# Postfix Main – plik konfiguracyjny



## Plik

```
# Postfix jest chrootowany do tej ścieżki (nie widzi nic w folderach nadrzędnych):
queue_directory = /var/spool/postfix

# Domyślnie, Postfix kieruje pocztę do /var/spool/mail/user albo do /var/mail/user. Można to zmienić:
# home_mailbox = .maildir/

command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
data_directory = /var/lib/postfix
mail_owner = postfix

# Niektórzy zalecają wpisanie tutaj pełnej nazwy, czyli "myhostname = acer-i7.$mydomain":
myhostname = asus-i7
mydomain = 3bird
inet_interfaces = all

# Do jakich adresów (domen) lokalnych będzie dostarczana poczta przychodząca (do innych nie będzie, chyba że są utworzone aliasy w /etc/postfix/aliases i /ect/postfix/virtual). Poczta dostarczana jest także na same lokalne nazwy użytkowników (bez małpy i bez nazwy domenowej):
mydestination = $myhostname, localhost.$mydomain, $myhostname.$mydomain, localhost

# Domyślna nazwa domeny FQDN (Fully Qualified Domain Name), jaka będzie doklejana do adresu przy wysyłaniu poczty lokalnej w trybie tekstowym (np. jeśli wyślemy list do użytkownika "adam", Postfix doklei mu domenę lokalną, czyli adres odbiorcy będzie jako "adam@$myorigin"; to samo w przypadku nazwy nadawcy, jeśli list pochodzi od "norbert", to Postfix doklei mu domenę i określi nadawcę jako "norbert@$myorigin"). Nazwa ta nie będzie doklejana, jeśli od razu podamy pełny adres nadawcy lub odbiorcy z jakąś domeną po znaku @. Możliwe jest tutaj tylko doklejanie domeny lokalnej (nie publicznej!).
#myorigin = $myhostname (domyślnie)
#myorigin = $mydomain
#myorigin = /folder/plik_z_nazwa_domeny
myorigin = $myhostname.$mydomain

#local_recipient_maps = unix:passwd.byname $alias_maps
unknown_local_recipient_reject_code = 550

# Określamy uprzywilejowaną grupę nadawców, która może wysyłać e-maile poprzez Postfiksa. E-maile pochodzące z innych źródeł nie będą przez Postfiksa wysyłane. Należy być świadomym wirusów, które też mogą wysyłać e-maile.
#mynetworks_style = class (Postfix ufa wszystkim maszynom mającym tę samą klasę IP)
#mynetworks_style = host (Postfix ufa tylko lokalnej maszynie)
# Postfix ufa wszystkim maszynom w podsieci (domyślnie):
mynetworks_style = subnet
```

mynetworks = 192.168.0.0/24, 127.0.0.0/8, 192.168.17.0/24, 192.168.7.0/24

########################## SASL

# Metoda ta nie sprawdzi się w przypadku użytkowników mobilnych (zmieniających sieci). W tym przypadku potrzebna będzie autoryzacja na podstawie SASL i/lub SSL/TLS. Poniżej aktywacja SASL (z pakietu Cyrus-SASL):

smtpd_sasl_auth_enable = yes

# Poniżej... dovecot lub cyrus:

smtpd_sasl_type = cyrus

smtpd_sasl_path = smtpd

# Nazwa nadawcy SASL umieszczana jest w nagłówku e-maila:

smtpd_sasl_authenticated_header = yes

# Jeśli z jakiegoś powodu zawiedzie uwierzytelnianie PLAIN, Postfix może zaoferować uwierzytelnianie ANONYMOUS (czyli brak uwierzytelniania). Nie chcemy tego i blokujemy to:

smtpd_sasl_security_options = noanonymous

# Gdy dwóch różnych użytkowników ma tę samą nazwę użytkownika, ale różne domeny:

smtpd_sasl_local_domain = $myhostname.$mydomain

# Czy Postfix ma próbować obsługi klientów, którzy mają niestandardowe wymagania względem komendy AUTH (np. wczesne wersje Outlooka). W przypadku aktywacji tej opcji, w sesji telneta pojawią się dwa wpisy AUTH, trochę różniące się między sobą:

broken_sasl_auth_clients = yes

# Pozwalamy na autoryzację użytkownika (polecenie AUTH) i hasła (zazwyczaj w plain-text) dopiero po nawiązaniu szyfrowanego połączenia TLS (jeśli nie mamy gotowego TLS, nie możemy uaktywniać tej opcji, bo SASL nie będzie autoryzował użytkowników):

#smtpd_tls_auth_only = yes

# Restrykcje dla poczty wychodzącej (w starszych wersjach było to smtpd_recipient_restrictions). Kolejność opcji nie jest bez znaczenia:

# smtpd_relay_restrictions= reject_unauth_pipelining, permit_mynetworks, permit_sasl_authenticated, check_relay_domains, reject_non_fqdn_recipient, reject_unauth_destination, check_policy_service inet:127.0.0.1:60000, permit:

# smtpd_sender_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_non_fqdn_sender, reject_unknown_sender_domain, reject_unauth_pipelining, permit

########################## Opcje TLS:

# smtp_sasl_tls_security_options = $smtp_sasl_security_options

smtpd_use_tls = yes

smtp_use_tls = yes

# Postfix zaoferuje zdalnym klientom obsługę TLS (słowo STARTTLS ESMTP), ale nie wymaga od nich konieczności szyfrowania TLS (wartość "may"), jeśli klient lub serwer nie ma możliwości obsługi takiej funkcji (nie dogadają się, co do tego --> "TLS handshake failed"), wtedy Postfix umożliwi klientowi wysłanie wiadomości bez obsługi TLS (jako zwykły nieszyfrowany tekst). Jeśli ustawiona jest wartość "may" lub "encrypt", wtedy wiadomość zostanie wysłana nawet wtedy, gdy certyfikat serwera jest niezaufany lub zawiera złą nazwę. Jeśli chcemy wymusić szyfrowanie TLS, należy poniżej wpisać wartość "encrypt" (mamy wtedy "TLS encryption", ale

nie "TLS authentication", gdyż certyfikat jest samopodpisany, i nie ma autentykacji publicznej instytucji), a jeśli chcemy, aby wiadomość została wysłana tylko po autentykacji zaufanych certyfikatów wystawionych przez publiczne instytucje, wtedy wprowadzamy wartość "verify":

```
smtpd_tls_security_level = may

# Możemy ustawić preferencje: do których domen ma być zastosowana wartość "may", a do których wartość "encrypt":
# smtp_tls_policy_maps = hash:/etc/postfix/tls_policy
# Przykładowa zawartość pliku "tls_policy":
# example.com       encrypt
# .example.com      encrypt
smtp_tls_note_starttls_offer = yes
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
tls_random_source = dev:/dev/urandom
smtpd_tls_CAfile = /etc/postfix/tls/cacert.pem
smtpd_tls_CApath  = /etc/postfix/tls

# Certyfikaty są wczytywane, choć manual mówi, iż w prywatnej sieci, Postfix nie powinien korzystać z certyfikatów (chyba) i powinien być parametr "none" (czyli wyłączona funkcja TLS):
smtpd_tls_cert_file = /etc/postfix/tls/smtpd.pem

# Klucz prywatny znajduje się w tym samym pliku, co certyfikat:
# smtpd_tls_key_file = $smtpd_tls_cert_file
smtpd_tls_key_file = /etc/postfix/tls/cakey.pem
smtpd_tls_ask_ccert = yes

# Nie pozwalamy, aby nasz Postfix służył innym sieciom jako open relay:
#relay_domains = $mydestination
relay_domains =

# Ustalamy, czy nasz Postfix sam wysyła pocztę bezpośrednio do adresata, czy też przekazuje ją innemu serwerowi SMTP do wysyłki. Jeśli całą pocztę wychodzącą z naszego serwera chcemy wysyłać za pośrednictwem innego serwa (takiego, na którym np. działa program antywirusowy lub np. nasz jest blokowany na firewallu) powinniśmy użyć relayhost. Wówczas każdy email wychodzący z naszego komputera przekazywany jest właśnie do niego:
#relayhost = $mydomain
#relayhost = [gateway.my.domain]

alias_maps = hash:/etc/mail/aliases
alias_database = hash:/etc/mail/aliases
mail_spool_directory = /var/spool/mail

# Wirtualne adresy domenowe (przeznaczone dla użytkowników wirtualnych,a nie realnych):
virtual_alias_maps = hash:/etc/postfix/virtual
# Jeśli chcemy mieć dodatkowe wirtualne (inne niż realne) lokalne domeny w adresach:
virtual_alias_domains = imagine
virtual_mailbox_domains= imagine
```

```
# Odwzorowanie (zamiana) lokalnego adresu nadawcy (np. "robert@server.3bird" lub samo "robert") na adres publiczny (np. "robertsurma@op.pl"), aby odbiorca wiadomości miał szansę na nią odpowiedzieć i przesłać przez publiczną sieć.
smtp_generic_maps = hash:/etc/postfix/generic
# W starszych wersjach stosowano zamiast tego nieaktualny już wpis: sender_canonical_maps = hash:/etc/postfix/sender_canonical

# Co Postfix ma robić, gdy odbierze list do nieistniejącego już użytkownika:
# relocated_maps = hash:/etc/postfix/relocated

# Każda kopia listu przechodzącego przez Postfixa trafia także pod wskazany adres (czyli inwigilacja!):
# always_bcc = czesiu@uop.pl

#Jeśli chciałbyś przechwytywać całą pocztę przychodzącą dla użytkowników, którzy w systemie nie istnieją, powinieneś skorzystać z parametru luser_relay. Możesz w ten sposób wyczajać spamerów i zapobiec odbijaniu poczty z interesującymi danymi w nagłówkach. Dużym minusem jest fakt, że jeśli osoba z zewnątrz popełniła literówkę w adresie odbiorcy - nie dowie się o tym, że list nie dotarł do adresata. Przykład:
#luser_relay = admin+$local

local_destination_concurrency_limit = 2
default_destination_concurrency_limit = 20
debug_peer_level = 2
debugger_command =
        PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
        ddd $daemon_directory/$process_name $process_id & sleep 5
sendmail_path = /usr/sbin/sendmail
newaliases_path = /usr/bin/newaliases
mailq_path = /usr/bin/mailq
setgid_group = postdrop

# Ścieżka do dokumentacji Postfix:
html_directory = no
manpage_directory = /usr/share/man
sample_directory = /etc/postfix
readme_directory = no
inet_protocols = ipv4

# Maksymalna ilość adresów w sekcji CC i BCC:
smtpd_recipient_limit = 10

# Maksymalna wielkość maila w bajtach:
message_size_limit = 1000000

# Maksymalna wielkość skrzynki pocztowej użytkownika w bajtach:
mailbox_size_limit = 5000000

# Ilość wolnego miejsca na partycji /var/spool, która nie może być spożytkowana przez Postfixa (chroni przed zapełnieniem partycji):
```

```
queue_minfree = 10000000

# W przypadku, gdy zdalny serwer nie odpowiada, sprawdzaj zdalnego co 20 minut i zwracaj błąd do nadawcy po dwóch dniach:
queue_run_delay = 20m
maximal_queue_lifetime = 2d

# Brak wstecznej kompatybilnosci:
compatibility_level = 2
```

Ostatnia aktualizacja: 11 sierpnia 2018.