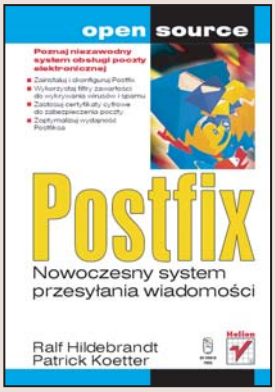
Postfix. Nowoczesny system przesyłania wiadomości



Autorzy: Ralf Hildebrandt, Patrick Koetter
Tłumaczenie: Adam Jarczyk
ISBN: 83-246-0145-7
Tytuł oryginału: The Book of Postfix: State-of-the-Art Message Transport
Format: B5, stron: 496

Poznaj niezawodny system obsługi poczty elektronicznej

- Zainstaluj i skonfiguruj Postfix
- Wykorzystaj filtry zawartości do wykrywania wirusów i spamu
- Zastosuj certyfikaty cyfrowe do zabezpieczenia poczty
- Zoptymalizuj wydajność Postfiksa

Poczta elektroniczna jest głównym nośnikiem informacji w większości firm. Niestety – czyhające na nią zagrożenia, takie jak spam i wirusy, dość skutecznie utrudniają korzystanie z niej. Zbudowanie bezpiecznego i wydajnego systemu do obsługi poczty elektronicznej wymaga zastosowania odpowiedniego oprogramowania. Takim oprogramowaniem niewątpliwie jest Postfix – serwer pocztowy dostępny na licencji open source, opracowany przez pracownika firmy IBM Wietse Venemę. Postfix może pełnić rolę zarówno prostego przekaźnika poczty, jak i serwera w ogromnym przedsiębiorstwie – odpowiednio skonfigurowany stanie się podstawą stabilnego systemu komunikacji.

Książka „Postfix. Nowoczesny system przesyłania wiadomości" odkrywa wszystkie tajniki Postfiksa. Dowiesz się z niej, skąd go pobrać, jak zainstalować i skonfigurować oraz jaką rolę pełnią jego poszczególne pliki i katalogi. Nauczysz się wykorzystywać filtry antywirusowe i antyspamowe, integrować Postfix z bazą danych, szyfrować pocztę za pomocą certyfikatów i automatyzować zadania. Poznasz możliwości Postfiksa i stworzysz w oparciu o niego doskonały system komunikacji.

- Przygotowanie serwera pocztowego
- Określenie rekordów DNS dla serwera poczty
- Konfiguracja Postfiksa dla jednej domeny
- Narzędzia wiersza poleceń w Postfiksie
- Struktura wiadomości e-mail
- Filtrowanie treści za pomocą filtrów wewnętrznych i zewnętrznych
- Współpraca Postfiksa z programem Microsoft Exchange Server
- Domeny wirtualnych skrzynek pocztowych obsługiwane przez bazę danych
- Uwierzytelnianie SMTP
- Korzystanie z protokołu TLS
- Optymalizowanie wydajności serwera pocztowego

Wykorzystaj Postfix do zarządzania pocztą elektroniczną w swojej firmie

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

Spis treści

O autorach **15**

O niniejszej książce **19**

Rozdział 1. Wprowadzenie **23**

Część I Podstawy **25**

Rozdział 2. Przygotowanie hosta i środowiska **27**

Nazwa hosta 28
Łączność 28
Port TCP 25 29
Czas systemowy i znaczniki czasowe 29
Syslog 30
Rozwiązywanie nazw (DNS) 31
DNS dla serwerów poczty 33
Rekordy A 34
Rekordy PTR 34
Rekordy MX 35

Rozdział 3. Serwer poczty dla jednej domeny **37**

Minimalna konfiguracja 37
Konfiguracja Postfiksa 38
Ustawienie nazwy hosta w nagłówku smtpd 38
Ustawienie domeny, dla której będzie przyjmowana poczta 39
Ustawienie domeny dodawanej do wychodzących wiadomości 40
Mapowanie poczty wysyłanej do użytkownika root na inną skrzynkę pocztową 41
Uruchomienie Postfiksa i test doręczania poczty dla użytkownika root 42
Mapowanie adresów e-mail na nazwy użytkowników 45
Ustawienie uprawnień dla przekazywania przez Postfix poczty z sieci lokalnej 47

Rozdział 4. Serwer poczty dla jednej domeny dostępny przez linię telefoniczną ... **49**

Wyłączenie rozwiązywania nazw DNS 51
Kontrola uprawnień do przekazywania 51
Ustawienie hosta przekaźnika ISP 52
Wstrzymywanie przesłania wiadomości 53
Wyzwalanie doręczania wiadomości 53
Konfiguracja uprawnień przekazywania dla hosta przekaźnika 54
POP-before-SMTP 54
Uwierzytelnianie SMTP 55

Rozdział 5. Anatomia Postfiksa 57
Demony Postfiksa 59
Kolejki 64
Mapy 66
Typy map 66
Odpytywanie map przez Postfix 69
Źródła zewnętrzne 70
Narzędzia wiersza poleceń 71
postfix 71
postalias 71
postcat 71
postmap 72
postdrop 72
postkick 72
postlock 73
postlog 73
postqueue 74
postsuper 74

Część II Kontrola zawartości 77

Rozdział 6. E-mail — elementarz administratora 79
Przesyłanie wiadomości — wprowadzenie 79
Po co wiedzieć to wszystko? 81
Kontrola komunikacji SMTP (koperta) 82
Kontrola zawartości wiadomości 85
Nagłówki 87
Treść 89
Załączniki 89

