instalacji	30
Wybór języka	31
Wybór ustawień instalacji	31
Przygotowanie dysków twardych	34
Konfiguracja systemu	35
Konfiguracja ustawień sieciowych	35
Przeprowadzanie internetowych aktualizacji	37
Konfiguracja usług	37
Konfiguracja informacji o użytkownikach	38
Konfiguracja sprzętu	40
Rozwiązywanie problemów	41
Podsumowanie	42
Rozdział 2. Aktualizacja serwera	43
Zachowywanie konfiguracji systemu	43
SuSEconfig	43
YaST (Yet another Setup Tool)	45
Dodawanie i usuwanie pakietów	48
Instalowanie pakietu	48
Usuwanie pakietów i podkomponentów	52
Dodawanie i usuwanie urządzeń	55
Przygotowania	56

Instalacja dysku twardego	57
Zmiana konfiguracji sieci	69
Parametry sieci	69
Używanie programu YaST do zarządzania konfiguracją sieci	70
Podsumowanie	75
Rozdział 3. Uruchamianie i zamykanie serwera	77
Programy ładujące	77
LILO	79
Grub	80
Start jądra	83
Proces init i poziomy pracy systemu	84
Zamknięcie systemu	86
Start awaryjny i odzyskiwanie systemu	87
Podsumowanie	89
Część II. Zarządzanie dostępem użytkowników i zabezpieczeniami	91
Rozdział 4. Zarządzanie użytkownikami i grupami	93
Identyfikatory użytkowników i grup	93
Pliki z danymi użytkowników i grup	100
Plik /etc/passwd	100
Plik /etc/shadow	103
Plik /etc/group	105
Aplikacje do zarządzania kontami użytkowników i grup	106
Tworzenie i edytowanie kont użytkowników	108
Ustawianie domyślnych właściwości kont użytkowników	116
Tworzenie i edytowanie grup	119
Zabezpieczenia	121
Stosowanie silnych haseł	122
Audytywanie domyślnych kont	131
Konto roota	131
Użytkownik należący do zbyt wielu grup	133
Podsumowanie	134
Rozdział 5. Zarządzanie środowiskiem użytkownika i jego zabezpieczanie	135
Audytywanie kont	135
Konfiguracja środowiska użytkownika	137
Domyślna powłoka	137
Skrypty logowania i zmienne środowiskowe	141
Zarządzanie zasobami użytkowników	143
Uwierzytelnianie za pomocą PAM	143
Konfiguracja modułów PAM	146
Zarządzanie zasobami	147
Zarządzanie czasem dostępu	149
Zarządzanie kwotami	152
Polecenia su i sudo	159
Podsumowanie	163

Rozdział 6. Bezpieczeństwo systemu plików	165
Uprawnienia do plików i katalogów	165
Zmienianie uprawnień	171
Zmienianie przynależności pliku	174
Uwagi na temat bezpieczeństwa	175
Domyślne uprawnienia dostępu	177
Specjalne uprawnienia do plików	180
Bity SUID/SGID a bezpieczeństwo	182
SGID a udostępnianie plików	184
Przykładowy program SUID	186
Ochrona przed programami SUID	188
Bit lepkości	189
Poszerzone atrybuty	190
Szyfrowanie danych i systemu plików	195
Bezpieczne usuwanie plików	200
Systemy plików z kronikowaniem	202
Podsumowanie	204
Rozdział 7. Zarządzanie systemem i jego monitorowanie	205
Najważniejsze polecenia Linuksa	205
Podstawowe polecenia	206
Dodatkowe narzędzia	207
Najwyższy poziom systemu plików	208
Sprawdzanie i monitorowanie systemu	210
Czas sprawności komputera	211
Przeglądanie dzienników	211
Procesy zajmujące najwięcej zasobów	213
Sprawdzanie aplikacji	215
Sprawdzanie zasobów systemowych	216
Rejestrowanie działalności użytkowników	218
Dostrajanie systemu	222
Dostrajanie parametrów jądra	223
Dostrajanie dostępu do systemu plików	225
Podsumowanie	228
Część III. Instalacja i konfiguracja usług sieciowych	229
Rozdział 8. Usługi sieciowe	231
Anioły i demony	232
Konfiguracja xinetd	233
Plik /etc/xinetd.conf	239
Stosowanie kontroli dostępu	244
Uwagi na temat bezpieczeństwa	245
Usługi czasu sieciowego	246
Konfiguracja klienta NTP	249
Konfiguracja serwera NTP	254
Rozwiązywanie problemów	257
Usługi pocztowe	261

