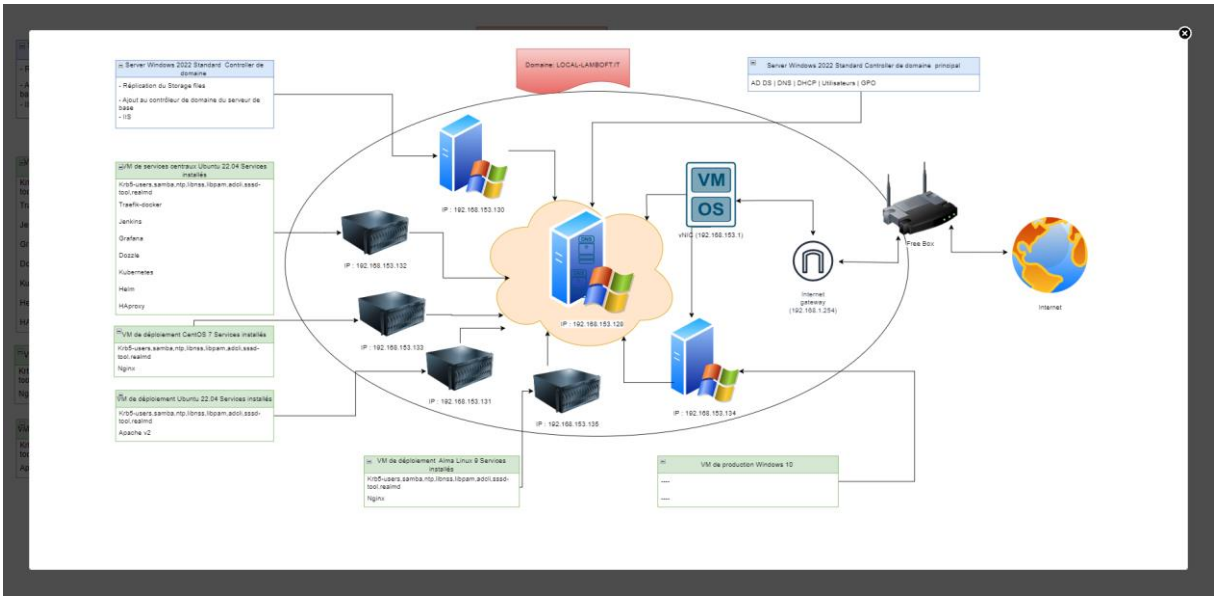

NB : chaque fois qu'on installe un service sur un OS lui affecter un utilisateur dédié ayant généralement les droits sudo. (plus besoin de le faire automatiquement Jenkins crée un compte de service nommé **Jenkins** au moment de l'installation du service).

C'est un reverse proxy et load balancer pour des applications dans un écosystème nécessitant de la haute performance.

On va organiser notre configuration haproxy en plusieurs fichiers de configurations

- Créer un répertoire conf.d/*.cfg
- Créer un script .sh dans /usr/local/bin/concat-haproxy-configs.sh

```
#!/bin/bash

# Destination du fichier de configuration concaténé
CONFIG_FILE="/etc/haproxy/combined-haproxy.cfg"
# Concaténer les fichiers de configuration
cat /etc/haproxy/haproxy.cfg /etc/haproxy/conf.d/*.cfg > $CONFIG_FILE

exit 0
```

- Le rendre exécutable
- Le rajouter dans le service haproxy en prédémarrage et en rechargement (reload)

```
[Unit]
Description=HAProxy Load Balancer
Documentation=man:haproxy(1)
Documentation=file:/usr/share/doc/haproxy/configuration.txt.gz
After=network.target

[Service]
EnvironmentFile=-/etc/default/haproxy
Environment="CONFIG=/etc/haproxy/combined-haproxy.cfg" "PID-
FILE=/run/haproxy.pid" "EXTRAOPTS=-S /run/haproxy-master.sock"
ExecStartPre=/usr/local/bin/concat-haproxy-configs.sh
ExecStartPre=/usr/sbin/haproxy -Ws -f $CONFIG -c -q $EXTRAOPTS
ExecStart=/usr/sbin/haproxy -Ws -f $CONFIG -p $PIDFILE $EXTRAOPTS
ExecReload=/usr/sbin/haproxy -Ws -f $CONFIG -c -q $EXTRAOPTS
ExecReload=/bin/kill -USR2 $MAINPID
ExecReload=/usr/local/bin/concat-haproxy-configs.sh
KillMode=mixed
Restart=always
SuccessExitStatus=143
Type=notify


[Install]
WantedBy=multi-user.target
```

