

Sadek  
Adel  
SIO2

---

## Installation SMTP,IMAP

---

-J'installe le paquet postfix

-Je définis une installation local uniquement

-Je met le fqdn de ma machine  
Qui sera smtp.booktic.info

J'installe le paquet mailutils pour les test plus tard

Je passe au DNS je le modifie

Je définis un enregistrement de type A qui pointera vers mon ip qui heberge le postfix

Ensuite je fais un CNAME de cet enregistrement vers imap.booktic.info

Ensuite je rajoute un enregistrement « MX » le premier champs est vide car le MX du domaine de base non d'un sous domaine

Ensuite je met mon serveur smtp

Ensuite je vais dans le fichier / etc /postfix /main.cf

Le fichier de configuration de postfix est **/etc/postfix/main.cf**. Il est par défaut très bien sécurisé.

Nous allons dans un premier temps y ajouter cette ligne :

```
home_mailbox = Maildir/Commentez (ajoutez un #) la ligne où se trouve  
mailbox_command pour que procmail ne soit pas utilisé
```

Dans mynetworks rajouter son réseau privé avec un masque en CIDR

Redémarrer le service postfix et regarder les log pour voir si il y'a une erreur

```
mynetworks = 127.0.0.0/8 172.17.1.0/24 [::ffff:127.0.0.0]/104 [::1]/128  
#mailbox_size_limit = 0  
home_mailbox = Maildir/
```

J'ajoute un user test à la machine j'envoie un mail avec

Il faut bien préciser notre hostname correctement dans le fichier de conf

Mes users sont baser sur les users présent dans ma machine qui héberge le serveur smtp donc /etc /shadow

Je vais sur une autre Debian sur une machine différente et j'installe un client SMTP avec le paquet swaks ensuite je vérifie si le DNS est correctement configuré

Ici je ne précise pas de serveur smtp destination je vais laisser le client regarder dans la zone DNS de booktic.info quel est le serveur MX (smtp) prioritaire il voit que c'est smtp.booktic.info il envoie le mail vers là-bas

```
root@debianAdel:~# swaks -t test@booktic.info -f client@booktic.info
=== Trying smtp.booktic.info:25...
=== Connected to smtp.booktic.info.
<- 220 smtp.booktic.info ESMTPostfix (Debian/GNU)
-> EHLO debianAdel.sio.jjr
<- 250-smtp.booktic.info
<- 250-PIPELINING
<- 250-SIZE 10240000
<- 250-VRFY
<- 250-ETRN
<- 250-STARTTLS
<- 250-ENHANCEDSTATUSCODES
<- 250-8BITMIME
<- 250-DSN
<- 250-SMTPUTF8
<- 250-CHUNKING
-> MAIL FROM:<client@booktic.info>
<- 250 2.1.0 Ok
-> RCPT TO:<test@booktic.info>
<- 250 2.1.5 Ok
-> DATA
<- 354 End data with <CR><LF>.<CR><LF>
-> Date: Tue, 12 Oct 2021 09:15:33 +0200
```

Je vais ensuite verifier dans le dossier

/home /test /Maildir /new de l'utilisateur qui est censé avoir reçu le mail

Si le mail vient d'arriver

```
test@smtp:~/Maildir/new$ ls -ls
total 12
4 -rw----- 1 test test 551 12 oct. 08:59 1634021974.V801Iffc9bM291311.smtp.booktic.local
4 -rw----- 1 test test 551 12 oct. 09:01 1634022096.V801Iffc9eM333203.smtp.booktic.local
4 -rw----- 1 test test 551 12 oct. 09:15 1634022933.V801Iffc9fM926779.smtp.booktic.local
test@smtp:~/Maildir/new$
```

