Avoir plusieurs domaines pour chaque service sur Modoboa

Cette configuration est utile lorsque vous placez votre Modoboa derrière un Reverse Proxy, ou bien si vous voulez simplement rendre plus instinctif la configuration de vos services. Je préciserais quelles sont les configurations sont à faire en cas de Reverse Proxy, il faudra simplement les ignorer si vous n'en avait pas.

L'objectif est donc d'avoir un domaine et avec leur certificat par type de service. Cette configuration est basée sur Let's Encrypt, mais si vous voulez utiliser une autre autorité, il vous faudra ignorer aussi simplement les étapes les concernant.

Les domaines vont être configurés comme ceci :

- Port 25 → mx01.virtit.fr
- Ports 80 et 443 → mail.virtit.fr (mais aussi autoconfig.virtit.fr et peut-être d'autres)
- Ports 587 → smtp.virtit.fr
- Ports 143 et 993 → imap.virtit.fr

Je vais volontairement omettre le POP3 pour une raison très simple : Il faut arrêter d'utiliser le POP3, c'est nul.

Configuration DNS et Pare-feu

Cette étape concerne surtout si vous avez un Reverse Proxy, si vous n'en avait pas, il faudra simplement mettre des règles de NAT / Filtrage classique.

Configuration IPv4

Dans le cas où vous n'avez qu'une seule IP, il va falloir re-diriger les ports 80 et 443 vers le Reverse Proxy, et les ports 25, 143, 587 et 993 vers le serveur Modoboa. Tous les domaines devront avoir pour entrée votre IP.

Si vous avez deux IP, il faudra simplement utiliser les mêmes configurations que pour l'IPv6.

Configuration IPv6

Je vais partir du principe que vous avez plusieurs IPv6, et donc une pour chaque machine. Comme pour l'IPv4, il va falloir configurer les ports 80 et 443 vers le Reverse Proxy, ainsi que les ports 25, 143, 587 et 993 vers le serveur Modoboa. Sauf, que s'ajoute a cette liste le port 80 vers le serveur Modoboa.

Configuration de Nginx

Cette étape est importante et obligatoire dans le cas où vous utilisez des certificats Let's Encrypt.

Pour simplifier l'usage, on ne va pas utiliser le module Nginx de Certbot[1)] mais le module webroot, non dépendant a un serveur web particulier.

Pour cela, il va falloir commencer par créer le dossier pour les challenges :

```
# mkdir -p /var/www/.well-known/acme-challenge/
```

ensuite il faudra ajouter dans le fichier **/etc/nginx/sites-available/default**, dans la section **server**, les lignes suivantes :

```
location /.well-known/acme-challenge/ {
    allow all;
    alias /var/www/.well-known/acme-challenge/;
}
```

et pour finir, il faudra re-charger Nginx :

```
# systemctl reload nginx
```

Dans le cas où vous votre Modoboa est derrière un Reverse Proxy, il va falloir le configurer de telle sorte a ce que les requêtes vers **/.well-known/acme-challenge/** des domaines **mx01.virtit.fr**, **smtp.virtit.fr** et **imap.virtit.fr** soient redirigées vers le Modoboa, alors que celle du domaine **mail.virtit.fr** doivent être conservé sur le Proxy.

Pour cela, on va ajouter la configuration suivante au Nginx du Reverse Proxy :

```
server {
        listen 80;
        listen [::]:80;
        server_name mx01.virtit.fr smtp.virtit.fr imap.virtit.fr;

        location /.well-known/acme-challenge/ {
                allow all;
                proxy_pass http://serveur-modoboa ;
        }

        return 302 https://mail.virtit.fr$request_uri;
}
```

Génération des certificats

Maintenant, pour générer les certificats, il faut simplement taper la commande suivante pour chaque domaine :

```
# certbot certonly --webroot -w /var/www/ --rsa-key-size 4096 -d
```

```
mx01.virtit.fr
```

Configurez les services

pour mx01.virtit.fr

Il faut modifier le fichier **/etc/postfix/main.cf** et remplacez les lignes suivantes :

```
myhostname = mx01.virtit.fr
[....]
smtpd_tls_key_file = /etc/letsencrypt/live/mx01.virtit.fr/privkey.pem
smtpd_tls_cert_file = /etc/letsencrypt/live/mx01.virtit.fr/fullchain.pem
```

ensuite, il vous faudra aussi remplacer le domaine dans le fichier **/etc/amavis/conf.d/05-node_id**

pour smtp.virtit.fr

Il faut modifier le fichier **/etc/postfix/master.cf** et ajouter, pour la section **submission** les lignes suivantes :

```
  -o smtpd_tls_cert_file=/etc/letsencrypt/live/smtp.virtit.fr/fullchain.pem
  -o smtpd_tls_key_file=/etc/letsencrypt/live/smtp.virtit.fr/privkey.pem
```

pour imap.virtit.fr

Il faut modifier le fichier **/etc/dovecot/conf.d/10-ssl.conf** et remplacez les lignes suivantes :

```
ssl_cert = </etc/letsencrypt/live/imap.virtit.fr/fullchain.pem
ssl_key = </etc/letsencrypt/live/imap.virtit.fr/privkey.pem
```

et pour l'ensemble des domaines

Il faudra modifier l'ensemble des domaines pour correspondre a votre réalité dans le fichier **/etc/automx.conf**, comme ceci:

```
# This file was automatically installed on 2020-12-30T16:23:00.311580
[automx]
provider = virtit.fr
domains = *

# Protect against DoS
memcache = 127.0.0.1:11211
memcache_ttl = 600
client_error_limit = 20
```

```
rate_limit_exception_networks = 127.0.0.0/8, ::1/128

[global]
backend = sql
action = settings
account_type = email
host = mysql://modoboa:XXXXXXXXXXXXXXXXXXXXX@localhost/modoboa
query = SELECT concat(first_name, ' ', last_name) AS display_name, email,
SUBSTRING_INDEX(email, '@', -1) AS domain FROM core_user WHERE email='%s'
AND is_active=1
result_attrs = display_name, email

smtp = yes
smtp_server = smtp.virtit.fr
smtp_port = 587
smtp_encryption = starttls
smtp_auth = plaintext
smtp_auth_identity = ${email}
smtp_refresh_ttl = 6
smtp_default = yes

imap = yes
imap_server = imap.virtit.fr
imap_port = 993
imap_encryption = ssl
imap_auth = plaintext
imap_auth_identity = ${email}
imap_refresh_ttl = 6

pop = no
```

Ensuite, il vous faudra simplement redémarrer les services :

```
# systemctl restart postfix dovecot amavis uwsgi
```

[1)]

outils pour générer des certificats Let's Encrypt