



MISE EN PLACE D'UNE SOLUTION DE TYPE REVERSE PROXY SOUS LINUX

Document qui explique la mise en place de la
solution de type reverse proxy

ASSURMER

Services informatiques



Version : 8.0



Service IT



14/10/2022



Kevin
ORTIZ



Antoine
ENGASSER



Antonyn
HIBOUX

DIFFUSION et VISAS

Diffusion			
Société / Entité	Destinataires	Fonction	Diffusion
Assurmer	Service IT	Procédure	Réseau

Visas			
Société / Entité	Nom	Fonction	Signature

SUIVI DES VERSIONS

Versions				
Version	Date	Auteur	Raison	Nombre de pages
V 8.0	14/12/2022	Kevin ORTIZ Antoine ENGASSER Antonyn HIBOUX	Solution de stockage	14

COORDONNEES

Contacts		
Nom	E-mail	Téléphone
Kevin ORTIZ	Kevin.ortiz@edu.esiiee-it.fr	07.50.03.94.59
Antoine ENGASSER	Antoine.engasser@edu.esiiee-it.fr	06.89.03.25.78
Antonyn HIBOUX	Antonyn.hiboux@edu.esiiee-it.fr	07.09.23.45.13



I. Installation de Haproxy

Préparation

Nous devons disposer de :

- Deux serveurs web linux avec apache2 installé.
- Un accès réseau

L'installation se fait entièrement en admin (root).

Premièrement, l'installation de apache2 sur les serveurs web (linux1 et linux2) est rapide.

Saisissez la commande :

```
Sudo apt-get install -y apache2
```

Une fois cela fait noter seulement les IP des serveurs web.

Installation de Haproxy

Ensuite, il nous reste notre serveur proxy. On installe Haproxy.

Saisissez la commande :

```
Sudo apt-get install haproxy
```

Une fois terminé, il faut nous déplacer au fichier haproxy.cfg

Saisissez la commande :

```
Cd /etc/haproxy  
Sudo nano haproxy.cfg
```

Nous venons d'accéder au fichier de configuration de haproxy.

```
global  
    log /dev/log      local0  
    log /dev/log      local1 notice  
    chroot /var/lib/haproxy  
    stats socket /run/haproxy/admin.sock mode 660 level admin expose-fd listeners  
    stats timeout 30s  
    user haproxy  
    group haproxy  
    daemon  
  
# Default SSL material locations  
ca-base /etc/ssl/certs  
crt-base /etc/ssl/private  
  
# See: https://ssl-config.mozilla.org/#server=haproxy&server-version=2.0.3&config=intermedi  
ssl-default-bind-ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDSA-AES128-GCM-SHA256:EC  
ssl-default-bind-ciphersuites TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_PO  
ssl-default-bind-options ssl-min-ver TLSv1.2 no-tls-tickets  
  
defaults  
    log global  
    mode http  
    option httplog  
    option dontlognull  
    timeout connect 5000  
    timeout client 50000  
    timeout server 50000  
    errorfile 400 /etc/haproxy/errors/400.http  
    errorfile 403 /etc/haproxy/errors/403.http  
    errorfile 408 /etc/haproxy/errors/408.http  
    errorfile 500 /etc/haproxy/errors/500.http  
    errorfile 502 /etc/haproxy/errors/502.http  
    [ Lecture de 34 lignes ]  
Aide      Écrire  Chercher Couper  Justifier Pos. cur. M-U Annuler  
Quitter   Lire fich. Remplacer Coller  Orthograp. Aller lig. M-E Refaire
```



Nous pouvons supprimer le contenu du fichier et le remplacer par :

```
defaults
mode http
timeout connect 2500
timeout server 2500
errorfile 503 /etc/haproxy/errors/503.http

frontend www-http
bind 0.0.0.0:80
default_backend www-backend

backend www-backend
balance roundrobin
server linux1 192.168.1.53:80 check
server linux2 192.168.1.54:80 check
```

Le premier paragraphe définit le délai de réponse des serveurs web. Ainsi le mode indique la charge équilibrée, « timeout connect » indique le délai de réponse du client, et « timeout server » le temps de réponse du serveur web. C'est pourquoi, si la latence est importante le proxy génère une erreur 503.

Le deuxième paragraphe traite les demandes. En effet « frontend » reçoit les demandes en provenance des utilisateurs, « bind » analyse si la source est autorisée (toutes les IP en provenance du port http 80 sont autorisées). Enfin, « default_backend » renvoie au groupe en charge de cette demande « www-backend ».

Le dernier paragraphe renvoie le paquet vers un des serveurs web. Nous avons « balance roundrobin », qui permet une répartition des charges sur les deux serveurs web, et ainsi diminuer la latence des serveurs. Enfin « server », il s'agit de l'indication des différents serveurs en charge du site.

Enfin une fois cela fait, vous utilisez la commande suivante afin de redémarrer le service Haproxy.

```
Systemctl restart haproxy
```

Ajout d'un nom de domaine

Pour conclure, vous pouvez lier l'adresse IP du proxy à un nom alphanumérique, pour nous c'est :

<http://srv-web/> lié à l'IP 192.168.1.56.

