

Installer un relais backup MX Postfix

Prérequis

- Un nom de domaine
- Un serveur MX principal
- Ouverture du port 25 sur le MX backup
- Un enregistrement MX sur le Postfix principal

```
host autographe.com
autographe.com has address 104.21.87.75
autographe.com has address 172.67.142.90
autographe.com has IPv6 address 2606:4700:3036::6815:574b
autographe.com has IPv6 address 2606:4700:3031::ac43:8e5a
autographe.com mail is handled by 10 mx1.bldwebagency.fr.
```

Création du record DNS pour le MX secondaire

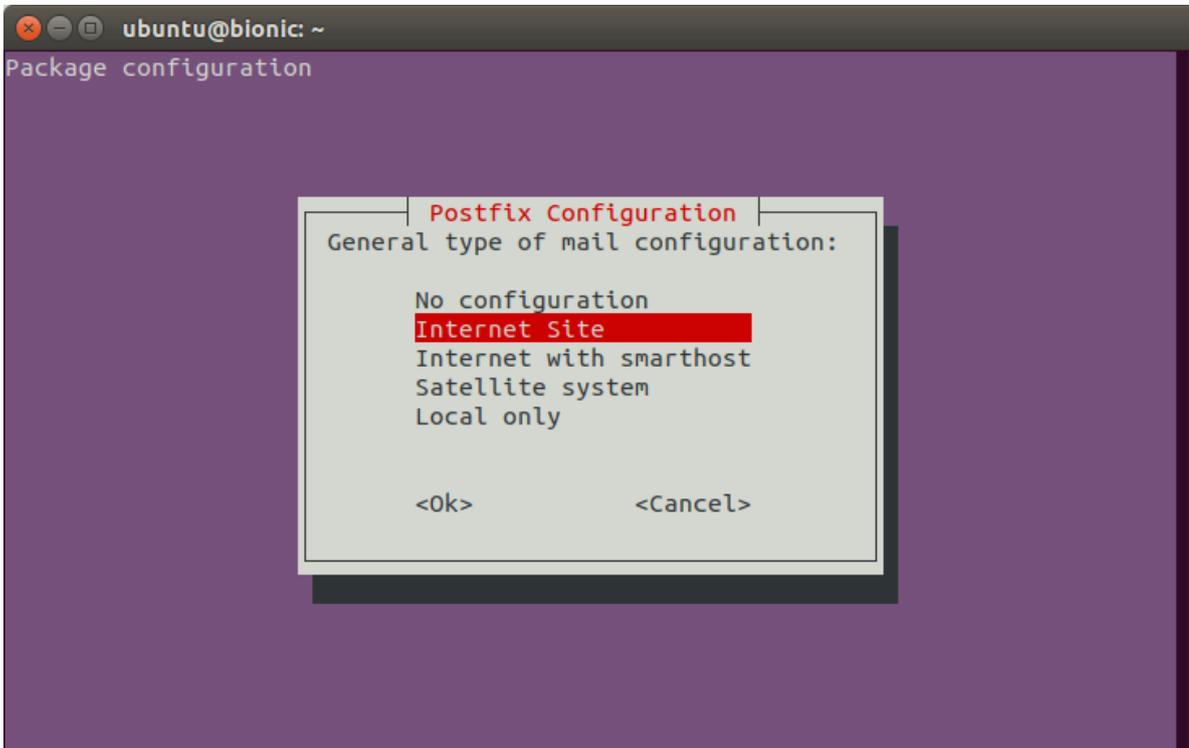
Nous allons créer dans la zone DNS un enregistrement pour le MX secondaire. Dans notre exemple nous allons donc ajouter :

```
mx2.autographe.com A 91.121.84.91
```