J'ouvre le mail reçu à 9h15

```
test@smtp:~/Maildir/new$ cat 1634022933.V801Iffc9fM926779.smtp.booktic.local
Return-Path: <client@booktic.info>
X-Original-To: test@booktic.info
Delivered-To: test@booktic.info
Received: from debianAdel.sio.jjr (unknown [172.17.1.90])
    by smtp.booktic.info (Postfix) with ESMTPostfix id D7E3817FB37
    for <test@booktic.info>; Tue, 12 Oct 2021 09:15:33 +0200 (CEST)
Date: Tue, 12 Oct 2021 09:15:33 +0200
To: test@booktic.info
From: client@booktic.info
Subject: test Tue, 12 Oct 2021 09:15:33 +0200
Message-Id: <20211012091533.001414@debianAdel.sio.jjr>
X-Mailer: swaks v20201014.0 jetmore.org/john/code/swaks/

This is a test mailing
```

Voilà le serveur smtp fonctionne correctement lorsque un client configure comme DNS mon DNS il peut envoyer des mail à des users de mon domaine grace à l'enregistrement MX comme vu au début du TP

Pour que les clients peuvent lire leur mail via un MUA tel outlook etc il faut que je met en place un serveur IMAP ou POP port 143/110

Pour imap apt-get install dovecot-imapd

Ensuite avant cela je dois rajouter un CNAME entre mon enregistrement IMAP et SMTP c'est ce que j'ai fais au debut du TP

IMAP sera l'alliase de SMTP

Configuration de dovecot :

Je suis aller dans /etc /dovecot /conf.d /

Et j'ai commencer à configurer le fichier 10-auth.conf

Je n'utilise pas de certificat les mdp seront donc transmit en clair je modifie la ligne

disable\_plaintext\_auth = no #Je met no pour que les mdp soient transmi en clair

Pour la securité sa sera plus tard lorsque je rajouterai des clé publique et privée à mon serveur smtp et imap

## 10-mail.conf

```
#
mail_location = maildir:~/Maildir
# mail_location = mbox:~/mail:INBOX=/var/mail/%u
# mail_location = mbox:/var/mail/%d/%1n/%n:INDEX=/var/indexes/%d/%1n/%n
# <doc/wiki/MailLocation.txt>
#
#mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

J'ai décoché la ligne en haut pour préciser à dovecot où sont stockés les mails

Et j'ai coché celle qui est en bas qui contient le mot INBOX car c'est le mauvais chemin

## 10-master.conf

Ici on veut que postfix attribue le service d'authentification à Dovecot

Dovecot regarde dans le fichier `/etc/shadow` pour regarder les mdp

