Configuration HAProxy

***IMPORTANT** : Cette section concerne le **serveur HAProxy mutualisé séparé**, pas le serveur Foreman.*

1 Installation de HAProxy

```
# Sur le serveur HAProxy (serveur séparé du serveur Foreman)
sudo dnf install -y haproxy
```

2 Génération des certificats SSL

Si vous n'avez pas encore de certificats SSL, vous pouvez utiliser Let's Encrypt ou générer des certificats auto-signés pour les tests :

```
# Certificats auto-signés (UNIQUEMENT POUR LES TESTS)
sudo mkdir -p /etc/haproxy/certs

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \
  -keyout /etc/haproxy/certs/foreman.key \
  -out /etc/haproxy/certs/foreman.crt \
  -subj "/C=FR/ST=IDF/L=Paris/O=MonOrganisation/CN=foreman.mondomaine.com"

# Combiner la clé et le certificat pour HAProxy
sudo cat /etc/haproxy/certs/foreman.crt /etc/haproxy/certs/foreman.key >
/etc/haproxy/certs/foreman.pem
sudo chmod 600 /etc/haproxy/certs/foreman.pem
```

3 Configuration HAProxy

Sauvegarder la configuration par défaut :

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

Créer la nouvelle configuration :

```
sudo vim /etc/haproxy/haproxy.cfg
```

Contenu de `/etc/haproxy/haproxy.cfg` :

```
#---------------------------------------------------------------------
# Global settings
#---------------------------------------------------------------------
global
    log         127.0.0.1 local2
    chroot      /var/lib/haproxy
    pidfile     /var/run/haproxy.pid
    maxconn     4000
    user        haproxy
    group       haproxy
    daemon

    # turn on stats unix socket
    stats socket /var/lib/haproxy/stats

    # SSL/TLS configuration
    ssl-default-bind-ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-
ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384
    ssl-default-bind-options ssl-min-ver TLSv1.2 no-tls-tickets

#---------------------------------------------------------------------
# Defaults settings
#---------------------------------------------------------------------
defaults
    mode                    http
    log                     global
    option                  httplog
    option                  dontlognull
    option                  http-server-close
    option                  forwardfor except 127.0.0.0/8
    option                  redispatch
    retries                 3
    timeout http-request    10s
    timeout queue           1m
    timeout connect         10s
    timeout client          1m
    timeout server          1m
    timeout http-keep-alive 10s
    timeout check           10s
```

```
    maxconn                 3000

#---------------------------------------------------------------------
# Frontend HTTP - Redirection vers HTTPS
#---------------------------------------------------------------------
frontend http_front
    bind *:80
    mode http

    # Redirection de tout le trafic HTTP vers HTTPS
    redirect scheme https code 301 if !{ ssl_fc }

#---------------------------------------------------------------------
# Frontend HTTPS - Interface Web Foreman (port 443)
#---------------------------------------------------------------------
frontend https_front
    bind *:443 ssl crt /etc/haproxy/certs/foreman.pem
    mode http

    # Headers de sécurité
    http-response set-header Strict-Transport-Security "max-age=31536000; includeSubDomains"
    http-response set-header X-Frame-Options "SAMEORIGIN"
    http-response set-header X-Content-Type-Options "nosniff"

    # ACL pour la WebUI
    acl is_foreman_ui hdr(host) -i foreman.mondomaine.com

    # Headers pour le backend
    http-request set-header X-Forwarded-Proto https
    http-request set-header X-Forwarded-Port 443
    http-request add-header X-Forwarded-Ssl on

    # Route vers le backend Foreman
    use_backend foreman_webui if is_foreman_ui
    default_backend foreman_webui

#---------------------------------------------------------------------
# Frontend HTTPS - Smart Proxy (port 8443)
#---------------------------------------------------------------------
frontend smartproxy_front
```

```
    bind *:8443 ssl crt /etc/haproxy/certs/foreman.pem
    mode http

    # Headers de sécurité
    http-response set-header Strict-Transport-Security "max-age=31536000; includeSubDomains"

    # ACL pour Smart Proxy
    acl is_smartproxy hdr(host) -i foreman.mondomaine.com

    # Headers pour le backend
    http-request set-header X-Forwarded-Proto https
    http-request set-header X-Forwarded-Port 8443
    http-request add-header X-Forwarded-Ssl on

    # Route vers le backend Smart Proxy
    use_backend foreman_smartproxy if is_smartproxy
    default_backend foreman_smartproxy

#---------------------------------------------------------------------
# Backend - Foreman WebUI
#---------------------------------------------------------------------
backend foreman_webui
    mode http
    balance roundrobin
    option httpchk GET /

    # Configuration du backend
    http-request set-header X-Forwarded-Host %[req.hdr(Host)]

    # Serveur Foreman backend
    # REMPLACER <IP_SERVEUR_FOREMAN> par l'IP réelle de votre serveur Foreman
    server foreman1 <IP_SERVEUR_FOREMAN>:80 check inter 5s rise 2 fall 3

    # Exemple avec une IP : server foreman1 192.168.1.100:80 check inter 5s rise 2 fall 3

#---------------------------------------------------------------------
# Backend - Smart Proxy
#---------------------------------------------------------------------
backend foreman_smartproxy
    mode http
```

```
    balance roundrobin
    option httpchk GET /

    # Configuration du backend
    http-request set-header X-Forwarded-Host %[req.hdr(Host)]

    # Serveur Smart Proxy backend
    # REMPLACER <IP_SERVEUR_FOREMAN> par l'IP réelle de votre serveur Foreman
    server smartproxy1 <IP_SERVEUR_FOREMAN>:8443 check ssl verify none inter 5s rise 2 fall 3

    # Exemple avec une IP : server smartproxy1 192.168.1.100:8443 check ssl verify none inter
5s rise 2 fall 3

#---------------------------------------------------------------------
# Stats page (optionnel)
#---------------------------------------------------------------------
listen stats
    bind *:9000
    mode http
    stats enable
    stats uri /stats
    stats realm HAProxy\ Statistics
    stats auth admin:VotreMotDePasse
    stats refresh 30s
```