Rozdział 7. Ograniczenia przesyłania wiadomości — wprowadzenie 93
Wyzwalacze ograniczeń 93
Typy ograniczeń 95
Ograniczenia ogólne 95
Ograniczenia przełączane 96
Ograniczenia przystosowywane 96
Dodatkowe parametry ochrony antyspamowej 97
Zakresy zastosowań 98
Budowanie ograniczeń 98
Sposób zapisu 99
Moment ewaluacji 99
Wpływ czynności na ewaluację ograniczeń 100
Spowalnianie klientów sprawiających problemy 101
Klasy ograniczeń 103

Rozdział 8. Ograniczenia przesyłania wiadomości — implementacja 105
Jak konstruować i testować ograniczenia? 105
Symulacja skutków ograniczeń 106
Natychmiastowe wprowadzanie ograniczeń 107
Domyślne ustawienia ograniczeń 107
Wymóg zgodności z RFC 108
Ograniczenie nazwy hosta w HELO/EHLO 108
Ograniczenia nadawcy koperty 111
Ograniczenia odbiorcy koperty 112

Utrzymanie zgodności z RFC ... 115
Puste pole nadawcy koperty ... 115
Konta specjalne ... 116
Kolejność przetwarzania ograniczeń RFC ... 117
Ochrona przed spamem ... 118
Zapobieganie oczywistym fałszerstwom ... 118
Fałszowane rekordy serwerów nazw ... 119
Odbicie do wielu odbiorców ... 121
Czarne listy DNS ... 122
Weryfikacja nadawcy ... 127
Kolejność przetwarzania ograniczeń ... 130
Zastosowania klas ograniczeń ... 131

Rozdział 9. Wbudowane filtry zawartości — wprowadzenie ... 133
Jak działają kontrole? ... 134
Stosowanie kontroli do poszczególnych części wiadomości ... 134
Dlaczego te parametry są tak ważne? ... 135
Kiedy Postfix przeprowadza kontrole? ... 136
Jakie akcje mogą wywoływać kontrole? ... 136

Rozdział 10. Wbudowane filtry zawartości — implementacja ... 139
Obsługa kontroli przez Postfix ... 140
Kompilacja Postfiksa z obsługą map PCRE ... 140
Bezpieczna implementacja filtrów nagłówka i treści ... 141
Dodanie wyrażenia regularnego i ustawienie akcji WARN ... 141
Tworzenie wzorca testowego ... 141
Czy wyrażenie regularne dopasuje testowy wzorzec? ... 142
Dodanie kontroli do głównej konfiguracji ... 142
Testowanie na rzeczywistej wiadomości ... 142
Kontrola nagłówków ... 143
Odrzucanie wiadomości ... 143
Wstrzymanie doręczenia ... 144
Usuwanie nagłówków ... 144
Odrzucanie wiadomości ... 145
Przekierowanie wiadomości ... 145
Filtrowanie wiadomości ... 145
Kontrola nagłówków MIME ... 146
Kontrola nagłówków w załączonych wiadomościach ... 147
Kontrola treści ... 148

Rozdział 11. Zewnętrzne filtry zawartości — wprowadzenie ... 151
Kiedy najlepiej jest filtrować zawartość poczty? ... 152
Filtry a modyfikowanie adresów ... 153
content_filter: kolejkowanie przed filtrowaniem ... 154
Demony delegujące do filtrów ... 156
Podstawy konfiguracji content_filter ... 157
smtpd_proxy_filter: filtrowanie przed kolejkowaniem ... 159
Zasady współpracy z filtrami ... 161
Podstawy konfiguracji smtpd_proxy_filter ... 161

Rozdział 12. Zewnętrzne filtry zawartości — implementacja ... 163
Dołączanie tekstu do wiadomości za pomocą skryptu ... 163
Instalacja alterMIME i utworzenie skryptu filtrującego ... 165
Konfiguracja Postfiksa do współpracy ze skryptem ... 167
Test filtra ... 168

Szukanie wirusów za pomocą content_filter i amavisd-new ... 170
Instalacja amavisd-new ... 170
Test amavisd-new ... 172
Optymalizacja wydajności amavisd-new ... 176
Konfiguracja Postfiksa do współpracy z amavisd-new ... 179
Testy filtra amavisd-new z Postfiksem ... 182
Kontrola antywirusowa przez smtpd_proxy_filter i amavisd-new ... 184
Konfiguracja Postfiksa do użycia amavisd-new z smtpd_proxy_filter ... 186

Część III Konfiguracje zaawansowane ... 189

Rozdział 13. Bramy pocztowe ... 191
Podstawowa konfiguracja ... 192
Uprawnienia przekazywania w bramie pocztowej ... 192
Ustawienia domen przekazywania w bramie pocztowej ... 192
Konfiguracja w bramie wewnętrznego hosta pocztowego ... 193
Definiowanie odbiorców przekazywania ... 193
Zaawansowana konfiguracja bramy ... 194
Poprawa bezpieczeństwa bramy pocztowej ... 195
Współpraca Postfiksa z programem Microsoft Exchange Server ... 196
Konfiguracja komunikacji pomiędzy Exchange i Postfiksem ... 207
Konfiguracja NAT ... 209

