MYDIGITALSCHOOL ANGERS — BTS SIO SISR

Mise en œuvre d'un Reverse Proxyavec Load Balancing (HAProxy)

Procédure d'installation HAProxy sur Debian

Rédacteur	Paul Barrault-Gautier
Établissement	MyDigitalSchool Angers
Formation	BTS SIO — option SISR (Session 2026)
Cadre	Travaux pratiques / Projet de formation
Date	Avril 2026
Version	1.0

1. Contexte et objectifs

Dans le cadre de la modernisation de l'infrastructure de Loste Tradi-France, un reverse proxy avec load balancing a été mis en place à l'aide de HAProxy. L'objectif est de répartir la charge entre plusieurs serveurs applicatifs back-end, d'assurer la haute disponibilité des services web exposés et de centraliser la terminaison SSL.

HAProxy (High Availability Proxy) est un logiciel open source reconnu comme référence pour le load balancing et le proxying TCP/HTTP en milieu de production. Cette procédure décrit son installation et sa configuration initiale sur un serveur Debian 12 (Bookworm).

1.1 Architecture cible

Composant	Rôle	Adresse IP	OS
haproxy-srv	Reverse proxy / LB	`192.168.10.10`	Debian 12
web-back-01	Serveur applicatif #1	`192.168.10.21`	Debian 12
web-back-02	Serveur applicatif #2	`192.168.10.22`	Debian 12
web-back-03	Serveur applicatif #3	`192.168.10.23`	Debian 12

2. Prérequis

2.1 Système

- Serveur Debian 12 (Bookworm) fraîchement installé, à jour
- Accès root ou sudo
- Connexion Internet pour les paquets (ou dépôt local)
- RAM minimum recommandée : 2 Go | CPU : 2 vCPU
- Résolution DNS fonctionnelle entre les serveurs

2.2 Réseau

- Le serveur HAProxy doit être joignable depuis l'extérieur (ports 80 et 443 ouverts)
- Communication interne entre HAProxy et les back-ends (port applicatif, ex. 8080) autorisée
- Certificat SSL/TLS disponible pour la terminaison HTTPS (Let's Encrypt ou PKI interne)

2.3 Vérifications préalables

```
# Vérifier la version Debian
cat /etc/os-release

# Mettre à jour le système
sudo apt update && sudo apt upgrade -y

# Vérifier la connectivité réseau vers les back-ends
ping -c 3 192.168.10.21
ping -c 3 192.168.10.22
ping -c 3 192.168.10.23
```

3. Installation de HAProxy

3.1 Installation depuis les dépôts Debian

HAProxy est disponible directement dans les dépôts officiels Debian 12. Pour disposer d'une version plus récente (recommandé pour la production), il est possible d'utiliser le dépôt officiel HAProxy.

```
# Installation depuis les dépôts Debian
sudo apt install -y haproxy
```

```
# Vérifier la version installée
haproxy -v
```

Pour installer HAProxy 2.8 LTS (recommandé) via le dépôt officiel :

```
# Ajouter le dépôt HAProxy
curl -fsSL https://haproxy.debian.net/bernat.debian.org.gpg | sudo gpg --dearmor -o
/usr/share/keyrings/haproxy.gpg
echo "deb [signed-by=/usr/share/keyrings/haproxy.gpg] http://haproxy.debian.net
bookworm-backports-2.8 main" | sudo tee /etc/apt/sources.list.d/haproxy.list
sudo apt update && sudo apt install -y haproxy=2.8.*
```

3.2 Activation du service

```
# Activer HAProxy au démarrage
sudo systemctl enable haproxy

# Démarrer le service
sudo systemctl start haproxy

# Vérifier l'état
sudo systemctl status haproxy
```

3.3 Sauvegarde de la configuration par défaut

```
sudo cp /etc/haproxy/haproxy.cfg /etc/haproxy/haproxy.cfg.bak
```

4. Configuration initiale

4.1 Structure du fichier de configuration

Le fichier de configuration principal est /etc/haproxy/haproxy.cfg. Il est organisé en sections :

Section	Rôle
`global`	Paramètres globaux du processus (logs, sécurité, performances)
`defaults`	Paramètres par défaut hérités par les frontends et backends
`frontend`	Point d'entrée (écoute sur IP:port, règles ACL de routage)
`backend`	Serveurs destination, algorithme de répartition, health checks
`listen`	Combinaison frontend + backend (usage moins courant)

4.2 Outils complémentaires

```
# Installer des outils utiles
sudo apt install -y socat curl openssl

# socat : interaction avec le socket de stats HAProxy
# curl : tests HTTP depuis le serveur
# openssl : gestion et vérification des certificats
```

5. Terminaison SSL/TLS

5.1 Préparation du certificat

HAProxy attend un fichier PEM combinant le certificat et la clé privée. Si vous utilisez Let's Encrypt :

```
# Combiner le certificat et la clé privée pour HAProxy
```

```
cat /etc/letsencrypt/live/mondomaine.fr/fullchain.pem \
    /etc/letsencrypt/live/mondomaine.fr/privkey.pem \
    | sudo tee /etc/haproxy/certs/mondomaine.fr.pem > /dev/null

sudo chmod 600 /etc/haproxy/certs/mondomaine.fr.pem
```

5.2 Renouvellement automatique

```
# Créer un hook de renouvellement Let's Encrypt
sudo tee /etc/letsencrypt/renewal-hooks/deploy/haproxy.sh << 'EOF'
#!/bin/bash
cat /etc/letsencrypt/live/mondomaine.fr/fullchain.pem \
    /etc/letsencrypt/live/mondomaine.fr/privkey.pem \
    > /etc/haproxy/certs/mondomaine.fr.pem
systemctl reload haproxy
EOF
sudo chmod +x /etc/letsencrypt/renewal-hooks/deploy/haproxy.sh
```

6. Validation de l'installation

6.1 Vérification syntaxique

```
# Vérifier la configuration sans redémarrer
sudo haproxy -c -f /etc/haproxy/haproxy.cfg
```

Un message OK confirme la validité de la configuration. En cas d'erreur, la ligne fautive est indiquée.

6.2 Vérification du service

```
sudo systemctl status haproxy
sudo ss -tlnp | grep haproxy

# Tester une requête HTTP
curl -I http://192.168.10.10/
curl -I https://mondomaine.fr/
```

6.3 Logs

```
# Consulter les logs HAProxy
sudo journalctl -u haproxy -f
sudo tail -f /var/log/haproxy.log
```

7. Sécurisation post-installation

- Désactiver les protocoles SSL/TLS obsolètes (SSLv3, TLSv1.0, TLSv1.1)
- Forcer TLS 1.2 minimum, recommander TLS 1.3
- Configurer les en-têtes de sécurité HTTP (X-Frame-Options, HSTS, etc.) via HAProxy
- Limiter l'accès à la page de statistiques HAProxy aux seuls réseaux d'administration
- Activer le logging complet vers un syslog centralisé
- Mettre en place des alertes sur les erreurs 5xx et les back-ends DOWN