Postfix: konfiguracja

Poziom: średni **Dotyczy: Postfix 3.x (Debian/Ubuntu i RHEL/Rocky)** **Czas: ~25 min**

Najczęstszy przypadek, jaki konfigurujemy, to nie pełny serwer pocztowy, tylko serwer aplikacyjny, który ma tylko wysyłać powiadomienia dalej przez zewnętrzny przekaźnik — ta strona pokazuje gotowy komplet dla takiego scenariusza.

Skróty użyte na tej stronie (5)

Skrót	Co znaczy
DKIM	DomainKeys Identified Mail: cyfrowy podpis wiadomości e-mail
IP	Internet Protocol: adres komputera w sieci; w elektryce: stopień ochrony obudowy (Ingress Protection)
MX	Mail Exchanger: rekord DNS wskazujący serwer poczty domeny
RHEL	Red Hat Enterprise Linux: komercyjna dystrybucja Linuksa
SMTP	Simple Mail Transfer Protocol: protokół wysyłania poczty

Fiszka

TYLKO ODCZYT

Podejrzenie faktycznie działającej konfiguracji: postconf -n

```
sudo postconf -n
```

> **Pojęcie: postconf -n.** Właściwy sposób oglądania konfiguracji Postfixa — wypisuje wyłącznie parametry, które faktycznie zostały jawnie ustawione w `main.cf`, pomijając setki parametrów pozostawionych na wartości domyślnej. Czytanie samego pliku `main.cf` przez `cat` pokazuje to samo, ale `postconf -n` jest odporne na komentarze, białe znaki i kolejność linii — dwie różnie sformatowane konfiguracje dające ten sam efekt wyglądają w `postconf -n` identycznie.

Przykład:

```
compatibility_level = 3.6
inet_interfaces = loopback-only
mydestination = $myhostname, localhost.$mydomain, localhost
myhostname = app01.ipa.zielona.example
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
myorigin = /etc/mailname
relayhost = [AdresPrzekaznika]:587
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
smtp_tls_security_level = encrypt
smtpd_banner = $myhostname ESMTP $mail_name
```

□□ TYLKO ODCZYT

Sprawdzenie wartości jednego parametru: postconf

```
postconf mydestination
```

Pytamy o wartość dokładnie jednego parametru, wliczając wartość domyślną, jeśli nie został jawnie ustawiony — wygodniejsze niż filtrowanie wyniku `postconf -n`, gdy szukamy parametru, którego nikt jawnie nie nadpisał.

Przykład:

```
mydestination = $myhostname, localhost.$mydomain, localhost
```

□□ ZMIENIA SYSTEM

Wczytanie nowej konfiguracji: systemctl reload

```
sudo systemctl reload postfix.service
```

Nakazujemy działającej instancji ponownie wczytać `main.cf` bez zrywania trwających sesji SMTP — standardowe zakończenie edycji `main.cf`, wykonywane po każdej zmianie.

SMTP = Simple Mail Transfer Protocol: protokół wysyłania poczty · **systemctl** = system control: sterowanie usługami systemd

Z życia wzięte

Z ŻYCIA WZIĘTE

Ola zgłasza w środę, że nowa aplikacja na `app01` nie wysyła powiadomień o błędach, a `postconf -n` wygląda identycznie jak na działającym serwerze. Tomek sprawdza `smtp_sasl_password_maps` i widzi, że plik `sasl_passwd` został zmieniony ręcznie, ale nikt nie uruchomił potem `postmap`. Po przebudowaniu bazy `.db` powiadomienia wychodzą do przekaźnika bez dalszych zmian w konfiguracji.

Czym są main.cf i master.cf

Pojęcie: main.cf. Główny plik konfiguracyjny instancji Postfixa, w standardowej instalacji leżący w `/etc/postfix/main.cf` — każdy parametr to jedna linia `nazwa = wartość`. To jest plik, który edytujemy w zdecydowanej większości zmian konfiguracyjnych.