- On veut pouvoir accéder au Dashboard de **Traefik** via un port défini dans **HAproxy**
  - ➔ Si on y accède directement et bien qu'on puisse avoir un message d'erreur qui nous dit que nous n'avons pas les autorisations nécessaires afin d'y parvenir.
  - ➔ Il faille connaitre le port d'écoute de **Traefik.**
  - ➔ Il faille définir un port dans **HAproxy** qui va rediriger le trafic vers le port de **Traefik** en backend (de l'encapsulation).
  - ➔ On va créer une règle de pare feu qui va bloquer les connexions externes sur le port 9091 de **Traefik** et autoriser une connexion en interne sur le port 9091 afin de permettre au serveur qui héberge le service **haproxy** de rediriger le trafic du port 8082 sur ce port 9091.

```
root@vms-002-Server:~# iptables -I INPUT  -p tcp --dport 9091 ! -s 192.168.153.132 -j DROP
```

Avec cette règle à l'intérieur de la machine 192.168.153.132 on peut accéder à traefik sur les ports 8082 et 9091 via la commande curl

Cependant à l'extérieur de la machine seulement sur le port 8082 qu'on peut avoir accès.

Sauvegarder les règles iptables créées

- Soit directement via la commande iptables-save

```
root@vms-002-Server:~# iptables-save > /etc/iptables/rules.v4
root@vms-002-Server:~# cat  /etc/iptables/rules.v4
# Generated by iptables-save v1.8.7 on Fri Jun 28 20:31:12 2024
*filter
:INPUT ACCEPT [75913:41734214]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [74947:62209868]
:DOCKER - [0:0]
:DOCKER-ISOLATION-STAGE-1 - [0:0]
:DOCKER-ISOLATION-STAGE-2 - [0:0]
:DOCKER-USER - [0:0]
-A INPUT ! -s 192.168.153.132/32 -p tcp -m tcp --dport 8080 -j DROP
-A INPUT ! -s 192.168.153.132/32 -p tcp -m tcp --dport 9091 -j DROP
```

- Soit en installant le paquet iptable-persistent

```
root@vms-002-Server:~# firewall-cmd --zone=public --list-all && firewall-cmd --zone=trusted --list-all
public
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
        rule family="ipv6" port port="9091" protocol="tcp" reject
        rule family="ipv4" port port="9091" protocol="tcp" reject
trusted (active)
  target: ACCEPT
  icmp-block-inversion: no
  interfaces:
  sources: 192.168.153.132
  services:
  ports: 9091/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Dans les pares-feux quelles sont les types de zones et pourquoi utiliser une zone plutôt qu'une autre ?

Les types de règles par zone ?

Le type de protocole utilisé dans une règle de pare-feu dépend de quoi ?

Quelle valeur pour un pare-feu ?

→Dans notre exemple, on va bloquer le trafic externe(zone public) sur le port 9091 pour les adresses en ipv4 et ipv6

→autoriser le trafic interne provenant du serveur haproxy (le même que celui de Traefik dans notre projet) [zone trusted]

→ Toujours dans la zone trusted ajouter le port 9091/tcp

En résumé : le trafic pourra passer par le port 8082 de haproxy pour accéder au Dashboard de Traefik. Cependant on n'aura pas un accès direct de Traefik sur le port 9091

Se rassurer que Traefik n'est accessible que depuis la machine sur laquelle est-elle installée dans la conf statique de Traefik (IP :port)