

**Instytut Teleinformatyki**

Wydział Inżynierii Elektrycznej i Komputerowej  
Politechnika Krakowska



Laboratorium Administrowania Systemami Komputerowymi

# *„Konfiguracja serwera pocztowego Postfix”*

ćwiczenie numer: 6

---

## Spis treści

<b>1. WSTĘPNE INFORMACJE .....</b>	<b>3</b>
1.1 <b>TEMAT ĆWICZENIA .....</b>	<b>4</b>
1.2 <b>ZAGADNIENIA DO PRZYGOTOWANIA .....</b>	<b>4</b>
1.3 <b>CEL ĆWICZENIA .....</b>	<b>4</b>
<b>2. PRZEBIEG ĆWICZENIA .....</b>	<b>5</b>
2.1 <b>PRZYGOTOWANIE ĆWICZENIA .....</b>	<b>6</b>
2.2 <b>ZADANIE NR 1 - KONFIGURACJA SERWERA POSTFIX.....</b>	<b>7</b>
2.3 <b>ZADANIE NR 2 – KONFIGURACJA SERWERA POP3S ORAZ IMAPS .....</b>	<b>9</b>
2.4 <b>ZADANIE NR 3 – KONFIGURACJA WIRTUALNYCH TABLIC KONT.....</b>	<b>13</b>
2.5 <b>ZADANIE NR 4 –KONFIGURACJA POSTGREY .....</b>	<b>14</b>
2.6 <b>ZADANIE NR 5 – KONFIGURACJA AUTORYZACJI START TLS .....</b>	<b>15</b>
2.7 <b>ZADANIE NR 6 – KONFIGURACJA NARZĘDZI DO ZARZĄDZANIA POCZTY.....</b>	<b>16</b>
2.8 <b>ZADANIE NR 7 – MONITOROWANIE POCZTY .....</b>	<b>17</b>
2.8 <b>ZAKOŃCZENIE ĆWICZENIA .....</b>	<b>18</b>
2.9 <b>OPRACOWANIE ĆWICZENIA I SPRAWOZDANIE.....</b>	<b>19</b>

---

# 1. Wstępne informacje

## 1.1 TEMAT ĆWICZENIA

Tematem ćwiczenia jest skonfigurowanie prostego serwera pocztowego.

## 1.2 ZAGADNIENIA DO PRZYGOTOWANIA

Przed przystąpieniem do wykonania ćwiczenia należy zapoznać się z następującymi zagadnieniami:

- Wirtualne tablice kont,
- Szare listy (greylisting),
- Protokoły pocztowe IMAP, POP3, SMTP,
- Zarządzanie pocztą przy pomocy programu Squirrelmail
- Monitorowanie poczty programem Mailgraph

## 1.3 CEL ĆWICZENIA

Dzięki temu ćwiczeniu wykonujący pozna:

- sposób konfiguracji oraz zarządzania serwerem pocztowym Postfix.

---

## **2. Przebieg ćwiczenia**

## 2.1 PRZYGOTOWANIE ĆWICZENIA

Po załączeniu komputera należy uruchomić system operacyjny o nazwie ASK. Jest to dedykowany system umożliwiający wykonanie niniejszego ćwiczenia.

### Logowanie

W celu wykonania ćwiczenia konieczne jest zalogowanie się na konto administratora (login: root, hasło: lab).

### Katalog laboratoryjny

Przed przystąpieniem do zajęć należy utworzyć katalog gdzie będą przechowywane kopie zapasowe wszystkich plików modyfikowanych w trakcie wykonywania ćwiczenia.

```
itilab1:~/#mkdir postfix
```

## 2.2 ZADANIE NR 1 - KONFIGURACJA SERWERA POSTFIX

Zadanie to polega na skonfigurowaniu serwera pocztowego. Zaczniemy od stworzenia kopii zapasowych plików konfiguracyjnych postfix'a i skopiujemy je do wyżej utworzonego katalogu. Plik, który będzie my modyfikować jest w następującej lokalizacji

```
/etc/postfix/main.cf
```