Rozdział 14. Serwer poczty dla wielu domen ... 211
Domeny aliasów wirtualnych ... 211
Zdefiniowanie nazwy domeny aliasów wirtualnych ... 212
Tworzenie mapy adresów odbiorców ... 212
Konfiguracja odbierania przez Postfix poczty dla domen aliasów wirtualnych ... 213
Testy ustawień domeny aliasów wirtualnych ... 213
Odwzorowania zaawansowane ... 214
Domeny wirtualnych skrzynek pocztowych ... 216
Obsługa agenta doręczającego virtual w Postfiksie ... 217
Podstawowa konfiguracja ... 217
Konfiguracja zaawansowana ... 221
Domeny wirtualnych skrzynek pocztowych obsługiwane przez bazę danych ... 225
Obsługa map MySQL przez Postfix ... 226
Kompilacja Postfiksa z obsługą map MySQL ... 227
Konfiguracja bazy danych ... 227
Konfiguracja Postfiksa do korzystania z bazy danych ... 230
Testy domen wirtualnych skrzynek pocztowych korzystających z bazy danych ... 234

Rozdział 15. Wprowadzenie do uwierzytelniania SMTP ... 239
Architektura i konfiguracja Cyrus SASL ... 239
Która metoda jest najlepsza? ... 242
SASL: Simple Authentication and Security Layer ... 242
Interfejs uwierzytelniania ... 244
Mechanizmy SMTP AUTH ... 244
Metody uwierzytelniania (usługi weryfikacji haseł) ... 246
Wewnętrzne systemy uwierzytelniania ... 247
Planowanie uwierzytelniania SMTP po stronie serwera ... 248
Znajdowanie klientów i obsługiwanych przez nie mechanizmów ... 248
Wybór systemu uwierzytelniania i usługi weryfikacji haseł ... 250
Instalacja i konfiguracja Cyrus SASL ... 250
Instalacja pakietu Cyrus SASL ... 251

Utworzenie pliku konfiguracyjnego aplikacji dla Postfiksa ... 253
Konfiguracja rejestrowania zdarzeń ... 253
Wybór usługi weryfikującej hasła ... 254
Wybór mechanizmów SMTP AUTH ... 254
Konfiguracja saslauthd ... 255
Konfiguracja pomocniczych modułów dodatkowych (auxprop) ... 259
Testy uwierzytelniania ... 264
Przyszłość SMTP AUTH ... 267

Rozdział 16. Uwierzytelnianie SMTP ... 269
Sprawdzamy, czy dana instalacja Postfiksa obsługuje SMTP AUTH ... 269
Dodanie obsługi SMTP AUTH do Postfiksa ... 270
Uwierzytelnianie SMTP po stronie serwera ... 271
Włączenie i konfiguracja serwera ... 272
Testy SMTP AUTH po stronie serwera ... 276
Zaawansowane ustawienia serwera ... 280
Uwierzytelnianie SMTP po stronie klienta ... 281
AUTH w kliencie SMTP Postfiksa ... 281
Testy SMTP AUTH po stronie klienta ... 284
Klient lmtp ... 286

Rozdział 17. Transport Layer Security — wprowadzenie ... 289
Podstawy TLS ... 290
Sposób działania TLS ... 291
Certyfikaty — wprowadzenie ... 292
Nawiązanie relacji zaufania ... 292
Który urząd certyfikacji będzie najlepszy? ... 292
Tworzenie certyfikatów ... 293
Wymagane informacje ... 293
Tworzenie certyfikatu CA ... 294
Dystrybucja i instalowanie certyfikatu CA ... 295
Tworzenie certyfikatu serwera ... 299
Podpisanie certyfikatu serwera ... 299
Przygotowanie certyfikatów do użycia w Postfiksie ... 300

Rozdział 18. Transport Layer Security — implementacja ... 303
Kontrola obsługi TLS w Postfiksie ... 303
Kompilacja Postfiksa z obsługą TLS ... 305
Kompilacja i instalacja OpenSSL z kodu źródłowego ... 305
Kompilacja Postfiksa z TLS ... 306
TLS po stronie serwera ... 307
Podstawowa konfiguracja serwera ... 308
Optymalizacja wydajności serwera ... 314
Zabezpieczenia wymiany potwierdzeń SMTP AUTH po stronie serwera ... 316
Przekazywanie oparte na certyfikatach po stronie serwera ... 321
Uszczelnianie serwera TLS ... 325
TLS po stronie klienta ... 326
Podstawowa konfiguracja klienta ... 326
Selektywne użycie TLS ... 330
Optymalizacja wydajności klienta ... 332
Zabezpieczanie SMTP AUTH w kliencie ... 332
Przekazywanie oparte na certyfikatach po stronie klienta ... 332
Uszczelnianie TLS po stronie klienta ... 334

Rozdział 19. Serwer poczty przedsiębiorstwa 337
Struktura ogólna 337
Struktura katalogu LDAP 338
Wybór atrybutów w schemacie Postfiksa 340
Projekt gałęzi 341
Budowanie obiektów użytkowników 342
Tworzenie obiektów list 343
Dodawanie atrybutów dla pozostałych serwerów 344
Konfiguracja podstawowa 345
Konfiguracja Cyrus SASL 345
Konfiguracja OpenLDAP 346
Konfiguracja LDAP w Postfiksie 349
Konfiguracja Courier maildrop 357
Konfiguracja Courier IMAP 366
Konfiguracja zaawansowana 371
Rozbudowa katalogu 371
Dodanie uwierzytelniania w serwerach 372
Ochrona danych w katalogu 378
Szyfrowanie zapytań LDAP 380
Wymuszanie poprawnego adresu nadawcy 387