```
# Postfix smtp-auth
unix_listener /var/spool/postfix/private/auth {
  mode = 0666
  user = postfix
  group = postfix
}
```

*Je teste une connexion avec thunderbird*

J'installe le paquet thunderbird

Set Up Your Existing Email Address  
Use your current email address

Your name:

Email address:

Password:

Remember password

✓ Configuration found by trying common server names

Protocol:  
Incoming: **IMAP** imap.booktic.info STARTTLS  
Outgoing: **SMTP** smtp.booktic.info STARTTLS  
Username: root

Cancel Configure manually... Done

apt-get install thunderbird

Ensuite j'essaie de me connecter à l'utilisateur root avec thunderbird

Comme ceci

J'ai utiliser un autre user finalement

J'eneleve le START TLS car il n'ya pas de certificat et clé privée sur le serveur smtp pour crypter les échanges etc

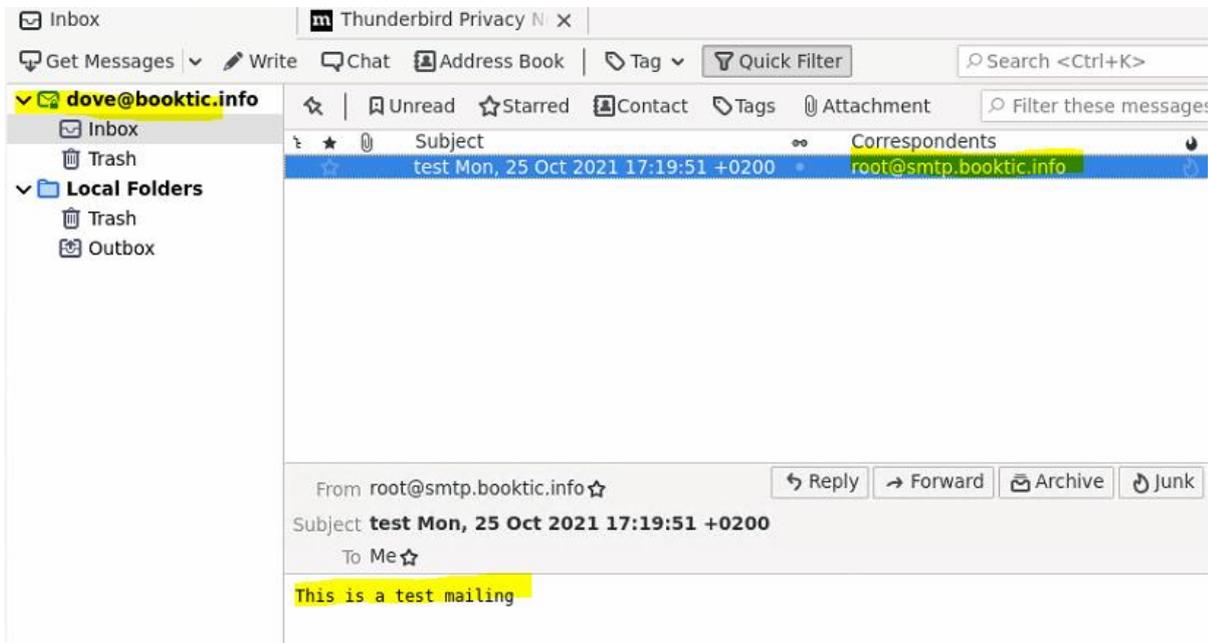
Une fois que c'est valider la connexion s'effectue et ce message s'affiche



J'accepte le risque

Me voila connecter

Et j'ai envoyer un mail depuis l'utilisateur root vers l'utilisateur dove qu'il a parfaitement reçu



## Mise en place de rainloop

*J'installe tout les paquets de la pile lampe avec quelques librairies php de base  
Le php à jour sa version aujourd'hui est 7.3*

*php7.3-mysql php7.3-mbstring php7.3-imap php7.3-xml php7.3-curl*

*Je crée un dossier rainloop dans /var /www /html*

*Je me dirige dedans et install rainloop comme ceci*

*wget -qO- https://repository.rainloop.net/installer.php | php*

```
root@smtp:~# mkdir /var/www/html/rainloop && cd /var/www/html/rainloop
root@smtp:/var/www/html/rainloop# wget -qO- https://repository.rainloop.net/installer.php | php
#!/usr/bin/env php
```

```
[RainLoop Webmail Installer]
```

```
* Connecting to repository ...
* Downloading package ...
* Complete downloading!
* Installing package ...
* Complete installing!

* [Success] Installation is finished!
```

```
root@smtp:/var/www/html/rainloop#
```

Etat : Exécution

**Allez dans `/etc/apache2/sites-available` et copiez le fichier « `000-default.conf` » en le renommant « `rainloop.conf` » :**

