

## T: Instalacja i konfiguracja serwera poczty.

Podczas wykonywania poniższych zadań w zeszycie w sprawozdaniu

1. podaj i wyjaśnij polecenia które użyjesz aby:
  - wyjaśnić pojęcia związane z ustawienia SSL w celu szyfrowania danych przesyłanych serwerami poczty elektronicznej,
  - zainstalować SSL w celu szyfrowania danych dla serwera poczty elektronicznej,
  - uruchomić lub zatrzymać SSL w celu szyfrowania danych,
  - konfigurować serwery poczty elektronicznej SSL w celu szyfrowania danych,
  - korzystać z ustawienia SSL w celu szyfrowania danych przesyłanych serwerami poczty elektronicznej.
2. podaj odpowiedzi na pytania zadane w treści zadań.

Uwaga: Ćwiczenie zakłada że przed nim wykonane zostało ćwiczenie **cw1 poczta**.

Wykonując ćwiczenie **cw1 poczta** nie wykonuj żadnych notatek, a tylko niezbędne czynności konfiguracyjne.

**Wszystkie polecenia konfiguracyjne zapisz w zeszycie z wyjaśnieniem ich działania.**

### Ustawienia SSL

Skonfiguruj ustawienia SSL w celu szyfrowania danych. SMTPS korzysta 465/TCP, POP3S korzysta 995/TCP, IMAPS korzysta 993/TCP.

[1] Tworzenie certyfikatów > Wykonaj sso\_1\99 SSL\ cw ssl.pdf

[2] Konfigurowanie Postfix i Dovecot SSL.

1. Utwórz plik konfiguracyjnym nano.

```
root@debian:~# nano ~/.nanorc
```

2. Dodaj wpisy do pliku ~/.nanorc

```
GNU nano 2.2.6 Plik: /root/.nanorc
```

```
set const
```

3. Wykonaj kopie /etc/postfix/main.cf do /etc/postfix/main.cf.bak

```
root@tu:~# cp /etc/postfix/main.cf /etc/postfix/main.cf.bak
```

Opisz w zeszycie:

- procedurę instalacji i konfiguracji oraz uruchomienia serwera pocztowego skonfigurowanego oparciu o ustawienia SSL w celu szyfrowania danych,
  - testowania uruchomionego serwera pocztowego skonfigurowanego oparciu o ustawienia SSL w celu szyfrowania danych.
4. Edytuj plik /etc/postfix/main.cf 

```
root@tu:~# nano /etc/postfix/main.cf
```

5. Dodaj wpisy na koniec pliku

```
smtpd_use_tls = yes
smtpd_tls_cert_file = /etc/ssl/private/server.crt
smtpd_tls_key_file = /etc/ssl/private/server.key
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
```

6. Wykonaj kopie `/etc/postfix/master.cf` do `/etc/postfix/master.cf.bak`

```
root@tu:/# cp /etc/postfix/master.cf /etc/postfix/master.cf.bak
```

7. Edytuj oraz odkomentuj linie 28-30 w `/etc/postfix/master.cf`

```
# -o milter_macro_daemon_name=ORIGINATING
smtps      inet      n       -       -       -       smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
# -o smtpd_sasl_auth_enable=yes
```

8. Wykonaj kopie `/etc/dovecot/conf.d/10-ssl.conf` do `/etc/dovecot/conf.d/10-ssl.conf.bak`

```
root@tu:/# cp /etc/dovecot/conf.d/10-ssl.conf /etc/dovecot/conf.d/10-ssl.conf.bak
```

9. Edytuj oraz zmodyfikuj linie 6 i odkomentuj i modyfikuj linie 12,13 w `dovecot/conf.d/10-ssl.conf`

```
GNU nano 2.2.6      Plik: /etc/dovecot/conf.d/10-ssl.conf
##
## SSL settings
##
# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = yes

# PEM encoded X.509 SSL/TLS certificate and private key. The
# dropping root privileges, so keep the key file unreadable
# root. Included doc/mkcert.sh can be used to easily generat
# certificate, just make sure to update the domains in dove
ssl_cert = </etc/ssl/private/server.crt
ssl_key = </etc/ssl/private/server.key
```

10. Wykonaj restart usług postfix dovecot.

```
root@tu:/# systemctl restart postfix
root@tu:/# systemctl restart dovecot
```

11. Pokaż status usług postfix.

```
root@tu:/# systemctl status postfix
• postfix.service - LSB: Postfix Mail Transport Agent
  Loaded: loaded (/etc/init.d/postfix)
  Drop-In: /run/systemd/generator/postfix.service.d
           └─50-postfix-$mail-transport-agent.conf
  Active: active (running) since czw 2017-01-26 17:53:26 CET; 39s ago
  Process: 1275 ExecStop=/etc/init.d/postfix stop (code=exited, status=0/SUCCESS)
  Process: 761 ExecReload=/etc/init.d/postfix reload (code=exited, status=0/SUCCESS)
  Process: 1297 ExecStart=/etc/init.d/postfix start (code=exited, status=0/SUCCESS)
  CGroup: /system.slice/postfix.service
          └─1407 /usr/lib/postfix/master
             └─1408 pickup -l -t unix -u -c
                └─1409 qmgr -l -t unix -u
                   └─1410 cleanup -z -t unix -u -c
                      └─1411 trivial-rewrite -n rewrite -t unix -u -c
```