Rozdział 20. Postfix w środowisku chroot 391
Jak działa klatka chroot? 392
Podstawowe zasady konfiguracji chroot 392
Implementacja techniczna 393
Jak chroot wpływa na Postfix? 393
Skrypty pomocnicze dla chroot 394
Demony w środowisku chroot 394
Biblioteki, pliki konfiguracyjne i inne pliki w chroot 396
Omijanie ograniczeń chroot 397

Część IV Dostrajanie Postfiksa 399

Rozdział 21. Ograniczenie liczby równoległych połączeń klientów i szybkości przesyłania żądań 401
Podstawy ograniczania przepustowości 401
Gromadzenie statystyk przepustowości 402
Włączenie demona anvil 403
Zmiana odstępów czasu rejestrowania przez anvil 403
Ograniczanie częstotliwości połączeń klientów 404
Testowanie limitów szybkości połączeń klientów 404
Ograniczanie liczby równoczesnych połączeń klienta 406
Testowanie limitów liczby równoczesnych połączeń klienta 406
Wyłączanie klientów z ograniczeń 408

Rozdział 22. Optymalizacja wydajności 409
Podstawowe ulepszenia 409
Przyspieszanie wyszukiwania w DNS-ie 409
Czy serwer nie jest wymieniony na liście otwartych przekaźników? 411
Odmowa przyjmowania wiadomości dla nieistniejących użytkowników 412
Blokowanie wiadomości z sieci znajdujących się na czarnych listach 413
Odrzucanie wiadomości z nieznanych domen nadawców 413
Ograniczanie częstotliwości ponawiania prób transmisji 414
Znajdowanie wąskich gardeł 414
Zatory w kolejce incoming 415

Zatory w kolejce maildrop ... 417
Zatory w kolejce deferred ... 418
Zatory w kolejce active ... 419
Nierównomierne przeciążenia kolejek przez asynchroniczne odbicia ... 421
Przekaźniki rezerwowe ... 423
Dostrajanie dla wyższej przepustowości ... 424
Konfiguracja alternatywnego transportu ... 425

Dodatki ... 427

Dodatek A Instalacja Postfiksa ... 429
Kod źródłowy Postfiksa ... 429
Wprowadzanie poprawek ... 430
Kompilacja i instalacja z kodu źródłowego ... 430
Uruchamianie i zatrzymywanie Postfiksa ... 431
Instalacja Postfiksa w systemie Debian Linux ... 431
Instalacja Postfiksa ... 431
Uruchamianie i zatrzymywanie Postfiksa ... 432
Instalacja aktualizacji ... 433
Kompilacja z pakietu kodu źródłowego Debiana ... 433
Instalacja Postfiksa w systemie Red Hat Linux ... 434
Źródła Postfiksa dla systemu Red Hat Linux ... 435
Kompilacja pakietu RPM z pakietu SRPM ... 436
Przełączenie na Postfix ... 438
Usunięcie MTA Sendmail ... 439
Uruchamianie i zatrzymywanie Postfiksa w systemie Red Hat Linux ... 439

Dodatek B Rozwiązywanie problemów ... 441
Problemy z uruchomieniem Postfiksa i dziennikiem zdarzeń ... 441
Łączenie z Postfiksem ... 444
Sprawdzenie sieci ... 445
Weryfikacja słuchających procesów ... 446
Zmuszenie Postfiksa do użycia naszych ustawień konfiguracji ... 446
Zgłaszanie problemów z Postfiksem ... 447
Gromadzenie dodatkowych informacji w dzienniku ... 447
Rejestrowanie zdarzeń związanych z konkretnym klientem ... 448
Rejestrowanie zdarzeń i qmgr ... 448
Inne błędy konfiguracji ... 449
Niuanse klatki chroot ... 449
Rozwiązywanie problemów z systemami plików ... 450
Piekło bibliotek ... 451
Niespójności demonów ... 451
Piekło namnażania procesów ... 452
Testy wydajności ... 452
Wydajność dysków ... 454
Zbyt wiele połączeń ... 455

Dodatek C Standardy CIDR i SMTP ... 457
Podsieci w notacji CIDR ... 457
Kody odpowiedzi serwera ... 457

Słowniczek ... 463

Skorowidz ... 475

Rozdział 2.

Przygotowanie hosta i środowiska

Na początku była nicość. I rzekł Bóg „Niech będzie światłość". Nadal pozostała nicość, lecz można ją było zobaczyć.

— Ignacio Schwartz

Masz już tę książkę w ręku, więc zapewne nie możesz doczekać się, by zacząć pracę z Postfiksem. Najpierw jednak musisz dowiedzieć się o jednym. Postfix został napisany przez Wietse Venemę, który naprawdę zna się na Uniksie, więc Postfix nie zawiera funkcjonalności, którą Unix zapewnia domyślnie. Oznacza to, że Postfix wymaga poprawnej konfiguracji systemu operacyjnego i może działać tylko tak dobrze, jak system, w którym jest zainstalowany.

Odradzamy pominięcie tego rozdziału, nawet jeśli wygląda na dobry dla małych dzieci. Radzimy poświęcić trochę czasu na jego lekturę i upewnienie się, że system jest właściwie skonfigurowany. Postfix wynagrodzi ten wysiłek, świadcząc szybkie, niezawodne i bezpieczne usługi.

Lista kontrolna dla Postfiksa wygląda następująco:

- Ustaw poprawną nazwę hosta.
- Sprawdź, czy połączenie sieciowe hosta działa poprawnie.
- Ustaw dokładny czas systemowy.
- Upewnij się, że usługa syslog może rejestrować komunikaty diagnostyczne Postfiksa.
- Skonfiguruj rozwiązywanie nazwy przez klienta.
- Skonfiguruj rekordy DNS dla serwera poczty.