```
root@smtp:/var/www/html/rainloop# cd /etc/apache2/sites-available/  
root@smtp:/etc/apache2/sites-available# ls  
000-default.conf default-ssl.conf  
root@smtp:/etc/apache2/sites-available# cp 000-default.conf rainloop.conf  
root@smtp:/etc/apache2/sites-available#
```

État : Exécution

**Aller dans document root et définir le répertoire des pages html à afficher celui ci :  
`DocumentRoot /var/www/html/rainloop`**

**activer le site avec la commande `a2ensite rainloop.conf`**

**Aller sur ce lien pour avoir accès à la page d'administration**

<http://smtp.booktic.info/rainloop/?admin>

**Les identifiants de connexion par défaut (qui peuvent et même DOIVENT être modifiés) sont :**

- Login : admin
- MDP : 12345
- Nouveau mdp : Siojrr\$1

**Modifier la langue mettre en français**

**On va déclarer notre domaine « `ent.lan` ». Allez dans le menu « Domaines » sur la droite et cliquez sur « + Ajouter un domaine ».**

The screenshot shows the RainLoop administration interface. On the left is a dark sidebar with navigation links: General, Domains, Login, Branding, Contacts, Security, Integrations, Plugins, Packages, Licensing, and About. The main content area has a white background. At the top, there are two warning messages: a yellow one about the default admin password and a red one about the data folder being accessible. Below these is the 'Interface' settings section, which includes dropdown menus for 'Language' and 'Language (admin)' (both set to English), and a 'Theme' dropdown set to 'Default'. There are several checkboxes with green checkmarks indicating they are enabled: 'Allow language selection on settings screen', 'Allow theme selection on settings screen', 'New "move to folder" button', 'Show thumbnails (attachments)', and 'Allow Gravatar'. There is also an unchecked checkbox for 'Allow background selection on settings screen'. At the bottom, the 'Main' section shows an 'Attachment size limit' set to '25 MB' and a PHP configuration summary: 'PHP: upload\_max\_filesize = 2M, post\_max\_size = 8M'.

## Je crée comme sa

### Ajouter le domaine "booktic.info" ✕

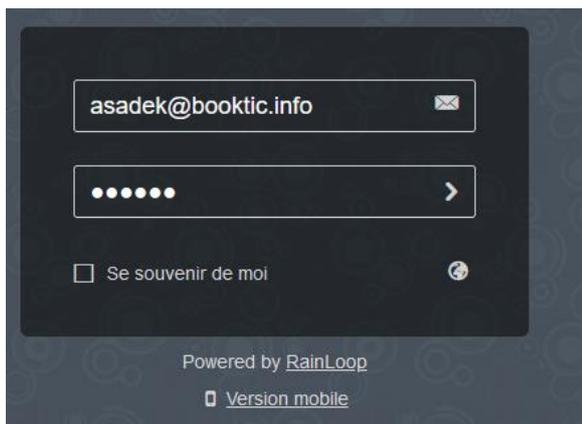
Nom (Jokers autorisés)  
booktic.info

Cette configuration de domaine vous permettra de travailler avec \*@booktic.info dans les adresses électroniques.

IMAP		SMTP	
Serveur	Port	Serveur	Port
imap.booktic.info	143	smtp.booktic.info	25
Sécurité		Sécurité	
Aucun		Aucun	
<input checked="" type="checkbox"/> Utiliser l'identifiant court (user@domain.com → user)		<input checked="" type="checkbox"/> Utiliser l'identifiant court (user@domain.com → user)	
		<input type="checkbox"/> Utiliser l'authentification	
<a href="#">Configuration sieve (bêta)</a>		<input type="checkbox"/> Utiliser la fonction mail() de php (bêta)	

🔍 Test 👤 Liste Blanche ✕ Fermer + Ajouter

## Je reviens ensuite sur la page d'authentification



asadek@booktic.info

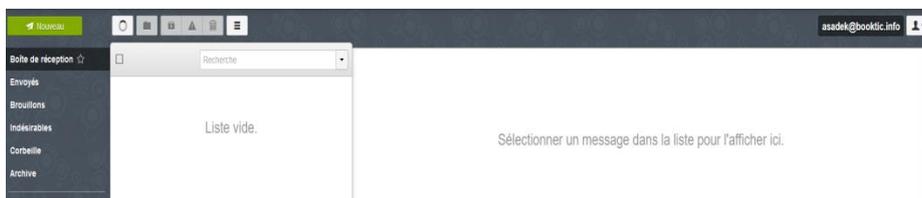
.....

Se souvenir de moi

Powered by [RainLoop](#)

[Version mobile](#)

## Me voila connecter



Je tente d'envoyer un mail de test vers mon mail [adel.sadek752@gmail.com](mailto:adel.sadek752@gmail.com)

Je le reçois parfaitement



Je configure

Le cryptage avec SSL pour le serveur web

Je crée un certificat et une clé privée comme ça

