SYNACKTIV

One mail for all

MrErne

12/11/2024

Une histoire d'argent

AliExpress propose une offre de bienvenue par défaut lors de votre prémière commande.
Celle-ci est liée à votre adresse email.

Offre de bienvenue

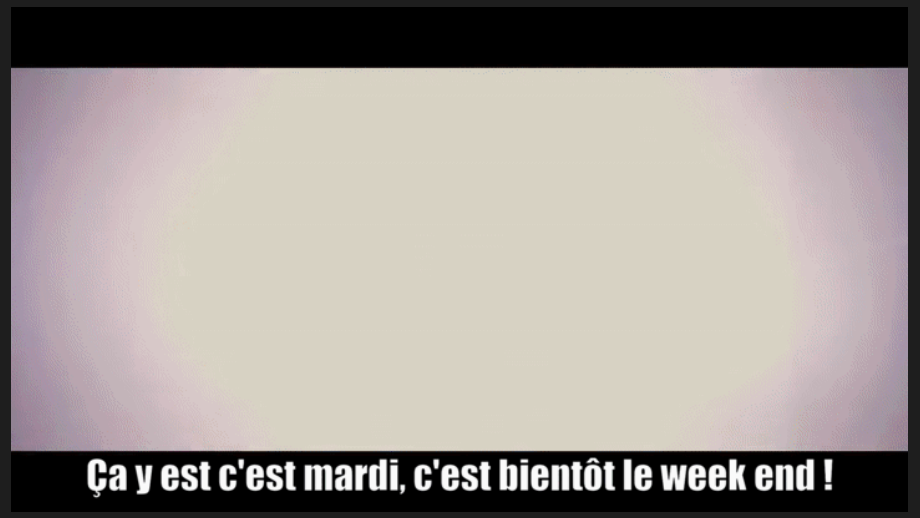
Pas d'offre

Augmentation de **295 %** ! 💸

Mhhhh...

#On prend soin de nos retraités 👴

N'hésitez pas à expliquer les réf. aux plus de 30 ans



Sommaire

SYNACKTIV

```
C'est l'histoire d'un serveur, d'un domaine et d'une IP qui rentrent dans un bar ...
```

- Rapide présentation réseau
- Docker Mail Server (DMS)
  - Configuration **DMS**
  - Setup DNS
  - Let's encrypt
  - Création des adresses & alias
- Quelques cas de figure
  - Premier Wildcard
  - Second Wildcard
- Trucs et machin à faire en plus

Présentation réseau

Protocoles réseau

SYNACKTIV

- **SMTP** (Simple Mail Transfer Protocol) - Port 25, **587**
  - Protocole de transfert de mail **sortant**
  - Authentification TLS sur le port 587 pour les clients
  - Utilisé pour l'envoi de mails
- **IMAP** (Internet Message Access Protocol) - Port 143, **993**
  - Synchronisation des messages entre client et serveur
  - **Conservation des messages sur le serveur**
  - Port 993 pour IMAPS (IMAP over SSL)
- **POP3** (Post Office Protocol) - Port 110, **995**
  - **Téléchargement des messages vers le client**
  - Suppression possible des messages du serveur
  - Tendance à ne plus être utilisé, Info: Mozzilla

Docker Mail Server

https://docker-mailserver.github.io/docker-mailserver/latest/

Architecture DMS 🛠️

SYNACKTIV

- Tous les ports sont sécurisés par TLS/SSL **si possible**
- Authentification requise pour l'envoi (SMTP 587) **en général** #OpenRelay
- Communication inter-serveurs sur le port 25 **

```
# Ports standards
25   : SMTP (entrant/sortant entre serveurs)
587  : SMTP Submission (envoi client avec auth)
993  : IMAPS (réception)
465  : SMTPS (legacy, optionnel)
```