Nazwa hosta

Serwer poczty, aby w niezawodny sposób komunikować się z innymi systemami, musi mieć zdefiniowaną pełną złożoną nazwę domeny (FQDN — ang. *fully qualified domain name*; patrz RFC 821, *ftp://ftp.rfc-editor.org/in-notes/rfc821.txt*), np. *mail.example.com*. Postfix przy witaniu zdalnych klientów i serwerów poczty automatycznie używa nazwy hosta przypisanej do serwera, chyba że ręcznie skonfigurujemy inną nazwę.

Pełna złożona nazwa domeny jest też ważna dlatego, że Postfix nie tylko przyjmuje pocztę od klientów — w trybie klienckim przesyła też wiadomości do innych serwerów poczty. Wiele takich serwerów sprawdza nazwę hosta podawaną przez klienta i nie przyjmuje wiadomości, jeśli klient nie zwróci pełnej złożonej nazwy domeny. Niektóre serwery sprawdzają nawet, czy podana FQDN jest rozwiązywana przez DNS.

System operacyjny ustawia swoją nazwę hosta podczas uruchomienia. Aby sprawdzić, czy system ma już FQDN, można zalogować się i wpisać polecenie `hostname`:

```
$ hostname -f
mail.example.com
```

Jeśli powyższe polecenie nie zwróci pełnej złożonej nazwy domeny, należy sprawdzić, jaką nazwę hosta ustawia system i poprawić ją. Jeśli jednak system ma już nazwę FQDN, a chcielibyśmy użyć innej w Postfiksie, ustawienie systemowe może pozostać niezmienione. Zamiast tego zastąpimy wartość domyślną, posługując się parametrem `myhostname`.

Opcja `-f` nie działa w systemach Solaris, z poleceniem GNU `hostname` i w kilku innych środowiskach. Jeśli w danym systemie opcja ta nie działa poprawnie, można spróbować ją pominąć. Jeśli to nie pomoże, należy sprawdzić składnię w dokumentacji.

Łączność

Należy sprawdzić, czy komputer może połączyć się z siecią, i czy hosty w sieci mogą się z nim komunikować. Pierwsza część zadania powinna być prosta — jeśli komputer może połączyć się z Internetem online i ma dostęp do stron WWW, oznacza to, że łączy się z siecią. Połączenia przychodzące sprawiają więcej kłopotu. Do ich przetestowania potrzebny jest klient w sieci, z której będą się łączyć z serwerem typowe klienty. Jeśli Postfix ma świadczyć usługi w całym Internecie, należy sprawdzić łączność z hosta, który jest całkowicie niezależny od naszego serwera.

Port TCP 25

W serwerze nic nie może blokować portu TCP 25. W razie korzystania z zapory sieciowej należy sprawdzić, czy jej reguły pozwalają na połączenia przychodzące i wychodzące z portem 25. Przypominamy, że dostawcy usług internetowych (ISP) czasem blokują w swoich routerach połączenia wychodzące na port 25. dla całego Internetu i trzeba ich prosić o usunięcie tego ograniczenia. Niektórzy ISP mogą nie zgodzić się na to, preferując przekazywanie wiadomości przez własne serwery poczty ISP z użyciem np. uwierzytelniania SMTP, opisanego w rozdziale 16.

Port TCP 25 musi być otwarty dlatego, że Postfix i inne serwery poczty oczekują na nim połączeń. Jest to port oficjalnie przydzielony przez IANA dla protokołu SMTP (pełna lista dostępna jest pod adresem *http://www.iana.org/assignments/port-numbers*). IANA utrzymuje centralny rejestr numerów przydzielonych w protokole IP, takich jak porty, protokoły, opcje, kody i typy.

Czas systemowy i znaczniki czasowe

Utrzymanie poprawnego czasu systemowego jest ważne przy „dostrajaniu" serwera i usuwaniu problemów. Gdy wychodzimy poza granice jednego systemu, aby rozwiązywać problemy z pocztą we współpracy z innymi administratorami poczty, poprawne znaczniki czasowe mogą być idealnym narzędziem do kojarzenia działań w naszych serwerach poczty ze zdarzeniami w innych serwerach, nad którymi nie mamy kontroli.

Postfix dokładnie rejestruje swoje działania w nagłówkach wiadomości. Przyjrzyjmy się na przykład temu nagłówkowi:

```
Received: from mail.example.net (mail.example.net [192.0.34.166])
        by mail.example.com (Postfix) with ESMTP id 6ED90E1C65
        for <recipient@example.com>; Sat, 7 Feb 2004 10:40:55 +0100 (CET)
Reply-To: sender@example.net
From: Sender <sender@example.net>
To: Recipient <recipient@example.com>
Subject: Keep correct system time
Date: Sat, 7 Feb 2004 10:42:01 +0100
```

Postfix zapisuje też informacje związane z datą w dzienniku poczty. Oto przykładowe komunikaty w dzienniku:

```
Feb 7 2004 10:40:55 mail postfix/pickup[32610]: 6ED90E1C65: uid=501 from=<sender>
Feb 7 2004 10:40:55 mail postfix/cleanup[398]: 6ED90E1C65: message-id=<20040416020209.
7D62343F30@mail.example.com
```

Wobec tego ważne jest, by utrzymywać jak najdokładniejszy czas systemowy. Nie można ufać zegarowi wbudowanemu w system: nie dość, że czas utrzymywany przez jądro Uniksa z czasem dryfuje, to dodatkowo układy stosowane przez producentów płyt głównych w podtrzymywanych bateryjnie zegarach są tanie i również nie utrzymują precyzyjnie czasu rzeczywistego. Nie można oczekiwać, że lokalny zegar będzie zsynchronizowany z czasem systemowym innych serwerów poczty.