```
root@smtp:/etc/apache2/sites-enabled# openssl req -x509 -SHA512 -days 10000 -key rainloop.key -out rainloop.crt
req: Unrecognized flag X509
req: Use -help for summary.
root@smtp:/etc/apache2/sites-enabled# openssl req -x509 -SHA512 -days 10000 -key rainloop.key -out rainloop.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:MONTMORENCY
Locality Name (eg, city) []:MONTMORENCY
Organization Name (eg, company) [Internet Widgits Pty Ltd]:BOOKTIC
Organizational Unit Name (eg, section) []:BOOKTIC
Common Name (e.g. server FQDN or YOUR name) []:smtp.booktic.info
Email Address []:asadek@booktic.info
root@smtp:/etc/apache2/sites-enabled#
```

Ensuite dans le fichier de conf du site je rajoute ça

Le Virtual host écoutera sur le port 443 et j'active SSL en précisant la clé publique (certificat) et clé privée

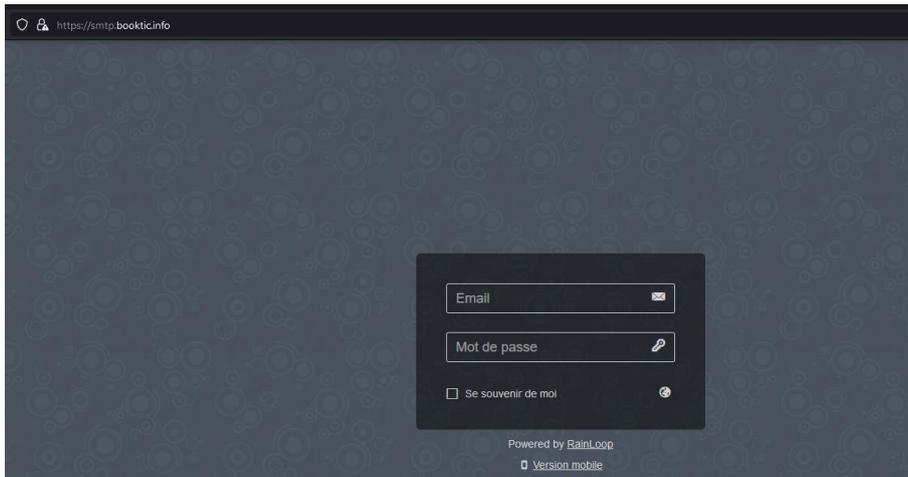
```
<VirtualHost *:443>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html/rainloop

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
    SSLEngine on
    SSLCertificateFile /var/www/ssl/rainloop.crt_
    SSLCertificateKeyFile /var/www/ssl/rainloop.key
```

Je redemarre



## Correction erreur fichier /etc/mailname pas présent

```
sudo hostname --fqdn > /etc/mailname
```

## Correction erreur relay access denied

C'est parceque l'ip du réseau avec son masque d'où vient le mail n'est pas autoriser dans mynetwork ou l'ip de la machine

## Restriction au niveau de l'expéditeur et receveur

Smtpd\_recipient\_restriction = filtre en lien avec le receveur

Smtpd\_sender\_restriction = filtre en lien avec l'expéditeur

On peut par exemple n'autoriser que les mails venant de mon réseau local  
Nous pouvons aussi n'autoriser que les mails partant de mon réseau local