Pojęcie: master.cf. Plik definiujący, jakie usługi (demony) Postfix uruchamia i na jakich portach nasłuchują — `smtp`, `submission` (port 587), `smtps` (port 465), lokalny `pickup`, `cleanup` i inne. Zmieniamy go rzadziej niż `main.cf`, głównie gdy chcemy włączyć albo dostosować nasłuch na porcie 587/465, albo uruchomić drugą, niezależną instancję Postfixa na tej samej maszynie.

Najważniejsze parametry main.cf

Parametr	Do czego służy
`myhostname`	pełna nazwa FQDN tej instancji, używana m.in. w bannerze SMTP i jako baza dla `myorigin` / `mydestination`
`mydomain`	domena tej instancji, domyślnie wyliczana z `myhostname` przez odcięcie pierwszego segmentu

Parametr	Do czego służy
`myorigin`	domena, jaka pojawia się jako nadawca w wiadomościach wysyłanych lokalnie bez pełnego adresu — zwykle wskazuje plik `/etc/mailname` albo wprost `$mydomain`
`inet_interfaces`	interfejsy sieciowe, na których Postfix nasłuchuje; `loopback-only` ogranicza nasłuch do `127.0.0.1`, co jest typowe dla serwera aplikacyjnego niepełniącego roli publicznego MTA
`mynetworks`	zakresy adresów IP, którym Postfix ufa i pozwala przekazywać pocztę dalej (relay) bez uwierzytelnienia
`relayhost`	adres zewnętrznego serwera, przez który Postfix przekazuje całą wychodzącą pocztę zamiast dostarczać ją bezpośrednio
`smtp_sasl_auth_enable`	włączenie uwierzytelniania SASL przy łączeniu się z `relayhost`
`smtp_sasl_password_maps`	wskazanie pliku z danymi logowania do przekaźnika (`sasl_passwd`)
`message_size_limit`	maksymalny rozmiar pojedynczej wiadomości w bajtach, wliczając załączniki
`smtpd_recipient_restrictions`	reguły decydujące, które wiadomości przychodzące Postfix w ogóle przyjmie

Konfiguracja serwera aplikacyjnego wysyłającego przez przekaźnik

> **Pojęcie: przekaźnik (relay, smart host).** Zewnętrzny serwer SMTP, przez który lokalny Postfix przekazuje całą wychodzącą pocztę, zamiast próbować dostarczyć ją bezpośrednio do serwerów MX odbiorców — typowe rozwiązanie dla serwera aplikacyjnego, który generuje powiadomienia (raporty, alerty, potwierdzenia), ale sam nie jest pełnoprawnym serwerem pocztowym wystawionym do internetu, nie ma własnego DKIM ani dobrej reputacji IP.

To jest najczęstszy scenariusz, jaki konfigurujemy — serwer aplikacyjny bez własnej domeny pocztowej, którego jedynym zadaniem jest bezpiecznie i wiarygodnie przekazać pocztę dalej przez przekaźnik firmowy albo zewnętrznego dostawcę SMTP.



Aplikacja wysyła pocztę do lokalnego Postfixa na loopback, a ten przekazuje ją dalej przez uwierzytelniony przekaźnik SMTP zamiast łączyć się bezpośrednio z internetem (kliknięcie otwiera pełny rozmiar)

Ustawienie własnej nazwy hosta

```
sudo postconf -e "myhostname = NazwaSerwera.zielona.example"
```

Ograniczenie nasłuchu do interfejsu lokalnego

```
sudo postconf -e "inet_interfaces = loopback-only"
```

Serwer aplikacyjny nie ma przyjmować poczty z zewnątrz, tylko lokalnie od procesów działających na tej samej maszynie (np. cron, aplikacja wysyłająca powiadomienia) — ograniczenie nasłuchu do `loopback-only` zamyka Postfix na porcie 25 dla całej reszty sieci.