Istnieją dwie metody utrzymania dokładnego zegara. Możemy posłużyć się protokołem NTP (ang. *Network Time Protocol*), który pozwala synchronizować czas przez sieć, albo wzorcem czasu dostępnym przez urządzenie GPRS (na całym świecie) lub DCF-77 (w większości Europy) i synchronizować czas drogą radiową. W razie braku dostępu do takich rozwiązań, jako ostatnią deskę ratunku można wypróbować clockspeed (*http://cr.yp.to/clockspeed.html*). Aplikacja ta wykorzystuje sprzętowy licznik taktów zegara do kompensowania regularnie spóźniającego się lub przyspieszającego zegara systemowego. Na podstawie kilku pomiarów czasu z wiarygodnego wzorca aplikacja oblicza i kompensuje błąd zegara.

Do skorzystania z serwera NTP niezbędny jest uruchomiony w systemie klient NTP (obecny w praktycznie każdym systemie operacyjnym). Poza tym zapora sieciowa musi przepuszczać przychodzące i wychodzące pakiety UDP (ang. *User Datagram Protocol*) na porcie 123. Dodatkowe informacje o tym, jak skonfigurować klienta NTP, zawiera serwis WWW NTP (*http://www.ntp.org*).

Syslog

Jednym z najważniejszych miejsc, gdzie możemy znaleźć komunikaty diagnostyczne jest dziennik pocztowy. Postfix wykorzystuje standardowe narzędzie rejestrujące komunikaty w systemie Unix o nazwie syslogd. Jest ono standardowo konfigurowane w pliku */etc/syslog.conf*. Oto przykładowa konfiguracja:

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none      -/var/log/messages
# The authpriv file has restricted access.
authpriv.*                                    -/var/log/secure
# Log all the mail messages in one place.
mail.*                                        -/var/log/maillog
# Log cron stuff
cron.*                                        -/var/log/cron
# Everybody gets emergency messages, plus log them on another
# machine
*.emerg                                       *
# Save mail and news errors of level err and higher in a
# special file.
uucp,news.crit                                -/var/log/spooler
# Save boot messages also to boot.log
local7.*                                      /var/log/boot.log
```

Przyjrzyjmy się na początek pierwszemu wpisowi, który zawiera pozycję `mail.none`. Dzięki niej komunikaty związane z pocztą nie są rejestrowane w pliku */var/log/messages*. Jest to istotne, ponieważ nie chcemy, aby komunikaty te zaśmiecały dziennik ogólnych komunikatów systemu. Jak widać, dziennik poczty ma tu własny wpis i plik (*/var/log/maillog*). Łącznik przed nazwą pliku oznacza, że syslogd powinien zapisywać komunikaty w pliku asynchronicznie, zamiast wymuszać zapis na dysku przy każdym pojawieniu się nowego komunikatu.

Niestety, syslogd może sprawić kilka problemów. Jeśli nie pojawiają się żadne nowe komunikaty w dzienniku, w pierwszej kolejności należy sprawdzić, czy syslogd jest w ogóle uruchomiony. Poniższy przykład pokazuje, jak możemy wyszukać demona, posługując się poleceniem ps:

```
# ps auxwww | grep syslog
root     15540  0.0  0.0  1444  524 ?        S    May21  18:20 syslogd -m 0 ❶
root     22616  0.0  0.0  1444  452 pts/0    R    18:09   0:00 grep syslog
```

❶ Pierwszy wiersz wyjścia wskazuje, że syslogd jest uruchomiony od 21 maja.

Poza tym przed poinstruowaniem narzędzia syslogd, by zapisywało komunikaty do dziennika, należy upewnić się, że plik ten istnieje, i że zapis w nim jest możliwy. Niektóre implementacje syslogd nie tworzą automatycznie plików i przestają działać bez żadnych objawów, jeśli wystąpi problem z plikiem dziennika. Złą sławą cieszy się pod tym względem syslogd z systemów Solaris.

Bardzo częstym błędem jest oddzielanie od siebie w pliku */etc/syslog.conf* typu dziennika od pliku spacjami zamiast znaków tabulacji. Wpisy w *syslog.conf* powinny wyglądać tak:

```
mail.*<TAB>-/var/log/maillog
```

Kolejnym problemem z *syslog.conf* jest rejestrowanie zdarzeń w innym hoście w sieci. Należy zwracać uwagę na wpisy typu:

```
mail.* @loghost
```

W tym przypadku syslogd wysyła wszystkie komunikaty do komputera *loghost*, więc należy sprawdzać dzienniki w tym hoście, a nie w serwerze poczty. Trzeba upewnić się, że faktycznie dysponujemy takim hostem. Nazbyt często zdarza się wysyłanie dzienników do niezaplanowanego hosta (lub w próżnię) z powodu błędnego wpisu w pliku *syslog.conf*.

Rozwiązywanie nazw (DNS)

Aby serwer poczty (np. Postfix) mógł przesłać wiadomość w odległe miejsce przeznaczenia, najpierw musi zlokalizować to miejsce. W Internecie do znajdowania zdalnych zasobów służy usługa DNS (ang. *Domain Name System* — system nazw domen). Serwer nazw zwraca adres IP odpowiadający nazwie hosta lub, odwrotnie, nazwę hosta odpowiadającą adresowi IP.

Dobrze funkcjonująca usługa DNS ma decydujący wpływ na wydajność agenta przesyłania poczty. Im szybciej Postfix rozwiąże docelowy adres IP, tym szybciej będzie mógł zacząć komunikować się z odległym serwerem poczty i przesłać wiadomość.

Marna wydajność usługi rozwiązywania nazw może stać się poważnym wąskim gardłem w dużych koncentratorach poczty. W razie problemów serwera może pomóc buforujący serwer nazw. Dla dużych systemów pocztowych należy zainstalować taki serwer. Trzeba pamiętać, że zabezpieczenia antyspamowe mogą zwiększyć liczbę zapytań DNS przeprowadzanych przez serwer poczty o kilka rzędów wielkości.

Zanim spróbujemy zwiększyć wydajność rozwiązywania nazw w systemie, możemy sprawdzić, czy system operacyjny poprawnie rozwiązuje zdalne nazwy, odpytując serwer nazw o rekord MX (zobacz punkt „Rekordy MX" w dalszej części rozdziału) domeny *postfix-book.com*, na przykład poleceniem:

```
$ dig postfix-book.com MX
```

Wynik powinien wyglądać mniej więcej tak:

```
; <<>> DiG 9.2.2-P3 <<>> postfix-book.com MX
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23929
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;postfix-book.com.              IN      MX

;; ANSWER SECTION:
postfix-book.com.       86400   IN      MX      10 mail.postfix-book.com. ❶

;; AUTHORITY SECTION:
postfix-book.com.       86400   IN      NS      ns3.ray.net. ❷
postfix-book.com.       86400   IN      NS      ns.state-of-mind.de.

;; ADDITIONAL SECTION:
mail.postfix-book.com.  86400   IN      A       212.14.92.89
ns3.ray.net.            172421  IN      A       194.77.1.3
ns.state-of-mind.de.    81566   IN      A       212.14.92.88

;; Query time: 58 msec
;; SERVER: 212.18.0.5#53(212.18.0.5)
;; WHEN: Sat Apr 17 03:56:47 2004
;; MSG SIZE  rcvd: 145
```

❶ Ten wiersz wskazuje, że *mail.postfix-book.com* jest serwerem poczty przyjmującym wiadomości dla odbiorców w obrębie domeny *postfix-book.com*.

❷ Te dwa wiersze wskazują, że *ns3.ray.net* i *ns.state-of-mind.de* są autorytatywnymi serwerami nazw dla domeny *postfix-book.com*.

Polecenie `dig` (ang. *Domain Information Groper*) nie jest standardowo dostępne na niektórych starszych platformach. Można pobrać narzędzie dig razem z dystrybucją BIND z ISC (*http://www.isc.org*). W systemach, w których zainstalowanie dig nie jest możliwe, można najczęściej zrealizować powyższe zapytanie za pomocą polecenia `host` lub `nslookup`. Polecenie `nslookup` zostało obecnie zarzucone.

Jeśli wyszukiwanie zakończyło się powodzeniem, Postfix może (teoretycznie) poprawnie rozwiązywać nazwy hostów. W razie niepowodzenia zapytania, jeśli nie można rozwiązać żadnej nazwy hosta, musimy natychmiast zrobić porządek z DNS-em.

Często spotyka się problem z rozwiązywaniem nazw polegający na tym, że nie działa ono, gdy serwer próbuje odpytać nieistniejące serwery nazw. Zajrzyjmy do pliku */etc/resolv.conf*. Powiedzmy, że wygląda jak poniżej — w takiej konfiguracji komputer odpytuje serwer nazw pod adresem localhost (127.0.0.1), a w razie niepowodzenia zwraca się następnie do 134.169.9.107:

```
nameserver 127.0.0.1
nameserver 134.169.9.107
```

Nic nie przeszkadza w odpytywaniu hosta `localhost`, jeśli w lokalnym komputerze uruchomiony jest buforujący serwer nazw. Jeśli jednak nie mamy go, to trochę potrwa, zanim upłynie dopuszczalny czas oczekiwania.

Jeśli zapytania do serwera nazw przeprowadzane poleceniem `dig` działają, lecz Postfix nie może znaleźć hosta (na przykład, jeśli w dzienniku pojawiają się komunikaty `no route to host`), to możliwe jest, że Postfix działa w środowisku chroot, więc ustawienia związane z rozwiązywaniem nazw bierze z innego pliku konfiguracyjnego. Na przykład, jeśli klatką chroot jest */var/spool/postfix*, to Postfix będzie pobierał ustawienia z pliku */var/spool/postfix/etc/resolv.conf*. W takim przypadku należy zsynchronizować pliki poleceniem `cp -p /etc/resolv.conf /var/spool/postfix/etc/resolv.conf`, a następnie zatrzymać i uruchomić ponownie Postfix.

DNS dla serwerów poczty

Niezbędna jest konfiguracja serwera nazw informująca resztę świata, że dany serwer może doręczać pocztę dla naszej domeny. Musimy poprosić osobę odpowiedzialną za prowadzenie serwera nazw w domenie (hostmastera) o wprowadzenie następujących wpisów:

Rekord A

Serwer poczty musi mieć pełną złożoną nazwę hosta, która pozwala klientom go znajdować. Rekord A mapuje FQDN na adres IP.

Rekord PTR

Nazwa hosta systemu powinna być rozwiązywalna wstecz. Serwery poczty, które zdobywają nazwę hosta naszego serwera z komunikacji SMTP, powinny mieć możliwość sprawdzenia, czy faktycznie to nasz serwer komunikuje się z nimi.

Rekord MX

Rekord MX informuje klienty, że nasz serwer jest odpowiedzialny za doręczanie poczty dla domeny lub określonego hosta.

Rekordy A

System nazw domen stosuje rekordy różnych typów do informowania hostów o zasobach w sieci. Jednym z najważniejszych jest rekord A, który odwzorowuje nazwy hostów na adresy. Klient wysyłający nazwę hosta do serwera nazw powinien w odpowiedzi otrzymać adres IP tego hosta. Poniższa przykładowa sesja pokazuje, że nazwa hosta *www.example.com* jest odwzorowana na adres IP 192.0.34.166:

```
$ dig www.example.com A

; <<>> DiG 9.2.1 <<>> www.example.com A
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30122
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 0

;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        172627  IN      A       192.0.34.166

;; AUTHORITY SECTION:
example.com.            172627  IN      NS      b.iana-servers.net.
example.com.            172627  IN      NS      a.iana-servers.net.

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Apr 17 16:43:40 2004
;; MSG SIZE  rcvd: 97
```

Rekordy PTR

Przeciwieństwem rekordu A jest rekord PTR, odwzorowujący adres na nazwę hosta. Gdy klient wysyła adres IP do serwera nazw, to w odpowiedzi powinien otrzymać nazwę hosta odpowiadającą temu adresowi, jak w poniższym przykładzie:

```
$ dig -x 192.0.34.166

; <<>> DiG 9.2.1 <<>> -x 192.0.34.166
;; global options:  printcmd

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55376
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 0

;; QUESTION SECTION:
;166.34.0.192.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
166.34.0.192.in-addr.arpa. 21374 IN     PTR     www.example.com.
```

```
;; AUTHORITY SECTION:
34.0.192.in-addr.arpa.  21374   IN      NS      ns.icann.org.
34.0.192.in-addr.arpa.  21374   IN      NS      svc00.apnic.net.
34.0.192.in-addr.arpa.  21374   IN      NS      a.iana-servers.net.
34.0.192.in-addr.arpa.  21590   IN      NS      b.iana-servers.org.
34.0.192.in-addr.arpa.  21374   IN      NS      c.iana-servers.net.

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Apr 17 16:44:39 2004
;; MSG SIZE  rcvd: 201
```

Dzisiaj, gdy spamerzy stanowią plagę Internetu, rozwiązywanie wstecz za pomocą rekordów PTR odpowiadających rekordom A jest ważniejsze niż kiedykolwiek. Wielu administratorów poczty tak konfiguruje swoje serwery, że przyjmują pocztę tylko po pomyślnym rozwiązaniu wstecz adresu łączącego się z nimi klienta.

To, że inne serwery poczty odrzucają pocztę na podstawie wyszukiwania wstecz nie oznacza, że należy tak robić. Często powoduje to problemy, ponieważ wielu dostawców usług internetowych nie deleguje rozwiązywania nazw wstecz do serwerów nazw swoich klientów i nie podaje odpowiednich informacji w swoim serwerze.

Rekordy MX

Serwer nazw może nie tylko rozwiązywać adresy zasobów — może też informować klienty o usługach oferowanych w domenie. Jedną z tych usług jest serwer poczty odpowiedzialny za domenę. Możemy skonfigurować rekord MX wskazujący na rekord A serwera poczty.

W usłudze DNS stosowany jest również rekord CNAME — alias, który może wskazywać na rekord A. Możemy, na przykład, utworzyć rekord CNAME, który wskazuje z *www.example.com* na *srv01.example.com*. Klienty żądające *www.example.com* otrzymają w odpowiedzi adres *srv01.example.com*.

Rekord MX nie powinien wskazywać na alias tego typu. Najpopularniejszy protokół transportowy poczty (SMTP) wymaga, aby nazwa domeny w adresie e-mail była zdefiniowana przez rekord A lub MX. W powyższym przykładzie nie można wskazać w rekordzie MX hosta *www.example.com*, lecz ponieważ dla *srv01.example.com* istnieje rekord A, można użyć tego hosta w rekordzie MX.

Możemy zdefiniować więcej niż jeden rekord MX, a ponadto możemy nadać serwerom poczty priorytety, dzięki którym klienty będą próbowały łączyć się z nimi w określonym porządku. Oto przykład:

```
$ dig m-net.de MX

; <<>> DiG 9.2.1 <<>> m-net.de MX
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3133
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 0
```

```
;; QUESTION SECTION:
;m-net.de.                      IN      MX

;; ANSWER SECTION:
m-net.de.               7200    IN      MX      50 mail-in.m-online.net. ❶
m-net.de.               7200    IN      MX      100 mx01.m-online.net. ❷
m-net.de.               7200    IN      MX      100 mx02.m-online.net.

;; AUTHORITY SECTION:
m-net.de.               7200    IN      NS      ns1.m-online.net.
m-net.de.               7200    IN      NS      ns2.m-online.net.

;; Query time: 27 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Apr 17 17:07:05 2004
;; MSG SIZE  rcvd: 140
```

❶ *mail-in.m-online.net* ma najwyższy priorytet, ponieważ ma najniższy numer (50). Klienty będą próbowały doręczyć pocztę do tego serwera w pierwszej kolejności.

❷ *mx01.m-online.net* i *mx02.m-online.net* mają drugi z kolei najwyższy priorytet, ustalony według numeru (100). Gdy komputer o najwyższym priorytecie wymieniający pocztę będzie niedostępny, klienty będą próbowały połączyć się z jednym z tych serwerów.