Diagnostyka dostarczania poczty

Poziom: średni **Dotyczy: Postfix 3.x** **Czas: ~20 min**

Zanim zaczniemy podejrzewać konfigurację, sprawdzamy log — niemal każde niepowodzenie dostarczenia zostawia w nim jasny ślad, o ile wiemy, czego szukać.

Skróty użyte na tej stronie (8)

Skrót	Co znaczy
IP	Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection)
RBL	Realtime Blackhole List: lista adresów IP, z których szła niechciana poczta; wiele serwerów odrzuca pocztę z adresów znajdujących się na takiej liście
RFC	Request for Comments: oficjalny dokument opisujący standard internetowy, na przykład sposób działania danego protokołu; w ITIL także Request for Change, czyli wniosek o zmianę
RHEL	Red Hat Enterprise Linux: komercyjna dystrybucja Linuksa
SMTP	Simple Mail Transfer Protocol: protokół wysyłania poczty
SPF	Sender Policy Framework: rekord DNS mówiący, które serwery mogą wysyłać pocztę domeny
TCP	Transmission Control Protocol: protokół sieciowy z potwierdzaniem dostarczenia
TLS	Transport Layer Security: szyfrowanie połączeń, np. w HTTPS

Fiszka

TYLKO ODCZYT

Śledzenie logu na żywo: tail -f

```
sudo tail -f /var/log/maillog
```

Widzimy kompletny przebieg jednej udanej wiadomości jako kilka kolejnych linii.

Przykład:

```
Sep 24 09:12:03 NazwaSerwera postfix/smtpd[18402]: 3F2C1A4B821:
client=localhost[127.0.0.1]
Sep 24 09:12:03 NazwaSerwera postfix/cleanup[18405]: 3F2C1A4B821: message-
id=<20260924071203.3F2C1A4B821@NazwaSerwera.zielona.example>
Sep 24 09:12:03 NazwaSerwera postfix/qmgr[1421]: 3F2C1A4B821:
from=<powiadomienia@zielona.example>, size=4821, nrcpt=1 (queue active)
Sep 24 09:12:04 NazwaSerwera postfix/smtp[18410]: 3F2C1A4B821:
to=<odbiorca@example.net>, relay=mail.example.net[203.0.113.20]:25, delay=1.2,
delays=0.1/0/0.6/0.5, dsn=2.0.0, status=sent (250 2.0.0 Ok: queued as A1B2C3D4)
Sep 24 09:12:04 NazwaSerwera postfix/qmgr[1421]: 3F2C1A4B821: removed
```

□□ **tail** = pokaż koniec pliku, z flagą -f śledzi plik na żywo

□□ TYLKO ODCZYT

Śledzenie jednej wiadomości po queue id: grep

```
sudo grep '3F2C1A4B821' /var/log/maillog
```

Przykład:

```
Sep 24 09:12:03 NazwaSerwera postfix/smtpd[18402]: 3F2C1A4B821:
client=localhost[127.0.0.1]
Sep 24 09:12:03 NazwaSerwera postfix/qmgr[1421]: 3F2C1A4B821:
from=<powiadomienia@zielona.example>, size=4821, nrcpt=1 (queue active)
Sep 24 09:12:04 NazwaSerwera postfix/smtp[18410]: 3F2C1A4B821:
to=<odbiorca@example.net>, relay=none, delay=0.1, delays=0.1/0/0/0, dsn=4.4.1,
status=deferred (connect to mail.example.net[203.0.113.44]:25: Connection timed out)
```

Uważaj: przy dużym ruchu ten sam krótki identyfikator queue id bywa reużyty przez Postfix po jego zwolnieniu z poprzedniej wiadomości — przy diagnozowaniu starszych wpisów warto dodatkowo filtrować po znaczniku czasu, żeby mieć pewność, że wszystkie znalezione linie dotyczą tej samej, a nie dwóch różnych wiadomości o tym samym identyfikatorze wydanym w różnych dniach.