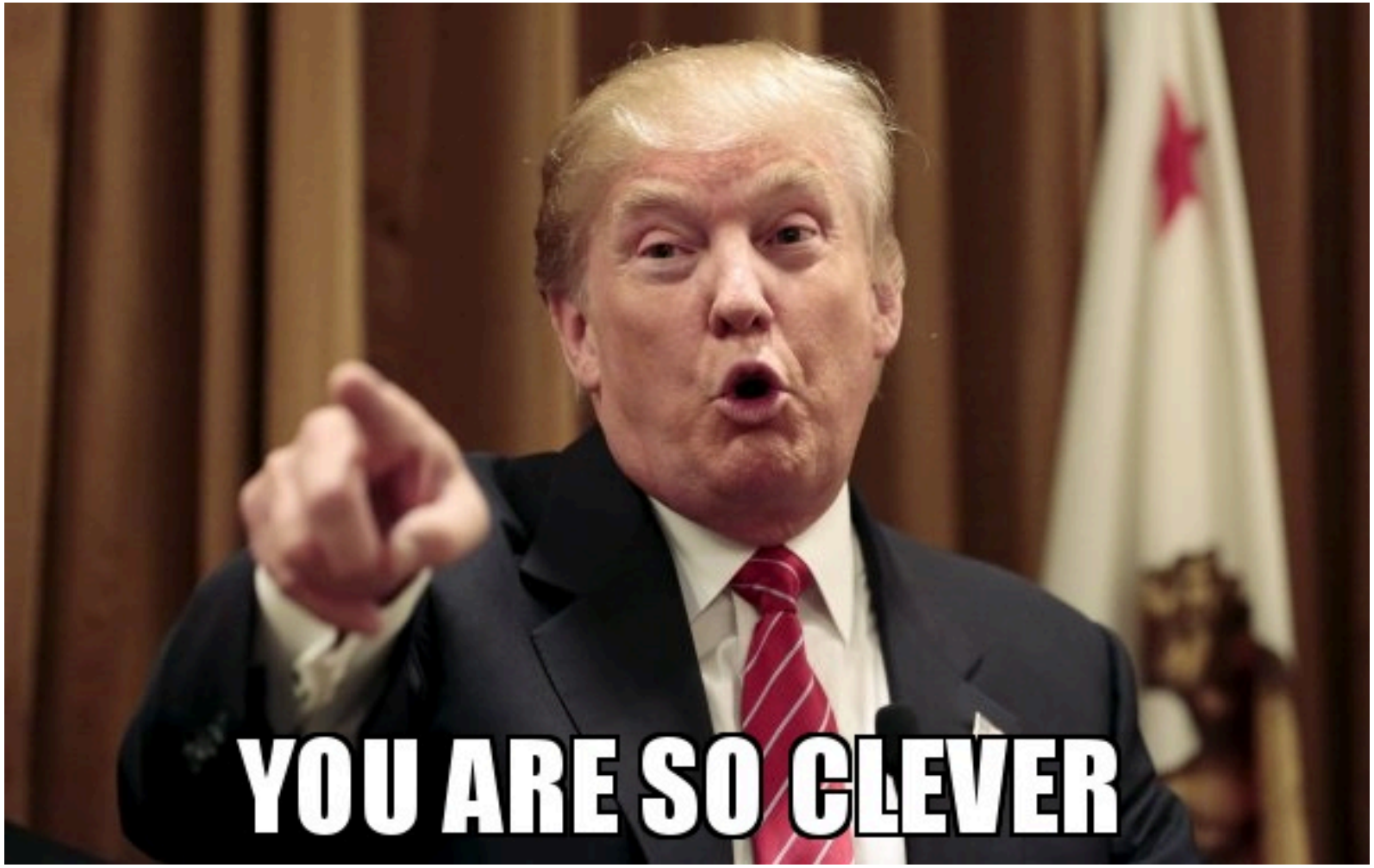
Docker Mail Server

Installation

Installation de Docker

SYNACKTIV

RTFM → https://docs.docker.com/engine/install/ubuntu/



Setup serveur DMS 📋

SYNACKTIV

Récupération des fichiers DMS

```
root@mail:~/mail_server# DMS_GITHUB_URL="https://raw.githubusercontent.com/docker-mailserver/docker-mailserver/maste
root@mail:~/mail_server# wget "${DMS_GITHUB_URL}/compose.yaml"
root@mail:~/mail_server# wget "${DMS_GITHUB_URL}/mailserver.env"

root@mail:~/mail_server# ls -la
total 36
drwxr-xr-x  2 root root  4096 Nov 10 03:16 .
drwxrwxrwt 14 root root  4096 Nov 10 03:17 ..
-rw-r--r--  1 root root  1263 Nov 10 03:16 compose.yaml
-rw-r--r--  1 root root 23996 Nov 10 03:16 mailserver.env
```

DOC → https://docker-mailserver.github.io/docker-mailserver/latest/usage/#get-all-files