Wykonujemy polecenie

```
hostname
```

Otwórzmy powyższy plik w edytorze i wklejmy do niego następującą konfigurację:

```
command_directory = /usr/sbin
mail_owner = postfix
mydomain = stanowisko01 //wpisujemy co zwróci hostname
myhostname = stanowisko01 //wpisujemy co zwróci hostname
myorigin = /etc/mailname
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = $mydomain, $myhostname, localhost,
localhost.localdomain,
mynetworks = 127.0.0.0/8
inet_interfaces = all
inet_protocols = ipv4
home_mailbox = Maildir/
mail_spool_directory = /home/
smtpd_banner = ESMTP on $myhostname !
mailbox_size_limit = 0
recipient_delimiter = +
biff = no
append_dot_mydomain = no
relayhost =
```

Po wpisaniu tej konfiguracji wykonujemy polecenie, które sprawdzi nam poprawność konfiguracji.

```
postfix check
```

Tworzymy bazę aliasów poleceniem:

```
newaliases
```

I restartujemy demona

```
/etc/init.d/postfix restart
```

Sprawdzamy teraz czy nasza konfiguracja poprawnie zadziała:

```
# telnet localhost 25

Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 ESMTTP on myhostname !
EHLO myhostname //to co wpisywaliśmy w main.cf
250-nazwa_komputera
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Pogrubione są polecenia które wpisujemy. Jeśli wynik jest taki jak powyżej wtedy wszystko działa poprawnie.



## 2.3 ZADANIE NR 2 – KONFIGURACJA SERWERA POP3S ORAZ IMAPS

Wykorzystamy w tym ćwiczeniu zestaw pakietów dovecot. POP3s oraz IMAPs są to protokoły do odbierania poczty z szyfrowaniem transmisji przez SSL. Jeśli w pliku *dovecot.conf* przy opcji *protocols* mamy wpisane *imap imaps pop3 pop3s*. Oznacza to, że na naszym komputerze działają proste serwery IMAP i POP3 jak i serwery szyfrowane.

Ustawiamy prawa do katalogów:

```
#chmod 755 /var/run/dovecot
#chgrp dovecot /var/run/dovecot/login/
```

Kolejnym krokiem jest stworzenie katalogu, w którym będziemy przechowywać nasz certyfikat

```
#mkdir -p /etc/postfix/ssl
```

Przechodzimy do tego katalogu i z jego poziomu tworzymy certyfikat:

```
# openssl req -new -x509 -nodes -out mail.pem -keyout mail.pem -days 365
Country Name (2 letter code) [AU]:PL
State or Province Name (full name) [Some-State]:POLAND
Locality Name (eg, city) []:Krakow
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Moj certyfikat
Organizational Unit Name (eg, section) []:POCZTA
Common Name (eg, YOUR name) []:myhostname
Email Address []:root@myhostname
```

W celu konfiguracji tworzymy kopię zapasową pliku, który znajduje się w poniższej lokalizacji, do naszego katalogu postfix

```
/etc/dovecot/dovecot.conf
```

Edytujemy go i wklejamy poniższą konfigurację:

```
base_dir = /var/run/dovecot/
protocols = imap imaps pop3 pop3s
listen = *
disable_plaintext_auth = no
shutdown_clients = yes

#logi
log_path=/var/log/dovecot.log
info_log_path = /var/log/mail.log
log_timestamp = "%Y-%m-%d %H:%M:%S "
syslog_facility = mail
```

```
login_process_size = 64
login_greeting = Welcome. I'm ready ...
login_log_format_elements = user=<%u> method=%m rip=%r lip=%l %c
login_log_format = %$: %s
login_chroot = no
login_user = dovecot
login_process_per_connection = yes
login_processes_count = 3
login_max_processes_count = 128
mail_location = maildir:~/Maildir
#SSL
ssl_cert_file = /etc/postfix/ssl/mail.pem
ssl_key_file = /etc/postfix/ssl/mail.pem
verbose_ssl = yes
mail_access_groups = postfix
protocol imap {
}
protocol pop3 {
    pop3_uidl_format = %08Xu%08Xv
}
protocol lda {
    postmaster_address = postmaster@myhostname
}
auth_verbose = yes
auth_debug = yes
auth default {
    mechanisms = plain login
    passdb pam {
    }
    userdb passwd {
    }
    user = root
}
dict {
}
plugin {
}
```

Startujemy demona

```
/etc/init.d/dovecot start
```

Sprawdzamy teraz poprawność powyższej konfiguracji. W tym celu musimy stworzyć dwóch użytkowników w systemie ustawiając im hasła „hasło”.