□□ **grep** = global regular expression print: szukaj wzorca w tekście

□□ TYLKO ODCZYT

Wysyłka testowa: swaks

```
swaks --to odbiorca@example.net --from powiadomienia@zielona.example --server localhost
--port 587 --auth LOGIN --auth-user NazwaUzytkownika --auth-password HasloUzytkownika --
tls
```

Przykład:

```
-> EHLO NazwaKlienta
<-  250-poczta.zielona.example
<-  250-STARTTLS
<-  250 AUTH LOGIN PLAIN
-> STARTTLS
<-  220 2.0.0 Ready to start TLS
-> AUTH LOGIN
<-  334 VXNlcm5hbWU6
-> ...
<-  235 2.7.0 Authentication successful
-> MAIL FROM:<powiadomienia@zielona.example>
<-  250 2.1.0 Ok
-> RCPT TO:<odbiorca@example.net>
<-  250 2.1.5 Ok
-> DATA
<-  354 End data with <CR><LF>.<CR><LF>
-> .
<-  250 2.0.0 Ok: queued as B7E1F209A3
```

swaks = Swiss Army Knife for SMTP: program do ręcznego wysyłania wiadomości testowych i podglądu rozmowy z serwerem poczty

TYLKO ODCZYT

Wysyłka testowa: sendmail

```
echo -e "Subject: Test\n\nTresc testowa" | sendmail -v odbiorca@example.net
```

Prostsza alternatywa bez zależności od dodatkowego pakietu — flaga `-v` włącza tryb gadatliwy, pokazujący przebieg lokalnego przekazania wiadomości do kolejki Postfixa.

Przykład:

```
odbiorca@example.net... Connecting to local...
odbiorca@example.net... Sent (3F2C1A4B821 Message accepted for delivery)
```

echo = od angielskiego echo: wypisuje podany tekst na standardowe wyjście, często łączone z przekierowaniem do pliku

TYLKO ODCZYT

Ręczna sesja SMTP przez telnet (port 25, bez szyfrowania)

```
telnet localhost 25
```

Ręczne wpisywanie komend SMTP (`EHLO`, `MAIL FROM`, `RCPT TO`, `DATA`) — przydatne do zweryfikowania, czy Postfix w ogóle odpowiada na porcie 25 i jakim bannerem, zanim zaczniemy podejrzewać coś bardziej złożonego.

SMTP = Simple Mail Transfer Protocol: protokół wysyłania poczty · **RCPT** = komenda protokołu SMTP wskazująca adres odbiorcy wiadomości

TYLKO ODCZYT

Ręczna sesja SMTP z STARTTLS na porcie 587: openssl s_client

```
openssl s_client -connect localhost:587 -starttls smtp
```

Przykład:

```
250 2.0.0 Ready to start TLS
depth=0 CN = poczta.zielona.example
verify return:1
```

SMTP = Simple Mail Transfer Protocol: protokół wysyłania poczty · **STARTTLS** = włączenie szyfrowania w trakcie już nawiązanej, nieszyfrowanej sesji pocztowej · **openssl** = zestaw narzędzi do certyfikatów i szyfrowania

Z życia wzięte

Z ŻYCIA WZIĘTE

W czwartek Ola zgłasza, że raport wysyłany co noc z `app01` nie dochodzi do jednego konkretnego klienta, a do reszty owszem. Tomek filtruje `maillog` po adresie tego odbiorcy i widzi powtarzający się kod `550 5.7.1 Service unavailable, client blacklisted`. Sprawdzenie adresu IP `app01` na publicznych listach RBL potwierdza wpis sprzed kilku miesięcy, o którym nikt w zespole nie wiedział.

Czytanie /var/log/maillog

Pojęcie: maillog. Log, do którego Postfix (oraz Dovecot i inne komponenty pocztowe na tej samej maszynie) zapisuje każdy etap obsługi wiadomości — na RHEL/Rocky domyślnie `/var/log/maillog`, na Debianie/Ubuntu zwykle `/var/log/mail.log`. Każda linia zaczyna się znacznikiem czasu, nazwą hosta i nazwą procesu, który ją zapisał (`postfix/smtpd`, `postfix/qmgr`, `postfix/smtp`).

Śledzenie jednej wiadomości po queue id

Pojęcie: queue id. Identyfikator wiadomości nadawany przez Postfix w momencie przyjęcia jej do kolejki (widoczny też w wyniku `mailq` i `postqueue -p`, opisanych na stronie Kolejka Postfiksa: podgląd, wymuszenie, czyszczenie) — ten sam identyfikator pojawia się we wszystkich liniach loga dotyczących danej wiadomości, aż do jej usunięcia z kolejki, co pozwala prześledzić całą jej drogę jednym poleceniem.