Setup serveur DMS 📋

SYNACKTIV

Configuration DMS : compose.yaml

```
root@mail:~/mail_server# cat compose.yaml
services:
  mailserver:
    image: ghcr.io/docker-mailserver/docker-mailserver:latest
    container_name: mailserver
    hostname: mail.jaidup1ng.fr  # ==> HOSTNAME Correspond au champ MX DNS
    env_file: mailserver.env
    ports:
      - "25:25"    # SMTP  (explicit TLS => STARTTLS, Authentication is DISABLED => use port 465/587 instead)
      - "143:143"  # IMAP4 (explicit TLS => STARTTLS)
      - "465:465"  # ESMTP (implicit TLS)
      - "587:587"  # ESMTP (explicit TLS => STARTTLS)
      - "993:993"  # IMAP4 (implicit TLS)
    volumes:
      - ./docker-data/dms/mail-data/:/var/mail/
      - ./docker-data/dms/mail-state/:/var/mail-state/
      - ./docker-data/dms/mail-logs/:/var/log/mail/
      - ./docker-data/dms/config/:/tmp/docker-mailserver/
      - /etc/localtime:/etc/localtime:ro
      - /etc/letsencrypt:/etc/letsencrypt # ==> A ajouter pour le TLS
    restart: always
    stop_grace_period: 1m
    # Uncomment if using `ENABLE_FAIL2BAN=1`:
    # cap_add:
    #   - NET_ADMIN
    healthcheck:
      test: "ss --listening --tcp | grep -P 'LISTEN.+:smtp' || exit 1"
      timeout: 3s
      retries: 0
```

Setup serveur DMS 📋

SYNACKTIV

Configuration DMS : mailserver.env

```
76  # [...]
77  TZ=Europe/Paris
```

```
233  # [...]
234  #empty => SSL disabled
235  #letsencrypt => Enables Let's Encrypt certificates
236  #custom => Enables custom certificates
237  #manual => Let's you manually specify locations of your SSL certificates for non-standard cases
238  #self-signed => Enables self-signed certificates
239  SSL_TYPE=letsencrypt
```

Autres configurations possibles :

- Fail2Ban
- SMTP Only
- Spamassassin
- ...

Configuration DNS

Type	Nom	Contenu
A	jaidup1ng.fr	51.195.41.96
CNAME	*	jaidup1ng.fr
CNAME	mail	jaidup1ng.fr
MX	jaidup1ng.fr	mail.jaidup1ng.fr 1
PTR	mail	jaidup1ng.fr

Records :

- A → Pointe le serveur c'est un **`AIO`**
- MX → Pointe l'ip du serveur DNS
- PTR → Recommanded
- CNAME * → Pour faire **`joujou ( ͡° ͜ʖ ͡°)`**
- DKIM, DMARC, SPF … 🤭

Let's encrypt 🔒

SYNACKTIV

```
1  # Installation de Certbot avec le plugin Cloudflare
2  root@mail:~/mail_server# apt install certbot python3-certbot-dns-cloudflare
3
4  # Configuration des credentials Cloudflare
5  root@mail:~/mail_server# echo "__REDACTED__" >> cloudflare.ini
6  root@mail:~/mail_server# chmod 600 cloudflare.ini
7  root@mail:~/mail_server# chown 0:0 cloudflare.ini
8
9  # Génération du certificat wildcard
10 root@mail:~/mail_server# certbot certonly --dns-cloudflare --dns-cloudflare-credentials cloudflare.i
11 -d jaidup1ng.fr -d *.jaidup1ng.fr
```

Doc: certbot-dns-cloudflare-wildcard

Setup serveur DMS ⏯️

SYNACKTIV

Start DMS

```
root@mail:~/mail_server# docker compose up -d #Det
[+] Running 2/2
 ✔ Network mail_server_default  Created
 ✔ Container mailserver         Started
```

Stop DMS

```
root@mail:~/mail_server# docker compose d
[+] Running 2/2
 ✔ Container mailserver Removed
 ✔ Network mail_server_default  Removed
```

Le pôle reverse qui ne comprend plus rien depuis la slide 6... 🤡

Présentation réseau

(La slide 6)

Création des adresses

- Ce n'est plus la slide 6 ! -

Création d'une adresse ✉️

SYNACKTIV

```
# Création d'un compte email

root@mail:~/mail_server# docker exec -it mailserver setup email add admin@jaidup1ng.fr
Enter Password: `UwU-kawainé`

# Configuration des alias wildcard
root@mail:~/mail_server# echo "/^.*@jaidup1ng\.fr$/ admin@jaidup1ng.fr" > docker-data/dms/config/postfix-rege
x

# On reboot
root@mail:~/mail_server# docker compose down && docker compose up -d
```

And voilà !

