Handbook of instructions for configuring Dovecot

In the handbook examples, we will assume that you have a bakery named CheezeKake and are configuring a self-hosted email service for its domain cheezekake.com, with email addresses of the form @cheezekake.com.

We are assuming that you have an Ubuntu machine with the IP address 20.227.211.113, where you have installed MySQL and Postfix.

1. Add the Ubuntu software repository from where you can download Certbot software.

```
sudo add-apt-repository ppa:certbot/certbot
```

2. Update your software repository cache

```
sudo apt update
```

3. Install Certbot

```
sudo apt install certbot
```

4. Make a new directory where you can store generated certificates. This should be inside your home directory.

```
mkdir -p certs/cheezekake.com
```

5. Switch to the directory where the certificate should be generated.

```
cd certs/cheezekake.com
```

6. Generate a new certificate for the domain cheezekake.com.

```
sudo certbot certonly --webroot -d cheezekake.com
```

In the question where it asks for the webroot, enter the directory where RainLoop is installed, e.g. /home/devop/webmail.

Your certificate should be inside /etc/letsencrypt/live/cheezekake.com. Two files named fullchain.pem and privkey.pem should have been generated.

7. To the file /etc/apache2/sites-available/default-ssl.conf, add the lines

```
Alias "/mail" "/home/devop/webmail/"
<Directory "/home/devop/webmail/">
    require all granted
</Directory>
```

8. Make the following two changes where the SSL settings are configured.

```
SSLCertificateFile      /etc/letsencrypt/live/cheezekake.com/fullchain.pem
SSLCertificateKeyFile   /etc/letsencrypt/live/cheezekake.com/privkey.pem
```

8. Enable the SSL enabled website with

```
sudo a2ensite default-ssl
```

9. Enable the SSL module of Apache web server.

```
sudo a2enmod ssl
```

10. Restart Apache web server

```
sudo systemctl restart apache2
```

11. Ensure that Apache is running on both port 80 and 443.

```
sudo netstat -ntlp | grep apache2
```

12. On the browser, navigate to https://cheezekake.com/mail
You should see the home page of webmail with its username and password prompts. You should also see the lock icon against the URL at the top of the browser.

13. Clicking on the lock should show you the details of the SSL certificate.

14. To secure your Postfix server, open the following file.

```
sudo vi /etc/postfix/master.cf
```

15. Uncomment the line (i.e. remove the leading # symbol) that says

```
smtps inet  n       -       y       -       -       smptd
```

16. In the file /etc/postfix/main.cf, ensure the following lines under TLS parameters. These lines make sure that if an SMTP client (such as Thunderbird) supports SSL, then the connection is secure.

```
smtpd_use_tls=yes
smtpd_tls_security_level=may
smtpd_tls_cert_file=/etc/letsencrypt/live/cheezekake.com/fullchain.pem
smtpd_tls_key_file=/etc/letsencrypt/live/cheezekake.com/privkey.pem
```

17. In the same file, ensure that the following line is also added below the lines in point 16. This line ensures that our Postfix connects to another email server (e.g. GMail) using SSL if that server supports SSL.

```
smtp_tls_security_level=may
```

Please note the use of the word 'smtp' instead of 'smptd' that was used in point 16.

18. Restart postfix for the changes to take effect.

```
sudo systemctl restart postfix
```

19. Test the SSL connection to Postfix.

```
openssl s_client -connect localhost:25 -starttls smtp
```

The output should show the Let's encrypt certificate that you configured in main.cf.

20. To secure Dovecot, open the following file.

```
sudo vi /etc/dovecot/conf.d/10-ssl.conf
```

21. Modify the lines to use the new SSL certificates.

```
ssl_cert = </etc/letsencrypt/live/cheezekake.com/fullchain.pem
ssl_key = </etc/letsencrypt/live/cheezekake.com/privkey.pem
```

22. Restart Dovecot

```
sudo systemctl restart dovecot
```

23. To test the SSL connection to Dovecot,

```
openssl s_client -connect localhost:143 -starttls imap
```

The output should show the configured certificate.