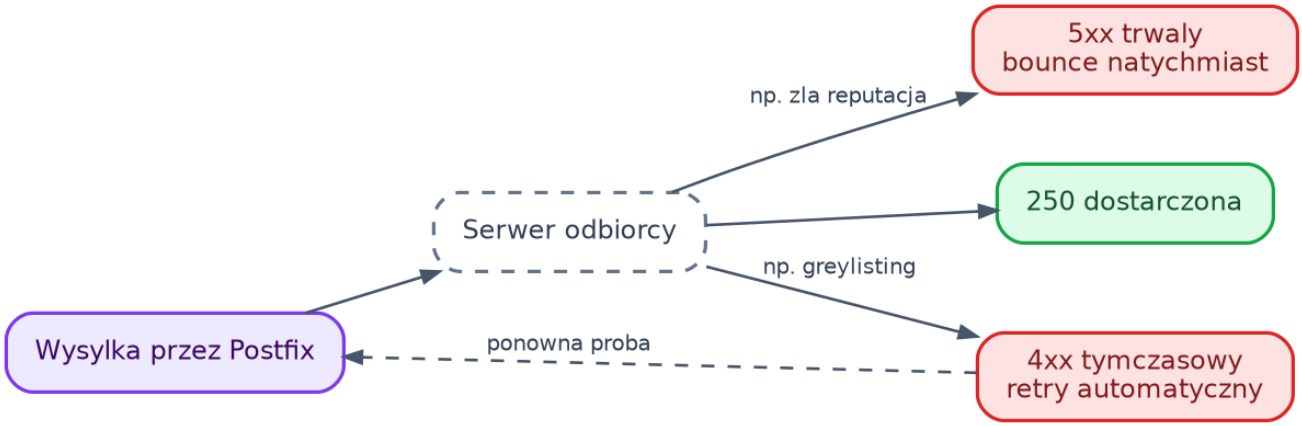
Kody odpowiedzi 4xx a 5xx

Pojęcie: kod DSN (Delivery Status Notification). Trzycyfrowy kod zwracany przez serwer odbiorcy (albo przez sam Postfix przy odrzuceniu lokalnym), którego pierwsza cyfra od razu mówi, czy problem jest tymczasowy, czy trwały.

Klasa kodu	Znaczenie	Zachowanie Postfixa

4xx (np. 450, 451, 421)	błąd tymczasowy — serwer odbiorcy prosi o ponowienie próby później	wiadomość trafia do `deferred` i Postfix próbuje ponownie automatycznie
5xx (np. 550, 554)	błąd trwały — serwer odbiorcy odrzuca wiadomość jednoznacznie i bezwarunkowo	Postfix nie ponawia próby, od razu odsyła nadawcy komunikat o niepowodzeniu (bounce)

Uważaj: rozróżnienie 4xx/5xx jest decyzją serwera odbiorcy, nie naszą — ten sam realny problem (np. greylisting) różni dostawcy sygnalizują różnymi kodami, więc samą liczbę zawsze czytamy razem z treścią komunikatu tekstowego, który za nią stoi.



Kod 4xx od serwera odbiorcy wraca do Postfixa jako sygnał do ponownej próby, kod 5xx kończy się natychmiastowym bounce bez ponawiania (kliknięcie otwiera pełny rozmiar)

Najczęstsze przyczyny odrzuceń

> **Pojęcie: greylisting.** Technika antyspamowa, w której serwer odbiorcy przy pierwszej próbie od nieznanej wcześniej trójki (adres IP nadawcy, adres nadawcy, adres odbiorcy) celowo odpowiada tymczasowym błędem 4xx, licząc na to, że prawdziwy serwer pocztowy — w odróżnieniu od większości oprogramowania spamowego — spróbuje ponownie po chwili, zgodnie ze specyfikacją SMTP. Postfix robi to automatycznie, więc greylisting jest niewidoczny dla użytkownika poza kilkuminutowym opóźnieniem pierwszej wiadomości do nowego odbiorcy.