Quelques cas de figure

SYNACKTIV

1️⃣ Premier wildcard

*@jaidup1ng.fr :

- **uber1**@jaidup1ng.fr, uber2, uber3…
- **aliexpress1**@jaidup1ng.fr, aliexpress2, aliexpress3, …
- **onlyft1**@jaidup1ng.fr, […], onlyft99, onlyft100 🙈🙉🙊
- **"DROP TABLES;"**@jaidup1ng.fr
- **##:)a**@jaidup1ng.fr
- **pharexenonvitreteintebendobendo**@jaidup1ng.fr
- \x31\xc0\x50\x68\x2f\x63\x61\x74\x68\x2f\x62\x69\x6e\x89\xe3\x50\x68\x6f\x00\x00\x00\x68\x68\x65\x6c\x6c\x89\xe1\x50\x51\x53\x89\xe1\x31\xc0\x83\xc0\x0b\xcd\x80@jaidup1ng.fr

Quelques cas de figure

SYNACKTIV

2️⃣ Second Wildcard

CNAME	*.*	jaidup1ng.fr
A	jaidup1ng.fr	51.195.41.96
CNAME	*	jaidup1ng.fr

@.jaidup1ng.fr → `/^.*[@.]jaidup1ng\.fr$/ admin@jaidup1ng.fr`

- **uber1**@**uber**.jaidup1ng.fr, uber2, uber3…
- **"DROP TABLES;"**@**COMMIT;**.jaidup1ng.fr
- **emmanuel.macr0n**@**gouv**.jaidup1ng.fr
- **michel.dupont**@**etud**.jaidup1ng.fr

Avec quelques records dns de plus → `*.*.jaidup1ng.fr. IN CNAME jaidup1ng.fr.`

- **lunetteteinte**@**pharexenon.vitreteinte**.jaidup1ng.fr

Quelques cas de figure

Wildcard n° 482654 🤯

Adresse	Réception
faitchier@jaidup1ng.fr	faitchier@jaidup1ng.fr
admin@jaidup1ng.fr	admin@jaidup1ng.fr
mission@*[.]jaidup1ng.fr	**faitchier@jaidup1ng.fr**
toto*@*[.]jaidup1ng.fr	**faitchier@jaidup1ng.fr**
@[.]jaidup1ng.fr	**admin@jaidup1ng.fr**

```
1   # /mail_server/docker-data/dms/config/postfix-regexp.cf
2
3   # 1. Capture toutes les adresses "mission@*"
4   /mission@.*jaidup1ng\.fr$/   faitchier@jaidup1ng.fr
5
6   # 2. Capture toutes les adresses "toto*@*"
7   /^toto.*@.*jaidup1ng\.fr$/    faitchier@jaidup1ng.fr
8
9   # 3. Exception nécessaire pour éviter que faitchier@jaidup1ng.fr soit capturé par la règle générique ci-dessous
10  /faitchier@jaidup1ng\.fr$/    faitchier@jaidup1ng.fr
11
12  # 4. Règle générique qui capture toutes les autres adresses sur le domaine et ses sous-domaines
13  /^.*[@.]jaidup1ng\.fr$/ admin@jaidup1ng.fr
```

Quelques cas de figure 💬

Sécurité ?

- **Utilisation de plusieurs alias mail**
  - Couple mail & login différents entre chaque usage
  - Eviter les leaks & ré-use
  - Traçabilité des fuites !
- uber@domaine.fr
- bank@my.domaine.fr
- ph@pro.domaine.fr
- **Eviter les problèmes d'implémentation du `'+'` : toto+uber@domain.fr**
  - Adresse jetable
- **Master mail pouvant être dissimulé**
- **Bypass filtre, règles**

👀 Trucs et machin à faire en plus 👀

- Faire les configs DKIM, DMARC, SPF
- Mettre Fail2Ban
- Nftables / Iptables
- Setup autodiscover
- Processus de whitelist

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://twitter.com/synacktiv

https://synacktiv.com