```
#useradd -m nadawca -u 999
#passwd nadawca

#useradd -m odbiorca -u 998
#passwd odbiorca
```

```
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 ESMTTP on myhostname !
EHLO myhostname
250-debian
250-PIPELINING
250-SIZE 10240000
250-VERFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
mail from: nadawca@myhostname
250 2.1.0 Ok
rcpt to: odbiorca@myhostname
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: mail testowy

to jest testowy mail
zaraz zobaczymy czy dojdzie:)
.
250 2.0.0 Ok: queued as A912CBACD
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Pogrubione są polecenia, które wprowadzamy.

Teraz sprawdzamy czy wyżej wysłany mail doszedł. W tym celu wykonujemy polecenie.

```
# ls -l /home/odbiorca
razem 4
drwx----- 5 odbiorca odbiorca 4096 2007-11-03 15:59 Maildir
```

Takie polecenie powinno zwrócić podobny wynik co oznacza, że nasz mail został wysłany i doszedł do odbiorcy. Teraz sprawdzamy serwer POP3 szyfrowany:

```
# openssl s_client -connect localhost:995
//tu pojawi się informacja o certyfikacie, który wcześniej
//został utworzony
+OK Welcome. I'm ready ...
user odbiorca
+OK
pass haslo
+OK Logged in.
stat
+OK 1 485
list
+OK 1 messages:
1 485
```

```
.  
retr 1  
+OK 485 octets  
Return-Path: <nadawca@myhostname>  
X-Original-To: odbiorca@ myhostname  
Delivered-To: odbiorca@ myhostname  
Received: from pk.edu.pl (localhost [127.0.0.1])  
        by debian (Postfix) with ESMTP id A912CBACD  
        for <odbiorca@myhostname >; Sat,  3 Nov 2007 15:54:52  
+0100 (CET)  
Subject: mail testowy  
Message-Id: <20071103145513.A912CBACD@debian>  
Date: Sat,  3 Nov 2007 15:54:52 +0100 (CET)  
From: nadawca@pk.edu.pl  
To: undisclosed-recipients:;  
  
to jest testowy mail  
zaraz zobaczymy czy dojdzie:)  
.  
quit  
+OK Logging out.  
Connection closed by foreign host.
```

Jeśli taki uzyskaliśmy efekt to znaczy, że wszystko działa poprawnie.

## 2.4 ZADANIE NR 3 – KONFIGURACJA WIRTUALNYCH TABLIC KONT

Dzięki takim tablicom możemy pozwolić konkretnym userom w systemie na dobieranie maili na adresy, które sami zdefiniujemy. Żeby poprawnie skonfigurować wirtualne domeny wykonujemy następujące polecenia.

Pierwszym krokiem jest stworzenie w systemie kont na potrzeby tego ćwiczenia i nadajemy im jednakowe hasło np. hasło. Przykładowo:

```
#useradd -m virtual1 -u 997
#useradd -m virtual2 -u 996
```

Tworzymy, lub edytujemy następujący plik i wpisujemy do niego następującą konfigurację:

```
#nano /etc/postfix/virtual

example                domain //ten tekst jest ignorowany
postmaster@example    postmaster
address1@example      virtual1
address2@example      virtual2
@example              odbiorca
```

Teraz musimy wskazać postfixowi gdzie ma szukać tych wirtualnych kont. W tym celu dodajemy do pliku main.cf konfigurację:

```
#virtual_alias_maps = hash:/etc/postfix/virtual
```

Pozostaje nam tylko restart demona postfix oraz aktualizujemy wpisy w pliku virtual.

```
postfix reload
postmap /etc/postfix/virtual
```

Żeby sprawdzić czy to działa wystarczy spróbować wysłać maile na adresy wyżej podane address1@example i zobaczyć czy został on dostarczony do użytkownika virtual1. Wykonujemy to tak jak w ćwiczeniu poprzednim, poleceniem telnet localhost 25. Żeby sprawdzić czy działa możemy wpisać polecenie

```
#ls -l /home/virtual1
```

Powinien się pokazać katalog Maildir, co oznacza, że nasz mail na adres address1@example doszedł do użytkownika virtual1.