Wskazanie przekaźnika: relayhost

```
sudo postconf -e "relayhost = [AdresPrzekaznika]:587"
```

Nawiasy kwadratowe wokół adresu wyłączają wyszukiwanie rekordu MX dla tego adresu — Postfix łączy się z nim bezpośrednio, tak jakby to była nazwa hosta, a nie domena pocztowa.

Włączenie uwierzytelniania SASL wobec przekaźnika

```
sudo postconf -e "smtp_sasl_auth_enable = yes"
sudo postconf -e "smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd"
sudo postconf -e "smtp_sasl_security_options = noanonymous"
sudo postconf -e "smtp_tls_security_level = encrypt"
```

`smtp_sasl_security_options = noanonymous` zabrania Postfixowi próby połączenia bez uwierzytelnienia, gdyby z jakiegoś powodu dane logowania okazały się niedostępne — wolimy błąd dostarczenia niż wysłanie nieuwierzytelnionej próby, którą przekaźnik i tak odrzuci.

Utworzenie pliku z danymi logowania do przekaźnika: sasl_passwd

```
echo "[AdresPrzekaznika]:587 NazwaUzytkownika:HasloUzytkownika" | sudo tee
/etc/postfix/sasl_passwd
```

Format pliku to jedna linia na przekaźnik: adres i port w nawiasach kwadratowych, spacja, `login:hasło`.

Zbudowanie bazy danych z pliku sasl_passwd: postmap

```
sudo postmap /etc/postfix/sasl_passwd
```

> **Pojęcie: postmap.** Postfix nie czyta plików typu `hash:` bezpośrednio w formacie tekstowym — `postmap` kompiluje plik tekstowy do binarnej bazy danych (`sasl_passwd.db`) w formacie zadeklarowanym w nazwie mapy (`hash`, `btree`). Po każdej zmianie samego pliku tekstowego trzeba ponownie wykonać `postmap`, inaczej Postfix nadal korzysta ze starej zawartości bazy.

Przykład (komenda przy powodzeniu nic nie wypisuje, sprawdzamy kod wyjścia):

```
echo $?
```

```
0
```

Ograniczenie uprawnień pliku z hasłami

```
sudo chmod 0600 /etc/postfix/sasl_passwd /etc/postfix/sasl_passwd.db
```

Plik zawiera hasło w postaci jawnej — ograniczamy odczyt wyłącznie do właściciela (roota), tak samo jak każdy inny plik z poświadczeniami na serwerze.

Wczytanie kompletu zmian

```
sudo systemctl reload postfix.service
```

Limit rozmiaru wiadomości: message_size_limit

```
sudo postconf -e "message_size_limit = 26214400"
```

Wartość podajemy w bajtach — powyższe 26214400 to 25 MB, typowy limit zgodny z ograniczeniami większości zewnętrznych przekaźników i skrzynek odbiorczych. Wiadomość przekraczająca ten limit jest odrzucana już przez lokalny Postfix, zanim w ogóle trafi do kolejki wychodzącej.

Ograniczenia dla wiadomości przychodzących: smtpd_recipient_restrictions

```
smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated,
reject_unauth_destination
```

> **Pojęcie: smtpd_recipient_restrictions.** Uporządkowana lista reguł sprawdzana przy każdej próbie dostarczenia wiadomości do lokalnej instancji, sprawdzana od lewej do prawej — pierwsza reguła, która jednoznacznie rozstrzyga (zezwól albo odrzuć), kończy sprawdzanie. `permit_mynetworks` przepuszcza połączenia z zaufanych sieci zdefiniowanych w `mynetworks`, `permit_sasl_authenticated` przepuszcza klientów, którzy poprawnie się uwierzytelnili, a `reject_unauth_destination` na końcu odrzuca wszystko, co próbuje przekazać pocztę dalej (relay) bez spełnienia żadnego z wcześniejszych warunków — to jest reguła zamykająca, chroniąca przed użyciem naszego serwera jako otwartego przekaźnika (open relay) dla całego internetu.