4 Démarrage et activation de HAProxy

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

# Si pas d'erreur, activer et démarrer HAProxy
sudo systemctl enable haproxy
sudo systemctl start haproxy

# Vérifier le statut
sudo systemctl status haproxy

# Configurer le firewall pour HAProxy
sudo firewall-cmd --permanent --add-port=80/tcp
```

```
sudo firewall-cmd --permanent --add-port=443/tcp
sudo firewall-cmd --permanent --add-port=8443/tcp
sudo firewall-cmd --permanent --add-port=8140/tcp  # Si option 1 pour Puppet
sudo firewall-cmd --permanent --add-port=9000/tcp  # Stats (optionnel)
sudo firewall-cmd --reload
```

Test de connectivité HAProxy → Foreman

Avant de continuer, vérifier que HAProxy peut bien communiquer avec le serveur Foreman :

```
# Depuis le serveur HAProxy, tester la connectivité
ping <IP_SERVEUR_FOREMAN>

# Tester les ports
nc -zv <IP_SERVEUR_FOREMAN> 80
nc -zv <IP_SERVEUR_FOREMAN> 8443
nc -zv <IP_SERVEUR_FOREMAN> 8140

# Tester l'accès HTTP
curl -v http://<IP_SERVEUR_FOREMAN>/
curl -kv https://<IP_SERVEUR_FOREMAN>:8443/

# Si tout fonctionne, tester via HAProxy depuis HAProxy lui-même
curl -kv https://localhost/
curl -kv https://localhost:8443/
```

5 Configuration Foreman pour fonctionner derrière HAProxy

Sur le **serveur Foreman**, modifier la configuration pour accepter les requêtes via proxy :

```
sudo vim /etc/foreman/settings.yaml
```

Ajouter/modifier :

```
:trusted_proxies:
  - <IP_SERVEUR_HAPROXY>
  # Remplacer <IP_SERVEUR_HAPROXY> par l'IP réelle de votre serveur HAProxy
  # Exemple : - 192.168.1.50

:require_ssl: true
```

IMPORTANT : Vous devez impérativement ajouter l'IP du serveur HAProxy dans la liste des proxies de confiance, sinon Foreman rejettera les requêtes.

Redémarrer les services Foreman :

```
sudo systemctl restart foreman
sudo systemctl restart httpd
```

6 Configuration Apache sur le serveur Foreman

Foreman doit être configuré pour accepter les connexions depuis HAProxy et gérer correctement les headers X-Forwarded :

```
# Éditer la configuration SSL de Foreman
sudo vim /etc/httpd/conf.d/05-foreman-ssl.conf
```

Ajouter dans le VirtualHost (avant la ligne `</VirtualHost>`) :

```
  # Configuration pour reverse proxy
  RemoteIPHeader X-Forwarded-For
  RemoteIPInternalProxy <IP_SERVEUR_HAPROXY>

  # Activer les modules nécessaires
  <IfModule mod_remoteip.c>
    RemoteIPHeader X-Forwarded-For
    RemoteIPTrustedProxy <IP_SERVEUR_HAPROXY>
  </IfModule>
```

Vérifier que le module remoteip est activé :

```
sudo dnf install -y mod_remoteip
sudo systemctl restart httpd
```

---

7 Configuration réseau et DNS

Puisque HAProxy et Foreman sont sur des serveurs séparés, vous devez configurer correctement le DNS et le routage.

Sur le serveur DNS (ou /etc/hosts des clients)

Le nom `foreman.mondomaine.com` doit pointer vers l'IP du serveur **HAProxy**, pas du serveur Foreman :

```
# DNS ou /etc/hosts
<IP_HAPROXY>  foreman.mondomaine.com
```

Sur le serveur HAProxy

Ajouter l'entrée pour le serveur Foreman :

```
sudo vim /etc/hosts
```

```
<IP_SERVEUR_FOREMAN>  foreman-backend.mondomaine.com foreman-backend
```

Sur le serveur Foreman

Le serveur Foreman doit pouvoir être contacté par HAProxy. Vérifier la configuration réseau :

```
# Vérifier la connectivité depuis HAProxy
ping <IP_SERVEUR_FOREMAN>

# Vérifier que les ports sont ouverts depuis HAProxy
nc -zv <IP_SERVEUR_FOREMAN> 80
nc -zv <IP_SERVEUR_FOREMAN> 8443
```

Configuration du hostname Foreman

Sur le serveur Foreman, le hostname doit correspondre au nom public :

```
sudo hostnamectl set-hostname foreman.mondomaine.com
```

Le fichier `/etc/hosts` sur le serveur Foreman :

```
127.0.0.1   localhost localhost.localdomain
<IP_LOCALE_FOREMAN>   foreman.mondomaine.com foreman
```

Revision #4
Created 2026-02-02 10:17:20 UTC by NoNo
Updated 2026-02-02 12:54:03 UTC by NoNo