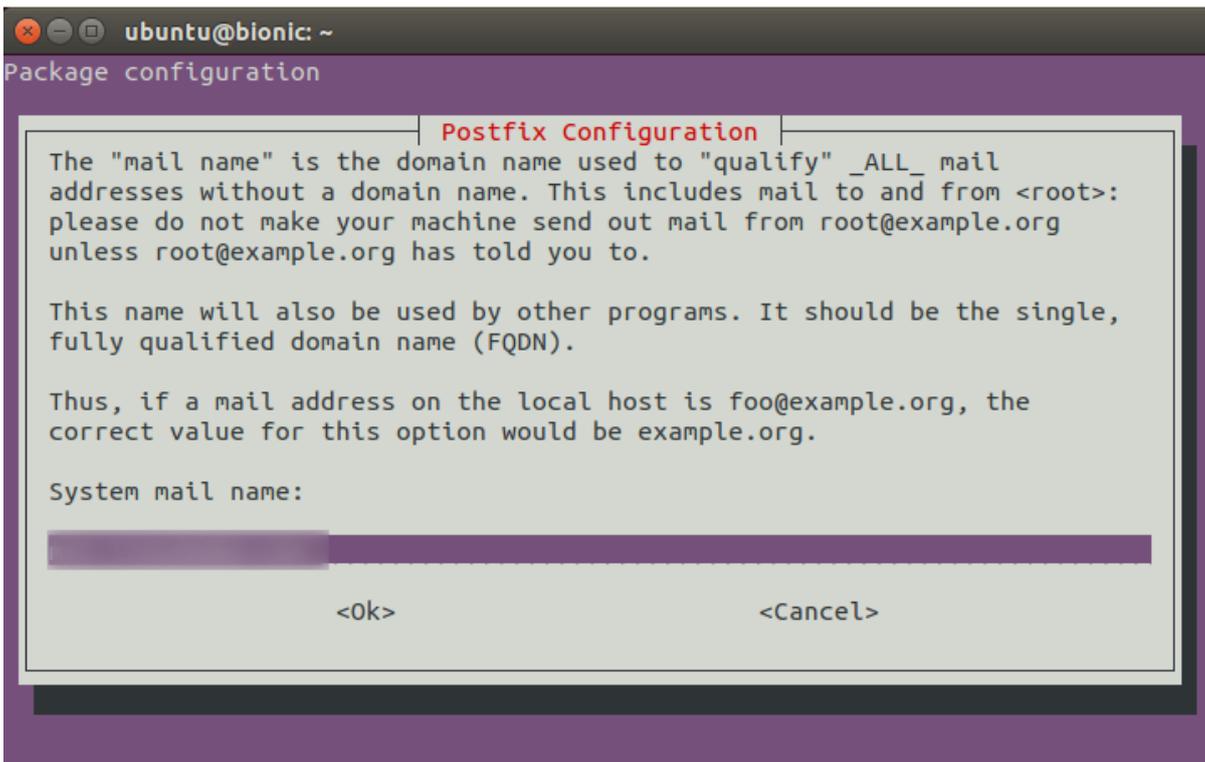
Installation de postfix sur le backup MX

```
apt install postfix
```

Dans la liste des proposition sur la configuration postfix, sélectionner **Internet Site** :



Ensuite, renseigner le nom de domaine du MX secondaire : mx2.bldwebagency.fr :



Configuration initiale de postfix

Nous allons ajouter quelques lignes à la configuration postfix (`/etc/postfix/main.cf`) par défaut pour autoriser les domaines à être relayés.

```
relay_domains = bldwebagency.fr, bldwebagency.com, autographe.com, domain3.com
myhostname = mx2.bldwebagency.fr
mydestination = $myhostname, mx2.bldwebagency.fr, localhost, localhost.localdomain, localhost
```

Configuration de la durée de vie des mails sur le backup :

```
maximal_queue_lifetime = 10d
```

Enfin, redémarrer postfix :

```
systemctl restart postfix
```

Configuration des relay recipients

Par défaut, postfix va relayer tous ce qui concerne les domaines renseignés dans relay_domains. Afin de sécuriser un peu la solution, nous allons restreindre cela aux adresses mails souhaitées. Ouvrez à nouveau le fichier **/etc/postfix/main.cf** :

```
relay_recipient_maps = hash:/etc/postfix/relay_recipients
```

Créez ensuite le fichier **/etc/postfix/relay_recipients** et ajoutez-y les adresses souhaitées, sous la forme :

```
user1@your-domain.com    OK
user2@your-domain.com    OK
user3@your-domain.com    OK
```

Postfix prend en charge les wildcards. Pour autoriser l'ensemble des adresses d'un domaine, ajoutez le domaine de cette façon :

```
user1@your-domain.com    OK
user2@your-domain.com    OK
user3@your-domain.com    OK
@2nd-domain.com          OK
```

Enfin, créez le fichier **relay_recipients.db** avec la commande suivante :

```
postmap /etc/postfix/relay_recipients
```

Activer l'encryption TLS sur le MX principal

Génération d'un certificat avec Certbot

Nous allons activer TLS sur ce backup MX. Pour cela, nous utiliserons **Certbot** pour générer gratuitement un certificat SSL :

```
apt install software-properties-common
add-apt-repository ppa:certbot/certbot
apt update
apt install certbot
```

Génération du certificat :

```
certbot certonly --standalone --preferred-challenges http --agree-tos --email contact@bldwebagency.fr -d
mx2.bldwebagency.fr
```

Installation du certificat dans Postfix

Ouvrez à nouveau le fichier **/etc/postfix/main.cf** et ajoutez-y les lignes suivantes :

```
smtpd_tls_cert_file=/etc/letsencrypt/live/mx2.bldwebagency.fr/fullchain.pem
smtpd_tls_key_file=/etc/letsencrypt/live/mx2.bldwebagency.fr/privkey.pem
```

Affinez la configuration TLS avec ces lignes :

```
smtpd_tls_security_level=may
smtpd_tls_protocols = !SSLv2, !SSLv3 !TLSv1
smtpd_tls_loglevel = 1
```

Puis redémarrez Postfix :

```
systemctl restart postfix
```

Activer les échanges TLS entre le MX principal et le backup MX

Ajoutez ces lignes au fichier **/etc/postfix/main.cf** :

```
smtp_tls_security_level = verify
smtp_tls_verify_cert_match = hostname, nexthop, dot-nexthop
smtp_tls_CApath = /etc/ssl/certs
smtp_tls_loglevel = 1
```

Créez le lien symbolique hash :

```
openssl rehash /etc/ssl/certs
```

Redémarrez postfix :

```
systemctl restart postfix
```

Revision #6

Created 26 January 2021 10:43:08 by Martin Bouillaud

Updated 26 January 2021 11:09:53 by Martin Bouillaud