Wielointancyjność Postfixa na jednym serwerze

> **Pojęcie: instancja Postfixa.** Osobny, niezależnie skonfigurowany zestaw plików (`main.cf`, `master.cf`, własny `sasl_passwd`) i osobna usługa systemd, działające obok siebie na tej samej maszynie, każda nasłuchująca na innym porcie lokalnym. Serwery aplikacyjne obsługujące kilku różnych klientów albo kilka niezależnych integracji pocztowych czasem uruchamiają po kilka takich instancji zamiast jednej wspólnej konfiguracji — każda z osobnym `relayhost`, osobnymi danymi logowania i osobną nazwą nadawcy.

Typowy układ katalogów przy kilku instancjach na jednym serwerze:

```
/etc/postfix/              — instancja domyślna, usługa postfix.service
/etc/postfix_klientA/      — druga instancja, usługa postfix_klientA.service
/etc/postfix_klientB/      — trzecia instancja, usługa postfix_klientB.service
```

Każda instancja ma własny plik `main.cf` pod swoją ścieżką, własną bazę `sasl_passwd` i własną jednostkę systemd o nazwie odpowiadającej nazwie katalogu — komendy `postmap`, `postconf -c SciezkaDoPliku` i `systemctl reload` trzeba wtedy wykonać osobno dla każdej instancji, której zmiana dotyczy.

```
sudo postmap /etc/postfix_klientA/sasl_passwd
sudo systemctl reload postfix_klientA.service
```

Uważaj: przy kilku instancjach na jednej maszynie zawsze sprawdzamy najpierw, której instancji dotyczy dana zmiana — część konfiguracji skrzynek bywa używana w więcej niż jednej instancji naraz, więc zmiana zrobiona tylko w jednej z nich, gdy powinna dotyczyć kilku, kończy się połowicznym, trudnym do zdiagnozowania efektem.

Częste błędy

Zapomniany postmap po zmianie sasl_passwd. Plik tekstowy jest już poprawny, ale Postfix nadal używa starych danych logowania, bo baza `.db` nie została przebudowana — każda zmiana pliku typu `hash:` wymaga ponownego `postmap`.

Brak reject_unauth_destination na końcu smtpd_recipient_restrictions. Serwer staje się otwartym przekaźnikiem, przez który dowolny nadawca z internetu potrafi wysyłać pocztę do dowolnego odbiorcy — to jest błąd konfiguracyjny prowadzący do umieszczenia adresu IP serwera

na czarnych listach w ciągu godzin.

Edycja main.cf bezpośrednio zamiast przez postconf -e. Ręczna edycja pliku jest w porządku, ale łatwo o literówkę w nazwie parametru, którą Postfix po prostu zignoruje bez ostrzeżenia — `postconf -e` sprawdza nazwę parametru względem znanej listy i od razu zwraca błąd przy literówce.

□□ Ćwiczenia

> Ćwiczenia zakładają lokalną instalację Postfixa i dostęp do dowolnego testowego konta SMTP z uwierzytelnianiem (np. skrzynka testowa na własnej domenie).

Ćwiczenie 1 — podgląd rzeczywistej konfiguracji

```
sudo postconf -n | sort
```

Wypisujemy i porównujemy z tabelą wyżej, które z najważniejszych parametrów są w naszej instalacji jawnie ustawione, a które pozostały na wartości domyślnej.

Odpowiedź

Świeża instalacja Postfixa zwykle ma ustawione tylko kilka parametrów (`myhostname`, `mydestination`, `mynetworks`, `inet_interfaces`) — reszta z tabeli, w tym cały blok `smtp_sasl_*` i `relayhost`, pojawia się dopiero po ręcznej konfiguracji przekaźnika.

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

Źródła: `man 5 postconf` · `man 1 postmap` · dokumentacja postfix.org, rozdział „STANDARD_CONFIGURATION_README" i „SASL_README"

Revision #37
Created 2026-09-25 07:40:18 UTC by Tomasz Konieczny
Updated 2026-10-26 14:16:01 UTC by Tomasz Konieczny