## 2.5 ZADANIE NR 4 – KONFIGURACJA POSTGREY

Teraz zajmiemy się konfiguracją usługi wspomagającej szare listy dla Postfixa. Proszę skopiować plik:

```
/etc/default/postgrey
```

Edytujemy powyższy plik i zmieniamy w następującą linijkę:

```
POSTGREY_OPTS="--inet=127.0.0.1:10023 --delay=3600"
```

Powyższa linia skonfiguruje postgreya tak aby nasłuchiwał na porcie 10023 (opcja --inet=10023) oraz ustawi czas odrzucania wiadomości na 1 godzinę (opcja --delay=3600). Domyślnie czas odrzucania wiadomości to 5 minut (300 sekund), jednak skuteczność greylist przy tak krótkim czasie odrzucania jest dużo niższa. Po wykonaniu tej czynności startujemy demona postgreya:

```
#/etc/init.d/postgrey restart
```

Teraz sprawdzmy czy demon postgrey działa poprawnie wpisując polecenie:

```
#netstat -ltnp | grep postgrey
tcp    0    0  127.0.0.1:10023    0.0.0.0:*        LISTEN
504/postgrey -d --i
```

I jeżeli wyniki jest podobny do tego jak wyżej to oznacza, że postgrey działa poprawnie. Teraz skonfigurujemy postfixa tak żeby korzystał z postgreya

Edytujemy plik i wpisujemy do niego następujące wartości:

```
smtpd_recipient_restrictions =
[...]
check_policy_service = inet:127.0.0.1:10023
```

Zapisujemy w nim zmiany, restartujemy demona postfixa i już wszystko gotowe.

```
#/etc/init.d/postfix restart
```

## 2.6 ZADANIE NR 5 – KONFIGURACJA AUTORYZACJI START TLS

Zajmijmy się teraz konfiguracją uwierzytelniania użytkowników za pomocą START TLS. Edytujemy plik main.cf i wpisujemy następującą konfigurację:

```
# nano /etc/postfix/main.cf

#TLS
smtpd_tls_auth_only = yes
smtp_use_tls = yes
smtpd_use_tls = yes
smtpd_tls_note_starttls_offer = yes
smtpd_tls_key_file = /etc/postfix/ssl/mail.pem
smtpd_tls_cert_file = /etc/postfix/ssl/mail.pem
smtpd_tls_CAfile = /etc/postfix/ssl/mail.pem
smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s
smtpd_tls_session_cache_database =
btree:${queue_directory}/smtpd_scache
smtpd_tls_session_cache_database =
btree:${queue_directory}/smtp_scache
tls_random_source = dev:/dev/urandom
```

Restartujemy postfixa i sprawdzamy czy działa:

```
# /etc/init.d/postfix restart
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 ESMTTP on myhostname !
EHLO myhostname
250-debian
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Jeśli widzimy linijkę **250-STARTTLS** to znaczy, że poprawnie skonfigurowaliśmy.

## 2.7 ZADANIE NR 6 – KONFIGURACJA NARZĘDZI DO ZARZĄDZANIA POCZTY

Kolejnym ćwiczeniem będzie skonfigurowanie narzędzia Squirrelmail dzięki, któremu w łatwy sposób będzie można zarządzać kontami pocztowymi przez przeglądarkę. Robimy symboliczne dowiązanie pliku apache.conf

```
# ln -s /etc/squirrelmail/apache.conf /etc/apache2/conf.d/squirrelmail
```

Edytujemy plik apache.conf:

```
# nano /etc/squirrelmail/apache.conf

Znajdujemy wartość:
Alias /squirrelmail /usr/share/squirrelmail

I zamieniamy ją na :
Alias /poczta /usr/share/squirrelmail
```

Zróbmy jeszcze dowiązanie do plików squirrelmail w katalogu WWW, żeby łatwiej było znaleźć:

```
# ln -s /usr/share/squirrelmail /var/www/poczta
```

Restartujemy apache:

```
# /etc/init.d/apache2 restart
```

Ustawiamy jeszcze w squirrelmaila nasz predefiniowany serwer IMAP czyli dovecot, w tym celu wykonaj polecenie:

```
# /usr/sbin/squirrelmail-configure
```

Pojawi się konfigurator squirrelmaila. Wpisujemy D i wciskamy enter. Teraz wpisujemy z jakiego serwera IMAP korzystamy i enter, w następnym okienku zostaw wszystko domyślnie. Zapisz ustawienia i wyjdź z konfiguratora. Sprawdzamy czy squirrelmail działa przez wpisanie w przeglądarce adresu:

```
http://localhost/poczta/src/login.php
```

Jeżeli pokaże się okno logowania to oznacza, że działa poprawnie. Możemy też zalogować się na jedno z wcześniej utworzonych kont, np. na to na które wysyłaliśmy maila, dzięki temu w łatwy sposób zobaczymy tego maila.



## 2.8 ZADANIE NR 7 – MONITOROWANIE POCZTY

Zajmiemy się teraz konfiguracją narzędzia do monitorowania poczty Mailgraph.

Wydaj polecenie:

```
# dpkg-reconfigure mailgraph

Should Mailgraph start on boot?      <-- Yes
Which logfile should be used by mailgraph?  <-- /var/log/mail.log
Count incoming mail as outgoing mail?  <-- Yes
```

Utwórz katalog:

```
# mkdir -p /var/www/cgi-bin/
```

Zrób link symboliczny do skryptów odpowiedzialnych za generowanie wykresów:

```
# ln -s /usr/lib/cgi-bin/mailgraph.cgi /var/www/cgi-bin/
```

Żeby zobaczyć nasze wykresy wpisujemy w przeglądarce:

```
http://localhost/cgi-bin/mailgraph.cgi
```

## 2.8 ZAKOŃCZENIE ĆWICZENIA

Po zakończeniu ćwiczenia proszę przywrócić skopiowane pliki z wcześniej utworzonego katalogu. Usuń utworzonych użytkowników nadawcę, odbiorcę, virtual1, virtual2 w ten sam sposób:

```
itilabl:~# deluser nadawca
```

oraz usunięcie w systemie macierzystym katalogu postfix/ssl w którym utworzyliśmy certyfikat, oraz katalogu virtual

```
itilabl:~# rm -rf /postfix/  
itilabl:~# rm -rf /etc/postfix/ssl  
itilabl:~# rm -rf /etc/postfix/virtual
```

## 2.9 OPRACOWANIE ĆWICZENIA I SPRAWOZDANIE

Wykonanie ćwiczenia polega na praktycznej realizacji wszystkich zadań **Rozdziału 2** niniejszej instrukcji zatytułowanego „**Przebieg Ćwiczenia**”. Należy sporządzić sprawozdanie z wykonania ćwiczenia (w formie dokumentu elektronicznego) i w ciągu najdalej dwóch tygodni od dnia wykonania ćwiczenia oddać je prowadzącemu zajęcia.

Kompletne opracowanie ćwiczenia powinno zawierać:

- ✓ Część opisową odnoszącą się do teorii przerabianego ćwiczenia. Ta część sprawozdania powinna wykazać dobrą ogólną znajomość zagadnień leżących u podstaw przerabianego tematu, znajomość odnośnej literatury, samodzielność myślenia i umiejętność pisania opracowań o charakterze technicznym.
- ✓ Wnioski praktyczne wynikające z wykonania ćwiczenia, a w tym:
  - uwagi odnoszące się do przebiegu ćwiczenia (np. czy dane ćwiczenie może być wykonane z pełnym rozumieniem zawartych w nim czynności i problemów, czy ćwiczenie jest możliwe do wykonania w czasie przeznaczonym na zajęcia, czy ćwiczenie jest zbyt trudne/ zbyt łatwe, itp.),
  - uwagi odnoszące się do sposobu przygotowania i jakości (waloru dydaktycznego) instrukcji do ćwiczenia,
  - uwagi odnoszące się do ewentualnych utrudnień technicznych lub organizacyjnych pojawiających się w trakcie wykonywania ćwiczenia,
  - postulaty merytoryczne i techniczne dotyczące usprawnienia/ulepszenia jakości wykonywanego ćwiczenia,
  - inne

Wnioski z drugiej części sprawozdania posłużą do usprawnienia i poprawy zajęć laboratoryjnych w latach następnych.