Przyczyna	Typowy komunikat w logu	Co sprawdzamy

brak albo zły SPF	`550 5.7.1 SPF check failed`	rekord TXT SPF domeny nadawcy, opisany na stronie Jak działa poczta: MTA, MDA, MUA, SMTP, kolejka
brak rekordu PTR	`450 4.7.1 Client host rejected: cannot find your reverse hostname`	rekord PTR adresu IP wysyłającego serwera u dostawcy łącza
greylisting	`450 4.2.0 Greylisted, please try again in 180 seconds`	nic nie robimy — Postfix ponowi próbę sam, problem znika po kilku minutach
zła reputacja adresu IP	`550 5.7.1 Service unavailable, client blacklisted`	sprawdzenie adresu IP na publicznych listach RBL (np. Spamhaus)
limit rozmiaru	`552 5.3.4 Message size exceeds fixed maximum message size`	`message_size_limit` po naszej stronie albo limit skrzynki odbiorcy

Test wysyłki z wiersza poleceń

> **Pojęcie: swaks.** Narzędzie zbudowane specjalnie do testowania sesji SMTP — w odróżnieniu od zwykłego klienta pocztowego pokazuje pełny przebieg rozmowy z serwerem linia po linii, wliczając moment negocjacji `STARTTLS` i uwierzytelnienia, co czyni je dużo wygodniejszym narzędziem diagnostycznym niż wysłanie zwykłej wiadomości testowej i czekanie na skutek.

> **Pojęcie: STARTTLS.** W odróżnieniu od portu 465, gdzie szyfrowanie zaczyna się natychmiast po nawiązaniu połączenia TCP, port 587 zaczyna sesję jako zwykłe, nieszyfrowane połączenie, a klient dopiero w trakcie rozmowy wysyła komendę `STARTTLS`, żądając przejścia na szyfrowanie. Flaga `-starttls smtp` w `openssl s_client` odwzorowuje dokładnie ten mechanizm, w przeciwieństwie do zwykłego połączenia TLS, które na porcie 587 zakończyłoby się błędem, bo serwer oczekuje najpierw zwykłego tekstu `EHLO`.

Częste błędy

Traktowanie greylistingu jako awarii. Pojedyncza wiadomość odrzucona z kodem 450 i komunikatem o ponowieniu próby za kilka minut to normalne działanie mechanizmu antyspamowego odbiorcy, nie usterka po naszej stronie — Postfix sam ją dostarczy przy kolejnej automatycznej próbie, bez żadnej interwencji.

Testowanie przez port 587 bez -starttls. `openssl s_client -connect host:587` bez flagi `-starttls smtp` kończy się błędem negocjacji TLS, bo serwer po nawiązaniu połączenia na tym porcie wysyła zwykły tekstowy banner SMTP, a nie od razu rozpoczyna handshake TLS.

Ignorowanie treści komunikatu przy kodzie 550. Sam kod mówi tylko „odrzucone trwale" — realna przyczyna (zła reputacja, SPF, zbyt duży rozmiar, nieistniejąca skrzynka) zawsze jest w tekście towarzyszącym kodowi, który trzeba przeczytać, a nie tylko sprawdzić pierwszą cyfrę.

□□ Ćwiczenia

> Ćwiczenia zakładają lokalną instalację Postfixa z dostępem do `/var/log/maillog`.

Ćwiczenie 1 — pełne prześledzenie jednej wiadomości

```
echo "test" | mail -s "sledzenie" odbiorca@example.net
sleep 2
qid=$(grep -oP '(?<=postfix/qmgr\[\d{1,6}\]: )[A-F0-9]+(?=: from=)' /var/log/maillog | tail -1)
grep "$qid" /var/log/maillog
```

Wysyłamy wiadomość testową, wyciągamy jej queue id z ostatniego wpisu `qmgr` i filtrujemy cały log po tym identyfikatorze.

Odpowiedź

Wynik powinien pokazać komplet linii dla tej wiadomości: przyjęcie przez `smtpd`, nadanie message-id przez `cleanup`, umieszczenie w kolejce przez `qmgr`, próbę dostarczenia przez `smtp` (lub `local`) i finalne usunięcie z kolejki po powodzeniu.

Powiązane: Kolejka Postfiksa: podgląd, wymuszenie, czyszczenie · Jak działa poczta: MTA, MDA, MUA, SMTP, kolejka · Postfix: konfiguracja

Źródła: `man 1 swaks` · dokumentacja postfix.org, rozdział „DSN_README" · RFC 5321

Revision #36
Created 2026-09-25 07:40:21 UTC by Tomasz Konieczny
Updated 2026-10-26 14:16:04 UTC by Tomasz Konieczny