```

smtpd_recipient_restrictions =
    reject_unauth_pipelining,
    reject_non_fqdn_recipient,
    reject_unknown_recipient_domain,
    permit_mynetworks,
    reject_unauth_destination,
    check_sender_access

smtpd_sender_restrictions =
    reject_mynetworks,
    reject_non_fqdn_sender,
    reject_unknown_sender_domain,
    permit

```

Je peux par exemple refuser les mails entrant ou sortant de domaine inconnu ne venant pas de mon réseau local ou qui n'ont pas de FQDN

## Rejeter les mails venant d'une certaines adresse sur le serveur postfix

### Certificat letsencrypt pour postfix

D'abord générer le certificat et clé privée comme ceci

```

root@smtp:/home/debian# certbot certonly --standalone -d smtp.agrepe.com
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator standalone, Installer None
Enter email address (used for urgent renewal and security notices)
(Enter 'c' to cancel): adel@agrepe.com

-----
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.3-September-21-2022.pdf. You must
agree in order to register with the ACME server. Do you agree?
(Y)es/(N)o: y

-----
Would you be willing, once your first certificate is successfully issued, to
share your email address with the Electronic Frontier Foundation, a founding
partner of the Let's Encrypt project and the non-profit organization that
develops Certbot? We'd like to send you email about our work encrypting the web,
EFF news, campaigns, and ways to support digital freedom.
(Y)es/(N)o: y
Account registered.
Requesting a certificate for smtp.agrepe.com
Performing the following challenges:
http-01 challenge for smtp.agrepe.com
Waiting for verification...
Cleaning up challenges
Subscribe to the EFF mailing list (email: adel@agrepe.com).

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at:
  /etc/letsencrypt/live/smtp.agrepe.com/fullchain.pem
  Your key file has been saved at:
  /etc/letsencrypt/live/smtp.agrepe.com/privkey.pem
  Your certificate will expire on 2023-09-11. To obtain a new or
  tweaked version of this certificate in the future, simply run
  certbot again. To non-interactively renew *all* of your
  certificates, run "certbot renew"
- If you like Certbot, please consider supporting our work by:
  Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
  Donating to EFF: https://eff.org/donate-le

root@smtp:/home/debian# cd /etc/letsencrypt/live/smtp.agrepe.com/

```

Fullchain.pem : clé publique

Privkey.pem : clé privée

Faut que je rajoute dans mon fichier main.cf comme ceci maintenant

Certificat letsencrypt pour dovecot

Même commande sauf que pour le domaine on met imap

Ensuite on se rend dans ce fichier

```
root@smtp:/etc/postfix# nano /etc/dovecot/conf.d/10-ssl.conf
```

```
# SSL/TLS support: yes, no, required. <doc/wiki/SSL.txt>
ssl = yes

# PEM encoded X.509 SSL/TLS certificate and private key. They're opened before
# dropping root privileges, so keep the key file unreadable by anyone but
# root. Included doc/mkcert.sh can be used to easily generate self-signed
# certificate, just make sure to update the domains in dovecot-openssl.cnf
#ssl_cert = </etc/dovecot/private/dovecot.pem
#ssl_key = </etc/dovecot/private/dovecot.key

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

Dovecot problème authentification avec domaine

Lorsque je veux me connecter au compte [adel@grepe.com](mailto:adel@grepe.com) par exemple

Le MUA demande à se connecter à l'utilisateur [adel@grepe.com](mailto:adel@grepe.com) hors que comme mon authentification est basé sur PAM je n'ai pas d'utilisateur de ce nom et la connexion est donc refusée

Du coup pour que la machine reconnaisse [adel@grepe.com](mailto:adel@grepe.com) par adel tout court je dois aller dans ce fichier

```
root@smtp:/etc/postfix# nano /etc/dovecot/conf.d/10-auth.conf
```

Et rajouter cela

```
# Username formatting before it's looked up from databases. You can use
# the standard variables here, eg. %Lu would lowercase the username, %n would
# drop away the domain if it was given, or "%n-AT-%d" would change the '@' into
# "-AT-". This translation is done after auth_username_translation changes.
auth_username_format = %n
```

Ensuite normalement ça fonctionnera