## 12. Pokaż status usług dovecot.

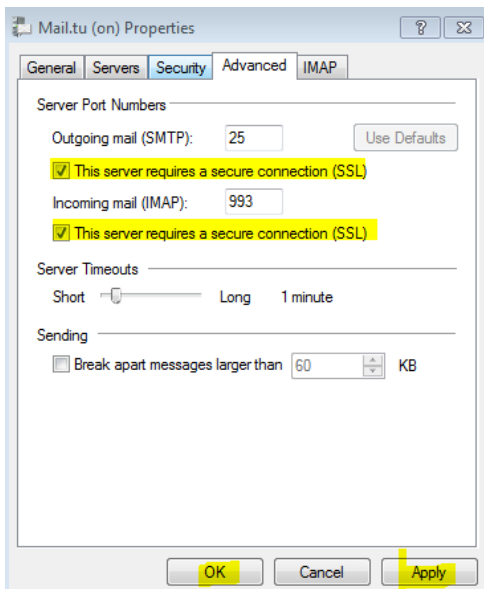
```
root@tu:/# systemctl status dovecot
• dovecot.service - Dovecot IMAP/POP3 email server
  Loaded: loaded (/lib/systemd/system/dovecot.service; enabled)
  Active: active (running) since czw 2017-01-26 17:55:01 CET; 2min 39s ago
  Main PID: 1452 (dovecot)
  CGroup: /system.slice/dovecot.service
          └─1452 /usr/sbin/dovecot -F
            └─1455 dovecot/anvil
              └─1456 dovecot/log
                └─1458 dovecot/config

sty 26 17:55:01 tu dovecot[1452]: master: Dovecot v2.2.13 starting up for i...d)
Hint: Some lines were ellipsized, use -1 to show in full.
```

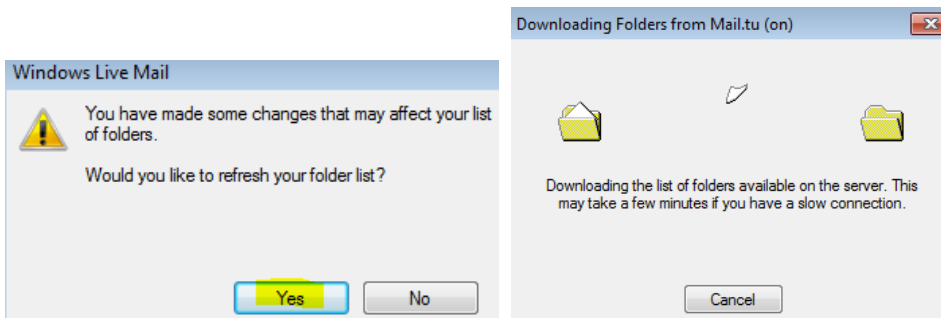
[3] Dla ustawień Klienta,

Windows Live\Mail

1. Zmień ustawienia jak poniżej. (Jeśli używasz PO3S, wejście portu 995 dla poczty przychodzącej)

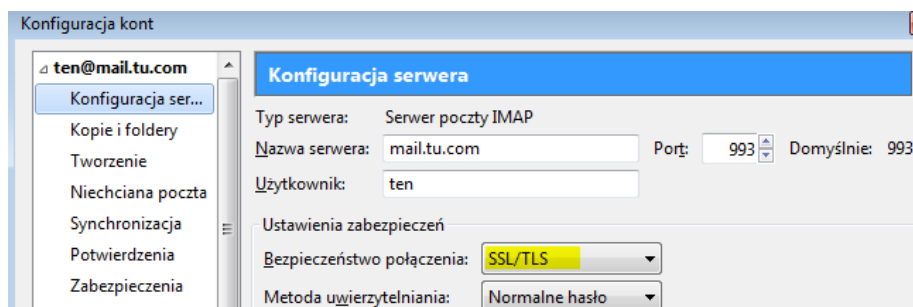


2. Kliknij synchronizuj na Windows Live Mail, a następnie następujące ostrzeżenie jest wyświetlana, ponieważ certyfikaty są własne tworzone na serwerze. To nie problem. Kliknij przycisk "Tak", aby kontynuować, to jest możliwe wysyłanie / odbieranie wiadomości e-mail za pośrednictwem połączenia SSL.



## ThunderbirdPortable

3. Zmień ustawienia jak poniżej. (Jeśli używasz PO3S, wejście portu 995 dla poczty przychodzącej)



Opisz w zeszytcie:

- procedurę instalacji i konfiguracji oraz uruchomienia serwera pocztowego skonfigurowanego oparciu o ustawienia SSL w celu szyfrowania danych,
- testowania uruchomionego serwera pocztowego skonfigurowanego oparciu o ustawienia SSL w celu szyfrowania danych.

**Zgłoś zakończenie ćwiczenia w celu sprawdzenia.**