Usługi transferu plików	266
Używanie Pure-FTPd.....	267
Używanie vsftpd	274
Używanie standardowego serwera TFTP	277
Usługi udostępniania plików w sieci	279
Konfiguracja serwera NFS.....	280
Konfiguracja serwera Samba	283
Usługi zdalnego zarządzania	291
Telnet	292
ssh	293
VNC i XDMCP	294
Zabezpieczanie zdalnego zarządzania systemem	295
Ograniczanie połączeń z wybranymi adresami IP	297
Bezpieczne środowisko zarządzania systemem.....	298
Usługi nazw sieciowych	299
Samba.....	299
Protokół SLP.....	299
Domain Name Service (DNS)	300
Dynamic Host Configuration Protocol (DHCP)	303
DNS i DHCP	306
Usługi WWW	306
Usługi uwierzytelniania.....	312
Network Information Services (NIS).....	313
Domeny Samba.....	313
Lightweight Directory Access Protocol (LDAP).....	313
Kerberos.....	314
Podsumowanie.....	315
Rozdział 9. Usługi drukowania	317
Konfiguracja drukarki.....	317
Drukarki lokalne	318
Drukarki sieciowe	319
Instalowanie drukarki lokalnej.....	319
Instalowanie drukarki sieciowej	322
Przebieg zadania wydruku.....	325
Buforowanie zadań	325
Stosowanie filtrów	325
Drukowanie informacji	326
Zarządzanie kolejkami.....	326
Konfiguracja kolejki w programie YaST.....	327
Konfiguracja kolejki w wierszu poleceń.....	328
Podstawowe informacje o kolejkach drukowania.....	330
Interfejs WWW usługi CUPS	331
Podsumowanie.....	336
Rozdział 10. Kopie zapasowe i odzyskiwanie danych	337
Strategie tworzenia kopii zapasowych	338
Implementacja strategii tworzenia kopii zapasowych.....	340

Metoda rotacyjna Dziadek-Ojciec-Syn	343
Metoda rotacyjna Wieża Hanoi	344
Kilka sztuczek i podpowiedzi	345
Kopie zapasowe baz danych: na zimno czy na gorąco?	348
Narzędzia do tworzenia kopii zapasowych i odzyskiwania danych	350
Tworzenie plików tarball	351
Archiwizowanie danych za pomocą programu cpio	355
Konwertowanie i kopiowanie danych za pomocą programu dd	358
Programy dump i restore	360
Mirroring danych za pomocą programu rsync	370
Moduły System Backup i Restore programu YaST	373
AMANDA	376
Harmonogram wykonywania kopii zapasowych	379
Komercyjne produkty do tworzenia kopii zapasowych	380
Dyskietki rozruchowe i awaryjne systemu SLES	382
Podsumowanie	384
Część IV. Zabezpieczanie serwera SUSE	385
Rozdział 11. Zagadnienia bezpieczeństwa sieci	387
Zasady bezpieczeństwa w przedsiębiorstwie	388
Bezpieczeństwo fizyczne	391
Konta użytkowników	394
Silne hasła	395
Zdalny dostęp	402
Zapory ogniowe	402
Zasada dopuszczalnego używania systemu	406
Ochrona informacji	408
Reagowanie na incydenty	410
Podsumowanie	411
Rozdział 12. Wykrywanie włamań	413
Definicja włamań	413
Zmniejszanie rozmiarów celu	415
Wykrywanie słabych punktów	416
nmap	417
Nessus	420
Wykrywanie włamań do sieci	428
Wykorzystanie zapory ogniowej do analizy ruchu	428
Systemy wykrywania włamań do sieci	429
Snort	430
ACID (Analysis Console for Intrusion Databases)	432
Wykrywanie włamań na hosty	439
Pliki dziennika	439
chrootkit	440
AIDE (Advanced Intrusion Detection Environment)	441
Dodatkowe narzędzia	446
Narzędzia do wykrywania skanowania	446

Programy MRTG i Cacti.....	447
Ethereal	448
Podsumowanie.....	449
Rozdział 13. Bezpieczeństwo systemu	451
Zasady uszczelniania systemu	452
Centralny serwer syslog.....	454
Uszczelnianie centralnego serwera syslog	456
Ukrywanie serwera syslog	460
Unikanie logowania się jako root	461
Zabezpieczanie usług sieciowych.....	462
Uszczelnianie zdalnych usług	463
Ograniczanie praw usług.....	465
Klatki chroot i User Mode Linux.....	467
Filtrowanie pakietów za pomocą iptables	469
Uszczelnianie fizycznej infrastruktury sieci	473
Bezpieczeństwo w sieciach bezprzewodowych.....	476
Pakiety do uszczelniania systemu.....	487
Automatyzacja uszczelniania systemu SLES	488
Więcej informacji na temat zagrożeń	491
Podsumowanie.....	492
Część V. Dodatki	493
Dodatek A. Certyfikaty bezpieczeństwa	495
Dodatek B. Zasoby	501
Linuksowe edytory tekstu.....	501
Zasoby internetowe.....	506
Internetowe strony związane z Linuxem i bezpieczeństwem	506
Grupy dyskusyjne i strony internetowe związane z systemem SUSE.....	508
Skorowidz.....	509